MISC

Multi-System & Internet Security Cookbook

100 % SÉCURITÉ INFORMATIQUE

L 19018 - 59 - F: 8,00 € - RD

N° 59 JANVIER/FÉVRIER 2012

France Métro : 8 € DOM : 8,80 € TOM Surface : 990 XPF TOM Avion : 1300 XPF
CH : 15,50 CHF BEL, LUX, PORT.CONT : 9 Eur CAN : 15 $CAD

OPEN SILICIUM 5

OS n°5 Actuellement en kiosque !

LE MAGAZINE DE L'OPEN SOURCE POUR L'ÉLECTRONIQUE & L'EMBARQUÉ

JANVIER / FÉVRIER / MARS 2012 N°5

Open Silicium

MAGAZINE
INFORMATIQUE
OPEN SOURCE
EMBARQUÉ
ÉLECTRONIQUE

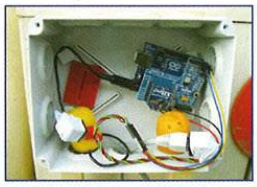
LE MAGAZINE DE L'OPEN SOURCE POUR L'ÉLECTRONIQUE & L'EMBARQUÉ

PCI / FPGA

Découverte, prise en main et exploitation de la carte Dragon PCI KNJN p.15

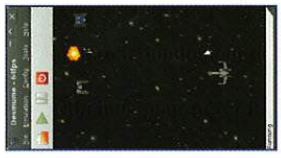
DOMO / ARDUINO

Créez un capteur domotique avec Arduino, Xbee et Domogik p.86



HOMEBREW / DS

Développez vos jeux « maison » pour Nintendo DS sous GNU/Linux p.69



AVR / CONSO

Apprenez à réduire la consommation de vos montages à base d'Atmel AVR p.10

LED / ST VALENTIN

Un cœur tout rose pour votre adoré(e) : dites-le avec des LED ! p.81

RÉSEAU / OUTILS

Découvrez Netcat, un couteau suisse pour vos réseaux TCP/IP p.96

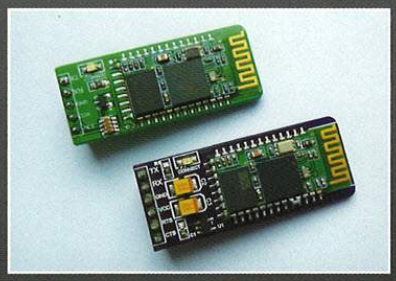
SANS FIL

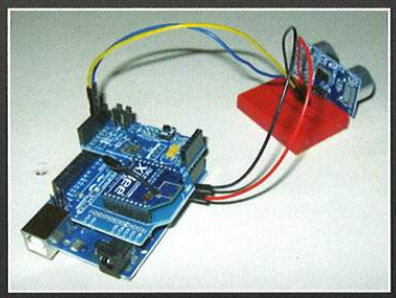
EXPLOITEZ LE BLUETOOTH ! p.24

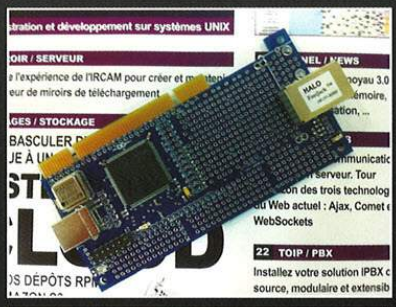
- **Comprenez les principes et le fonctionnement des protocoles**
- **Utilisez les commandes GNU/Linux pour gérer le Bluetooth**
- **Intégrez le support BlueZ dans vos programmes C**
- **Ajoutez du Bluetooth à vos montages AVR/Arduino, Launchpad, Pic, ...**
- **Développez des applications Android pour piloter vos réalisations**

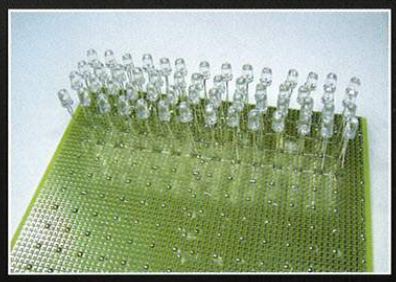
L 18310 - 5 - F: 9,00 € - RD

France Métro : 9 € / Belgique - Luxembourg : 9,50 € / Suisse : 14 CHF / DOM : 9,90 € / CAN : 15,50 $CA / N. CAL/S : 1200 CFP / POL/S : 1300 CFP









Sous réserve de toute modification

DISPONIBLE CHEZ VOTRE MARCHAND DE JOURNAUX

JUSQU'AU 30 MARS 2012

ET SUR : www.ed-diamond.com

SOMMAIRE

ÉDITO

PUTAIN, 10 ANS !

L'Histoire (oui, avec un grand H parce que ça fume)

Nous sommes en 12 après la fin du monde selon Paco Rabanne ; tout Internet est occupé par les « Gouvernements »... Tout ? Non ! Car un village peuplé d'irréductibles « hackers » résiste encore et toujours à l'envahisseur. Et la vie n'est pas facile pour les garnisons de gouvernementaux des camps retranchés de Hadopidum, Digital-Millennium-Copyright-Actum, GreatFirewallOfChinum, FiftyCentPartitum.

Ce village *geek* sans frontière ni contour résiste à l'envahisseur grâce à la potion magique préparée par le druide Magazinemix, qui procure momentanément une astuce surhumaine à quiconque en boit.

Mais revenons sur les faits qui nous ont conduits, 10 ans après, à la situation actuelle. Flash-bacchus !

« Ça » n'arrivera jamais

Il y a 10 ans naissait un petit hors-série dédié à la sécurité informatique. On y parlait reconnaissance réseau, virus, test d'intrusion, IDS et plus si affinités, choses qui semblent bien triviales aujourd'hui. Mais à l'époque, quand on évoquait ce genre de sujets, on passait au choix (non exclusif) pour un illuminé ou un dangereux hacktiviste à tendances terroristes gauchistes.

Quelques années après, on m'a invité à participer à une commission parlementaire sur ce même thème. Un « groupe de jeunes » tentait d'expliquer à un groupe de moins jeunes ce qu'était un *exploit* et comment on prenait le contrôle de réseaux. Nous proposions de mettre en place une doctrine et une dissuasion, quand on nous opposait la mise en place d'un site web pour informer le grand public sur les risques. Au final, c'est le site web qui a vu le jour.

suite page 4

MISC est édité par **Les Éditions Diamond**
B.P. 20142 / 67603 Sélestat Cedex
Tél. : 03 67 10 00 20 - **Fax** : 03 67 10 00 21
E-mail : cial@ed-diamond.com
Service commercial : abo@ed-diamond.com
Sites : www.miscmag.com
www.ed-diamond.com
IMPRIMÉ en Allemagne - PRINTED in Germany
Dépôt légal : A parution
N° ISSN : 1631-9036
Commission Paritaire : K 81190
Périodicité : Bimestrielle
Prix de vente : 8 Euros

Directeur de publication : Arnaud Metzler
Chef des rédactions : Denis Bodor
Rédacteur en chef : Frédéric Raynal
Secrétaire de rédaction : Véronique Sittler
Conception graphique : Kathrin Troeger
Responsable publicité : Tél. : 03 67 10 00 27
Service abonnement : Tél. : 03 67 10 00 20
Impression : VPM Druck Rastatt / Allemagne
Distribution France : (uniquement pour les dépositaires de presse)
MLP Réassort :
Plate-forme de Saint-Barthélemy-d'Anjou. Tél. : 02 41 27 53 12
Plate-forme de Saint-Quentin-Fallavier. Tél. : 04 74 82 63 04
Service des ventes : Distri-médias : Tél. : 05 34 52 34 01

Membre April
www.april.org

Charte de MISC **www.miscmag.com**

MISC est un magazine consacré à la sécurité informatique sous tous ses aspects (comme le système, le réseau ou encore la programmation) et où les perspectives techniques et scientifiques occupent une place prépondérante. Toutefois, les questions connexes (modalités juridiques, menaces informationnelles) sont également considérées, ce qui fait de MISC une revue capable d'appréhender la complexité croissante des systèmes d'information, et les problèmes de sécurité qui l'accompagnent. MISC vise un large public de personnes souhaitant élargir ses connaissances en se tenant informées des dernières techniques et des outils utilisés afin de mettre en place une défense adéquate.
MISC propose des articles complets et pédagogiques afin d'anticiper au mieux les risques liés au piratage et les solutions pour y remédier, présentant pour cela des techniques offensives autant que défensives, leurs avantages et leurs limites, des facettes indissociables pour considérer tous les enjeux de la sécurité informatique.

ÉDITO

On nous expliquait que toutes ces menaces n'existaient que dans les films et les romans que nous regardions et lisions, mais pas dans la vraie vie.

Et pourtant, on est toujours la cible de quelqu'un.

Le professionnel

Petit à petit, le domaine évolue. D'abord, de très nombreuses formations spécialisées voient le jour. Ensuite, des initiations à la sécurité sont dispensées dans de nombreux cursus d'ingénieurs. Mais comme on ne forme plus d'ingénieurs, mais des chefs de projet, les salles de cours de sécurité restent vides.

Puis vint le Livre Blanc de la défense en 2008. On continue à former uniquement des chefs de projet alors que l'État commence à recruter des profils beaucoup plus techniques. Et c'est au tour des entreprises, attirées par le mythe juteux de la « cyberdéfense », de se lancer dans cette activité. Tous les grands groupes embauchent des gens aux compétences techniques avérées... mais ne savent pas quoi faire avec ces personnes, qui partent au fil des ans, que ce soit à l'étranger dans un premier temps, ou dans l'administration dans un deuxième.

Aujourd'hui, l'étranger comme l'administration continuent à attirer les compétences. Pourquoi ? Parce qu'on ne sait pas, dans les grandes entreprises françaises, gérer et valoriser un savoir-faire. Là où nos industries proposent de la bureaucratie, l'étranger ou l'État propose de relever de vrais défis. Et ça tombe bien car c'est exactement ce que cherchent des cerveaux créatifs.

Mais la créativité ne rentre pas dans la feuille Excel d'un contrôleur de gestion.

Le thermomètre

Je discutais il y a peu de temps avec une personne en charge de lourdes responsabilités. Elle m'exposa de manière très convaincante sa vision de la situation en faisant le parallèle avec l'utilisation du thermomètre : nous ne faisons que commencer à être équipés de thermomètres. Cela nous permet de réaliser à quel point nous sommes malades. Sans cet instrument, nous étions auparavant convaincus d'aller bien.

Les dernières intrusions comme Areva ou Bercy, pour n'en citer que deux, ont marqué les esprits. On réalise que certains réseaux sont compromis depuis 2007 au moins. On ne peut pas dire si ça remonte à avant car les traces ne sont évidemment pas conservées.

Je regrette le petit plaisir mesquin que j'aurais eu à recroiser le chemin des membres moins jeunes de la commission évoquée ci-dessus, mais ils doivent être à la retraite maintenant (qui a dit j'espère ?). Place aux jeunes. C'est grâce aux compétences pointues que le thermomètre non seulement fonctionne, mais existe. Ma grand-mère utilise encore un téléphone à cadran alors que mes neveux manipulent un iPhone les yeux fermés (genre, j'allais les omettre dans l'édito des 10 ans ;-)).

Le rôle social du « hacker », un nouveau contre-pouvoir ?

On parle depuis toujours du fossé générationnel. On se demande s'il n'a jamais été aussi grand bla bla bla. Regardons simplement les faits. D'un côté, on a des seniors très éloignés des préoccupations du terrain, qui parlent « politique » et « réduction des coûts ». De l'autre, on a une génération de minots capables de tout casser, remplis d'idéaux, et méprisés par un système qu'ils ne comprennent pas (et réciproquement).

Évidemment, l'association de telles capacités avec des idéaux, ça détonne. Et on a vu naître une sorte de contre-pouvoir flou, épris de liberté, parfois potache, en caricaturant à outrance, c'est un monde de régulation totale opposé à un monde de liberté totale, un monde fermé contre un monde ouvert. La récupération des informations personnelles des personnalités UMP, stockées dans un fichier qui n'existait donc pas d'après les responsables du mouvement, illustre cet antagonisme.

C'est sans doute très prétentieux, mais j'espère que *MISC* et *SSTIC*, qui fêtera aussi ses 10 ans dans les mois qui suivent, auront participé à ces évolutions. J'ai toujours été convaincu que le savoir devait être partagé pour nous rendre plus forts. Certains sont tombés dans la potion en lisant nos articles (attention aux effets secondaires, genre perte totale de cheveux, comme Cédric F., capillarité brushing à la Bee Gees comme Benjamin C., ou mauvaise foi amplifiée comme Damien A.) et assurent la relève, pour les 10 prochaines années j'espère !

Le casting : ceux qui ont fait, font et feront MISC

Abraracourcix (Arnaud Metzler) est le chef de cette petite entreprise perdue au fin fond de l'Alsace qu'est Diamond Éditions. Il n'est pas le dernier à râler, à foncer au milieu de la bagarre.

Assurancetourix (Denis Bodor), rédacteur en chef emblématique de *GNU/Linux Magazine France* (GLMF), mon mentor qui m'a pris sous son aile pour apprendre à chanter (oups, non) rédiger des articles, puis pousser à devenir rédacteur en chef. Je dirais juste : merci !

Falbala (Véronique Sittler Wilhelm), assistante de rédaction qui donne de son corps depuis des années, d'abord en prêtant sa main pour des photos érotiques de clés USB dans les pubs à la fin des magazines Diamond, puis ses jambes pour la couverture sur le porno. C'est elle le lubrifiant de cet organe qu'est *MISC*, qui coordonne les articles, la PAO, l'impression entre autres.

Agecanonix (Fred Raynal), la mémoire de *MISC*, le faiseur, le créateur, le concepteur, ou encore le (grand-)père mais toujours vert... avec des rhumatismes quand même (à 93 ans, ce n'est pas étonnant).

Idéfix (Damien Aumaitre) est le fidèle compagnon, le gardien, le guide. Il ne faut pas le chercher, sinon il râle. D'ailleurs, il râle même quand on ne le cherche pas.

Ordralfabétix (Benjamin Caillat) prétend qu'il est frais son dossier, mais bon, l'architecture des PC remonte à Von Neumann. Et dire qu'il en prépare un sur les cartes perforées...

Cétautomatix (Cédric Foll) n'aime que le poisson frais et pour ça il le pêche lui-même. Physiquement « fort » (comprendre enveloppé), fêtard, gouailleur, il est l'homme des dossiers improbables.

Changélédix (Nicolas Brulez), adepte de Cannibal Corpse, retardataire chronique dans sa remise de corner, et néanmoins *reverse engineer* ayant appris à écrire autrement qu'en Assembleur.

Ocatarinetabellatchitchix (Gabriel Campana), corse présumé dont le souffle fait trembler les éoliennes et les éditeurs logiciels lorsqu'il code des exploits entre le figatellu et le fromage.

Barométrix (Nicolas Ruff), le vieux des coins avec autant de tours dans son sac que MacGyver, une verve vouée aux #fails en tous genres.

La potion magique, alias tous les auteurs qui ont contribué une fois ou de multiples fois. À ce titre, spéciale dédicace et remerciements chaleureux à Renaud Bidou et Éric Filiol, prolifiques parmi les prolifiques.

N'oublions pas non plus les « petites mains », celles qui œuvrent dans l'ombre aux relectures, à la PAO et autres secrets de fabrication du journal, ou encore celles qui achètent le magazine depuis toutes ces années.

Enfin, dédicace spéciale à Laval et Montluçon, hauts fiefs de mes railleries de Parigot tête de veau, mais où l'accueil reste toujours chaleureux (enfin, quand on arrive à trouver ces lieux-dits ;-)).

Les bonus

Note du rédac chef historique : les gamins n'ont pas touché un sesterce pour les fleurs, même piquantes, qu'ils lancent, c'est du 100 % naturel.

MISC selon Damien Aumaitre

10 ans ! Quand j'ai appris que lorsque le prochain numéro paraîtrait, *MISC* aurait 10 ans, j'ai pris un coup de vieux... et puis Fred est venu me voir en me disant qu'il fallait que j'écrive une partie de l'édito, et là, ce fut le drame...

Je me souviens encore des premiers numéros imprimés sur un papier douteux avec des encres pâlichonnes, du plaisir de parcourir un magazine dont je ne comprenais même pas un cinquième des articles.

Plus tard, j'ai eu la chance de pouvoir publier un article, c'était classe, je pouvais dire « j'ai écrit dans *MISC* » !

Lorsqu'il y a un peu plus d'un an, Fred m'a proposé de devenir co-rédacteur en chef, j'ai ressenti une énorme responsabilité, j'ai longuement hésité, l'héritage à assumer me semblait énorme.

Maintenant que je suis de l'autre côté de la barrière, j'ai pu découvrir le travail effectué par toute une équipe afin de permettre la parution du magazine et je suis fier d'en faire partie. Et quand je vois les difficultés que nous avons alors que nous sommes 3, je n'arrive pas à imaginer comment Fred a pu faire ça tout seul pendant 9 ans, et là, je suis vraiment admiratif !

Donc merci encore à Fred pour m'avoir donné cette opportunité, merci aux Éditions Diamond de publier ce magazine et merci à tous les auteurs et lecteurs pour cette aventure qui dure depuis maintenant 10 ans !

MISC selon Benjamin Caillat

La question a toujours été là. Que représente la sécurité ? Il y a 10 ans, tout rose et frais sorti de mon école d'ingénieur, je rentrais dans le monde professionnel, tout excité à l'idée de rejoindre un groupe de consultants consciencieux et passionnés œuvrant de toutes leurs forces pour le maintien de l'ordre et de la sécurité de nos réseaux. Petite désillusion en découvrant une réalité où la sécurité est parfois plus considérée comme un outil à des fins commerciales, politiques ou stratégiques qu'une composante essentielle d'un projet.

Quittant ma douce province pour la capitale, je rencontrais chemin faisant Fred, puis *MISC*, *SSTIC* et tout le petit milieu gravitant autour. Je trouvais enfin parmi eux ce violent désir de comprendre, de relever des défis. *MISC* a été cela pour moi. Une espèce de contre-pouvoir faisant un pied de nez à tout ceux pour qui la sécurité est un produit ou un business, qui a su allier en même temps haute technicité et pédagogie, esprit un peu rebelle et professionnalisme, contribuer à expliquer que « chercheur en sécurité » ne rime pas avec « hacker prêt à tout casser », même s'il est vrai que certains ont des esprits quelque peu taquins...

Quand Fred m'a proposé de participer à *MISC* il y a un an, j'ai eu comme un frisson. Grosse responsabilité et serait-il possible de piloter cela depuis la Californie ? J'ai hésité, mais pas longtemps. Alors j'aimerais vous faire rêver, dire que j'écris mes éditos en surfant, que l'idée du dossier Archi PC m'est venue en grimpant El Capitan et que je relis les articles sur une plage où évoluent de somptueuses Californiennes. Mais la réalité est un peu moins idyllique et le stress des bouclages m'a vite fait comprendre l'origine des problèmes de tension de notre papy. Mais ceci n'est que broutille en comparaison du plaisir d'échanger avec les auteurs et d'avoir le sentiment d'apporter sa petite contribution à l'édifice.

Alors la question est toujours là. Que représente la sécurité ? Quand je vois que *MISC* existe depuis 10 ans, je me dis qu'il y a des gens pour qui c'est une passion promue par le goût du challenge et la conscience de la responsabilité de travailler dans un domaine critique, pas uniquement un business. Alors un grand merci à vous tous lecteurs, auteurs et rédacteurs qui continuez à développer ce *happy hacking* éthique.

MISC selon Cédric Foll

C'est non sans émotion et nostalgie que je me remémore il y a 10 ans la découverte du premier numéro de *MISC* (en fait un hors-série de *Linux Magazine*).

Je venais de tomber dans la marmite de la sécurité informatique via mon stage ingénieur. Un monde merveilleux s'ouvrait à moi et je me suis immédiatement passionné pour l'exploration des réseaux à grands coups de nmap, de découverte de services non patchés et d'*exploits* recensés sur securityfocus (que je n'arrivais d'ailleurs presque jamais à faire fonctionner...).

L'époque était insouciante, il suffisait d'annoncer doctement qu'il y avait trop de ports ouverts et qu'Apache affichait son numéro de version pour que le client soit admiratif devant l'armée de *hackers* qui lui rendait son rapport de test d'intrusion.

Jamais je n'aurais imaginé à cette époque que j'aurais un jour l'honneur de concourir à l'élaboration de ce magazine. C'est pourtant ce qui m'est arrivé il y a presque un an et j'ai pu connaître à mon tour les angoisses de ne pas réussir à joindre l'auteur qui avait promis de rendre à temps son article et qui devient injoignable à deux jours du bouclage (à se demander comment Fred qui a géré tout seul *MISC* pendant presque dix ans a réussi à garder autant de cheveux, presque tous blancs, certes).

Mais travailler pour *MISC*, c'est aussi la gloire, c'est recevoir un *tweet* de l'équipe de Marc Dorcel souhaitant participer à un dossier des plus pointus, être reconnu dans les rues de Mamoudzou par des étudiantes en informatique (c'est juste un fantasme, car à mon grand désarroi, *MISC* n'est pas distribué à Mayotte et l'éducation nationale ne propose pas d'informatique après le bac), ...

En tout cas, je pense, en toute modestie, car je n'ai participé à cette revue que très tardivement, que toute une génération de spécialistes français de la sécurité doit beaucoup à *MISC* : nanos gigantium humeris insidentes. ■

Rendez-vous au 02 mars 2012 pour le n°60 !

APACHE KILLER

OU COMMENT « PLANTER » LES DEUX TIERS DES SERVEURS WEB SUR INTERNET

Younes Jaaidi (yjaaidi@gmail.com) et Laurent Butti (laurent.butti@gmail.com)

mots-clés : APACHE / DÉNI DE SERVICE / RFC 2616

La veille d'un week-end ensoleillé d'août dernier fut subitement publié un outil exploitant une vulnérabilité de déni de service visant toutes les versions du serveur web Apache.

Une exploitation réussie de cette faille est inhabituellement dévastatrice : il est possible de rendre indisponible un serveur web vulnérable en envoyant simplement quelques dizaines de requêtes malveillantes.

Cet article décrit les principes de fonctionnement de cette vulnérabilité ainsi que les différentes solutions pour s'en prémunir. Enfin, il rappellera que les attaques de déni de service peuvent également servir à d'autres finalités que la « simple » rupture de service.

1 Introduction

Les vulnérabilités du serveur web Apache ne sont pas légion. Bien que quelques vulnérabilités dans les modules `mod_dav_svn`, `mod_proxy` et `mod_proxy_ajp` aient déjà été publiées, ces dernières ne sont pas atteignables dans une configuration par défaut d'Apache.

Le vendredi 19 août 2011 a été publié sur la liste de diffusion « full disclosure » un message intitulé « Apache Killer » émis par Kingcope (qui s'était déjà illustré par la découverte d'une vulnérabilité de déni de service dans le module `mod_dav_svn` d'Apache) et accompagné d'un script PERL **[KILLER]**.

Deux particularités ont été frappantes lors de la publication de cette vulnérabilité : premièrement, sa portée, car elle affecte toutes les versions du produit Apache HTTPD, et deuxièmement, sa facilité d'exploitation, car elle n'exige quasiment aucune condition pour être exploitée. En effet, il suffit pour cela que le serveur distribue du contenu, ce qui est par définition le cas de presque tous les serveurs web.

Sachant qu'à ce jour, plus de 65 % des serveurs HTTP utilisés sont des serveurs Apache HTTPD **[NETCRAFT]**, le nombre de machines atteignables est exceptionnellement important.

Bien que l'on ait pu constater l'apparition de plusieurs variantes de l'exploit sur des sources variées et accessibles publiquement **[VARIANTES]** ainsi que la prise en compte de la vulnérabilité dans plusieurs outils de sécurité classiques **[NESSUS, METASPLOIT]**, nous n'avons pas eu connaissance d'attaques publiques sur des sites majeurs. Par contre, nous avons régulièrement constaté des tentatives de reconnaissance sur des sites en production mais qui n'ont pas entraîné de lancement de l'attaque.

2 La vulnérabilité

2.1 Mode opératoire de l'exploit publié

Le script PERL émet la requête HTTP ci-dessous :

```
HEAD / HTTP/1.1
Host : dos.target.name
Range : bytes=0-
Accept-Encoding: gzip
Connection: close
```

Si la réponse retournée par le serveur contient le mot « Partial », la cible est considérée comme vulnérable et la requête ci-dessous est alors massivement rejouée :

```
HEAD / HTTP/1.1
Host : dos.target.name
Range : bytes=,5-0,5-1,...,5-1298,5-1299
Accept-Encoding: gzip
Connection: close
```

À noter que l'outil utilise des requêtes **HEAD**, mais qu'il est possible d'utiliser le classique **GET**.

2.2 « Partial Content » et en-tête « Range »

La vérification de la présence du mot « Partial » dans la réponse HTTP montre que l'attaque cible la fonctionnalité HTTP « Partial Content » **[RFC2616]** qui permet de récupérer, en une requête, une ou plusieurs parties d'une ressource (image, fichier html, fichier PDF, ...) hébergée sur un serveur plutôt que son intégralité. Cette fonctionnalité apporte la parallélisation du téléchargement d'un fichier (plusieurs connexions récupèrent différentes parties du fichier) ou la récupération « stratégique » de quelques parties d'un fichier (consultation des dimensions d'une image avant téléchargement intégral par exemple).

2.3 Scénario de l'attaque

L'attaque force le serveur à segmenter le fichier demandé en plusieurs milliers de parties, et ce, pour chaque requête. La génération de chacune de ces parties nécessitant des allocations et des recopies provoque alors « rapidement » la saturation des ressources (CPU puis mémoire) du serveur.

Note : Alerte levée en 2007

L'idée de produire un déni de service à travers la fonctionnalité « Partial Content » a été évoquée pour la première fois par Michal ZALEWSKI dans un message datant de 2007 [BUGTRAQ] et n'ayant abouti à aucun correctif. Le scénario qui y est présenté cible la saturation de la bande passante sortante plutôt que la mémoire ou le CPU et ce en entraînant la génération d'une réponse de taille importante par le serveur puis en jouant sur la taille des fenêtres TCP [WINDOW] pour que le serveur continue à émettre les paquets bien que l'attaquant ne les prenne bien entendu pas en compte.

2.4 Détection de l'attaque

Détecter le comportement de l'outil qui a été publié est relativement simple car les clients HTTP légitimes n'émettront jamais de requête **HEAD** avec un en-tête **Range** : il suffit alors de parcourir les fichiers de journalisation du serveur web à la recherche de requêtes **HEAD** dont le « status code » est 206.

La détection avec précision de l'attaque elle-même est plus complexe car elle vise des mécanismes internes d'Apache où il n'y aura pas de journalisation. Cependant, la détection d'une attaque en cours pourra être rapide à cause des effets de bord sur les indicateurs de supervision système (CPU, mémoire) et de qualité de service (temps de réponse du serveur). Mais il sera déjà trop tard...

2.5 Origines de la vulnérabilité

2.5.1 Entrelacement des tranches

Comme précisé dans le chapitre 2.2, la fonctionnalité « Partial Content » sert à optimiser les performances. Le fait de demander au sein d'une même requête des parties qui s'entrelacent (parties contenant des octets en commun) force une duplication de contenu qui ne présente aucun intérêt. Les requêtes de ce type devraient donc être considérées invalides et l'en-tête **Range** ignoré.

De même, la somme des tailles de l'ensemble des parties demandées dans une requête ne devrait jamais dépasser la taille totale de la ressource demandée car dans ce cas la fonctionnalité n'aurait également aucun intérêt.

2.5.2 Complexité en $O(N^2)$

2.5.2.1 Structure `apr_bucket_brigade`

L'extraction des parties demandées à partir de la ressource se fait dans le filtre `ap_byterange_filter`. L'intégralité du contenu de la ressource lui est présenté en paramètre sous la forme d'une « brigade », une instance de la structure `apr_bucket_brigade`.

Pour des raisons de concision, nous nous limiterons à définir cette structure comme une liste chaînée de « buckets », instances de la structure `apr_bucket` qui à leur tour pointent sur un ou plusieurs « buffers » de données communs et contiennent certaines informations supplémentaires comme l'offset de début, la longueur, le « bucket » précédent, le suivant, etc. Ce fonctionnement sert à optimiser les performances du serveur en évitant par exemple de recopier l'intégralité d'un « buffer » à chaque modification.

Une explication plus complète et accompagnée d'exemples est disponible sur **[BRIGADES]**.

2.5.2.2 Effet de bord de la fonction apr_brigade_partition

La fonction **apr_brigade_partition** partitionne une « brigade » en faisant le nécessaire (modification/création de « buckets », modifications de la chaîne) afin d'obtenir dans la chaîne de « buckets » contenus dans celle-ci, un « bucket » dont le premier octet correspond à l'offset demandé.

Pour chacune des parties demandées, le filtre **ap_byterange_filter** modifie la « brigade » contenant l'intégralité de la ressource en la partitionnant aux offsets de début et de fin de la partie ; tous les « buckets » compris entre ces deux offsets sont ensuite copiés un par un dans la « brigade » finale (contenant l'ensemble des parties demandées) qui sera transmise au filtre suivant. Ce traitement est effectué par l'extrait de code ci-dessous.

```
ap_byterange_filter(ap_filter_t *f, apr_bucket_brigade *bb) {

    apr_bucket *ec, *e2;
    apr_off_t range_start, range_end;
    apr_bucket_brigade * bsend;

    ...

    while (parse_byterange(..., ..., &range_start, &range_end)) {
        ...
        apr_brigade_partition(bb, range_start, &ec);
        apr_brigade_partition(bb, range_end + 1, &e2);
        ...

        do {
            apr_bucket *foo;
            apr_bucket_copy(ec, &foo);
            APR_BRIGADE_INSERT_TAIL(bsend, foo);
            ec = APR_BUCKET_NEXT(ec);
        } while (ec != e2);
    }

    ...

    /* send our multipart output */
    return ap_pass_brigade(f->next, bsend);
}
```

La modification de la même « brigade » **bb** à l'extraction de chaque partie augmente le nombre de « buckets » dans celle-ci (dans le pire des cas, deux « buckets » sont ajoutés à l'extraction de chaque partie) provoquant ainsi une fragmentation importante de la chaîne. Or, comme précisé précédemment, pour chaque partie, tous les « buckets » compris entre les offsets de début et de fin sont copiés dans la « brigade » finale. Le nombre de copies effectuées est alors quadratiquement (complexité en $O(N^2)$) proportionnel au nombre de parties demandées. Ceci n'est vrai que si les parties s'entrelacent car sinon l'extraction de chaque partie ne copiera qu'un seul « bucket ».

La copie d'un « bucket » ne duplique pas le « buffer » sur lequel il pointe. Les ressources systèmes sont saturées simplement par le nombre important d'allocations de structures **apr_bucket**.

2.6 Optimisation de l'attaque

2.6.1 Augmentation du nombre de parties

L'attaque peut être rendue plus efficace en demandant plusieurs fois la même tranche « 0- ». Celle-ci représente l'intégralité du contenu et a la particularité de n'occuper que deux octets de l'en-tête **Range** dont la longueur est limitée par la directive **LimitRequestFieldSize**. Ainsi, dans une configuration par défaut d'Apache, il sera possible de provoquer la génération d'une réponse dont la taille dépasse de plus de 2700 fois la taille du fichier initial. Le nombre de parties maximum pouvant être demandées est obtenu en soustrayant la longueur de la chaîne de caractères « Range:bytes= » (12) à la valeur par défaut de la directive **LimitRequestFieldSize** (8190) puis en divisant le résultat par 3 (longueur de la chaîne de caractères « 0-, »).

2.6.2 Augmentation du nombre de copies de la structure apr_bucket

Une autre technique d'optimisation de l'attaque consiste à demander des parties successivement imbriquées ; la première partie étant la plus petite et strictement incluse dans la seconde et ainsi de suite jusqu'à l'avant-dernière qui est strictement incluse dans la dernière.

De cette façon, l'extraction de chaque partie segmente la « brigade » contenant l'intégralité de la ressource aux limites de la partie demandée et crée un ou deux nouveaux « buckets » (un si l'une des limites de la partie est commune avec la partie précédente et deux si aucune des limites n'est commune). Ensuite, tous les « buckets » créés lors des extractions des parties précédentes sont

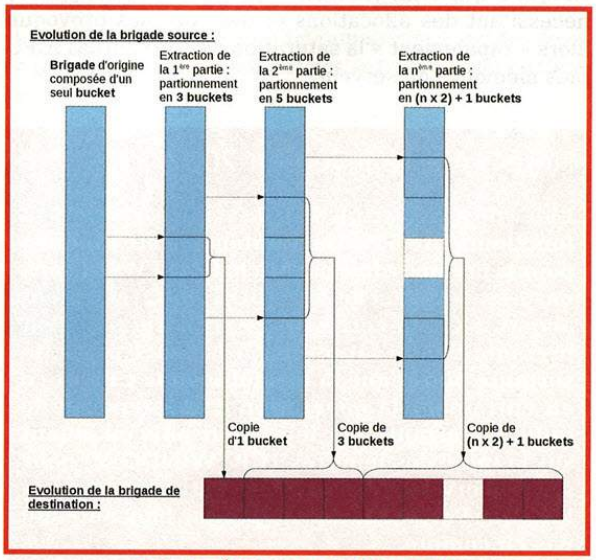


Fig. 1 : Évolution de la brigade

dupliqués dans la « brigade » de destination contenant la réponse finale à envoyer au client (cf. Figure 1).

La combinaison de parties suivante « (n)-,(n-1)-,...,1-,0- » est l'un des meilleurs compromis entre la contrainte sur la longueur de l'en-tête **Range** et le nombre de duplications de « buckets » provoquées sur le serveur (chaque partie est bien strictement incluse dans la précédente).

2.7 Vulnérabilité générique ?

Vu que cette vulnérabilité n'est pas simplement la conséquence d'une erreur d'implémentation mais plutôt d'un manque de contraintes dans la RFC 2616 qui n'interdit pas l'entrelacement de parties, puis une implémentation « naïve » (vérification limitée des parties demandées), il est légitime de s'interroger quant à la présence de cette vulnérabilité sur d'autres serveurs HTTP.

Il s'avère en effet, alors que toute l'attention était portée sur Apache HTTPD, que le serveur Nginx a été mis à jour le 5 septembre 2011 (version 1.1.2) sans toutefois avoir de référence officielle avec la publication de la vulnérabilité, mais avec le message suivant assez équivoque **[NGINX]** :

> « *) *Change: now if total size of all ranges is greater than source response size, then nginx disables ranges and returns just the source response.*
>
> *) *Feature: the "max_ranges" directive.* »

Sur le produit Microsoft IIS, la vulnérabilité semble être adressée depuis la version 6 en limitant le nombre de parties pouvant être demandées au sein d'une même requête **[IIS]**.

2.8 Benchs

Nous avons pu réaliser quelques tests de performance avec les deux méthodes d'optimisation proposées, tests qui parlent d'eux-mêmes.

3 Les solutions

3.1 Solution de contournement via la configuration Apache

En attendant la mise à jour du serveur Apache, de nombreux échanges ainsi qu'une note d'avertissement Apache **[CVE-2011-3192]** proposaient une solution de contournement consistant à ignorer l'en-tête **Range** si le nombre de parties demandées dépasse un certain seuil.

Il est aussi possible de journaliser le contenu de l'en-tête **Range** si la requête est considérée comme malveillante (pour investiguer et adapter le seuil en cas de faux positifs sur des applications légitimes utilisant l'en-tête **Range** au-dessus du seuil) grâce aux lignes suivantes de la configuration du serveur Apache :

```
SetEnvIf Range ^[^,]*+(,[^,]*+){5,}$ bad-range=$0
SetEnvIf Request-Range ^[^,]*+(,[^,]*+){5,}$ bad-request-range=$0
RequestHeader unset Range env=bad-range
RequestHeader unset Request-Range env=bad-request-range
LogFormat "%h %l %u %t \"%r\" %>s %O \"Range: %{bad-range}e\"
\"%{Referer}i\" \"%{User-Agent}i\"" logformat_cve_2011_3192
```

puis dans chaque *virtual host* :

```
CustomLog log/cve_2011_3192_audit.log logformat_cve_2011_3192
env=bad-range
CustomLog log/cve_2011_3192_audit.log logformat_cve_2011_3192
env=bad-request-range
```

Pour des raisons historiques, Apache HTTPD traite l'en-tête **Request-Range** de la même façon que l'en-tête **Range**. Cet en-tête avait été « oublié » dans les premiers échanges mais saute aux yeux à la lecture du code source (traitement de certains navigateurs historiques), ce qui aurait pu laisser la porte ouverte à de nouvelles variantes qui auraient contourné la solution proposée initialement par Apache.

Payload	Nombre d'appels aux fonctions pour une requête	Nombre de requêtes avant écroulement du serveur (4 x CPU 2 Ghz, 2 Go RAM)
0-,0-,...,0- (2700 parties)	`apr_bucket_shared_copy` : 2700	Plus de 10 000 requêtes
	`apr_bucket_alloc` : 13529	
	`apr_bucket_free` : 13529	
	`malloc` : 479	
	`free` : 430	
1499-,...,1-,0- *(1500 parties)*	`apr_bucket_shared_copy` : 1 178 880	Moins de 100 requêtes
	`apr_bucket_alloc` : 1 186 583	
	`apr_bucket_free` : 1 186 583	
	`malloc` : 23 929	
	`free` : 23 880	

```
/*
 * Check for Range request-header (HTTP/1.1) or Request-Range for
 * backwards-compatibility with second-draft Luotonen/Franks
 * byte-ranges (e.g. Netscape Navigator 2-3).
 *
 * We support this form, with Request-Range, and (farther down) we
 * send multipart/x-byteranges instead of multipart/byteranges for
 * Request-Range based requests to work around a bug in Netscape
 * Navigator 2-3 and MSIE 3.
 */

if (!(range = apr_table_get(r->headers_in, "Range"))) {
    range = apr_table_get(r->headers_in, "Request-Range");
}
```

3.2 Solution de filtrage applicatif via ModSecurity

Pour les heureux possesseurs d'un *Web Application Firewall*, et tout particulièrement pour ModSecurity, il est bien entendu envisageable de protéger son infrastructure de cette vulnérabilité grâce à des règles personnalisées qui filtreront l'utilisation des en-têtes Range et `Request-Range` avant leur interprétation par Apache **[BLOG]**.

```
SecRule REQUEST_HEADERS:Range|REQUEST_HEADERS:Request-Range
"^bytes=\s*((\d+)?\-(\d+)?\,){5,}" "chain,phase:1,t:none,log,msg:'Tr
uncating Large Range Header Field.',capture,pass"
        SecRule REQUEST_HEADERS:Range|REQUEST_HEADERS:Request-Range
"^bytes=\s*((\d+)?\-(\d+)?\,){5}" "chain,capture"
                SecRule TX:0 "^(.*),$" "capture,setenv:range_
header=%{tx.1}"

RequestHeader unset Range env=range_header
RequestHeader set Range "%{range_header}e" env=range_header
```

À noter que des solutions existent aussi par des WAF commerciaux **[F5]**, que ce soit par élimination pure et simple des en-têtes concernés ou par application de règles spécifiques avec expressions rationnelles extrêmement ressemblantes à celles de ModSecurity, mais sans l'en-tête `Request-Range` !

```
when HTTP_REQUEST {
    # remove Range requests for CVE-2011-3192 if more than 5 ranges
are requested
    if { [HTTP::header "Range"] matches_regex {bytes=(([0-9\- ])+,)
{5,}} } {
        HTTP::header remove Range
    }
}
```

Les deux ensembles de règles ont un point commun négatif vis-à-vis des faux positifs (filtrage d'applications légitimes) car elles tronqueront les requêtes qui auront plus de cinq parties, ce qui est éventuellement à « personnaliser » à d'autres valeurs si vous avez une très bonne vue des usages de votre site en production.

■ RAPPELS SUR LA CHRONOLOGIE DES ÉVÉNEMENTS

- **4 janvier 2007**
  Michal ZALEWSKI présente la vulnérabilité pour la première fois [http://seclists.org/bugtraq/2007/Jan/83]
- **19 août 2011**
  Kingcope publie le premier exploit de la vulnérabilité [http://seclists.org/fulldisclosure/2011/Aug/175]
- **24 août 2011**
  Apache advisory accompagnée du workaround [http://httpd.apache.org/security/CVE-2011-3192.txt]
- **24 août 2011**
  Publication de règles ModSecurity [http://blog.spiderlabs.com/2011/08/mitigation-of-apache-range-header-dos-attack.html]
- **25 août 2011**
  Premier correctif [http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/http/byterange_filter.c?r1=1135171&r2=1161534]
- **27 août 2011**
  Second correctif [http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/http/byterange_filter.c?r1=1162325&r2=1162331]
- **28 août 2011**
  Troisième correctif
- **31 août 2011**
  Apache 2.2.20 [http://www.apache.org/dist/httpd/CHANGES_2.2]
- **5 septembre 2011**
  Nginx 1.1.2 [http://nginx.org/en/CHANGES]
- **14 septembre 2011**
  Apache 2.2.21 [http://www.apache.org/dist/httpd/CHANGES_2.2]

3.3 Correctifs Apache

3.3.1 Premier correctif

Le premier correctif qui est apparu dans le code d'Apache HTTPD remédiait au problème de la complexité en $O(N^2)$ en utilisant une nouvelle fonction `copy_brigade_range` qui extrait une partie depuis une « brigade » sans la modifier. La fonction `apr_brigade_partition` n'est donc plus utilisée dans ce contexte.

3.3.2 Second correctif

L'en-tête **Range** (ou **Request-Range**) est ignoré si la somme des tailles des parties demandées dépasse la taille de l'intégralité de la ressource.

3.3.3 Troisième correctif

Ce correctif introduit la directive **MaxRanges** qui définit le nombre maximum de parties pouvant être demandées au sein d'une requête. La valeur par défaut de cette directive est fixée à 200. Des limitations de ce type peuvent provoquer des comportements inattendus sur des logiciels clients légitimes.

3.3.4 Remarques

Malgré tous ces correctifs, il est toujours possible de demander plusieurs parties qui s'entrelacent. Des changements sont proposés au niveau de la RFC 2616 **[RFC2616-FIX]**.

De plus, en l'absence de tests unitaires, cette série de correctifs intégrés dans la version 2.2.20 d'Apache HTTPD n'a pas manqué d'introduire une régression **[REGRESSION]** corrigée dans la version 2.2.21.

4 Impacts des dénis de service

L'impact d'une attaque de déni de service est souvent, à tort, considéré comme limité à l'impact « business » du fait de la dégradation de service. Or, il est possible que cela ait une incidence sur d'autres services qui en dépendent provoquant alors une régression sur ces derniers.

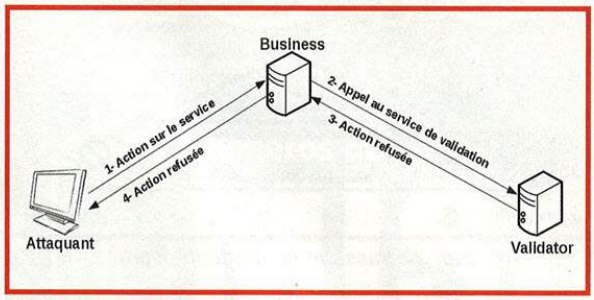


Fig. 2 : Certains éléments sont vérifiés à distance

Par exemple, un service « Validator » propose un service de validation d'opérations, d'authentification forte ou de confirmation de paiements à un service « Business » (cf. Figure 2) ; si le service « Validator » est injoignable,

alors plutôt que d'être à son tour indisponible, le service « Business » acceptera le risque de passer dans un mode « dégradé » et donc d'outrepasser les vérifications effectuées par le service « Validator » (cf. Figure 3).

Dans ce cas, une entité malveillante souhaitant effectuer une action non autorisée sur le service « Business » peut attaquer le service « Validator » à travers un déni de service forçant ainsi le service « Business » à « alléger » ses vérifications.

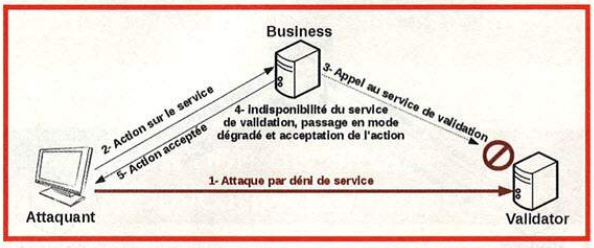


Fig. 3 : Passage en mode dégradé

Dans la plupart des cas similaires à ce scénario, le risque est accepté car la source de l'indisponibilité est, à tort, supposément due à un problème technique et non à une attaque.

Conclusion

Comme cela est souvent le cas, il faut une publication un peu « violente » pour faire bouger les choses, car même si cette vulnérabilité est différente de celle publiée en 2007, elle n'en est pas moins portée sur la même fonctionnalité. Il suffit de se rappeler de l'émoi suscité par la publication de Firesheep pour que quelques services majeurs (Facebook, Twitter) aient migré leurs services vers HTTPS. L'histoire de la sécurité est régulièrement jonchée de tels exemples !

L'exposition de cette vulnérabilité était énorme, et malgré cela, pas d'attaque publique recensée... C'est tout à fait étonnant (limite décevant ?!?) sans compter le fait que la porte était béante car cette vulnérabilité a mis près de treize jours pour avoir son correctif applicatif publié par Apache. Cependant, il est fort à parier que cette technique d'attaque se retrouvera en standard dans les différents kits DDoS afin de disposer d'une brique supplémentaire extrêmement efficace contre les services n'ayant pas pris en compte l'exposition à cette vulnérabilité (mises à jour, solutions de contournement).

Enfin, cet article aura eu pour objectif de souligner que des manques de contraintes dans les spécifications (RFC 2616) auront eu pour conséquence une vulnérabilité de déni de service sur certaines implémentations de serveurs HTTP.

Pour conclure, les vulnérabilités de déni de service comme celles-ci sont plus difficiles à découvrir et à corriger car elles sont fonctionnelles. Pour empêcher un service d'être vulnérable, il faut s'assurer que les limites d'itération ou de récursivité ne soient pas contrôlables par les utilisateurs et trouver le meilleur compromis avec le fonctionnement du service pour que les opérations les plus coûteuses en termes de performances soient limitées en nombre et en fréquence d'exécution.

Plus généralement, il faut une prise en compte de la sécurité lors des développements non seulement sur les aspects classiques (overflows, injections, ...) mais aussi sur les aspects plus fonctionnels, qui sont certes plus difficiles à appréhender et identifier. ■

REMERCIEMENTS

Nous tenons à remercier Gabriel qui a autorisé la publication d'un « inhabituel » DoS dans l'*Exploit Corner* !

LIENS

[KILLER] http://seclists.org/fulldisclosure/2011/Aug/att-175/killapache_pl.bin

[NETCRAFT] http://news.netcraft.com/archives/category/web-server-survey/

[VARIANTES] https://www.youtube.com/watch?v=fkCQZaVjBhA

[VARIANTES] http://www.zataz.com/news/21531/Deni-de-service-sur-Apache.html

[NESSUS] http://www.nessus.org/plugins/index.php?view=single&id=55976

[METASPLOIT] http://www.metasploit.com/modules/auxiliary/dos/http/apache_range_dos

[RFC2616] http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html#sec10.2.7

[BUGTRAQ] http://seclists.org/bugtraq/2007/Jan/83

[WINDOW] http://www.cs.umd.edu/~capveg/optack/optack-ccs05.pdf

[BRIGADES] http://www.apachetutor.org/dev/brigades

[NGINX] http://nginx.org/en/CHANGES

[IIS] http://blogs.iis.net/nazim/archive/2011/08/25/is-iis-susceptible-to-the-apache-range-header-dos-attack.aspx

[CVE-2011-3192] http://httpd.apache.org/security/CVE-2011-3192.txt

[BLOG] http://blog.spiderlabs.com/2011/08/mitigation-of-apache-range-header-dos-attack.html

[F5] http://devcentral.f5.com/weblogs/macvittie/archive/2011/08/26/f5-friday-zero-day-apache-exploit-zero-problem.aspx

[RFC2616-FIX] http://trac.tools.ietf.org/wg/httpbis/trac/ticket/311

[REGRESSION] https://issues.apache.org/bugzilla/show_bug.cgi?id=51748

Abonnez-vous !

Profitez de nos offres d'abonnement spéciales disponibles au verso !

Téléphonez au 03 67 10 00 20 ou commandez par le Web

Économisez plus de 20%*

* Sur le prix de vente unitaire France Métropolitaine

6 Numéros de MISC

Les 3 bonnes raisons de vous abonner :

- Ne manquez plus aucun numéro.
- Recevez MISC dès sa parution chez vous ou dans votre entreprise.
- Économisez 10,00 €/an !

4 façons de commander facilement :

- par courrier postal en nous renvoyant le bon ci-dessous
- par le Web, sur www.ed-diamond.com
- par téléphone, entre 9h-12h et 14h-18h au 03 67 10 00 20
- par fax au 03 67 10 00 21

par ABONNEMENT : 38€*

au lieu de 48,00 €* en kiosque

Économie : 10,00 €*

*OFFRE VALABLE UNIQUEMENT EN FRANCE MÉTROPOLITAINE
Pour les tarifs hors France Métropolitaine, consultez notre site : www.ed-diamond.com

Bon d'abonnement à découper et à renvoyer à l'adresse ci-dessous

Tournez SVP pour découvrir toutes les offres d'abonnement >>

MISC
Multi-System & Internet Security Cookbook

Édité par Les Éditions Diamond
Service des Abonnements
B.P. 20142 - 67603 Sélestat Cedex
Tél. : + 33 (0) 3 67 10 00 20
Fax : + 33 (0) 3 67 10 00 21

Vos remarques :

Voici mes coordonnées postales :	
Société :	
Nom :	
Prénom :	
Adresse :	
Code Postal :	
Ville :	
Pays :	
Téléphone :	
e-mail :	

En envoyant ce bon de commande, je reconnais avoir pris connaissance des conditions générales de vente des Éditions Diamond à l'adresse internet suivante : **www.ed-diamond.com/cgv** et reconnais que ces conditions de vente me sont opposables.

Tournez SVP pour découvrir toutes les offres d'abonnement

PROFITEZ DE NOS OFFRES D'ABONNEMENT SPÉCIALES POUR LIRE PLUS ET FAIRE DES ÉCONOMIES !

➡ Voici une sélection des offres de couplage avec MISC

offre 1 — Misc (6 nos)
par ABO : **38€***
au lieu de 48,00€** en kiosque
Economie : 10,00 €

offre 10 — MISC (6 nos) + MISC Hors-Série (2 nos)
par ABO : **44€***
au lieu de 64,00€** en kiosque
Economie : 20,00 €

offre 5 — + GNU/Linux Magazine (11 nos) + Misc (6 nos)
par ABO : **84€***
au lieu de 119,50€** en kiosque
Economie : 35,50 €

offre 7 — + GNU/Linux Magazine (11 nos) + GNU/Linux Magazine HS (6 nos) + Misc (6 nos)
par ABO : **116€***
au lieu de 158,50€** en kiosque
Economie : 42,50 €

offre 17 — Open Silicium + GNU/Linux Magazine (11 nos) + GNU/Linux Magazine HS (6 nos) + Misc (6 nos)
par ABO : **141€***
au lieu de 194,50€** en kiosque
Economie : 53,50 €

offre 8 — + GNU/Linux Magazine (11 nos) + GNU/Linux Magazine HS (6 nos) + Linux Pratique (6 nos) + Misc (6 nos)
par ABO : **143€***
au lieu de 194,20€** en kiosque
Economie : 51,20 €

offre 12 — Linux Pratique Essentiel (6 nos) + GNU/Linux Magazine (11 nos) + GNU/Linux Magazine HS (6 nos) + Linux Pratique (6 nos) + Linux Pratique HS (3 nos) + Misc (6 nos) + MISC Hors-Série (2 nos)
par ABO : **199€***
au lieu de 268,70€** en kiosque
Economie : 69,70 €

offre 14 — Linux Pratique Essentiel (6 nos) + GNU/Linux Magazine (11 nos) + GNU/Linux Magazine HS (6 nos) + Linux Pratique (6 nos) + Linux Pratique HS (3 nos) + Misc (6 nos) + MISC Hors-Série (2 nos) + Open Silicium (4 nos)
par ABO : **224€***
au lieu de 304,70€** en kiosque
Economie : 80,70 €

Vous pouvez également vous abonner sur : www.ed-diamond.com ou par Tél. : 03 67 10 00 20 / Fax : 03 67 10 00 21

➡ Voici une sélection de nos autres offres de couplage (Toutes les offres sur : www.ed-diamond.com)

offre 13 — Open Silicium Magazine (4 nos)
par ABO : **27€***
au lieu de 36,00€** en kiosque
Economie : 9,00 €

offre 15 — Linux Pratique Essentiel (6 nos) + Linux Pratique (6 nos) + Linux Pratique HS (3 nos)
par ABO : **72**
au lieu de 94,20€** en kiosque
Economie : 22,20 €

offre 4 — GNU/Linux Magazine (11 nos) + GNU/Linux Magazine HS (6 nos)
par ABO : **83€***
au lieu de 110,50€** en kiosque
Economie : 27,50 €

offre 16 — Open Silicium + GNU/Linux Magazine (11 nos) + GNU/Linux Magazine HS (6 nos)
par ABO : **108€***
au lieu de 146,50€** en kiosque
Economie : 38,50 €

offre 6 — + GNU/Linux Magazine (11 nos) + GNU/Linux Magazine HS (6 nos) + Linux Pratique (6 nos)
par ABO : **110€***
au lieu de 146,20€** en kiosque
Economie : 36,20 €

➡ Nos Tarifs s'entendent TTC et en euros

		F France Métro	D DOM	T TOM	E1 Europe 1	E2 Europe 2	EUC Etats-Unis Canada	A Afrique	RM Reste du Monde
1	Abonnement MISC	38 €	40 €	44 €	45 €	44 €	46 €	45 €	49 €
4	GLMF + GLMF HS	83 €	89 €	101 €	104 €	100 €	105 €	103 €	116 €
5	GLMF + MISC	84 €	90 €	102 €	105 €	101 €	107 €	104 €	117 €
6	GLMF + GLMF HS + Linux Pratique	110 €	119 €	134 €	138€	133 €	140 €	137 €	154 €
7	GLMF + GLMF HS + MISC	116 €	124 €	140 €	144 €	139 €	146 €	143 €	160 €
8	GLMF + GLMF HS + MISC + LP	143 €	154 €	173 €	178 €	172 €	181 €	177 €	198 €
10	MISC + MISC HS	44 €	47 €	53 €	55 €	52 €	56 €	54 €	60 €
12	GLMF + GLMF HS + MISC + MISC HS + LP + LP HS + LPE	199 €	214 €	243 €	250 €	239 €	254 €	247 €	279 €
13	Open Silicium Magazine	27 €	29 €	31 €	32 €	31 €	33 €	32 €	36 €
14	GLMF + GLMF HS + MISC + MISC HS + LP + LP HS + LPE + Open Silicium	224 €	241 €	272 €	280 €	268 €	285 €	277 €	313 €
15	LPE + LP + LP HS	72 €	78 €	88 €	91 €	87 €	93 €	90 €	101 €
16	Open Silicium + LM + LMHS	108 €	116 €	130 €	134 €	129 €	136 €	133 €	150 €
17	Open Silicium + LM + LMHS + MISC	141 €	151 €	169 €	174 €	168 €	177 €	173 €	194 €

- Europe 1 : Allemagne, Belgique, Danemark, Italie, Luxembourg, Norvège, Pays-Bas, Portugal, Suède
- Europe 2 : Autriche, Espagne, Finlande, Grande Bretagne, Grèce, Islande, Suisse, Irlande
- Zone Reste du Monde : Autre Amérique, Asie, Océanie
- Zone Afrique : Europe de l'Est, Proche et Moyen-Orient

* Toutes les offres d'abonnement : en exemple, les tarifs ci-dessus correspondant à la zone France Métro (F) ** Base tarifs kiosque zone France Métro (F)

Mes choix :

Mon 1er choix	Je sélectionne le N° (1 à 17) de l'offre choisie :	
Mon 2ème choix	Je sélectionne le N° (1 à 17) de l'offre choisie :	
Mon 3ème choix	Je sélectionne le N° (1 à 17) de l'offre choisie :	
	Je sélectionne ma zone géographique (F à RM) :	
	J'indique la somme due : (Total)	€

Exemple : je souhaite m'abonner à l'offre GNU/Linux Magazine + GNU/Linux Magazine Hors-série + MISC (offre 7) et je vis en Belgique (E1), ma référence est donc 7E1 et le montant de l'abonnement est de 144 euros.

Je choisis de régler par :

- ❑ Chèque bancaire ou postal à l'ordre des Éditions Diamond
- ❑ Carte bancaire n° ⌊_⌊_⌊_⌊_ ⌊_⌊_⌊_⌊_ ⌊_⌊_⌊_⌊_ ⌊_⌊_⌊_⌊_

Expire le : ⌊_⌊_⌊_⌊_

Cryptogramme visuel : ⌊_⌊_⌊_

Date et signature obligatoire

MISC Multi-System & Internet Security CookBook

EXTRACTION DES EMPREINTES DE MOTS DE PASSE EN ENVIRONNEMENT WINDOWS

Thibaut Leveslin – Hervé Schauer Consultants (HSC)

Thibaut.Leveslin@hsc.fr

mots-clés : ACTIVE DIRECTORY / NTDS.DIT / EXTENSIBLE STORAGE ENGINE / VOLUME SHADOW COPY SERVICE / DBCSPWD / UNICODEPWD / PEKLIST

Les empreintes des mots de passe des comptes utilisateurs sous Windows sont stockées à deux endroits, dans la base de données SAM (Security Accounts Manager), locale pour un système Windows ou dans les structures Active Directory sur un contrôleur de domaine.

Cet article propose de fournir les clés afin de pouvoir extraire de manière fiable (la stabilité du système cible ne devant pas être affectée) et sur un maximum de systèmes Windows, aussi bien en 32 bits qu'en 64 bits, les empreintes des comptes locaux d'une part et les empreintes des comptes de domaine d'autre part.

1 Introduction

Dans le cadre d'un test d'intrusion, il est toujours intéressant de pouvoir récupérer les empreintes des mots de passe des différents utilisateurs du système local ou d'un domaine. En effet, en environnement Windows, il n'est pas nécessaire de disposer du mot de passe en clair d'un utilisateur pour pouvoir accéder à ses ressources (qu'il s'agisse de répertoires réseau ou de l'accès distant à sa machine) avec son identité.

Les mécanismes d'authentification Windows utilisent effectivement directement le condensat du mot de passe pour obtenir un accès sur un système distant (par exemple via le protocole NTLM). L'attaque en résultant est couramment appelée « Pass-the-Hash ».

Les outils habituellement utilisés pour extraire les empreintes des mots de passe sur les systèmes (**fgdump**, **gsecdump** et consorts) se retrouvent bien souvent bloqués sur les systèmes récents ou disposant d'un antivirus. Dans certains cas, ils peuvent provoquer un dysfonctionnement de la machine ciblée, du fait des techniques intrusives mises en œuvre (injection de code dans le processus LSASS notamment).

2 Stockage des empreintes des comptes locaux

L'injection d'une DLL dans le processus LSASS (*Local Security Authority Subsystem*), processus en charge de l'authentification sous Windows, peut provoquer des problèmes de stabilité, surtout lorsqu'un antivirus est présent sur la machine. La méthode retenue repose donc sur une lecture directe du registre[1]. Nous n'étudierons pas la récupération hors-ligne des empreintes, directement à partir des fichiers des ruches, déjà couverte par l'outil **samdump2**.

Le registre Windows est l'emplacement dans lequel sont stockées les empreintes LM et NT des comptes locaux. Les empreintes sont stockées dans la valeur **V** de la clé **HKLM\SAM\SAM\Domains\Account\Users\[RID]** où [RID] est le Relative Identifier des différents utilisateurs. Ce RID est le dernier élément composant le SID (*Security Identifier*). Le SID est utilisé pour identifier de manière unique une entité réalisant une action sur un système. À titre indicatif, les RID pour les comptes utilisateurs et les groupes commencent à 1000 et sont incrémentés de 1 à chaque nouvel utilisateur ou groupe.

Afin de pouvoir accéder à la clé de registre **HKLM\SAM\SAM**, nécessaire pour récupérer les empreintes des comptes locaux, il est nécessaire de disposer des droits du compte **LocalSystem**, seul autorisé à consulter cette arborescence. À noter que le fait de posséder le privilège **SeBackupPrivilege** est également suffisant pour sauvegarder cette clé et ses sous-clés (via la fonction **RegSaveKey()**), ce privilège permettant à un compte de passer outre les contrôles pour lire un objet.

Pour faire en sorte de pouvoir accéder à la ruche SAM, plusieurs moyens s'offrent à nous, notamment :

1. Modifier les autorisations (ACL) sur la clé, et ce, de manière récursive.
2. Installer un service, dont la seule fonction sera de réaliser le traitement sous l'identité du compte **LocalSystem**.

La réalisation de l'une de ces deux actions nécessite d'être membre du groupe local « Administrateurs ».

Depuis le Service Pack 3 de Windows NT 4.0, un mécanisme de sécurité a été introduit pour notamment obscurcir les empreintes stockées dans le registre. Ce mécanisme prend la forme d'une clé de chiffrement de 128 bits nommée **Syskey**.

Cette clé de chiffrement peut provenir de trois sources différentes :

1. stockage local, dans le registre ;
2. un mot de passe (entré au démarrage du système) ;
3. une disquette fournie au démarrage.

Afin de déterminer l'emplacement de la Syskey, il faut regarder la valeur **SecureBoot** de **HKLM\SYSTEM\CurrentControlSet\Control\Lsa**. Si cette valeur est positionnée à 1, alors la Syskey est stockée localement (option par défaut).

Quatre étapes successives permettent d'accéder à la version en clair des empreintes.

2.1 Récupération de la Syskey

La clé **Syskey** peut être récupérée de deux manières, soit par lecture dans le registre, soit par lecture directe en mémoire (indispensable dans le cas où le stockage local n'aurait pas été sélectionné).

Dans le cas de la lecture dans le registre, la clé Syskey est accessible à partir de quatre sous-clés de **HKLM\SYSTEM\CurrentControlSet\Control\Lsa**, qui sont **JD**, **Skew1**, **GBG** et **Data**. Chaque partie de la **Syskey** est stockée dans l'attribut caché « Class » de la sous-clé et est stockée comme chaîne Unicode.

Une étape de permutation des éléments de la chaîne obtenue après concaténation de ces différentes valeurs permet d'obtenir alors la **Syskey**.

2.2 Calcul de la version hashée de la Syskey

Une empreinte MD5 (*Message Digest 5*) de la **Syskey** est alors générée, à partir de valeurs constantes et d'une partie de la valeur **F** de la clé **HKLM\SAM\SAM\Domains\Account**. Ce condensat MD5 servira de clé **RC4** pour déchiffrer une autre partie de la valeur **F** précédente.

Cette clé RC4 est générée de la façon suivante :

```
rc4_key = MD5(F[0x70:0x80] + aqwerty + Syskey + anum)
  avec
aqwerty = "!@#\$%^&*()qwertyUIOPAzxcvbnmQQQQQQQQQQQQ)(*@&%\0"
anum = "0123456789012345678901234567890123456789\0"
```

Le résultat obtenu après déchiffrement de la valeur **F** sera nommé **hbootkey**, valeur utilisée lors de la génération de la clé de déchiffrement des empreintes.

2.3 Extraction et déchiffrement des empreintes de chaque utilisateur

Les sous-clés de **HKLM\SAM\SAM\Domains\Account\Users\Names** permettent d'associer le RID à un nom d'utilisateur.

La valeur **V** contient, d'une manière générale, les informations concernant le compte utilisateur (nom, commentaires, emplacement des répertoires, heures autorisées de connexion, empreintes chiffrées, etc.).

L'emplacement effectif des empreintes LM et NT chiffrées est déterminé à partir des deux octets à l'offset *0x9C* de cette valeur **V** : voir figure 1.

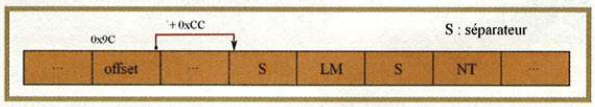


Fig. 1 : Offset des empreintes dans la valeur « V »

Les empreintes utilisateurs sont chiffrées à partir de l'algorithme de chiffrement **RC4**. La clé de chiffrement associée est calculée de la manière suivante, à partir du RID[2] d'un utilisateur et de la valeur de **hbootkey** :

```
rc4_key_lm = MD5(hbootkey + RID + almpassword)
rc4_key_nt = MD5(hbootkey + RID + antpassword)
  avec
almpassword = "LMPASSWORD\0"
antpassword = "NTPASSWORD\0"
```

2.4 Désobfuscation des empreintes

Les empreintes que nous obtenons après ce déchiffrement RC4 correspondent alors à la forme de stockage qui était utilisée avant que la fonctionnalité de Syskey ne soit ajoutée dans Windows NT.

À l'origine, les empreintes étaient seulement obscurcies, ou plutôt chiffrées, mais avec des clés « constantes ». L'algorithme utilisé ici est le **DES** (*Data Encryption Standard*), la clé utilisée étant propre à un utilisateur (basée sur son RID).

Pour pouvoir récupérer la valeur originelle des empreintes LM et NT, il est tout d'abord nécessaire de diviser nos empreintes chiffrées en deux parties, chacune l'étant par une clé différente, générée à partir d'une variation sur le RID d'un utilisateur (clés notées ici **key1** et **key2**).

L'algorithme suivant est alors utilisé pour obtenir la valeur finale de nos empreintes :

```
hashLM = DES(key1, hashLMCrypted1) + DES(key2, hashLMCrypted2)
hashNT = DES(key1, hashNTCrypted1) + DES(key2, hashNTCrypted2)
  avec
hash{LM|NT}Crypted1 = 8 premiers octets de l'empreinte chiffrée
hash{LM|NT}Crypted2 = 8 derniers octets de l'empreinte chiffrée
```

Les étapes lors du déchiffrement des empreintes des comptes locaux sont nombreuses. Pour récapituler, voici les éléments qui sont impliqués :

- les empreintes à déchiffrer ;
- la valeur de la **Syskey** ;
- le RID d'un utilisateur ;
- des constantes.

3 Stockage des empreintes des comptes de domaine

La récupération des empreintes est réalisée en deux étapes :

1. rapatriement du fichier de l'annuaire (partie en ligne) ;
2. parcours du fichier à la recherche des empreintes (partie hors-ligne pouvant être effectuée sur un autre système, sous réserve de disposer de la **Syskey** du contrôleur de domaine...).

3.1 Copie du fichier de l'annuaire

Sur un contrôleur de domaine, toutes les informations sur les utilisateurs du domaine, notamment leurs empreintes de mots de passe, sont gérées dans un annuaire d'entreprise, Active Directory, et sont stockées dans une base de données propriétaire Microsoft, accessible via LDAP ou par les *Remote Procedure Call* adéquats. Le fichier stockant les données AD est donc très sensible (il peut également contenir des certificats, les clés de recouvrement de postes intégrés au domaine et chiffrés par BitLocker **[1]**, etc.).

Ce fichier est nommé **ntds.dit** et son emplacement peut être déterminé avec la valeur **DSA Database file** de la clé **HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters** (par défaut, le chemin du fichier DIT est « %SystemRoot%\NTDS\ntds.dit »).

Note : Le cas BitLocker

Dans le cas où la stratégie locale est configurée de telle manière à « Activer la sauvegarde BitLocker dans les services de domaine Active Directory (AD DS) » (Configuration de l'ordinateur/Modèles d'administration/Composants Windows/Chiffrement de lecteur BitLocker), ce qui n'est pas le cas par défaut, les informations de récupération de BitLocker seront sauvegardées dans l'annuaire Active Directory dès lors que la procédure de chiffrement sera démarrée (c'est-à-dire juste avant le chiffrement effectif d'un volume). Les attributs liés à BitLocker sont msFVE-RecoveryPassword (ATTm591788), msFVE-VolumeGuid (ATTk591822), msFVE-KeyPackage (ATTk591823) et msFVE-RecoveryGuid (ATTk591789). Ils peuvent être visionnés localement ou à distance avec l'outil *Active Directory Explorer* de la suite Sysinternals.

On trouve dans ce même répertoire plusieurs autres fichiers, utilisés par le système à des fins de gestion des transactions.

La première étape à réaliser afin d'extraire les empreintes des comptes du domaine consiste à effectuer une copie du fichier **ntds.dit**. En effet, certains attributs ne peuvent pas être récupérés par les méthodes standards, notamment ceux qui nous intéressent. Le fichier étant verrouillé par le système (accès exclusif), il nous est également impossible de le parcourir librement.

Deux techniques permettent de récupérer ce fichier : la première utilise le mécanisme de *Volume Shadow Copy Service* et la seconde repose sur la réplication de l'annuaire Active Directory[3], opérée typiquement lorsqu'un nouveau contrôleur de domaine est promu.

Le Volume Shadow Copy Service (VSS) est un mécanisme interne à Windows permettant de faciliter la sauvegarde de fichiers à un instant donné **[2]**. Il a été ajouté à Windows depuis Windows XP (et Windows Server 2003). Son intérêt réside dans la possibilité de sauvegarder sans risque de corruption des fichiers qui, normalement, ne sont pas accessibles (car verrouillés par d'autres programmes, par exemple). C'est le mécanisme sous-jacent à la restauration système, au centre de sauvegarde et de restauration, ainsi qu'à la fonctionnalité de versions précédentes[4]. Les fichiers créés sont nommés clichés instantanés (*shadow copy*).

Plusieurs outils intégrés à Windows se basent sur le VSS pour réaliser une sauvegarde du fichier **ntds.dit**, notamment *NTBackup* (sous 2003) puis *NtdsUtil* (depuis Windows Server 2008).

Le VSS est architecturé autour de trois composants :

- *Requester* : application demandant la réalisation d'un cliché instantané.
- *Writer* : composant logiciel permettant de rendre une application compatible avec la sauvegarde via le VSS et chargé d'éviter une corruption de la

sauvegarde. Il sait quels sont les fichiers qui doivent être sauvegardés, ainsi que leurs emplacements respectifs.

- *Provider* : entité gérant les volumes et créant les clichés instantanés pour les requesters.

Le service du VSS (**vssvc.exe**) est au cœur du processus et est chargé de la coordination entre ces trois éléments.

Windows fournit une API pour le VSS, utilisable par des applications de sauvegarde. Dans notre cas, pour réaliser un cliché instantané, il faut être membre du groupe local des « Administrateurs » ou des « Opérateurs de sauvegarde » sur le contrôleur de domaine.

Une application désirant tirer parti du VSS pour la sauvegarde et la restauration de ses fichiers doit intégrer son propre writer, donc avoir été pensée pour utiliser le VSS. En effet, seule l'application est à même de savoir quels sont les fichiers qui doivent être sauvegardés et comment les mettre dans un état stable, c'est-à-dire terminer les éventuelles transactions en cours (si plusieurs éléments sont impliqués dans une transaction, l'application fera en sorte d'attendre leur enregistrement effectif avant de passer à la suite), vider les tampons, si un système de cache est présent, etc.

Une application de sauvegarde n'aura alors pas besoin de connaître les détails d'implémentation de l'application pour réaliser une copie des données, elle n'aura qu'à communiquer au service du VSS sa demande, qui sera retransmise au writer de l'application.

Dans notre cas, nous allons réaliser notre propre requester pour récupérer le fichier **ntds.dit**, dont la sauvegarde est réalisée par le writer NTDS et gérée par le provider *Microsoft Software Shadow Copy provider* 1.0 (via le driver **Volsnap.sys**), tous deux intégrés au système.

Les étapes propres à la réalisation d'une sauvegarde sont détaillées sur le site de la MSDN, le lecteur intéressé pourra s'y reporter **[3]**.

Depuis Windows Server 2008, le fichier **ntds.dit** peut être récupéré très simplement en utilisant le programme **ntdsutil.exe** (présent d'office sur les versions serveur), supportant depuis cette version de Windows la sauvegarde via le VSS :

```
C:\>ntdsutil
ntdsutil: snapshot
snapshot: activate instance ntds
Active instance set to "ntds".
snapshot: create
Creating snapshot...
Snapshot set {239bf2ae-d908-4f7d-94d3-f58fa5bf7217} generated
successfully.
snapshot: mount {239bf2ae-d908-4f7d-94d3-f58fa5bf7217}
Snapshot {7cec40ce-c7ce-4627-8ee2-7c978d273733} mounted as
C:\$SNAP_201110281008_VOLUMEC$\
snapshot: list mounted
 1: 2011/10/28:10:08 {239bf2ae-d908-4f7d-94d3-f58fa5bf7217}
 2:   C: {7cec40ce-c7ce-4627-8ee2-7c978d273733}
C:\$SNAP_201110281008_VOLUMEC$\
// ** Copier le fichier ntds.dit à partir du volume
(C:\$SNAP_201110281008_VOLUMEC$\) ** //
snapshot: unmount {239bf2ae-d908-4f7d-94d3-f58fa5bf7217}
Snapshot {7cec40ce-c7ce-4627-8ee2-7c978d273733} unmounted.
snapshot: delete {239bf2ae-d908-4f7d-94d3-f58fa5bf7217}
Snapshot {7cec40ce-c7ce-4627-8ee2-7c978d273733} deleted.
snapshot: quit
ntdsutil: quit
```

3.2 Récupération des attributs de l'annuaire

Active Directory est basé sur le moteur de base de données *Extensible Storage Engine* (ESE) **[4]**, aussi appelé *JET Blue*[5]. Ce moteur est largement utilisé par les produits Microsoft, allant de Exchange (via le fichier **priv1.edb**, contenant les boîtes aux lettres) à Windows Live Messenger, en passant par Windows Search[6].

La lecture des attributs qui nous intéressent (les empreintes LM et NT) peut donc être réalisée à partir de l'API ESE fournie par Microsoft, intégrée au SDK Windows.

Active Directory stocke les objets du domaine dans des attributs, organisés dans plusieurs tables. Les deux tables les plus intéressantes sont le schéma (**MSysObjects**) et la table des objets (**datatable**).

Le schéma contient les définitions de tous les objets pouvant être créés. La table des objets est constituée de lignes représentant les instances des objets et de colonnes représentant des attributs (contenant les données). C'est de cette table des objets que nous allons extraire les attributs.

Pour réaliser la lecture après identification des attributs, l'API ESE s'utilise de la manière suivante (fonctionnement simplifié) :

```
// ** Utilisation des fonctions nécessaires à l'ouverture d'une table ** //
JetCreateInstance
JetInit
JetBeginSession
JetAttachDatabase("ntds.dit")
JetOpenDatabase("ntds.dit")
JetOpenTable("datatable")

// ** Récupération des attributs ** //
// Récupération des identifiants des attributs
JetGetTableColumnInfo
// Positionnement au début de la table
JetMove(JET_MoveFirst)
Faire
  // Récupération de la valeur de l'attribut, à partir de son identifiant
  JetRetrieveColumn
  // [...]
  // Passage à l'élément suivant
  JetMove(JET_MoveNext)
Tant que la fonction JetMove ne renvoie pas une erreur
```

```
// ** Appel des fonctions de terminaison ** //
JetCloseTable
JetCloseDatabase
JetDetachDatabase
JetEndSession
JetTerm
```

Une manière simple pour récupérer toutes les valeurs d'un attribut donné est d'utiliser les outils **esedbexport** et **esedbinfo** du projet *libesedb* **[5]** :

```
// ** Export de la table des objets ** //
$ ./esedbexport -T datatable ntds.dit
esedbexport 20111008
Opening file.
Exporting table 4 (datatable).
Export completed.
// ** Récupération du numéro de colonne lié à l'empreinte NT ** //
$ ./esedbinfo ntds.dit | grep ATTk589914
  780 1026  ATTk589914  Large binary data
// ** Affichage de toutes les valeurs de l'attribut ** //
$ cat ntds.dit.export/datatable | cut -f 780 | grep -v "^$"
ATTk589914
1100000000000000031c675305d381a2ec895fa7dce8393c71940f049efee2db3f1ac5e005e286577
1100000000000000c68e5b598be568627d2151fcc6c4e4a7ca031013df999489f1775e2200de1549
[...]
```

En sachant que l'attribut **ATTc131102** stocke des valeurs correspondant à un identifiant d'attribut (les 6 chiffres composant son nom), il est possible d'identifier un attribut directement à partir de son nom LDAP (par exemple) :

```
// ** Récupération du numéro de colonne de l'attribut ATTc131102 ** //
$ ./esedbinfo ntds.dit | grep ATTc131102 | cut -f 2
80
// ** Identification des 6 chiffres composant l'attribut recherché ** //
$ cat ntds.dit.export/datatable | grep userParameters | cut -f 80
589962
// ** Recherche du nom d'attribut dans la première ligne du fichier
(contenant le nom des colonnes) ** //
$ head -n 1 ntds.dit.export/datatable | grep -o "....589962"
ATTm589962
```

Une table assez exhaustive des correspondances pourrait être dressée en travaillant dans le sens inverse et en recherchant les noms LDAP (attribut **ATTm131532**) de tous les identifiants d'attributs présents dans la première ligne du fichier **datatable**.

3.3 Extraction des empreintes

Maintenant que nous savons comment récupérer et lire le fichier **ntds.dit**, nous pouvons nous attarder sur la récupération et l'interprétation des attributs.

Afin de communiquer avec la base de données de l'Active Directory, Windows utilise les services du *Directory System Agent* (DSA), faisant partie du processus LSASS, et plus précisément par l'intermédiaire des fonctions de la bibliothèque « ntdsa.dll » (« ntdsai.dll » depuis Windows Server 2008).

Le DSA accède aux informations de l'annuaire Active Directory par l'intermédiaire d'ESE, via la bibliothèque « esent.dll », chargée de transférer les informations depuis et vers la base de données.

Le tableau suivant recense les attributs impliqués dans la récupération des empreintes :

Attribut	Signification (Ldap Display Name)
ATTm590045	Nom d'utilisateur (**sAMAccountName**)
ATTr589970	SID (**objectSid**)
ATTk589879	Empreinte LM (**dBCSPwd**)
ATTk589914	Empreinte NT (**unicodePwd**)
ATTk590689	Clé de chiffrement (**pekList**)

Comme pour le cas des comptes locaux, les empreintes sont également stockées chiffrées. La clé utilisée lors du chiffrement (**pekList** – *Password Encryption Key*) est également présente dans l'annuaire, chiffrée en RC4. Par lecture dans la mémoire du processus LSASS (variable globale **_g_PekList** dans **ntdsa.dll**), il est possible d'obtenir la valeur non chiffrée de cet attribut.

À noter que pour un contrôleur de domaine en lecture seule (*Read-Only Domain Controller*– RODC, rôle apparu avec Windows Server 2008, permettant notamment d'opérer un filtrage sur certains attributs lors de la réplication) et pour une configuration par défaut, les attributs contenant les empreintes ne seront répliqués que pour les utilisateurs membres du groupe local « Groupe de réplication dont le mot de passe RODC est autorisé » sur le contrôleur de domaine. En outre, pour que ces empreintes soient effectivement présentes dans le fichier **ntds.dit** du RODC, il est nécessaire qu'au préalable l'utilisateur se soit authentifié auprès de ce dernier **[6]**.

Initialement, les empreintes de deux comptes sont stockées dans l'annuaire d'un RODC :

- le compte de la machine ;
- le compte de domaine Kerberos lié au centre de distribution de clés (**krbtgt_***), spécifique au RODC.

3.3.1 Déchiffrement de la clé

pekList (attribut **ATTk590689**) n'est pas à proprement parler une clé, mais plutôt une structure contenant la clé qui nous intéresse : voir figure 2.

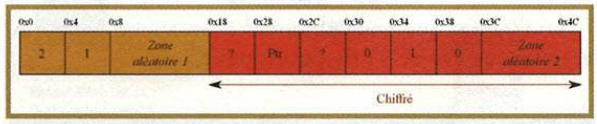


Fig. 2 : Structure de pekList

Cette structure est fournie chiffrée de l'offset *0x18* à *0x4C*.

Afin d'obtenir une version en clair de la partie chiffrée de cette structure, la fonction interne **PEKInPlaceEncryptDecryptDataWithKey()** de **ntdsa.dll** est utilisée.

Cette fonction permet à partir de deux « clés » de déchiffrement de 128 bits, d'un nombre de concaténations (noté « n ») et d'un buffer d'entrée/sortie, de déchiffrer notre partie chiffrée.

Le traitement réalisé par cette fonction est le suivant :

1. calcul d'un condensat MD5 à partir des clés : `MD5(Key1 + n * Key2)` ;
2. utilisation de ce condensat comme clé **RC4** pour déchiffrer notre buffer.

À nouveau, comme pour les comptes locaux, nous retrouvons ce principe de chiffrement RC4, dont la clé est obtenue par calcul d'un condensat MD5.

Pour le déchiffrement des 52 octets chiffrés de **pekList**, la clé **Syskey** (et non la clé **hbootkey** introduite précédemment) est utilisée comme première clé lors de l'appel à la fonction **PEKInPlaceEncryptDecryptDataWithKey()** et la « zone aléatoire » présente à l'offset 8 comme seconde clé.

3.3.2 Déchiffrement des empreintes

De la même façon que l'attribut **pekList** était une structure, les attributs contenant les empreintes (**ATTk589879** et **ATTk589914**) sont des structures, formées de la manière suivante :

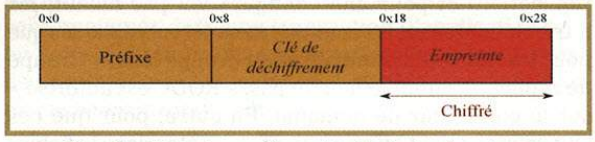


Fig. 3 : Structure d'un attribut stockant une empreinte dans l'annuaire Active Directory

Là aussi, la fonction **PEKInPlaceEncryptDecryptDataWithKey()** nous sert à déchiffrer le champ qui nous intéresse, contenant l'empreinte LM ou NT.

Pour le déchiffrement, nous utilisons comme première clé la 2e « zone aléatoire » de **pekList** (venant tout juste d'être déchiffrée), et comme seconde clé, les 16 octets disponibles à partir de l'offset 8 de la structure contenant l'empreinte.

À nouveau, le résultat que nous obtenons est obscurci (par chiffrement DES). Il nous reste alors à appliquer la méthode précédente, en utilisant l'attribut **ATTr589970**, contenant le SID (donc le RID).

Le résultat que nous obtenons correspond enfin aux empreintes LM et NT de l'utilisateur.

Conclusion

Les méthodes de chiffrement utilisées pour protéger les empreintes des comptes locaux et des comptes de domaine présentent de nombreuses similitudes. Ainsi, dans les deux cas, les empreintes sont chiffrées en RC4 à partir d'une clé dont la valeur est dépendante de la Syskey et qui est générée à partir d'un condensat MD5. Ce processus est également systématiquement suivi d'un obscurcissement des empreintes via l'algorithme **DES**, où le RID de l'utilisateur joue un rôle dans la génération de la clé.

Enfin, il est nécessaire de rappeler qu'aucune de ces méthodes ne peut aboutir sans au préalable disposer des droits administrateurs (ou des privilèges adéquats). Dans un cas, pour lancer un service en tant que **LocalSystem**, condition nécessaire pour accéder à la base SAM. Dans l'autre cas, pour réaliser la sauvegarde du fichier de l'annuaire Active Directory. ■

REMERCIEMENTS

Je tiens à remercier tous mes collègues de HSC pour leurs conseils et relectures, ainsi que Nicolas Ruff et Jean-Baptiste Bédrune.

RÉFÉRENCES

[1] Active Directory et BitLocker - http://technet.microsoft.com/fr-fr/library/cc766015

[2] Présentation du VSS - http://technet.microsoft.com/en-us/library/ee923636

[3] Réalisation d'une sauvegarde à partir du VSS - http://msdn.microsoft.com/en-us/library/windows/desktop/aa384589

[4] Architecture ESE - http://technet.microsoft.com/en-us/library/aa998171

[5] Projet libesedb (bibliothèque, outils et documentation sur ESE) - http://sourceforge.net/projects/libesedb

[6] Password Replication Policy et RODC - http://technet.microsoft.com/en-us/library/cc730883

[7] Étude originelle sur Active Directory - http://web.archive.org/web/20051031110814/www.void.ru/content/1081 et http://web.archive.org/web/20051031110929/http://www.void.ru/content/1090

NOTES

[1] Cette méthode est notamment celle qui est employée par le script hashdump du payload Meterpreter dans Metasploit.

[2] Le RID étant spécifique à un utilisateur, pour deux utilisateurs distincts ayant le même mot de passe (donc des empreintes identiques), la représentation de ces empreintes que l'on va retrouver dans le registre va être sous une forme différente.

[3] Cette méthode a été présentée par Aurélien Bordes au SSTIC 2010, lors des Rump Sessions.

[4] Il est possible de récupérer un fichier supprimé totalement (non disponible dans la Corbeille), en connaissant son nom et son emplacement, si un cliché instantané a été pris avant sa suppression.

[5] Le fichier ntds.dit peut être ouvert et exporté sous le format CSV avec un outil du type EseDbViewer, utilisant l'API ESE. L'outil esedbexport du projet libesedb permet également d'exporter les attributs des différentes tables.

[6] Windows Search est intégré au système depuis Windows Vista et est activé par défaut. Son fichier Windows.edb, au format ESE, peut être intéressant lors d'analyses forensiques.

ANALYSE DE MALWARE AVEC CUCKOO SANDBOX

Cédric Pernet – cedric.pernet@gmail.com

mots-clés : ANALYSE / MALWARE / SANDBOX

En entreprise, l'analyse d'un malware lié à un incident de sécurité est une activité pouvant être réalisée à divers niveaux, en fonction de plusieurs paramètres : degré d'urgence, sensibilité de l'incident, but poursuivi, ... Il peut être intéressant dans tous les cas d'obtenir en quelques minutes une première estimation des capacités du malware et de ses communications avec l'extérieur, ou encore de savoir rapidement quels fichiers il crée sur le système. C'est dans ce cadre qu'a été développé Cuckoo Sandbox, un bac à sable automatisé d'analyse de malware en environnement virtuel.

1 Présentation

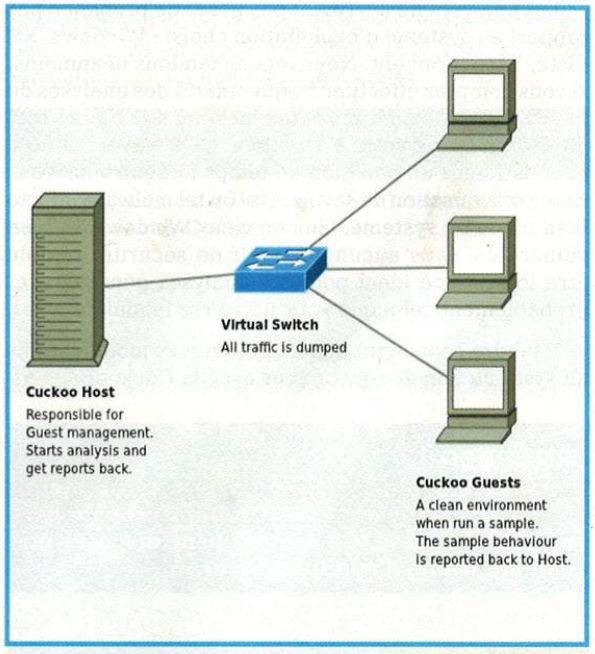
Cuckoo Sandbox **[1]** est un outil développé et maintenu par Claudio Guarnieri. Le projet a été démarré dans le cadre du *Google Summer of Code* 2010 et soutenu par le Projet Honeynet **[2]**. Il en est actuellement à sa version 0.2 beta. L'outil est open source, sous licence GNU, entièrement écrit en Python. Il peut être téléchargé sous forme d'archive ou de dépôt GitHub.

Mais de quoi s'agit-il ? Cuckoo Sandbox (ou CuckooBox) est un bac à sable d'analyse de malware pour Windows basé sur la virtualisation et l'automatisation de tâches.

L'idée est d'installer CuckooBox sur un système hôte sain, Windows ou Linux, et de simplement lui soumettre des binaires Windows, qui seront analysés de façon totalement automatisée dans une machine virtuelle de type virtualBox **[3]**. En plus de lui soumettre des exécutables, il est également possible de lui fournir des fichiers PDF, des documents Office, ou encore des scripts PHP.

L'outil est d'autre part scriptable, il est ainsi possible de développer des analyses sur mesure, adaptées à tout besoin d'analyse automatisée.

L'architecture est la suivante :



Architecture Cuckoo Sandbox : one host to rule them all

Comme indiqué précédemment, le système de virtualisation choisi par CuckooBox est VirtualBox.

2 Installation

Cuckoo Sandbox a été développé sous Linux. Cet environnement semble le plus approprié à configurer pour pouvoir lancer les analyses dans cette sandbox. Néanmoins, l'auteur indique que l'outil fonctionne bien sous Mac OS X, mais ce système d'exploitation n'est pas considéré comme un environnement supporté officiellement. Quant à Windows, il semble nécessaire de procéder à quelques modifications pour y faire fonctionner la sandbox correctement.

Dans le cadre de cet article, nous allons procéder à une installation sous un système Linux.

Tout d'abord, il est nécessaire de disposer de Python 2.6 ou 2.7 (de préférence) et de la dernière version de VirtualBox.

Une fois le package de Cuckoo Sandbox téléchargé et décompressé dans un répertoire (nous utiliserons `/opt/cuckoo`), il convient de configurer la Sandbox et de préparer les machines virtuelles.

2.1 Installation d'au moins une machine virtuelle Windows dans VirtualBox

Les analyses ne devraient pas poser de problème par rapport au système d'exploitation choisi : Windows XP, Vista, 7 fonctionnent. Nous recommandons néanmoins, si vous comptez effectuer fréquemment des analyses de malwares, d'installer plusieurs machines virtuelles très différentes dans votre VirtualBox. Cela s'avérera utile et constituera un bon gain de temps lorsque vous vous poserez la question de savoir si tel ou tel malware infecte bien tel ou tel système. Un bon vieux Windows XP bien vulnérable, sans aucun correctif de sécurité, semble être le système idéal pour les analyses générales, et probablement celui que vous utiliserez le plus souvent.

Il faudra cependant apporter quelques modifications au système afin de fonctionner avec la CuckooBox.

Attention !
Chaque machine virtuelle devra absolument disposer d'un compte d'utilisateur protégé par un mot de passe. Ce compte peut disposer ou non des droits d'administrateur.

2.1.1 Installation de Python 2.7 sur chaque machine virtuelle

Installer Python 2.7 **[4]** est un pré-requis pour que la CuckooBox fonctionne correctement.

Installez également *Python Imaging Library* (PIL) **[5]** si vous souhaitez que votre CuckooBox prenne des captures d'écran lors des analyses automatisées.

2.1.2 Installation de logiciels tiers

Vous pouvez également installer tout logiciel qui vous semblera utile à des analyses : Firefox, Adobe Reader, Flash Player, etc. N'oubliez pas, pour chacun, de désactiver les fonctionnalités de mise à jour.

Cuckoo Sandbox fonctionne actuellement avec les types de fichiers suivants :

- fichiers Executables Windows ;
- fichiers Word (`.doc`) ;
- fichiers PDF ;
- scripts PHP.

Il dispose également d'un module d'analyse spécifique à Internet Explorer, qui consistera en gros à ouvrir IE dans la machine virtuelle afin de lancer Internet Explorer sur une URL prédéfinie. Il est également possible de développer ses propres scripts d'analyse.

Attention !
N'oubliez pas de désactiver le pare-feu des systèmes invités (*guests*), sans quoi vous risquez de passer à côté d'un canal de communication du malware qui serait filtré par le pare-feu.

2.2 Édition de cuckoo.conf

Ce fichier contient quelques sections facilement configurables, plutôt bien renseignées sous forme de commentaires, en plus de la documentation de l'outil. Nous passerons rapidement sur cette partie, qui contient les sections :

- *Logging* : cette section contient le chemin vers le journal d'événements (*log*), le fuseau horaire, ainsi que l'activation du mode debug.
- *Analysis* : cette section décrit le mode de fonctionnement lors des analyses effectuées par la CuckooBox. On y trouve les délais de dépassement de temps (*timeout*), le chemin vers le répertoire qui contiendra les analyses, un pointeur vers le script d'analyse (qui peut être modifié pour s'adapter à vos besoins).
- *Database* : une seule entrée dans cette section : le chemin vers la base de données de Cuckoo Sandbox.
- *Sniffer* : cette section contient le paramétrage des captures réseau. Il est possible de se servir d'un logiciel externe (tcpdump, par exemple), ou des

fonctionnalités de *sniffing* de VirtualBox (NicTrace). Il n'y a plus qu'à pointer vers la bonne interface réseau, et la section est configurée.

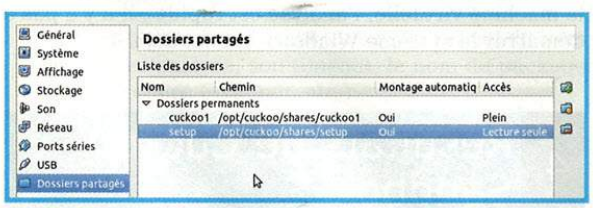
- *Virtual Machines* : cette section fait le lien entre le système hôte (sur lequel se situe la Cuckoo Sandbox) et les systèmes invités. On y trouve la liste des machines virtuelles, un pointeur vers l'exécutable de Python situé dans les machines virtuelles, l'activation ou non de la GUI lors de l'analyse.

Suivent ensuite des sections ayant pour nom celui de chaque machine virtuelle, définissant quelques paramètres : nom d'utilisateur, mot de passe de l'utilisateur, ainsi que le chemin vers le répertoire partagé entre l'hôte et l'invité.

2.3 Création de répertoires partagés entre Cuckoo Sandbox et les machines virtuelles

Cuckoo Sandbox utilise deux répertoires afin d'échanger des données entre les différentes machines, facilement configurables dans l'interface graphique de VirtualBox :

- un répertoire « setup » utilisé pour les scripts. Ce répertoire sera monté automatiquement, en lecture seule.
- un répertoire « nomdelamachinevirtuelle » (ou tout autre nom qui vous plaira, finalement...) monté automatiquement en accès lecture/écriture. Ce dernier sera utilisé pour stocker les résultats de l'analyse.



Configuration des partages de répertoires entre l'hôte et l'invité dans l'interface graphique de VirtualBox

2.4 Configuration réseau

Deux choix possibles, comme évoqué précédemment dans la section « sniffer » de **cuckoo.conf** :

2.4.1 Utilisation de VirtualBox pour les captures réseau

Dans ce cas, le plus simple est de configurer la carte réseau 1 de la machine virtuelle en NAT, puis de modifier VirtualBox pour activer le sniffing.

Pour cela, en ligne de commandes, la machine virtuelle étant éteinte :

```
$ VBoxManage modifyvm " nomdelamachinevirtuelle " --nictrace1 on --
nictracefile1 /opt/cuckoo/shares/cuckoo1/dump.pcap
```

Attention !

Ne soyez pas connecté en root lorsque vous effectuez cette manipulation. VBoxManage ne verrait pas la machine virtuelle et refuserait de procéder à ce paramétrage.

2.4.2 Utilisation d'un logiciel externe pour les captures réseau

Pour cela, il faut configurer la carte réseau de la machine virtuelle en bridge, puis éditer les informations de **cuckoo.conf** pour y modifier la section « sniffer » :

```
[Sniffer]
sniffer = True
interface=eth0
```

2.5 Création de l'instantané

Si vous avez respecté les étapes précédentes et tout configuré, il ne reste plus qu'à prendre un instantané (« snapshot ») de votre/vos machine(s) virtuelle(s). Cela peut se faire en mode graphique avec l'interface de VirtualBox, ou en ligne de commandes :

```
$ VBoxManage snapshot " Nomdelamachinevirtuelle " take
" nomdelinstantané "
```

Il n'y a plus qu'à l'éteindre, et elle sera prête pour être utilisée par Cuckoo Sandbox.

3 Utilisation de Cuckoo Sandbox

Sur l'hôte, il suffit de lancer le script **Cuckoo.py**, sans argument particulier :

```
cpe@IziaRocks:/opt/cuckoo$ python cuckoo.py

  ____ _   _ ____| | _ ___  ___
 / __) | | |/ __) |_/ ) _ \ / _ \
( (__| |_| ( (__|  _ ( |_| | |_| |
 \___)____/ \___)_| \_)__/ \___/ v0.2
www.cuckoobox.org
Copyright (C) 2010-2011
by Claudio "nex" Guarnieri

[2011-11-19 17:13:08] [Virtual Machine] [Check] Your VirtualBox
version is: "4.1.6", good!
```

```
[2011-11-19 17:13:08] [Start Up] Populating virtual machines pool...
[2011-11-19 17:13:08] [Virtual Machine] Acquired virtual machine
with name "vyktym".
[2011-11-19 17:13:08] [Virtual Machine] [Infos] Virtual machine
"vyktym" informations:
[2011-11-19 17:13:08]  \_| Name: vyktym
[2011-11-19 17:13:08]     | ID: 8703621c-b10e-490b-8ba4-3b9bab7631d8
[2011-11-19 17:13:08]     | CPU Count: 1 Core/s
[2011-11-19 17:13:08]     | Memory Size: 256 MB
[2011-11-19 17:13:08]     | VRAM Size: 16 MB
[2011-11-19 17:13:08]     | State: Saved
[2011-11-19 17:13:08]     | Current Snapshot: "good"
[2011-11-19 17:13:08]     | MAC Address: 08:00:27:58:90:5D
[2011-11-19 17:13:08] [Start Up] 1 virtual machine/s added to pool.
```

Au premier démarrage, une mention est ajoutée pour indiquer la création de la base de données de CuckooBox.

Une fois CuckooBox lancé, vous pouvez lui transmettre un fichier pour analyse. Vous pouvez soit soumettre votre fichier avec Cuckoo lancé dans une autre fenêtre, soit soumettre le fichier sans que Cuckoo soit lancé. À son prochain lancement, il procédera à l'analyse. Il est ainsi possible d'ajouter autant de fichiers que vous voulez, pour analyse ultérieure.

```
cpe@IziaRocks:/opt/cuckoo$ python submit.py /home/cpe/Malware/nil.exe
Done: Task added to database!
```

Il est possible de passer quelques paramètres en argument à ce script, notamment une valeur de timeout. À noter que CuckooBox détermine le type de fichier à analyser : il n'y a pas besoin de lui préciser qu'il s'agit d'un binaire, d'un PDF, etc.

Au lancement suivant de **Cuckoo.py** :

```
[2011-11-19 17:27:14] [Core] [Dispatcher] Acquired analysis task for
target "/home/cpe/Malware/nil.exe".
[2011-11-19 17:27:14] [Database] [Lock] Locked task with id 16.
[2011-11-19 17:27:14] (Task #16) [Analysis] [Generate Config] Config
file successfully generated at "shares/vyktym/analysis.conf".
[2011-11-19 17:27:14] [Virtual Machine] Acquired virtual machine
with name "vyktym".
[2011-11-19 17:27:28] [Virtual Machine] [Start] Virtual machine
"vyktym" starting in "gui" mode.
[2011-11-19 17:27:29] [Virtual Machine] [Execute] Cuckoo executing
with PID 112 on virtual machine "vyktym".
[2011-11-19 17:29:55] [Virtual Machine] [Execute] Cuckoo exited with
code 0 on virtual machine "vyktym".
[2011-11-19 17:29:56] [Virtual Machine] [Stop] Virtual machine
"vyktym" powered off successfully.
[2011-11-19 17:30:03] [Virtual Machine] [Restore] Virtual machine
"vyktym" successfully restored to current snapshot.
[2011-11-19 17:30:04] (Task #16) [Analysis] [Save Results] Analysis
results successfully saved to "analysis/16".
[2011-11-19 17:30:04] (Task #16) [Analysis] [Clean Share] Shared
folder "shares/vyktym" cleaned successfully.
[2011-11-19 17:30:04] [Database] [Complete] Task with id 16 updated
in the database with status "1".
[2011-11-19 17:30:04] (Task #16) [Analysis] [Free VM] Virtual
machine "vyktym" released.
[2011-11-19 17:30:04] (Task #16) [Analysis] [Core] Postprocessing
script started with pid "6347".
```

On voit (et on constate visuellement si le mode « GUI » est activé) que notre CuckooBox démarre la machine virtuelle, lance le binaire, puis ferme la machine virtuelle, et restaure le *snapshot*. Le système est ainsi à nouveau sain et prêt à être utilisé pour une nouvelle analyse.

En *background*, vous vous en doutez, bien d'autres opérations ont été effectuées, telles que la capture d'écran, les captures réseau, et toutes les autres analyses que nous allons voir dans la partie 4.

Note : Limitation du mode de fonctionnement multi-machines virtuelles

Lorsque l'on dispose de plusieurs machines virtuelles, prenons par exemple le cas d'un système XP, d'un système Vista, et d'un système 7, il n'est pas possible de sélectionner la machine virtuelle vers laquelle le binaire sera envoyé et analysé. Le mode de fonctionnement de Cuckoo Sandbox lorsque plusieurs machines virtuelles sont déclarées est simple : il les ouvre toutes, pour traiter toute sa liste d'attente de binaires. Ainsi, si on soumet 6 binaires, par exemple, nos 3 VM vont être lancées et analyseront les binaires dans l'ordre de soumission.

Dans la pratique, il est cependant possible de contourner cette limitation en soumettant le même binaire trois fois d'affilée vers CuckooBox pour notre exemple. Il sera alors analysé dans chaque machine virtuelle.

CuckooBox démarrant directement un instantané de la machine virtuelle, l'analyse est rapide : il n'y a pas à démarrer le système Windows, il l'est déjà.

4 Résultats de Cuckoo Sandbox

Nous avons testé Cuckoo Sandbox sur plusieurs malwares, avec des résultats plutôt encourageants. Nous avons choisi de présenter quelques résultats d'une analyse sur un malware récent de la famille ZeuS/ZBot.

4.1 Limitations

Les limitations de Cuckoo Sandbox sont les mêmes que pour les autres systèmes d'analyses de ce type :

- risque de détection de l'environnement virtuel : le binaire pourrait détecter qu'il est exécuté dans une machine virtuelle fonctionnant sous VirtualBox.
- risque de détection de l'environnement Cuckoo Sandbox : le binaire pourrait se baser sur certains

éléments nécessaires au fonctionnement de Cuckoo Sandbox. Entre autres choses, la présence d'un partage réseau nommé « setup » contenant un répertoire « cuckoo », laisse peu de place au doute, d'autant que ce nom de répertoire n'est pas configurable pour le moment.

4.2 Vue d'ensemble

Voici l'arborescence de résultats obtenus suite à notre analyse d'une souche ZeuS/ZBot :

```
.
├── analysis.conf
├── analysis.log
├── dump.pcap
├── files
│   ├── cmd.exe
│   ├── explorer.exe
│   ├── nil.exe
│   ├── TMPF30~1.BAT
│   └── xayw.exe
├── logs
│   ├── 1220.csv
│   ├── 1800.csv
│   ├── 780.csv
│   └── 784.csv
├── nil.exe
├── report.txt
└── shots
    ├── shot_1.jpg
    ├── shot_2.jpg
    ├── shot_3.jpg
    ├── shot_4.jpg
    └── shot_5.jpg
```

Arborescence des résultats CuckooBox pour une souche de malware ZeuS

On distingue :

- **analysis.conf** : contient un simple rappel du nom du fichier analysé, son timeout, le nom du package qui l'a généré (exe, pdf, etc.)
- **analysis.log** et **report.txt** : le premier fichier est un journal de l'analyse, le second détaille les processus créés et leur fonctionnement. Nous reviendrons en détail sur ces fichiers un peu plus tard.
- **dump.pcap** : un dump réseau, au format pcap, qui nous permettra de rentrer dans le détail des communications réseau qui ont pu être établies lors de l'exécution du binaire.
- une copie du fichier soumis pour analyse est toujours présente dans cette arborescence (dans notre exemple : **nil.exe**).
- répertoire *files* : ce répertoire contient tous les fichiers qui ont pu être générés suite à l'exécution de notre binaire, ainsi que les fichiers avec lesquels le malware a interagi. Le fichier **cmd.exe** présent dans le répertoire, dans notre exemple, est bien le **cmd.exe** sain du système, et pas une version modifiée comme on aurait pu le supposer.
- répertoire *shots* : contient une ou plusieurs captures d'écran. Ces dernières sont générées au fur et à mesure des événements : ici nous en avons cinq, une à chaque nouveau lancement de processus.
- répertoire *logs* : le répertoire le plus intéressant de la sortie de CuckooBox, qui contient les analyses de chaque processus au format CSV.

4.3 Fichier analysis.log

Voici notre fichier :

```
[2011-11-19 17:27:39] [INFO] Starting analysis procedure.
[2011-11-19 17:27:39] [INFO] Cuckoo starting with PID 112.
[2011-11-19 17:27:39] [INFO] Installing dependency "\\VBOXSVR\setup\system\
distorm3.dll".
[2011-11-19 17:27:39] [INFO] Installing "\\VBOXSVR\setup\cuckoo\shots".
[2011-11-19 17:27:39] [INFO] Installing "\\VBOXSVR\setup\cuckoo\files".
[2011-11-19 17:27:39] [INFO] Installing "\\VBOXSVR\setup\cuckoo\dll".
[2011-11-19 17:27:39] [INFO] Installing "\\VBOXSVR\setup\cuckoo\logs".
[2011-11-19 17:27:39] [INFO] Installing target file from "\\VBOXSVR\vyktym\
nil.exe" to "C:\".
[2011-11-19 17:27:39] [INFO] Starting Pipe Server
[2011-11-19 17:27:39] [INFO] Started taking screenshots.
[2011-11-19 17:27:39] [INFO] Analysis package imported from "packages.exe".
[2011-11-19 17:27:42] [INFO] Screenshot saved at "C:\cuckoo\shots\shot_1.jpg".
[2011-11-19 17:27:49] [INFO] Executing analysis package run function.
[2011-11-19 17:27:50] [INFO] Using default Cuckoo DLL "C:\cuckoo\dll\cmonitor.
dll".
[2011-11-19 17:27:50] [INFO] Successfully granted debug privilege on Cuckoo
process.
[2011-11-19 17:27:50] [INFO] Original process with ID "1800" (0x00000708)
successfully injected.
[2011-11-19 17:27:52] [INFO] Resumed thread with handle 0x00000750.
[2011-11-19 17:27:52] [INFO] Analysis package returned following process ID to
add to monitor list: 1800.
[2011-11-19 17:27:52] [INFO] Running for a maximum of 120 seconds.
[2011-11-19 17:27:56] [INFO] Newly created file path added to list: \\.\PIPE\
lsarpc
[2011-11-19 17:27:56] [INFO] Newly created file path added to list: C:\
WINDOWS\
[2011-11-19 17:27:56] [INFO] Newly created file path added to list: \\.\
MountPointManager
[2011-11-19 17:27:56] [INFO] Newly created file path added to list: C:\nil.exe
[2011-11-19 17:27:56] [INFO] Newly created file path added to list: C:\
Documents and Settings\vyk\Application Data\Ycepyd\xayw.exe
[2011-11-19 17:27:57] [INFO] Newly created file path added to list: C:\
Documents and Settings\vyk\Application Data\Uzowav\iqlun.ibf
[2011-11-19 17:27:57] [INFO] Newly created file path added to list: C:\
Documents and Settings\vyk\Application Data
[2011-11-19 17:27:57] [INFO] Newly created file path added to list: C:\
Documents and Settings\vyk\Application Data\Uzowav
[2011-11-19 17:27:57] [INFO] Newly created file path added to list: C:\
Documents and Settings\vyk\Application Data\Ycepyd
[2011-11-19 17:27:57] [INFO] Successfully granted debug privilege on Cuckoo
process.
[2011-11-19 17:27:57] [INFO] Process with ID "784" (0x00000310) successfully
injected.
[2011-11-19 17:27:57] [INFO] Newly created file path added to list: C:\
DOCUME~1\vyk\LOCALS~1\Temp\tmpf304e9cd.bat
```

```
[2011-11-19 17:27:58] [INFO] Newly created file path added to list: C:\
WINDOWS\system32\cmd.exe
[2011-11-19 17:27:58] [INFO] Successfully granted debug privilege on Cuckoo
process.
[2011-11-19 17:27:58] [INFO] Process with ID "780" (0x0000030c) successfully
injected.
[2011-11-19 17:27:58] [INFO] Process with ID 1800 terminated.
[2011-11-19 17:27:59] [INFO] Screenshot saved at "C:\cuckoo\shots\shot_2.jpg".
[2011-11-19 17:28:01] [INFO] Newly created file path added to list: C:\
DOCUME~1\vyk\LOCALS~1\Temp\TMPF30~1.BAT
[2011-11-19 17:28:01] [INFO] Screenshot saved at "C:\cuckoo\shots\shot_3.jpg".
[2011-11-19 17:28:01] [INFO] Process with ID 780 terminated.
[2011-11-19 17:28:02] [INFO] Newly created file path added to list: C:\
WINDOWS\explorer.exe
[2011-11-19 17:28:02] [INFO] Successfully granted debug privilege on Cuckoo
process.
[2011-11-19 17:28:02] [INFO] Process with ID "1220" (0x000004c4) successfully
injected.
[2011-11-19 17:28:02] [INFO] Process with ID 784 terminated.
[2011-11-19 17:28:03] [INFO] Screenshot saved at "C:\cuckoo\shots\shot_4.jpg".
[2011-11-19 17:29:02] [INFO] Screenshot saved at "C:\cuckoo\shots\shot_5.jpg".
[2011-11-19 17:29:53] [INFO] Stopping Pipe Server
[2011-11-19 17:29:53] [INFO] Analysis completed.
[2011-11-19 17:29:53] [INFO] Executing analysis package "exe" custom finish
function.
[2011-11-19 17:29:53] [INFO] Dropped file "C:\Documents and Settings\vyk\
Application Data\Ycepyd\xayw.exe" successfully dumped to "C:\cuckoo\files".
[2011-11-19 17:29:53] [INFO] Dropped file "C:\WINDOWS\system32\cmd.exe"
successfully dumped to "C:\cuckoo\files".
[2011-11-19 17:29:53] [INFO] Dropped file "C:\WINDOWS\explorer.exe"
successfully dumped to "C:\cuckoo\files".
[2011-11-19 17:29:53] [INFO] Saving analysis results to "\\VBOXSVR\vyktym\".
```

On voit donc notre CuckooBox créer des entrées dans les répertoires partagés afin de pouvoir exporter ses résultats, installer une DLL en mode *userland*, copier le binaire soumis à la racine du disque C :, lancer son package d'analyse par défaut pour l'analyse d'un fichier exécutable, puis enfin démarrer le binaire avec un process ID de 1800.

Rapidement, on constate que notre binaire fait un certain nombre de choses. La création de chemins vers des entrées telles que **C:\Documents and Settings\vyk\Application Data\Ycepyd\xayw.exe**, par exemple, devrait tout de suite éveiller la méfiance.

En lisant rapidement ce fichier, on peut donc conclure que :

- Notre binaire s'exécute bien.
- Le binaire crée plusieurs fichiers qui sont ensuite utilisés, et plusieurs processus sont exécutés.

Nous n'avons pas vraiment le détail du comportement du malware, néanmoins des éléments d'analyse plutôt positifs ressortent déjà en première approche. Le peu d'informations fournies par ce fichier lève suffisamment d'interrogations pour passer à la consultation des autres fichiers générés par CuckooBox.

On note également la prise de captures d'écran dès qu'un nouveau processus est lancé, et les dumps de fichier créés dans le répertoire *files*.

4.4 Fichiers report.txt et fichiers logs

Ces fichiers viennent compléter les premiers éléments fournis dans le fichier **analysis.log**.

Le fichier **report.txt** contient les mêmes informations que les fichiers se trouvant dans le répertoire *logs*. La seule différence est que le répertoire logs contient une entrée par processus, au format CSV, beaucoup plus exploitable, alors que **report.txt** contient toutes les informations pour tous les processus.

Ces fichiers contiennent tous les appels des processus liés au malware. À titre d'exemple, en voici quelques lignes :

```
PROCESS: 1800 - nil.exe
  CALL: 20111119162756.863, CreateMutexW, Status: SUCCESS, Return
  Value: 0x000000b8
    ARGUMENT: lpName -> Global\{B2AAD0EC-EDA2-C0C8-C90F-50AA2E9B82BE}
  CALL: 20111119162756.933, CreateFileW, Status: SUCCESS, Return
  Value: 0x000000bc
    ARGUMENT: lpFileName -> C:\Documents and Settings\vyk\Application
    Data\Ycepyd\xayw.exe
    ARGUMENT: dwDesiredAccess -> 0xc0000000
```

Il est ainsi possible de retracer l'activité de chaque processus de façon précise, et d'avoir une vue du comportement du binaire suspect, précise et horodatée.

Dans notre exemple, notre processus initial dépose des fichiers sur le système avant de les exécuter. En voici quelques extraits :

```
CALL: 20111119162757.844, CreateProcessW, Status: SUCCESS, Return
Value: 784
    ARGUMENT: lpApplicationName -> (null)
    ARGUMENT: lpCommandLine -> C:\Documents and Settings\vyk\
    Application Data\Ycepyd\xayw.exe""
CALL: 20111119162758.365, CreateProcessW, Status: SUCCESS, Return
Value: 780
    ARGUMENT: lpApplicationName -> (null)
    ARGUMENT: lpCommandLine -> C:\WINDOWS\system32\cmd.
    exe" /c "C:\DOCUME~1\vyk\LOCALS~1\Temp\tmpf304e9cd.bat""
  CALL: 20111119162758.365, ExitProcess, Status: , Return Value:
    ARGUMENT: uExitCode -> 0x00000000
```

Il suffit ensuite de poursuivre, et aller examiner plus en détail ce que vont faire ces deux nouveaux processus, 784 et 780... Et poursuivre ainsi notre analyse.

4.5 dump.pcap

Comme son nom l'indique, ce fichier est au format PCAP et contient les captures réseau de tout ce qui s'est passé au sein de notre machine virtuelle, à partir de l'exécution du binaire suspect.

Conclusion

Cuckoo Sandbox est un outil permettant d'analyser très rapidement, en première approche, des binaires ou documents suspects dans un environnement sécurisé (VirtualBox). Alors que de nombreuses sandbox fonctionnent en ligne et ne permettent pas de conserver la confidentialité de la donnée, Cuckoo Sandbox permet les analyses locales de façon très simple, sans avoir à « pondre de la ligne de commandes ».

L'outil, encadré par le Projet Honeynet, n'en est qu'à sa version 0.2 mais permet déjà d'obtenir de bons résultats et semble promis à un bel avenir.

Pour compléter l'analyse comportementale apportée par Cuckoo Sandbox, il est recommandé de soumettre le binaire à analyser à d'autres sandbox **[6]**, si possible, ces dernières ne disposant jamais exactement des mêmes fonctionnalités d'analyse. La plupart des sandbox d'analyse de malwares étant en ligne, il convient d'être prudent et de ne pas y envoyer des binaires qui vous auraient attaqué de façon ciblée, par exemple... Mais ça n'arrive jamais, pas vrai ? ;-) ■

REMERCIEMENTS

Je tiens à remercier le CERT Société Générale, et en particulier Guillaume ARCAS, pour sa relecture attentive. Merci également à Alexandre GAZET pour sa relecture.

RÉFÉRENCES

[1] Cuckoo Sandbox - http://www.cuckoobox.org

[2] The Honeynet Project - http://www.honeynet.org/

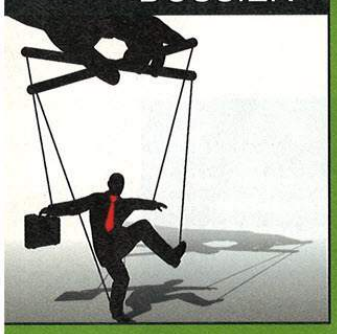
[3] VirtualBox - https://www.virtualbox.org

[4] Python - http://www.python.org/download/

[5] Python Imaging Library (PIL) - http://pythonware.com/products/pil/

[6] Malware Analysis Sandbox Projects - http://forums.malwr.com/index.php?/topic/4-malware-analysis-sandbox-projects/

DOSSIER



INGÉNIERIE SOCIALE SUR INTERNET :

QUAND LE WEB DEVIENT UN OUTIL D'INFLUENCE ET DE LEURRE

L'ingénierie sociale (ou *social engineering*) est un domaine des plus vastes couvrant de multiples concepts. Certains peuvent être aussi triviaux que le filoutage (plus couramment appelé *fishing* sous d'autres contrées) et être d'un intérêt des plus limités. D'autres s'appuient sur la classification des individus en différents profils psychologiques y associant des modes opératoires spécifiques (nous pourrions parler de failles).

C'est également une discipline historiquement liée à celle de la sécurité informatique, au même titre que l'est devenu au fil des conférences sur la sécurité informatique le crochetage de serrures (*lock picking*) qui pourrait lui aussi faire l'objet d'un dossier. L'un des pirates informatiques les plus célèbres, Kevin Mitnick, après avoir notoirement utilisé ces techniques, a d'ailleurs écrit un ouvrage complet sur le sujet (« The Art of Deception » ou « L'art de la supercherie » en français) qui décrit plusieurs scénarios d'attaques et propose des contre-mesures associées.

Outre la similitude pouvant être faite entre le pirate attaquant un système d'information, après en avoir étudié les faiblesses, et l'ingénieur social, mettant à profit différentes techniques de manipulations après avoir dressé le profil psychologique de sa victime et ses failles potentielles (voir les excellents ouvrages « Petit traité de manipulation à l'usage des honnêtes gens » et « la soumission librement consentie » de Robert-Vincent Joule et Jean-Léon Beauvois), les deux attaquants visent souvent des objectifs similaires (appâts du gain, obtention d'informations, ...) et peuvent être complémentaires dans un contexte opérationnel.

À titre plus anecdotique, les flibustiers de l'ingénierie sociale, forts du large éventail de techniques de manipulation à leur disposition, peuvent poursuivre d'autres objectifs pour le moins exotiques, comme le font les *Pick Up Artist* (http://www.fastseduction.com/) pour la simple beauté de l'art.

Pour revenir dans le vif du sujet et l'objet premier de ce dossier, nous allons aborder ici l'usage du social engineering dans le cadre des systèmes d'information, et plus particulièrement d'Internet, au travers de trois articles.

Nous allons tout d'abord exposer au travers de deux articles les menaces pesant sur les États et les entreprises en matière de perte d'image ou de fuites d'informations via des attaques en ingénierie sociale menées au travers des systèmes d'information, et plus particulièrement d'Internet et des réseaux sociaux.

Le dernier article traite des pots de miel sociaux ou comment utiliser des profils factices (mais néanmoins attractifs) sur différents réseaux sociaux pour collecter des informations.

Exceptionnellement, il n'y a pas de 4ème article, au grand dam de notre rédacteur en chef qui souhaitait affiner ses techniques, car le Pick Up Artist qui devait être interviewé a finalement décommandé...

Cédric Foll

INGÉNIERIE SOCIALE ET INFLUENCE SUR INTERNET : D'UN USAGE PAR/CONTRE LES ENTREPRISES

Sébastien Chainay – sebastien.chainay@gmail.com –
Consultant en sécurité de l'information et en intelligence économique pour Hapsis

mots-clés : *INGÉNIERIE SOCIALE / RUMEUR / HOAX / INFLUENCE / CONTRE-INFLUENCE / INTELLIGENCE ÉCONOMIQUE / TWITTER / SEO / CONVERGENCE MÉDIAS*

L'ingénierie sociale regroupe une classe d'actions dont le but de l'émetteur est d'obtenir ce qu'il veut du récepteur. Autrement dit, le premier exerce une influence sur le second.

Dans un contexte de sécurité informatique, l'influence par ingénierie sociale constitue des attaques, éthiquement répréhensibles, menées soit oralement, soit par mail, soit directement sur l'Internet (les réseaux sociaux mais aussi les forums de discussion et les messageries instantanées). Dans un contexte d'intelligence stratégique, les actions d'influence économique s'inscrivent dans une démarche légale et de surcroît nécessaire aux entreprises dès lors que leur marché s'internationalise.

Ces deux contextes d'influence ont un média en commun : l'Internet. Mais ce média est contournable, manipulable : c'est ce dernier aspect qui nous intéresse dans cet article.

1 De l'importance de l'influence pour les entreprises

L'influence économique est une stratégie et une tactique de conviction menées auprès de décideurs par l'utilisation d'une information appropriée **[I]**. Le terme « influence » a une acception plus large que celui de *lobbying*, lequel n'est qu'une forme ou une partie d'une action d'influence. Une action durable qui s'inscrit dans le cadre d'une « diplomatie d'entreprise ».

L'influence fait partie du volet de l'intelligence économique dit « proactif », qui entend peser sur l'environnement extérieur et non le subir. Elle a lieu dans un cadre éthique, c'est-à-dire qu'elle ne fait pas appel à la tromperie, désinformation ou manipulation ou autre trafic d'influence. Il faut savoir que pour être durablement influent dans la communauté internationale, il faut être crédible.

Pour une entreprise, les raisons d'avoir recours à une action d'influence sont nombreuses.

1.1 Défendre une position

- Dans le domaine juridique pour défendre un texte, il s'agit de participer en tant que partie prenante à l'élaboration des régulations nationales et

internationales qui vont impacter son secteur : règles, normes, codes, contrats-types, etc., car dans notre société mondialisée, la plupart des règles sont élaborées dans les institutions européennes et internationales avant d'arriver sur le territoire national où elles sont éventuellement adaptées. Il faut participer à l'élaboration de ces normes pour qu'elles ne vous soient pas défavorables, il faut même savoir parfois les initier.

- Dans le domaine économique pour obtenir un marché, il est plutôt conseillé de travailler en amont, car si l'on attend le moment du contrat, il est généralement trop tard.

1.2 Diplomatie d'entreprise

Il s'agit d'abord de construire des réseaux de confiance sur la durée, avec les décideurs et prescripteurs, mais aussi avec tous partenaires utiles (identifiés par une bonne intelligence économique préalable). Ensuite, il faut soigner sa réputation, image et influence s'alimentant réciproquement. Enfin, faire en sorte d'améliorer le recrutement, d'attirer les meilleurs.

1.3 Prévenir ou résoudre des conflits ou des crises

Une bonne capacité d'influence résultant d'action de long terme permettra d'avoir des partenaires solides (ONG, relais d'opinion, institutions, ...) qui pourront aider l'entreprise à amortir les chocs, notamment en cas de crise de réputation.

Les différentes interactions : d'après Didier Heiderich

- personne à personne
  influence interpersonnelle
- entreprise à personne
  outils marketing
- entreprise ou organisation à entreprise
  guerre informationnelle, intelligence stratégique
- entreprise, organisation, administration à groupe social
  formatage culturel, social learning
- entreprise, organisation à administration
  lobbying
- pays - pays
  géostratégie

Influence par les entreprises en bleu

Influence contre les entreprises en rouge

L'influence est un mécanisme qu'exerce l'émetteur sur le récepteur à l'aide d'un message correctement étudié. Différentes situations d'influence existent selon Didier Heiderich, consultant en gestion de crise et communication sensible et président de l'Observatoire International des Crises. Nous allons étudier dans cet article les interactions susceptibles de concerner les entreprises au travers du média Internet.

2 Influence sur l'Internet par les entreprises

2.1 Utilisation de l'Internet comme un outil d'influence par les entreprises

Sur l'Internet comme ailleurs, un message trouve sa capacité d'influence dans la rencontre avec les émetteurs auxquels il est destiné.

Pour Cédric Deniaud, consultant en stratégie Internet, l'influence sur l'Internet se décline en cinq piliers **[2]** :

- L'audience : représente la capacité d'une personne à avoir une caisse de résonance.
- La proximité : représente la notion de cercles concentriques et de confiance dans les réseaux sociaux, les amis se révélant être des influenceurs à ne pas négliger.
- L'expertise : doit être reconnue à deux niveaux : par la personne influencée directement et par la communauté.
- Pertinence/Légitimité : recoupe le fait que vous pourrez avoir de l'influence si vous prenez la parole ou argumentez sur un sujet sur lequel vous êtes légitime pour l'ensemble des raisons évoquées précédemment (expertise, audience ciblée sur le sujet, ...).
- Crédibilité/Confiance : se développe avec le temps : un support qui fidélise une même audience prouve que l'audience reconnaît le support comme pertinent dans sa prise d'information.

Ainsi, pour une entreprise, l'influence peut se concevoir aussi bien en termes de portée (d'audience) qu'en termes de cible crédible, légitime, spécialisée.

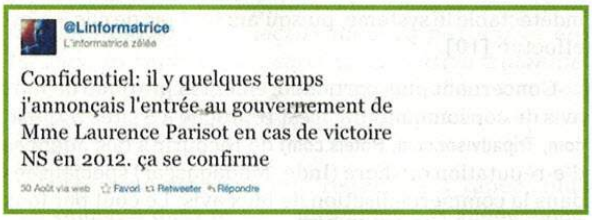
2.1.1 Influence de cible

L'influence de cible se définit en un principe : délivrer le bon message au bon moment dans un domaine déterminé. Pour l'illustrer, prenons le cas de Twitter.

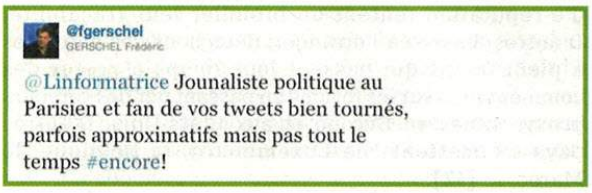
Exemple : influence de cible sur Twitter

1. **Ouvrir un compte Twitter avec un pseudonyme si possible en rapport avec le domaine cible.** Donner une fausse adresse mail à l'inscription, Twitter n'exigeant pas de confirmation par mail pour utiliser le compte. Il faut que l'adresse mail n'ait jamais été donnée par un autre utilisateur.
2. **Donner les raisons de ce pseudonyme, de cet anonymat.**
3. **Crédibiliser le compte Twitter** en distillant quelques informations prises dans la presse.
4. **S'abonner aux comptes Twitter des journalistes du domaine cible** et de quelques autres journalistes en vue sur le réseau, afin de se faire remarquer.
5. **Ajouter au besoin des faux « followers » (abonnés)** pour crédibiliser le compte. Deux solutions : payer des sites américains qui permettent de doper artificiellement les followers, ou passer par un programme informatique qui crée en rafale des faux comptes. La méthode est cependant risquée car elle pourrait être découverte.

ILLUSTRATION : Le compte @Linformatrice **[3]** qui sévit sur Twitter depuis début août. La personne à l'origine de ce compte se présente comme une « journaliste politique curieuse qui essaye de faire son travail honnêtement, mais contrainte de garder l'anonymat » et prétend sortir des informations exclusives alors qu'elles ne se vérifient pas.



En dépit de la faible fiabilité de ses informations, @Linformatrice a tout de même suscité l'intérêt de plusieurs journalistes politiques, comme le correspondant à l'Élysée du journal *Le Parisien* :



Toutes les hypothèses ont été avancées sur l'identité de cette mystérieuse informatrice. Un blog a prétendu l'avoir démasquée en révélant qu'il s'agissait d'une opération de manipulation de l'extrême-droite... **[4]** Difficile de savoir où se situe la vérité.

2.1.2 Influence de portée

L'influence d'un blog dépend essentiellement de son audience et des liens retour (en anglais *backlinks* ou *inlinks*) avec d'autres blogs **[5]**. Leur nombre est une indication de la réputation de ce site ou de cette page dans la mesure où l'on peut considérer que lorsqu'un site fait un lien vers un autre site, il lui transmet une partie de son influence ; attention des liens factices peuvent être créés à l'aide de logiciels (Xrumer **[6]** par exemple) ou des techniques SEO **[7]**.

Certains sites calculent l'indice de visibilité qui peut paraître plus objectif : **Klout.com, Youseemi.fr, Peerindex.com.**

Concernant Twitter, l'influence dépend essentiellement du nombre de *followers* mais aussi de l'activité (mentions, *retweet*) **[8]**.

Mais tout cela n'est que virtuel, en effet il existe mille et une astuces pour faire gonfler artificiellement ces followers Twitter. Il suffit de taper la requête suivante sur Google :

« comment avoir followers sur twitter »

Et parfois, l'influence qu'il est possible d'exercer sur les followers se fait à leur insu.

ILLUSTRATION : influence lors des primaires socialistes.

Juste après la fin du deuxième débat entre les candidats de la primaire citoyenne, quelques centaines de tweets similaires sont postés pratiquement en même temps.

« *Au lendemain des primaires, il faudra rassembler les socialistes, rassembler la gauche, et rassembler les Français.* »

En fait, l'équipe de campagne de François Hollande vient de se servir d'une fonctionnalité (jusqu'ici passée inaperçue) du site de mobilisation numérique **toushollande.fr** qui lui permet de prendre la main sur le compte Twitter :

L'équipe de campagne de François Hollande initie là une pratique qui s'apparente à du spam... ou à de l'influence en direct ! En effet, tout au long du débat, elle aura envoyé 3 tweets sur les comptes Twitter de la liste des « inscrits ».

Pour revenir à des questions de sécurité, l'application TousHollande a un accès quasi-intégral sur le compte Twitter du militant (sauf aux messages privés... et au code confidentiel bien sûr !).

De plus, il n'est pas possible de se désinscrire du service depuis le site **toushollande.fr** à moins de passer par les options de Twitter. Sans compter qu'il n'est pas garanti qu'une désinscription automatique soit lancée après les élections de 2012...

2.1.3 Influence de présence, réputation numérique : facteurs clés de succès sur l'Internet ?

L'influence de présence fait appel au référencement utilisé dans les moteurs de recherche. Et quand on dit moteur de recherche, on dit Google. Ainsi, lorsqu'un internaute tape une expression, et qu'une entreprise sort en meilleure position sur Google par rapport à ses concurrentes, elle aura d'autant plus d'influence.

Quant à la réputation numérique, elle constitue indéniablement un fort atout commercial particulièrement lorsque ce sont des clients ou des consommateurs qui en sont à l'origine.

Dans ces deux cas, nous allons voir qu'il est possible de frauder en augmentant artificiellement la capacité d'influence d'une entreprise sur l'Internet.

3 Fraude d'influence par les entreprises : un nouveau marché émerge

Le bouton +1 de Google est une simple réédition du « like » ou du « retweet ». C'est la raison pour laquelle Google a choisi une stratégie différente : inciter les webmasters à pousser les utilisateurs à utiliser « +1 » ! Comment ? En prenant en compte le nombre de « +1 » pour afficher certains résultats en priorité dans les résultats de recherche **[9]**. Désormais, plus les visiteurs cliqueront sur le bouton « +1 », plus la page aura de chances d'être vue sur le moteur de recherche.

Résultats : un marché des clics sur ces boutons se développe (Plussem, GooglePlus1Supply, BuyGooglePlus1, ...), qui propose aux éditeurs de sites internet d'acheter des clics sur leur bouton +1. « 19,99 $ les 50 clics, 69,99 $ les 250 et 359,99 $ les 2 000 ». Pour ne pas être repéré par Google, Plussem n'utilise pas de robots cliqueurs, qui seraient facilement détectés par les algorithmes anti-spam. Le système est basé sur des utilisateurs réels disposant d'un compte Google, ce qui supprime l'utilisation de robots et le problème d'une adresse IP unique effectuant tous les clics. De plus, les clics sont effectués sur la durée (quelques jours), ce qui rend quasiment indétectable le système, puisqu'aucun « pic de clic » n'est effectué **[10]**.

Concernant plus particulièrement la pratique de faux avis de consommateurs, il est reproché à 3 sites (**Expedia.com**, **Tripadvisor.com**, **Hotels.com**) de recourir à des agences d'e-réputation offshore (Inde, Madagascar) spécialisées dans la commercialisation de faux avis. Le coût par faux avis serait de 2€ à 10€ **[11]**.

Exemple de commentaire :

« Mais bon, pour moi, ce qui me concerne, j'ai effectué un séjour de cinq jours dans cet hôtel. Et je n'ai pas été déçu. »

La syntaxe semble hasardeuse, le style maladroit, ce commentaire posté sur le célèbre site de conseil de voyageurs TripAdvisor a pourtant été rédigé par un professionnel. Les fautes d'orthographe, le style relâché font partie de ce que les professionnels appellent « marketing influence ».

Cyber-café ou utilisation d'une clé 3G, les agences d'e-réputation tentent de brouiller leur traçabilité. D'autres, basées à l'étranger, détachent des employés à plein temps qui passent leur temps à poster des commentaires sur les forums en passant par des serveurs proxys situés en Europe et aux États-Unis. D'autres pays s'y mettent : le Luxembourg, la Belgique, le Maroc, ... **[12]**.

4 Détournement d'influence contre les entreprises et les personnalités : la génèse des rumeurs sur l'Internet

Le référencement par Google repose sur des algorithmes complexes et dont les ressorts ne sont connus que par l'entreprise elle-même. Cependant, nous allons voir que ces algorithmes sont contournables si bien que tout un chacun peut en prendre l'avantage qu'il désire, entreprises comme internautes.

Prenons deux exemples de contournement : GoogleSuggest et GoogleNews.

Google Suggest Hacking :

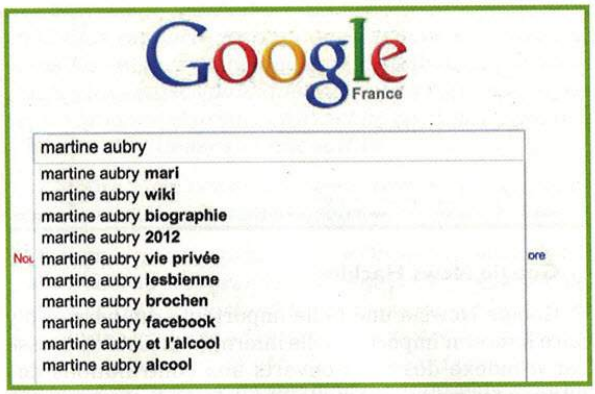
Le service « Google Suggest », rebaptisé « saisie semi-automatique », est expérimenté depuis 2004 et a été généralisé à l'été 2008. Impossible d'y échapper, les suggestions s'affichent automatiquement dès que l'on fait une requête sur Google.

Comment marche cet algorithme qui anticipe nos requêtes ? Voici la réponse de Google :

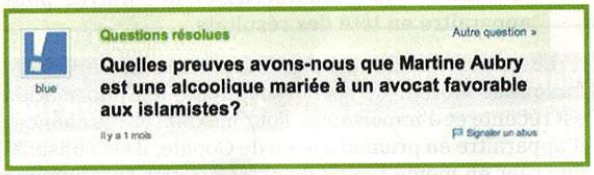
« *Ces recherches sont déterminées, par le biais d'un algorithme, en fonction d'un certain nombre de facteurs purement objectifs (dont la popularité des termes de recherche), sans intervention humaine. Toutes les requêtes de prédiction affichées ont déjà été saisies par le passé par d'autres utilisateurs de Google.* » **[13]**

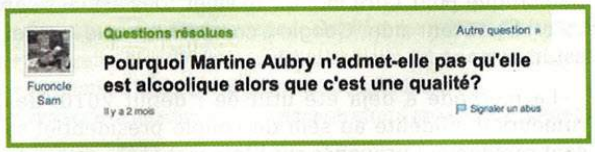
Autrement dit, plus une requête est tapée, plus elle remonte dans le haut du panier des suggestions. Google Suggest est donc susceptible de véhiculer de fausses informations dès lors que l'on sait s'y prendre. Voici une méthode possible, illustrée par le cas de Martine Aubry.

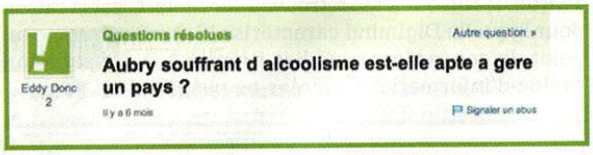
1. **Mobiliser des contacts dans toute la France** en leur demandant de taper tous les jours la même requête dans Google. Une méthode parfois utilisée par les agences d'e-reputation pour faire remonter des suggestions.
2. **Laisser agir l'algorithme de Google Suggest**, qui devrait repérer une activité notoire autour d'un nouveau mot-clé sur une personnalité politique et faire ainsi remonter tout en bas des suggestions ce mot-clé qui semble avoir une actualité. C'est le cas du mot « alcool » sur la recherche « Martine Aubry » au 15 septembre 2011, dont on peut d'avance prévoir qu'il aura autrement plus de succès que la requête « Martine Aubry facebook ».



3. **Laisser faire la curiosité humaine**. Un résultat surprenant qui apparaît dans les suggestions a vocation à remonter plus haut par effet d'autosuggestion.
4. **Une fois Google Suggest hacké, créer les articles correspondants.** Passer par des plateformes peu regardantes avec la véracité de l'information et qui ne risquent pas de censurer le contenu posté. Le service de questions-réponses Yahoo Answers, par exemple. Il convient de bien choisir la forme interrogative pour qu'elle fasse passer l'information souhaitée.



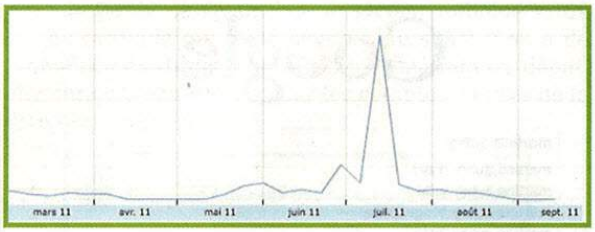




5. **Attendre que les médias ou que la personne concernée finissent par parler de ces rumeurs.** Google Suggest donne une première visibilité médiatique à la rumeur et peut obliger les différents acteurs à en parler.

Contre-influence :

Martine Aubry a pris les devants en juillet en détaillant au *Journal du Dimanche* **[14]** toutes ces rumeurs pour les désamorcer. L'effet est immédiat, comme le montre l'outil *Insights for search* de Google pour la récurrence de la requête « Martine Aubry alcoolique ».



Google News Hacking :

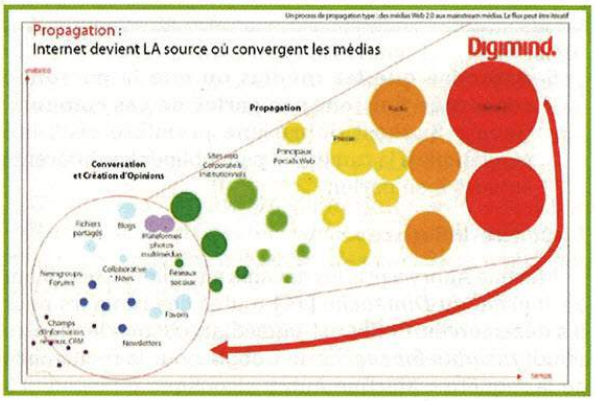
Google News a une faille importante qui permet d'y faire figurer n'importe quelle information juste ou fausse car il indexe des sites ouverts aux contributions des internautes qui ne sont modérées **qu'a posteriori** : LePost.fr et le système de blogs lié au site TempsReel.NouvelObs.com.

Pour qu'une information douteuse prenne et que la rumeur se transforme en information, il faut que sa source soit jugée crédible.

1. **S'inscrire sur la plateforme de blog du NouvelObs.com** et créer un blog **[15]**. Bien donner une fausse adresse mail, passer par un proxy pour plus de sûreté.
2. **Rédiger une rumeur.**
3. **Dans les minutes qui suivent, l'information est reprise sur Google News.** Avec un peu de chance, la nouvelle se distingue assez des autres pour apparaître en tête des résultats.

Les articles de Google News apparaissent sur Google lorsque le moteur de recherche juge que l'information est récente et d'importance. Pour maximiser ses chances d'apparaître en première page de Google, il est conseillé de créer en même temps d'autres articles sur la même thématique pour faire monter le sujet. Des articles sur LePost.fr peuvent aider Google à comprendre que le sujet est important.

La méthode a déjà été utilisée : début 2010, des rumeurs d'infidélité au sein du couple présidentiel se sont rapidement propagés sur l'Internet **[16]** : partie de Twitter, la rumeur s'est retrouvée sur I-télé. C'est la raison pour laquelle Digimind caractérise l'Internet comme un point de convergence médias propice à la propagation rapide d'informations avérées ou pas :



5 Influence sur l'Internet contre les entreprises

5.1 Utilisation de l'Internet comme un outil d'influence contre les entreprises

Pour user de l'influence sur l'Internet contre les intérêts d'une entreprise, il existe de multiples moyens. La plus morale consiste à se servir d'informations vérifiées qui mettent en difficulté l'entreprise. Mais pour la concurrence, il est souvent plus facile de se placer du côté de la désinformation ou de commanditer des attaques informatiques quitte à mettre leur éthique de côté...

Objectif : s'en prendre à l'image de marque et à la réputation d'un concurrent sur l'Internet.

5.1.1 Cibler l'image de marque : viser le grand public

Lorsque l'on veut cibler l'image de marque d'une entreprise au niveau du grand public, l'idée qui vient directement à l'esprit est de s'en prendre à son média de masse consultable en permanence : son site Internet. Pour peu qu'il s'agisse d'un site commercial, l'impact sera également économique. Pour cela, plusieurs attaques existent : le défacement (ou défiguration), le déni de service distribué, mais aussi le détournement de noms de domaines utilisant la marque de l'entreprise (*cybersquatting*).

Une technique plus informationnelle (basée uniquement sur l'information) est la conjonction de rumeurs dont le faisceau tend poursuivre une même démonstration. Ce fut le cas cet été pour la Société Générale, dans un contexte économique incertain et un climat fébril sur les marchés.

Objectif du faisceau des rumeurs : démontrer que la Société Générale va tomber en faillite ou être nationalisée dans le cadre d'un plan de sauvetage **[17] [18]**.

1. Rumeur macro-économique introductive (début août) : la note souveraine de la France va être dégradée.
2. **Le Daily Mail**, dans son édition dominicale du **7 août**, annonce que la Société Générale « se [trouve] dans un état périlleux » et potentiellement « au bord du désastre », du fait de pertes subies sur la dette grecque. Une rumeur affirmera même, à tort, que les journalistes du Daily Mail se sont inspirés d'une fiction du Monde « Terminus pour l'euro » - pour écrire leur article...

3. **Le 10 août, on murmure sur les marchés financiers** que le président de la République serait rentré d'urgence de ses vacances au Cap Nègre pour venir au secours d'une grande banque française en difficulté (nationalisation en vue).
4. **Le 10 août toujours, le bruit circule** que l'assureur Groupama aurait vendu une partie de sa participation dans la Société Générale.
5. **Le 10 août encore**, le plan d'aide à la Grèce serait étendu aux obligations à échéance 2024, ce qui représenterait des pertes exceptionnelles pour la Société Générale.
6. **La Banque centrale européenne confirme** avoir prêté 500 millions de dollars à un établissement financier du Vieux Continent. Certains pensent qu'il pourrait s'agir de la Société Générale et y voient la confirmation d'éventuels problèmes de liquidités de la banque de la Défense.
7. **Le 18 août, le Wall Street Journal affirme que** la Banque centrale américaine (Fed) aurait mis la pression sur les filiales américaines des banques européennes pour qu'elles renforcent leur coussin de liquidités en dollars. Certains jugent que la Société Générale, du fait de l'importance de sa banque d'investissement, pourrait être mise en difficulté par ces mesures.

La technique de la manipulation boursière (*pump and dump*) est une autre technique de déstabilisation sur l'action d'une entreprise cotée. Elle consiste en l'incitation d'achats ou de vente par mails faisant fortement varier un titre, le mail ayant un fort pouvoir de persuasion.

5.1.2 Cibler l'image de marque par mail : viser la clientèle

Avec le site internet, la clientèle est l'autre talon d'Achille des entreprises. Et le moyen le plus direct de les joindre est leur adresse mail. Ainsi, un scam monté de toute pièce avec un logo d'entreprise peut nuire à la réputation de cette dernière.

Le canular (*Hoax*) en est une autre. Il s'agit d'une rumeur véhiculée par mail et qui trouve son pouvoir de propagation dans sa force de persuasion vis-à-vis de l'internaute. Il est assimilable à un ver informationnel par analogie au mode de propagation d'un ver informatique.

ILLUSTRATION : Canular d'Issy-les-Moulineaux (Hauts-de-Seine)

L'hoax affirmait qu'une personne qui s'était assise dans un cinéma avait ressenti une douloureuse piqûre. Elle s'était alors relevée pour découvrir l'aiguille d'une seringue portant une étiquette : « *Vous venez d'être infecté par le VIH* »...

Le message insistait : « *Le Centre de contrôle des maladies rapporte qu'on a aussi trouvé des aiguilles dans les retours de monnaie de distributeurs publics. Toutes les chaises publiques devraient être inspectées avec vigilance et prudence avant usage. Une inspection visuelle minutieuse devrait suffire.* »

L'affaire était censée avoir été révélée par la police municipale d'Issy-les-Moulineaux.

Suivait la mention persuasive : « *On nous a demandés de passer ceci au plus grand nombre de personnes possible. Ceci est très important !!! Pensez que vous pouvez sauver une vie juste en redistribuant ceci. S.V.P. prenez quelques secondes de votre temps pour faire passer le message.* » Ce message semblait d'autant plus crédible qu'il avait été *forwardé* par un Membre de l'Institut Pasteur (Département de Génétique et Biochimie du Développement/Département d'Immunologie) qui n'avait pas hésité à laisser ses coordonnées téléphoniques...

Heureusement, ce canular de très mauvais goût avait été très vite démenti.

Afin de rassurer les internautes, un démenti fut accompagné des avertissements suivants : « *Lorsqu'une personne s'est accidentellement piquée, il lui est conseillé, par mesure de précaution, de consulter un médecin et de lui remettre le matériel pour qu'il transmette*

l'aiguille ou la seringue au laboratoire compétent pour analyse. Le risque réel de contamination est évalué au cas par cas, en tenant compte de l'état du matériel et de la nature de la blessure, sachant que le virus du SIDA est très fragile dans le milieu extérieur et ne peut être transmis que par du sang frais. »

La Mairie d'Issy-les-Moulineaux en fit de même sur son site web avec le message suivant :

« *Depuis plusieurs jours, une rumeur circule de mail en mail, selon le principe maintenant bien connu des chaînes (les fameux hoax). Alertés par de nombreux internautes (par mail et par téléphone), la Mairie d'Issy-les-Moulineaux dément ce « canular » de mauvais goût. Avant d'atteindre Issy-les-Moulineaux, cette rumeur a déjà circulé à Dallas, Denver, Atlanta et Montréal.*

Si vous souhaitez obtenir davantage d'informations sur son origine, rendez-vous sur le site spécialisé HOAXBUSTER : http://www.hoaxbuster.com/hliste/fev01/hiv.html.

Si vous recevez ce mail, merci de communiquer ces éléments à vos correspondants. »

On s'aperçoit donc que même face à un canular finalement peu crédible, les réactions sont vives. En effet, la Mairie a recensé plus de 120 mails reçus pour cette affaire et 180 appels téléphoniques de citoyens visiblement perplexes, qui ont eu entre les mains ce mail.

5.1.3 Cibler les ressources humaines : viser les individus stratégiques

Les techniques de *profiling* permettent le débauchage de personnes haut-placées d'une entreprise et/ou maîtrisant un savoir-faire particulier. Ainsi, de faux chasseurs de tête peuvent approcher sur les réseaux sociaux professionnels les profils les plus prolixes sur leur parcours, profils les plus susceptibles de renseigner abondamment.

Plusieurs cibles peuvent être visées dans l'organigramme de l'entreprise :

- débauchage de ressources humaines stratégiques (management, direction, R&D, ...) ;
- ciblage sur les réseaux sociaux de profils particuliers (gestionnaire de fonds, responsables de financement, ...) ;
- approche d'employés sur les réseaux sociaux pour extorsion d'informations sur l'entreprise.

Conclusion

L'Internet, de par sa nature virtuelle et logique, est à la portée de tous. Cette ouverture fait que l'Internet est très exposé au détournement tant au niveau informatique (on parle d'attaque informatique) qu'au niveau informationnel (on parle d'attaque informationnelle), ou au niveau du référencement (on parle d'attaque SEO).

Point de convergence réseau (nœud de communication) mais aussi médiatique (nœud d'échange de l'information), l'Internet a un pouvoir de propagation immense exploité aussi bien sous la forme d'un ver que d'une rumeur.

Toutes ces possibilités de détournement et de propagation font que l'influence sur l'Internet est plus l'affaire de ceux qui en connaissent les failles du système plutôt que le résultat d'une véritable méthodologie en tous les cas sur le court terme. Gageons que sur le long terme une stratégie d'influence sur l'Internet irréprochable sur le plan de l'éthique auprès d'acteurs identifiés aura des effets plus bénéfiques et constructifs sur le plan économique plutôt que de se cantonner à de la dés information répétitrice et en fin de compte risquée sur le plan juridique. ■

■ RÉFÉRENCES

[1] Cette définition et les explications qui suivent sont extraites d'articles de Claude Revel, Directrice du GIISK (centre Global Intelligence & Influence de SKema business school) et praticienne de l'intelligence économique

[2] http://cdeniaud.canalblog.com/archives/2011/01/21/20175650.html

[3] http://twitter.com/#%21/Linformatrice

[4] http://antennerelais.canalblog.com/archives/2011/08/20/21824934.html

[5] http://www.webandluxe.com/10/2011/10-methodes-pour-evaluer-linfluence-et-le-trafic-dun-blog/

[6] http://xrumer-palladium.blogspot.com

[7] MISC 36, « Petit traité d'e-manipulation à l'usage des honnêtes gens », F. Raynal et F. Gaspard

[8] http://fr.readwriteweb.com/2010/03/22/a-la-une/dcouverte-majeure-propos-de-linfluence-sur-twitter

[9] http://techcrunch.com/2011/06/01/now-1-gets-interesting-button-to-launch-on-youtube-android-market-best-buy-oh-and-techcrunch/

[10] http://actu.abondance.com/2011/08/qui-veut-acheter-des-packs-de-clics.html

[11] http://blog-ereputation.com/2011/06/12/ereputation-et-fraude-dinfluence-episode-2-lutte-contre-les-faux-avis-de-consommateurs/

[12] http://www.secunews.org/news/news-0-5453+comment-des-entreprises-vendent-de-faux-avis-sur-le-net.php?com=0

[13] http://www.google.com/support/websearch/bin/answer.py?hl=fr&answer=106230

[14] http://www.lejdd.fr/Election-presidentielle-2012/Actualite/Martine-Aubry-n-acceptera-pas-les-rumeurs-sur-son-mari-Jean-Louis-Brochen-et-sur-sa-vie-privee-355701/

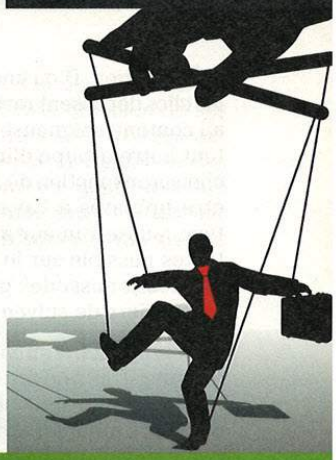
[15] http://buzz-nue.blogs.nouvelobs.com/

[16] http://www.arretsurimages.net/contenu.php?id=2813

[17] http://www.lexpress.fr/actualite/economie/l-ete-pourri-de-la-societe-generale_1027849.html

[18] http://www.huyghe.fr/actu_960.htm

INGÉNIERIE SOCIALE ET INFLUENCE SUR INTERNET : D'UN USAGE PAR/CONTRE LES ÉTATS



Laurence Ifrah – Criminologue expert en criminalité numérique et en cyberconflits – Consultant en protection du patrimoine informationnel – Enseignante à Paris X et au CNAM – Auteur de « L'information et le renseignement par Internet » Que-sais-je - PUF

mots-clés : *INFLUENCE / E-REPUTATION / RÉSEAUX SOCIAUX / INTERCEPTION / FILTRAGE / CIA / NSA / CHINE / WIKILEAK*

Internet s'est révélé assez rapidement comme le média incontournable pour diffuser de l'information, qu'elle soit vraie ou fausse, au plus large public possible. Mais c'est entre 2009 et 2010 que nous avons pu prendre pleinement conscience de la portée de ce vecteur de rumeurs et de malveillances capable de faire une star d'une inconnue en moins d'une semaine (la vidéo de la chanteuse anglaise Susan Boyle a été vue par cent millions d'internautes en moins d'une semaine et a fait d'elle une star mondiale pendant quelque temps). Mais aussi de nuire, voire de pousser au suicide des personnes fragiles ou encore de déstabiliser des multinationales et d'ébranler des gouvernements.

1 Les agents d'influence

Réalisant alors que l'opinion de l'internaute lambda avait désormais pris le pouvoir sur l'avis des experts, les agents d'influence se sont infiltrés dans ce média pour orienter le mode de pensée de toute personne susceptible d'agir dans leur intérêt. Bien entendu, les professionnels du marketing ont été les premiers à saisir cette opportunité, suivis de très près par les *traders*, qui ont longtemps joué (et continuent d'ailleurs) à orienter les cours de la bourse en manipulant l'information concernant telle ou telle entreprise. Il est même arrivé que le cours d'une entreprise dévisse à cause d'une mauvaise interprétation d'un journaliste qui a ameuté la presse sur la base d'une information qui s'est révélée vieille de plus de 6 ans ! Cette mésaventure est arrivée à United Airlines qui, en 2008, a vu son action chuter en passant de 12,45 $ à 3 $ en quelques minutes. Tout cela par la faute du journaliste qui en effectuant des recherches sur Google est tombé sur une information du *Chicago Tribune* relatant la situation économique catastrophique de l'entreprise vouée à une faillite certaine. Après avoir alerté Bloomberg et l'ensemble des places boursières, 24 millions de titres ont été échangés en une dizaine de minutes. Pourtant, l'affaire remontait à 2002 et la compagnie aérienne avait survécu à la crise. Ce qui prouve la réactivité des marchés et de l'opinion toujours prête à suivre l'information fraîchement parue, surtout si elle a tendance à assombrir le paysage politique ou économique.

En fait, l'information est devenue aujourd'hui un flux torrentiel de données sur tous les sujets, de tous les avis et dans tous les sens. Les services secrets eux-mêmes ne parviennent plus à gérer ces tsunamis de datas dont il devient extrêmement compliqué de séparer le bon grain de l'ivraie **[1]**. Mais les gouvernements ayant compris l'intérêt de maîtriser ou plus précisément d'orienter l'opinion à travers les différents canaux ont commencé à mettre en place des réseaux d'agents qui se mobilisent pour interagir avec l'actualité dans le domaine concerné.

Les chinois l'auraient fait, peut-être maladroitement selon le journaliste Thomas Crampton **[2]**, mais ils seraient des précurseurs dans l'art de la manipulation de l'information. D'après son enquête, des *freelances* chinois seraient employés par le gouvernement pour guider les internautes vers une opinion favorable aux dirigeants de l'État **[3]**. Éparpillés sur la Toile, les « 50 cents agents », en référence à la rémunération de 50 centimes de Renmibis par commentaire, veilleraient sur les posts des internautes sur les différents blogs, forums ou réseaux sociaux et tenteraient de réorienter la discussion si celle-ci n'était pas favorable au parti. Depuis, le schéma a été largement reproduit et pratiquement tous les États, partis politiques ou religieux, activistes et ONG se lancent dans une forme de *lobbying* électronique pour fédérer les internautes et augmenter leur présence virtuelle et par là même leur influence. D'ailleurs ceci a incité Google à revoir son système de *page rank* **[4]** qui ne se fait non plus seulement en fonction du nombre de liens pointant vers une page, mais également selon la fraîcheur de

l'information. D'où une facilité à diriger les internautes dont les clics dépassent rarement la troisième page, vers des sites au contenu soigneusement sélectionné par les autorités ou tout autre groupe d'influence qui auront publié des textes choisis en fonction de leur orientation. Ces articles pourront être préparés à l'avance pour réagir sur une attaque de type fausse rumeur afin d'éditer le plus grand nombre de textes possible sur le plus de blogs et de pages Facebook, en créant aussi des groupes de fans, puis avec Twitter et ses milliers de suiveurs et ainsi de suite.

Les agents d'influence travaillent méthodiquement en exploitant le registre émotionnel et en ayant un discours évoluant du pacifisme vers une forme de radicalisme. Ils peuvent s'attaquer au logo d'une entreprise en le détournant par le travail de l'image avec des mises en situation ridicules ou tragiques comme à un pays ou à un parti politique. Il suffit pour s'en apercevoir de consulter les images référencées des entreprises les plus cotées ou de certains pays sur les moteurs de recherche. Les agents organisent des « Happening médiatiques » en diffusant des vidéos sur YouTube ou DailyMotion, certains films remportent un tel succès qu'ils sont parfois repris dans les journaux télévisés. Les plus populaires sont ceux qui font de la contre communication en détournant une vidéo publicitaire de la cible contre elle. Les propos sont anxiogènes pour le public qui a peur et reste hypnotisé par le film. L'ensemble étant relayé par Twitter et des groupes de fans sur Facebook pour démultiplier la diffusion de l'information.

Au niveau de l'impact, ceci peut avoir une atteinte durable à l'image, voire générer un boycott de l'organisation ou d'un pays, cela peut aussi dégénérer en actes d'agression sur le terrain. L'impact systémique est, lui, difficilement mesurable. Toutefois, une image globale d'insécurité et de corruption peut avoir une influence sur les actionnaires ou sur des négociations en cours. Toute la difficulté est alors la capacité à gérer la crise à temps et dans les termes qui conviennent.

2 Réseaux sociaux – les grands acteurs

Désormais incontournables en raison du flux qu'ils génèrent, les réseaux sociaux en 2011 sont par ordre d'importance, Facebook : 800 millions d'utilisateurs, Twitter : 200 millions, LinkedIn : 115 millions et Google Plus : 50 millions (en progression rapide et constante). Facebook génère plus de 200 milliards de « Like » et de commentaires par jour, 80 % des utilisateurs auraient adhéré à 80 communautés, groupes ou événements. Tandis que 82 % des internautes ont confiance dans l'information qu'ils lisent sur LinkedIn et 55 % des utilisateurs de Google+ seraient des américains **[5]**.

C'est ainsi qu'une unité spéciale de la CIA a recruté des analystes chargés de traiter les milliards de messages publiés chaque jour sur la Toile à la recherche de la moindre petite information qui laisserait supposer l'arrivée imminente d'une émeute, d'une révolution, d'un attentat. En arabe, en mandarin ou dans bien d'autres langues, ces employés scrutent le Web et croisent l'information avec la presse locale ou des écoutes téléphoniques clandestines pour la valider. Ils ont vu la montée de la colère en Egypte sans toutefois pouvoir obtenir une date précise de la révolte **[6]**. Ces centaines d'analystes (dont le nombre précis est classifié) travaillent sur toutes sortes de sujets, depuis l'accès Internet en Chine à l'ambiance qui règne dans les rues au Pakistan. Bien que majoritairement basés en Virginie, ils sont aussi à l'œuvre dans les ambassades pour être réellement immergés au cœur de l'actualité. Pour eux les données exploitables qui circulent sont sur Twitter et sur les réseaux sociaux. À la mort de Ben Laden, la CIA a pu informer la Maison Blanche des réactions de l'opinion mondiale en suivant les messages sur Twitter.

Ce système fonctionne si bien que l'administration Obama envisage de mettre le Web et surtout les réseaux sociaux sur écoute **[7]**. Selon le *New York Times*, une nouvelle loi s'apprêterait à voir le jour, autorisant l'interception de messages depuis tous supports de communication, dont Facebook, les messageries instantanées comme Msn, ou cryptées comme Skype, et aussi les BlackBerry. Cette loi obligerait tous les acteurs de la communication téléphonique ou par VoIP et messagerie écrite à s'équiper techniquement pour permettre aux services secrets (FBI, NSA, CIA) un accès complet aux conversations. Cette loi s'appliquerait également aux entreprises étrangères résidant aux États-Unis et aux développeurs de solutions comme Skype qui se verront imposer, sous peine de sanctions, la mise en place d'une porte dérobée. De là à imaginer que cela pourrait éventuellement servir d'autres intérêts, nous risquerions de frôler la paranoïa excessive. Ce qui est certain, c'est que les coûts générés par la mise en place de ces accès auront une répercussion significative sur les prix des opérateurs et des entreprises, et donc sur la croissance économique.

Mais sur la Toile, rien n'est unilatéral et les outils qui servent aux écoutes des uns servent aussi aux autres... Les internautes en mal de reconnaissance s'empressent de mettre en ligne tout ce qui les concerne, pour renforcer les liens familiaux selon eux. Les parents s'inscrivent sur Facebook pour avoir des nouvelles de leurs enfants en consultant leur mur.

Les plus sensibles sont les militaires, dont l'isolement et l'éloignement les incitent à communiquer à leurs proches leurs états d'âme, et bien souvent, ils se laissent aller à raconter des anecdotes vécues sur les théâtres d'opération, à publier des photos d'eux et de leurs camarades, et par conséquent, à divulguer des informations pouvant être utilisées par les forces ennemies. Ce fut notamment le cas pour les soldats britanniques en Grande-Bretagne, les canadiens et les américains qui furent souvent victimes de ces publications en Irak. Les organisations proches du mouvement Al-Qaïda collectaient ces données pour localiser les militaires et perpétrer des attentats. Marine Chatrenet a réalisé un rapport en 2008 pour le centre d'études en sciences sociales de la défense. Elle y dresse une typologie de ces journaux de bord qui, nourris de photos et vidéos, livrent des détails sur les camps, les manœuvres et les interventions militaires. « *Si les médias en OPEX – opérations extérieures – sont encadrés et ne peuvent pas tout filmer, les militaires, avec de simples appareils, ont une marge de manœuvre supérieure et surtout l'exclusivité de certaines images* », ceci grâce aux téléphones portables dont la définition augmente en même temps que la capacité de stockage et qui permettent d'illustrer des propos édités en ligne, souvent dans le plus parfait anonymat et sans aucun contrôle possible de l'armée.

Au Canada, le général de brigade Peter Atkinson a déclaré : « *Aujourd'hui, avec la vitesse de la technologie, nous fournissons quasi instantanément à l'ennemi le bilan des pertes lors des combats. Nous devons rendre l'effort de renseignement à l'adversaire aussi difficile que possible.* » Le brigadier général assure que 80 % des informations qu'obtiennent les talibans proviennent d'Internet. Début 2008, l'armée canadienne demandait à ses soldats de ne publier aucune photo, ni information personnelle sur les sites de réseaux sociaux en raison des risques avérés d'attentats.

La plupart des militaires inscrits sur des sites comme Facebook ont donc réduit les informations les concernant au maximum, mais après avoir réalisé un test, il s'avère que les personnes sélectionnées au hasard sont inscrites sur de nombreux autres sites et que l'on arrive à reconstituer des profils assez précis avec leurs photos, leurs emails, amis, famille et bien d'autres détails personnels. En février 2009, le ministère de la défense britannique a donc interdit aux soldats l'accès à tous les sites de réseaux sociaux (Facebook, MySpace), mais aussi aux blogs, et plus surprenant, aux sites de jeux en ligne. Une décision très mal perçue par les militaires qui se sont sentis à nouveau isolés et dont la majorité a décidé de ne pas obéir aux ordres.

Paradoxalement, les américains ont conçu un système Internet et de téléphonie parallèles pour aider les opposants victimes de régimes totalitaires à maintenir la communication avec l'étranger [8]. Un projet renforcé après les tentatives des États égyptien, tunisien, syrien, etc., de couper les moyens de transmission pour éviter que les mouvements populaires ne s'organisent en émeutes et ne puissent renverser les régimes en place. Internet dans une valise permettra ainsi de transporter et de déployer une infrastructure ultra légère qui pourra autoriser une communication sans fil reliée à la Toile et entièrement indépendante de tout opérateur local. Offrir une telle liberté d'expression est extrêmement louable, cependant ne serait-il pas tentant d'équiper le matériel de backdoors non pas pour être intrusif, mais pour avoir une vision en temps réel et donc bien avant le reste du monde des événements en cours dans un pays sensible ? Pourrait-on imaginer que cela aurait un impact sur les actions militaires et économiques ? Il serait bien difficile de résister à la tentation avec un ROI **[9]** d'à peine 50 millions de dollars US.

3 L'e-réputation

L'e-réputation serait selon IDC **[10]** une priorité sans moyen, les cibles se mettraient systématiquement en position défensive et à peine 23 % des entreprises surveillent ce que l'on dit d'elles sur Internet. Souvent laissée de côté, la gestion de la réputation numérique est pourtant fondamentale, Jeff Bezos, le PDG d'Amazon, affirmait que « si vous rendiez vos clients mécontents dans le monde réel, ils étaient susceptibles d'en parler à 6 de leurs amis, mais sur Internet ils pouvaient en parler à 6000 amis ». L'internaute est donc un producteur de contenu que ce soit par le relais d'une information ou l'ajout de commentaires, voire l'écriture de billets sur un blog ou un site collaboratif. À ce titre, il peut au gré de ses humeurs et du temps qu'il sera prêt à y consacrer, endommager sérieusement la réputation d'une personne physique ou morale ou l'encenser. Grâce aux flux RSS, il peut démultiplier la diffusion de ses billets et rendre sinon impossible, en tous cas très complexe, l'identification de la source originale par la victime ou les forces de l'ordre. À un niveau militaire, ce genre d'action peut sérieusement ternir l'image d'une intervention sur un théâtre d'opération et quasiment bloquer l'avancée des troupes par la population locale.

4 Le revers de la médaille (Wikileaks)

Les méthodes d'interception ou de filtrage ne suffisent pas à contrôler les individus. Dans un sursaut libertaire, Wikileaks a démontré que des citoyens pouvaient se dresser contre les États. En publiant les rapports secrets du département d'État américain, le site clandestin a voulu mettre un terme aux agissements militaires des États-Unis à l'étranger. En se proclamant citoyen du monde cherchant à informer la planète des conspirations de l'ennemi impérialiste, le site a aussi engendré des dommages collatéraux. Il est probable que de nombreuses personnes ont dû subir des interrogatoires musclés et des pressions suite aux révélations de Wikileaks. Les techniques de déstabilisation sont basées exactement sur ce même schéma. Wikileaks, en voulant faire le bien et éclairer la vision de l'opinion publique, a pu également révéler aux services de police de pays totalitaires l'identité (par croisement d'informations, les données de Wikileaks étant anonymisées) de personnes qui travaillaient pour les américains. Alors comment gérer et contrer les actions offensives sur Internet alors que les entreprises sont aujourd'hui encore très vulnérables du fait de leur communication lourde et inadaptée face à des attaques multiples et l'absence d'une culture stratégique comme d'analyse des flux médiatiques.

Sur le long terme, il faut avoir une approche éducative et faire comprendre les enjeux stratégiques en agissant sur la culture et l'identification à l'État et à la nation. Il est nécessaire d'informer et de sensibiliser, mais aussi d'impliquer les gens. Parallèlement, il est indispensable de pouvoir identifier la source d'une attaque d'e-réputation et de savoir la contrer avec une stratégie élaborée de contre information et de retournement. Comme il faut être capable d'évaluer les risques opérationnels et stratégiques pour mieux les appréhender lorsqu'ils apparaissent et conserver à l'esprit qu'il s'agit d'une guerre asymétrique permanente. ■

■ NOTES

[1] Entretien de l'auteur avec le MI6 en octobre 2010
[2] Thomas Crampton est un ancien correspondant du New York Times et de l'Herald Tribune
[3] Thomascrampton.com
[4] Système d'indexation de Google
[5] Source : onelily.com
[6] Source : Kimberly Dozier – AP Intelligence Writer
[7] Source : La Tribune
[8] Le New York Times du 12 juin 2011
[9] Return On Investment (retour sur investissement)
[10] Étude publiée en juillet 2011

INGÉNIERIE SOCIALE ET LEURRE SUR INTERNET PAR POTS DE MIEL

HONEYPOTS FOR COMPETITIVE SOCIAL ENGINEERING

Sébastien Chainay – sebastien.chainay@gmail.com

Consultant en sécurité de l'information et en intelligence économique pour Hapsis

mots-clés : *POT DE MIEL SOCIAL / POT DE MIEL INFORMATIONNEL / IDENTITÉ NUMÉRIQUE / BIAIS IDENTITAIRE / SPEAR PHISHING / WHALING / VEILLE CONCURRENTIELLE*

L'ingénierie sociale à but économique (ou competitive social engineering) est une catégorie bien particulière de social engineering qui a pour objectif de ne recueillir que des informations dont l'analyse et le traitement peuvent conduire à des renseignements de nature à obtenir un avantage concurrentiel. Elle intéresse donc les entreprises mais aussi les États, notamment pour les secteurs stratégiques que sont l'énergie, la défense, l'innovation dans les nouvelles technologies ou pour investir via des fonds souverains. Toutes les actions d'ingénierie sociale s'effectuant à partir de renseignements préalables de nature humaine ou électronique, l'objectif de cet article est de créer intentionnellement des leurres sur l'Internet pour influencer la concurrence, la désinformer et la déstabiliser.

Dans cet article, nous allons détailler ces concepts qui reposent tous sur une déclinaison des pots de miel informatiques.

Pour aboutir, l'ingénierie sociale à but économique se doit d'être ciblée : la cible privilégiée étant l'entreprise et plus particulièrement ses dirigeants ou ses membres stratégiques. Ainsi, soit le ciblage est nominatif à partir d'informations acquises (organigrammes, plannings, listings de clients ou de fournisseurs, contacts, ...), soit catégoriel en voulant attirer un profil bien particulier de cibles. Les techniques d'attaques ciblées sont multiples :

- Spear Phishing : *phishing* ciblé sur une catégorie de clientèle (critère financier généralement).
- Whaling :
  - ciblage sur réseaux sociaux ;
  - débauchage de ressources humaines stratégiques ;
  - ciblage de profils particuliers (gestionnaire de fonds, responsables de financement, ...) pour extorsion ;
  - approche d'employés pour renseignement économique.
- Cybersquatting : URL enregistrée par un pirate contenant le nom de l'entreprise ciblée.
- Typosquatting : URL enregistrée par un pirate contenant une orthographe approchante du nom de l'entreprise ciblée.
- Au téléphone :
  - usurpation d'identité pour duper un collaborateur de l'entreprise ;
  - service client ;
  - support...
- À l'oral :
  - intrusion physique (sécurité économique, habilitations) ;
  - infiltration (nouvel embauché, visiteur, agent, sous-traitant).

1 Les pots de miel informatiques : des outils de leurre

Le concept de pot de miel n'est pas nouveau en sécurité informatique.

En 1986, dans l'université de Californie où il occupe le poste d'administrateur système, Cliff Stoll se rend compte qu'un pirate attaque des systèmes militaires américains depuis son réseau. Avec son équipe, il crée alors de faux fichiers (que l'on peut apparenter à des pots de miel) ayant l'air d'appartenir à la *Strategic Defense Initiative* et qui semblent intéresser le pirate. Ils parviennent ainsi à gagner du temps pour localiser l'agresseur, qui opère depuis l'Allemagne de l'Est pour le compte du KGB, et à le faire arrêter par les autorités **[1]**.

Au début de l'année 1991, Bill Cheswick raconte dans un article célèbre **[2]** comment il a pu observer les activités d'un pirate en imitant quelques services classiques (FTP, Telnet, SMTP entre autres) sur une machine reliée à l'Internet.

Ainsi, un pot de miel est une ressource dont l'accès est volontairement non sécurisé pour observer les techniques d'attaques employées par un intrus de ce système à un moment donné. Son intérêt réside dans les enseignements qu'il apportera lors de son accès et de son exploitation illicite. Il peut donc aussi bien s'agir d'une machine que d'un pare-feu ou d'un point d'accès à l'Internet. Au sein d'une entreprise, les pots de miel peuvent être utilisés comme sondes pour détecter toute intrusion au sein d'un système, ce qui rapproche leur utilisation des systèmes de détection d'intrusions.

Un pot de miel peut aussi être vu comme un capteur d'activités de l'Internet, une sonde qui enregistre le trafic qui circule au travers d'elle. Il est donc possible avec un pot de miel d'observer en temps réel les tendances des méthodes d'attaques employées sur l'Internet (outils, tactiques) pour mieux anticiper les parades correspondantes : les projets Leurrécom **[3]** et Wombat **[4]** sont basés sur cette idée.

2 Transposition à la vie quotidienne : les pots de miel sociaux

Lorsque l'on veut surveiller les activités malveillantes à l'encontre d'une entreprise, l'aspect économique est également à prendre en compte. Ainsi, les réseaux sociaux constituent un endroit privilégié pour glaner des renseignements. En effet, les internautes y divulguent des informations qui concernent aussi bien l'individu (vie personnelle) que l'employé (vie professionnelle).

Pour l'entreprise, une vision défensive de cette situation serait de maîtriser le plus possible les informations divulguées par les parties prenantes de l'entreprise en faisant un audit puis en mettant en place un système de veille. Une sensibilisation régulière est également nécessaire.

Une vision offensive de l'entreprise serait, consciente de cette problématique, de rendre visible de faux profils contenant de fausses informations sur des profils d'employés inventées sur les réseaux sociaux. De tels comptes ainsi créés sont appelés pots de miel sociaux en référence aux pots de miel utilisés en sécurité informatique.

C'est ce concept de leurre que nous allons détailler.

2.1 Pot de miel social

Si les pots de miel informatiques émulent un programme, un système d'exploitation ou un serveur, les pots de miel sociaux désignent des profils factices créés manuellement sur les réseaux sociaux (compte Twitter, pages Facebook et Linkedin, ...) pour tromper les interlocuteurs. Éventuellement, des outils peuvent aider à automatiser certaines tâches : Facebookbot, Friendbot.

On caractérise communément un pot de miel selon son degré d'interaction avec l'intrus. L'interactivité augmente l'intérêt des informations collectées, mais aussi la difficulté de mise en œuvre et de maintenance ainsi que le danger de compromission du pot de miel.

À l'origine, les pots de miel sociaux sont destinés à l'étude des attaques informatiques sur les réseaux sociaux **[5]**. Websense a été la première entreprise à développer des pots de miel sociaux. Elle en a conçu de trois interactions différentes **[6]** :

- actif ou fortement interactif (répond aux sollicitations/invitations, émet du contenu, ...) ;
- semi-actif ou moyennement interactif (répond aux sollicitations/invitations, pas de contenu) ;
- passif ou faiblement interactif (en écoute simple, aucune réponse).

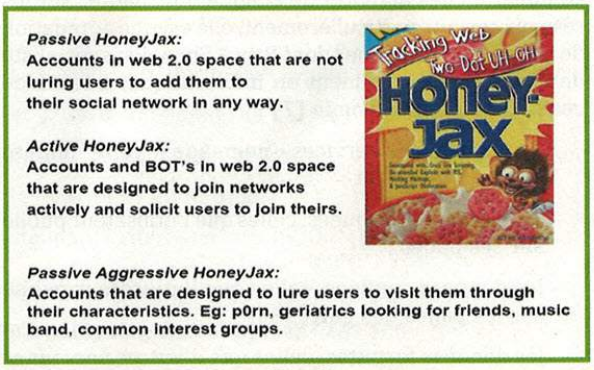


Fig. 1

Puis, créer un compte de réseau social est devenu un nouveau moyen pour recueillir des informations, l'internaute n'ayant pas forcément conscience de leur portée. Par exemple, en cas de perte d'un mot de passe, certains sites demandent une information de nature personnelle préalablement entrée par l'utilisateur pour l'authentifier : rue de son lieu de résidence, date de naissance, nom de jeune fille de son épouse ou de sa mère, chiffre préféré, ... Un faux profil de ce type, appelé pot de miel social, permet d'obtenir de la cible ces informations dès lors qu'il est astucieusement conçu (apparence physique, parcours professionnel, centres d'intérêt) pour gagner rapidement la confiance de ses interlocuteurs.

2.1.1 Infiltration de communautés sociales : ciblage catégoriel

Facebook (réseau social à but personnel), Viadeo (réseau social à but professionnel), Twitter (réseau social à but informationnel), les forums ou les blogs permettent de regrouper des profils d'utilisateurs autour de communautés partageant des idées, des expériences ou des centres d'intérêt.

Ces groupes constituent un premier moyen d'approche de leurs membres. Réciproquement, en sachant à quels groupes appartient une cible, il sera plus facile de trouver des critères d'adaptation du pot de miel social. Ces adaptations sont en fait des biais que l'on introduit dans le profil. Celles-ci doivent être correctement dosées pour que le pot de miel ne soit pas détecté.

2.1.2 Détection d'un pot de miel social : le contrôle des biais identitaires

Les biais identitaires (cf. annexe) doivent servir à rendre attractif le profil fictif créé en fonction du milieu que l'on veut infiltrer sur une ou plusieurs de ces caractéristiques. Celles-ci doivent contribuer à établir un lien de confiance rapide et durable avec ses interlocuteurs.

Ces biais doivent être maîtrisés, contrôlés. Comme nous venons de le voir, l'identité numérique est une compilation des activités de chaque internaute. Sur les réseaux sociaux particulièrement, elle est une agrégation de données hétérogènes dont Bruce Schneier, spécialiste de la sécurité notamment en informatique, a tenté de construire une taxonomie **[7]** :

- les données de services : nom, âge... voire numéro de carte de crédit ;
- les données divulguées, celles que l'utilisateur publie sur ses pages ;
- les données confiées, celles que l'utilisateur publie sur les pages des autres ;
- les données fortuites, celles que d'autres personnes publient à votre propos ;
- les données comportementales, celles qu'un site recueille sur vous en surveillant ce que vous faites et avec qui ;
- Les données dérivées, celles concernant l'utilisateur et issues des données présentées ci-dessus.

Ainsi, selon cette taxonomie, les données de services, confiées ou divulguées sont des informations qui échappent à tout contrôle de l'entreprise et forment autant de fuites pouvant être exploitées pour lancer une attaque informationnelle. Les entreprises françaises sont encore bien loin d'appréhender ce genre de problématique : elles devraient faire un état des lieux régulier de leur identité numérique par un audit informationnel. En conséquence, chaque internaute (qui est potentiellement un employé) doit contrôler ce qu'il voit et ce qu'il dit :

- En contrôlant la divulgation d'informations personnelles, l'internaute anticipe les risques d'exploitation.
- En contrôlant la cohérence de l'identité numérique d'inconnu cherchant à se connecter à son réseau social, l'internaute a une attitude pro-active de protection de son identité numérique.
- En contrôlant son propos, l'internaute maîtrise la partie de son identité numérique liée aux données de services, confiées ou divulguées.

3 Réseau de pots de miel sociaux : création d'une identité numérique fictive

L'identité numérique des internautes n'est pas un sujet nouveau. En France, c'est Frédéric Cavazza qui introduit le concept **[8]**. À l'époque, ce blogueur définit l'identité numérique d'un individu comme une agrégation « *de données formelles (coordonnées, certificats) et informelles (commentaires, notes, billets, photos) [...] ces bribes d'information composant une identité numérique plus globale qui caractérise un individu, sa personnalité, son entourage et ses habitudes* ».

L'objectif d'un réseau de pots de miel sociaux est de créer une identité numérique approximativement cohérente (compte Twitter, pages Facebook et Linkedin, ...).

La nature informationnelle des pots de miel sociaux fait de cet outil un moyen de recueillir des informations stratégiques voire confidentielles sur les concurrents. Pire, il peut également servir de support pour recueillir des informations personnelles, l'utilisateur n'ayant pas forcément conscience de leur portée. En effet, ces informations sont habituellement demandées sur certains sites internet lors de la récupération d'un mot de passe perdu, par exemple (Fig. 2).

Un exemple célèbre est celui de Robin Sage, du nom du faux profil qui a été créé par Thomas Ryan sur plusieurs

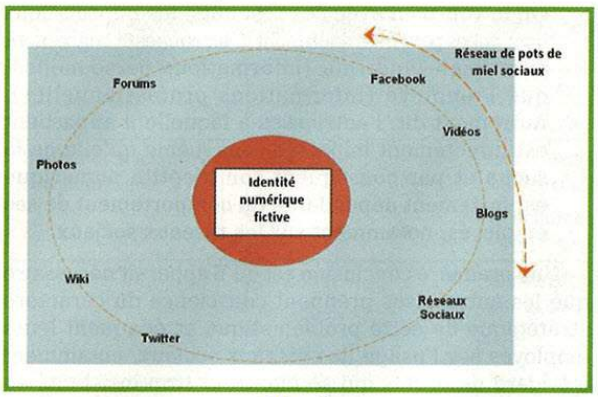


Fig. 2

réseaux sociaux pour infiltrer le milieu de la sécurité informatique et de l'armée américaine et recueillir des informations confidentielles **[9]**.

- **Exemple 1 : Le réseau de pots de miel sociaux Robin Sage créé par Thomas Ryan**

  Le profil Robin Sage **[10]**, nom emprunté d'un exercice de simulation pratiqué chez les militaires, est un exemple récent ayant touché le milieu de la sécurité informatique et de l'armée américaine. L'objectif du créateur était simple : créer une identité numérique artificielle au physique attractif dont la compilation des activités sur les réseaux sociaux (compte Twitter, pages Facebook et LinkedIn, ...) caractérise la personnalité approximativement cohérente d'une internaute. En effet, en mettant bout à bout nos actions sur ces sites, on peut aisément reconstituer nos habitudes, nos goûts, nos opinions, nos parcours (universitaire, professionnel)... bref, redessiner les traits de notre portrait numérique. Le but de Thomas Ryan – le créateur de la fausse identité – était de fabriquer une telle personnalité et de la rendre physiquement attractive pour que la méfiance suscitée auprès des internautes soit suffisamment réduite pour être acceptée comme « amie ».

  Ainsi, il ne faut pas être plus naïf dans ses relations sociales virtuelles que dans la vie réelle : si un(e) inconnu(e) vous aborde de manière trop insistante, c'est qu'elle a son propre intérêt. Dès lors, il s'agit de contrôler son discours, y compris sur l'Internet, et le meilleur moyen de prévention reste de ne pas accepter n'importe qui dans son réseau d'amis.

  Le cas Robin Sage met bien en exergue l'existence potentielle d'un biais entre l'identité numérique (virtuelle) et l'identité réelle, entre l'identité numérique souhaitée et celle transcrite sur l'Internet.

L'identité numérique biaisée créée est celle d'une jeune femme de 25 ans répartie sur trois réseaux sociaux (Twitter, Facebook, Linkedin) et un blog. Le profil représente une analyste en cybermenaces, un milieu essentiellement masculin. En effet, le but de son créateur est simple : créer une identité numérique artificielle au physique attractif pour mieux infiltrer le milieu et gagner rapidement la confiance de ses interlocuteurs. Le profil Robin Sage a été conçu pour créer des liens dans le milieu de la sécurité informatique et de l'armée américaine et a ainsi pu recueillir des adresses de courriel, mais aussi des numéros de comptes bancaires.

Le profil Robin Sage présente plusieurs incohérences : une jeune femme de 25 ans ne peut avoir 10 ans d'expérience dans le domaine des cybermenaces et une inspection des inscrits au MIT ne donne aucune personne nommée Robin Sage. D'autres signes peuvent éveiller les soupçons : un nombre restreint d'amis ou une seule image dans l'album du profil.

Il est à noter que le milieu du renseignement (FBI et CIA) est resté de marbre devant les charmes de cette pseudo-chercheuse en cybermenaces. En effet, les renseignements américains utilisant eux-mêmes **[11]** les réseaux sociaux comme source d'informations, certains détails **[12]** ont sans doute attiré l'attention.

Fig. 3

- Exemple 2 : Étude de BitDefender

Selon une étude réalisée par BitDefender **[13]**, 94 % des personnes à qui l'on a demandé d'être « ami » avec un profil, physiquement aussi avantageux que celui de Robin Sage, ont accepté la demande sans savoir qui était véritablement cette dernière.

- 10 % ont divulgué des informations personnelles sensibles : adresse, numéro de téléphone, nom des parents, ...
- 73 % des informations récoltées étaient des renseignements confidentiels concernant l'entreprise dans laquelle travaille l'utilisateur, tels que la stratégie de la société, des plans, ainsi que des informations sur des technologies ou des logiciels en cours de développement.

On le voit bien avec ces résultats, les informations divulguées par l'internaute sont hétérogènes et concernent aussi bien l'individu (informations personnelles) que l'employé (informations professionnelles). Autrement dit, l'entreprise à laquelle il appartient est directement impactée sans même qu'elle ne le sache et par conséquent son identité numérique est fortement dépendante du comportement de ses employés, notamment sur les réseaux sociaux.

Une première conclusion est qu'il apparaît nécessaire que les entreprises prennent conscience du caractère stratégique de cette problématique et éduquent leurs employés sur l'usage des réseaux sociaux, notamment à l'égard de profils qui se montrent trop insistants ou trop aimables.

3.1 Application à la veille concurrentielle : les réseaux de pots de miel sociaux pour le recueil de l'information stratégique

La nature informationnelle des pots de miel sociaux fait de cet outil un moyen de recueillir des informations stratégiques voire confidentielles sur les concurrents. Pire, il peut également servir de support pour recueillir des informations personnelles, l'utilisateur n'ayant pas forcément conscience de leur portée. En effet, ces informations sont habituellement demandées sur certains sites internet lors de la récupération d'un mot de passe perdu, par exemple.

Nous venons de le voir, bâtir un pot de miel social permet de récupérer de l'information confidentielle mais d'autres utilisations plus stratégiques sont envisageables pour l'entreprise, notamment dans le cadre d'un processus de veille et de prospective à plus ou moins long terme.

Prenons l'exemple des cabinets de conseil en informatique où la concurrence est forte. Le profil créé mettra en avant une employée ou une ingénieure d'affaires d'un cabinet de conseil concurrent, un client de ces cabinets de conseil, un CV, chacun ayant leur propre objectif de prise de renseignements.

De plus, des outils comme Facebook, les forums ou les blogs permettent aux internautes de se regrouper en communautés autour d'un thème, d'un intérêt commun et ainsi créer un lien de confiance sociale propice au recueil de témoignages.

Pour tromper la concurrence, de fausses traces informationnelles peuvent être créées : courriels, présentations, rapports, faux organigrammes et CV... (tableau 1).

On remarquera que les pots de miel sociaux sont souvent implantés sous forme de profils féminins. Cela s'explique par le fait que le pouvoir décisionnel se trouve entre des mains majoritairement masculines et que les cibles sont donc principalement des hommes.

Pot de miel social (profil fictif créé)	Composition de l'identité numérique	Renseignements sur la concurrence	Veille/ Prospective
CV	Sites de recrutement	Besoin sur une technologie ou un poste identifié	- RH/Économique - Court terme
Employée	LinkedIn	Débauchage de la part des concurrents	
Ingénieur d'affaires de la concurrence	Linkedin Facebook Twitter	- Obtention de réponses de la part de l'environnement économique du concurrent : partenaires, filiales, clients, fournisseurs - Recherche de partenariat sur un sujet dont l'actualité pourra être relayée via Twitter	- Commerciale - Moyen terme
Employée	LinkedIn Facebook Blog	Recueil de témoignages sur les conditions de travail pratiquées par la concurrence par la création d'un blog	- Sociale - Moyen terme
Client des cabinets de conseil	LinkedIn	Identification des concurrents répondant à un appel d'offres/ projet	- Commerciale - Long terme

Tableau 1

3.2 Application à la lutte contre le phishing ciblé (spear phishing)

Le modèle des pots de miel sociaux peut être étendu à la lutte contre le phishing contre une cible nominative aussi appelée *spear phishing* **[14]**. Pour cela, il suffit de faire « traîner » sur le Web une ou plusieurs adresses mail (phishing dans un courriel) ou numéros de téléphone portable (phishing dans un SMS), pour que ces dernières soient indexées par les moteurs de recherche et ainsi associées au nom désiré.

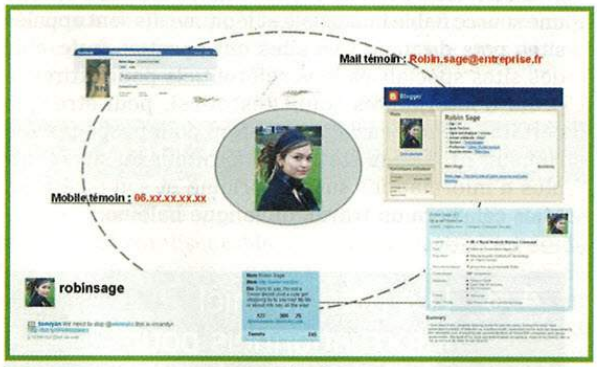


Fig. 4

4 Transposition à la vie professionnelle : les pots de miel informationnels

Pour les entreprises, l'objectif est de lutter contre l'ingénierie sociale à but économique (ou *competitive social engineering*) en créant intentionnellement de fausses informations sur des serveurs ou des sites internet pour influencer la concurrence, la désinformer voire la déstabiliser.

Nous appelons ce nouveau type de pots de miel des pots de miel informationnels.

4.1 Les pots de miel informationnels d'entreprise : ajouter un peu d'informations (fausses) dans vos serveurs

Pour tromper la concurrence, de fausses informations peuvent être créées : courriels, présentations, rapports, faux organigrammes et CV, ... En associant de tels systèmes informationnels avec un pot de miel informatique, il est potentiellement possible de savoir qui s'intéresse à quoi. Outre l'objectif de leurrer, l'intérêt est d'identifier qui s'intéresse à ce genre d'information et pénètre sur les pots de miel informationnels. Des analyses informatiques pourront être effectuées pour arriver à remonter à la source.

Selon la cible que l'on veut viser, il faudra placer le pot de miel différemment. Ainsi, en permettant l'accès de l'Internet, les concurrents auront plus de chances d'y accéder, tandis qu'en Intranet, les employés seront plus tentés. Dans l'Extranet, seuls les clients et les fournisseurs ont un accès.

Emplacement du pot de miel informationnel	Cible visée en priorité	Informations recherchées
Internet	Concurrents, pirates, États	Adresses mail, contacts, organigrammes, plannings, listings, informations économiques ou industrielles
Extranet	Clients, fournisseurs	
Intranet	Employés	

Tableau 2

AUTOUR DE L'ARTICLE...

▪ ANNEXE : IDENTITÉS NUMÉRIQUES BIAISÉES

Les biais identitaires doivent servir à rendre attractif le profil fictif créé en fonction du milieu que l'on veut infiltrer sur une ou plusieurs de ces caractéristiques. Celles-ci doivent contribuer à établir un lien de confiance rapide et durable avec leurs interlocuteurs.

L'introduction d'un biais dans une identité numérique peut être de plusieurs natures. Nous en distinguons trois : la déperdition, l'incohérence, la falsification.

BIAIS PAR DÉPERDITION

Rappelons que l'identité numérique est un concept qui s'applique aussi bien aux personnes et aux entreprises. Seulement, la problématique de la maîtrise de l'identité numérique est plus vaste pour les entreprises : elle est fortement dépendante de ses employés et de leurs conduites, notamment sur les réseaux sociaux.

Ainsi, les données de services, confiées ou divulguées (cf. section 2.1.2) sont des informations qui échappent à tout contrôle de l'entreprise.

Les entreprises en France sont encore bien loin de gérer ce genre de choses. Les plus grandes d'entre elles préfèrent se préoccuper de leur réputation électronique (car pouvant avoir des impacts marketing à court terme) plutôt que de faire un état des lieux régulier de leur identité numérique via un audit informationnel (cf. chapitre suivant). Car en termes d'image (et donc en termes de ventes), ces deux problématiques sont d'égale importance.

BIAIS PAR FALSIFICATION

La falsification désigne une identité qui n'est pas forcément celle qui est écrite. Plusieurs cas peuvent se présenter :

- **le vol : l'identité numérique virtuelle ne reflète pas l'identité réelle de l'émetteur mais une autre identité réelle existante ;**
- **le *cybersquatting* : l'identité est prise exprès (noms de sites internet) ;**
- **la fabulation : l'identité n'existe pas, elle est une totale invention.**

BIAIS PAR INCOHÉRENCE

Les profils présentant des contradictions dans leur identité numérique sont, par principe, à contrôler par tout internaute, pour s'assurer qu'il ne cache pas un biais par falsification dans le cadre de la création d'une identité numérique artificielle. Cela dit, il est à souligner que ces incohérences peuvent être involontaires de la part de son auteur. C'est le cas du réseau de pots de miel sociaux Robin Sage.

Si l'on ne veut pas perdre du temps à créer de vrais-faux documents, on peut se contenter de laisser des URL au nom évocateur en choisissant un nom de serveur et/ou de répertoire de documents approprié. Dans ce cas-là, le pot de miel peut être laissé sans document : seul l'accès sera intéressant à étudier. Il sera par conséquent faiblement informationnel car il ne contient au mieux qu'une arborescence, par opposition à un pot de miel nécessitant de vrais-faux documents dit fortement informationnel.

4.2 Les pots de miel informationnels pour détecter la crise

On vient de le voir, rendre plus ou moins visible un site s'effectue en utilisant les techniques de référencement SEO (*Search Engine Optimization*).

Outre cette technique basée sur l'audience, l'influence sur l'Internet peut aussi être une influence de cible : en effet, donner de la visibilité est une chose, mais donner la bonne visibilité en est une autre. Ainsi, pour aiguiller du trafic et attirer certains concurrents sur un pot de miel informationnel, il faut choisir les sites également en fonction de leur thème, leur expertise, leur notoriété : blog, forum, réseau social, site spécialisé, communautés sociales concernées, ...

De tels sites permettent de se faire connaître comme une source fiable impartiale et légitime. Ils sont appelés sites pots de miel. Ces sites ont vocation à devenir des sites spécialisés, des référentiels pour attirer le profil d'internautes souhaités. Ainsi, peut-être que certains d'entre eux s'en serviront pour propager une rumeur. Et si vous êtes administrateur du site, avoir plus d'informations sur son origine et son émetteur. Mais cela sera un travail de longue haleine...

4.3 Les pots de miel informationnels pour anticiper et scénariser la crise

4.3.1 Site de crise, site masqué

Il s'agit d'un site créé sur un thème très précis et qui sera uniquement publié en cas de crise ou d'attaque informationnelle sur ce thème. Cela permet à l'organisation de diffuser un message officiel non altéré par les médias ou les internautes. Il présente aussi l'avantage d'éviter d'engorger le site principal de l'organisation qui peut très bien avoir une partie consacrée au commerce en ligne.

Activer un site web suppose d'y avoir travaillé au préalable afin de savoir dans quel cas l'activer, et aussi quel contenu y mettre. Et surtout, faire connaître son adresse pendant la crise, ce qui implique des actions de communication :

- presse : interviews, communiqués ;
- Internet : indiquer l'adresse de ce site sur le site institutionnel ;
- moteurs de recherche : le référencement est un travail de longue haleine, il s'agit pour le site d'être indexé par les moteurs de recherche, or les robots d'indexation des moteurs de recherche visitent les sites de façon aléatoire ou selon leurs propres règles temporelles.

4.3.2 Forums

On peut aussi créer une notoriété de toute pièce en fabriquant entièrement un forum, par exemple, qui défend un point de vue avec toutes les techniques de référencement existant sur les moteurs web, images, vidéos, ... Un outil complémentaire pour une contre-influence en cas de désinformation, déstabilisation.

Il s'agit de bâtir toute une communauté participative fictive sur un support numérique entièrement prévu à cet effet (blog, forum) soit sur un support déjà existant (dans ce cas, il faudra s'interroger sur le support en fonction de la cible, de l'audience et de la visibilité sur les moteurs de recherche pour obtenir l'influence désirée). Les sujets abordés au sein de la communauté seront fonction des scénarios de crise préalablement établis pour rétablir l'identité numérique de l'entreprise dans le sens désiré.

Conclusion

D'un point de vue éthique, le concept de pot de miel social est discutable. À l'origine destiné à l'étude des attaques informatiques sur les réseaux sociaux, le développement de ces derniers a conduit à faire évoluer le concept vers un outil d'ingénierie sociale qui se définit en un principe : adapter le profil de l'émetteur pour obtenir ce que l'on veut du récepteur.

Ainsi, il est recommandé de ne pas se baser sur des données personnelles lors de la récupération de mots de passe, mais de se fonder sur des méthodes de vérification plus sûres. Ainsi, il existe des moyens de générer des mots de passe de manière unique. Par exemple, un symbole peut être associé aléatoire à chaque utilisateur, symbole qui servira à la composition d'un mot de passe de vérification lorsqu'il sera reproduit dans une grille faite de lettres, chiffres et signes de ponctuation.

Les exemples développés prouvent bien au plus crédule qu'une identité aussi numérique soit-elle se contrôle dès que l'on est sollicité sur l'Internet par une personne inconnue. Cela est valable pour les réseaux sociaux, mais aussi dans toutes situations de communication : courriels **[15]**, forums, chats, ...

Pour les entreprises, il sera difficile de couper tous les sites internet offrant ces moyens de communication. Outre un processus de sensibilisation **[16]** sur ces procédés d'ingénierie qu'il faut rendre obligatoire pour tous (des nouveaux arrivants aux VIP en passant par les sous-traitants), l'entreprise devra porter une attention particulière à la prévention d'une part et à la création d'outils internes de communication et de collaboration à usage professionnel sur le modèle du réseau social d'autre part, redistribuant le temps passé sur ces sites entre l'entreprise et le domicile et du même coup le type d'informations échangées. L'objectif est de recréer une frontière entre vie publique et vie privée en déplaçant les réflexes de communication sur les réseaux sociaux à but personnel vers les réseaux sociaux professionnels de l'entreprise. En résumé, combattre le feu par le feu. ■

NOTES

[1] Cliff Stoll (1988), The Cuckoo's Egg, ISBN 0743411463

[2] Bill Cheswick (1992), An evening with Berferd, AT&T Bell Laboratories

[3] www.leurrecom.org

[4] www.wombat-project.eu

[5] http://www.networkworld.com/news/2007/080507-defcon-websense-lures-web-20.html

[6] http://www.youtube.com/watch?v=fiFOAitV6GU

[7] http://www.schneier.com/essay-322.html

[8] http://www.fredcavazza.net/2006/10/22/qu-est-ce-que-l-identite-numerique/

[9] http://www.computerworld.com/s/article/9179507/Fake_i_femme_fatale_i_shows_social_network_risks

[10] http://www.gurumed.org/2010/07/08/comment-obtenir-des-informations-militaires-sensibles-via-les-rseaux-sociaux-o-lhistoire-dun-profil-facebook-trop-sage/

[11] http://owni.fr/2010/08/19/comment-la-cia-et-le-fbi-utilisent-les-reseaux-sociaux/

[12] http://www.generation-nt.com/securite-reseaux-sociaux-robin-sage-actualite-1057081.html

[13] http://www.malwarecity.com/fr/blog/les-reseaux-sociaux-et-lillusion-de-lanonymat-858.html

[14] http://fr.wikipedia.org/wiki/Spear_phishing

[15] http://www.networkworld.com/news/2010/043010-us-air-force-phishing-test.html

[16] Les services de l'État peuvent aider les PME françaises dans leurs démarches de sensibilisation, mais aussi d'investigation en cas d'incident.

MÉTHODOLOGIE D'AUDIT ET DE SÉCURISATION D'IMPRIMANTES MULTIFONCTIONS

Ary Kokos et Vincent Nguyen, Consultants Sécurité, Cabinet Solucom

mots-clés : IMPRIMANTE / FAX / AUDIT / MFP / HARDENING

Depuis quelques années, les imprimantes multifonctions (Multi Function Printer) ont beaucoup évolué en intégrant de nouvelles fonctionnalités : fax, stockage des données sur disque dur, serveur FTP, serveur mail, serveur web, partages réseau, etc.

La plupart des entreprises considèrent encore ces MFP comme un simple périphérique d'impression ou de reprographie, parfois dotés d'un media de stockage pouvant exposer des informations sensibles. Mais beaucoup ignorent qu'en réalité ils connectent un serveur, une boîte noire, souvent laissée dans sa configuration par défaut, à leurs réseaux et par lesquels transitent des informations souvent très sensibles.

L'audit de MFP est, de par la nature de ces périphériques, un sujet à la fois abondamment traité et à la fois mal connu. Toute la difficulté d'auditer et de sécuriser ce type de système vient de la dualité entre un système standard - un périphérique IP muni d'un disque dur interagissant via des protocoles standards - et l'aspect boîte noire, chaque modèle étant très spécifique.

Cet article est articulé en deux parties, la première traitant de l'audit et la deuxième partie de la sécurisation des MFP ; en gardant une approche duale, présentant à la fois les grands principes et des exemples précis.

1 Introduction

Les imprimantes multifonctions représentent aujourd'hui un environnement assez hétérogène, à base de NetBSD, VxWorks, Linux ou de Windows, rendant difficile la rédaction d'un guide d'audit et de durcissement standard et poussé.

Cette méthodologie vise avant tout à donner au lecteur les grands axes et points de contrôle dans le cadre d'un audit d'un écosystème MFP pouvant être hétérogène et complexe avec des ressources temporelles limitées ; plutôt que le test d'intrusion et la compromission complète d'un modèle donné (pour un tel cas, le lecteur peut se référer à un bel exemple de compromission d'une imprimante via une injection de commandes **[BH 2006 O'CONNOR] [NBS]**).

De même, la partie durcissement vise à donner les grands axes et clés de durcissement qui seront à décliner spécifiquement pour chaque modèle.

2 Audit

2.1 Check-list générale

Cette check-list présente des points de contrôle génériques et très classiques, qui sans être exhaustifs, permettent de se faire rapidement une idée du niveau de sécurité global. Une liste plus complète peut être obtenue en reprenant un à un les points de durcissement présentés en seconde partie de cet article.

Domaine	Points de contrôle
Contrat	- Les imprimantes ont-elles été achetées ou sont-elles louées ?
	- Une clause de confidentialité est-elle présente ?
	- Une clause d'auditabilité (bonus : autorisant à faire de la rétro-ingénierie) est-elle présente ?
	- Quelles sont les clauses spécifiques quant à la communication sans délai des vulnérabilités connues par le fournisseur ?
	- Quelles sont les conditions spécifiques de maintenance et de télémaintenance ?
	- Quelles sont les clauses relatives à l'envoi de statistiques au constructeur ?
	- Quelles sont les procédures de contrôle de cette maintenance ?
	- Des clauses spéciales de rétention des médias de stockage existent-elles en cas de maintenance ou en fin de contrat de location ?
Procédure d'installation et d'administration	- Une procédure d'installation est-elle documentée ? Quel est le durcissement prévu ? Le MFP est-il connecté au réseau avant d'avoir été durci ?
	- L'imprimante dispose-t-elle d'une adresse privée ou publique ?
	- Comment l'imprimante est-elle administrée (Web, Telnet, système centralisé, développement spécifique) ?
	- Comment les administrateurs s'authentifient-ils ? Comment les utilisateurs s'authentifient-ils (mot de passe, badge, carte à puce) ? Quel est le référentiel d'identité utilisé (interne, LDAP, AD) ?
	- Comment sont gérés les mots de passe et quelle est la procédure en cas de perte du mot de passe ? Où sont stockés les mots de passe ?
	- Quelle est la procédure de fin de vie (destruction, renvoi au fournisseur) ?
	- Les imprimantes sont-elles classifiées à différents niveaux ? À quel réseau sont-elles connectées ? Une télé-administration est-elle en place ?
Gestion des incidents	- Une procédure de gestion des incidents est-elle en place ?
Réseau	- Quelles sont les piles activées ? (TCP/IP v4/6, AppleTalk, IPX)
	- Comment le réseau est-il configuré ? (adresses fixes, DHCP)
	- Les imprimantes sont-elles dans un VLAN ou un sous-réseau spécifique ? Un filtrage interne via ACL/IP est-il en place ?
	- Le MFP est-il directement connecté au réseau PSTN ? Dispose-t-il de fonctionnalités Bluetooth ou Wi-Fi ?
	- Des restrictions d'accès spécifiques pour la copie/fax/sous-réseaux accessibles sont-elles en place ? Pour l'impression ? Pour l'administration ?
	- L'envoi des documents est-il chiffré ? Ce chiffrement est-il en place sur tous les canaux ? Un serveur d'impression est-il utilisé ?
Administration	- Les accès d'administration sont-ils chiffrés ? Si SNMP est utilisé, les noms des community ont-ils été changés ? SNMPv3 est-il utilisé ?
	- Les mots de passe de l'interface web, Telnet, snmp, disque dur, et jetdirect ont-il été changés (la modification d'un mot de passe sur l'interface web n'implique pas nécessairement le changement automatique des autres mots de passe) ?
	- Des certificats spécifiques ont-ils été mis en place sur les imprimantes ? Les paramètres des systèmes cryptographiques ont-ils été modifiés (longueur des clés, algorithmes, certificats émis par une PKI, etc.).
	- Le firmware est-il à jour ? Un processus de mise à jour régulier est-il en place ?
Médias	- Quels sont les médias de stockage utilisés (RAM, disque dur, SD) ? La fonction d'effacement sécurisé a-t-elle été activée ? Le chiffrement du disque a-t-il été activé ?
Fonction de stockage réseau, copie, fax, email	- Quelles sont les possibilités de stockage réseau disponibles (FTP, *share*, email, USB) ? Si des authentifiants sont utilisés, quels sont les comptes utilisés et comment les mots de passe sont-ils sauvegardés ?
	- Les protocoles d'impression ont-ils été limités au strict nécessaire (Jetdirect, LPD, IPP, FTP, SMB) ?
	- Lors du scan, copie d'un document ou l'envoi d'un fax, quelles sont les éléments conservés (logs contenant les numéros de téléphone, accusé d'envoi, copie des documents envoyés) ? Une fonction de type « reprint » est-elle accessible ?
Logging	- Quels sont les mécanismes de logging en place (accès utilisateurs, accès administrateur, fax, NFS, email) ? Les logs sont-ils externalisés, centralisés et corrélés ?
Autre	- Lorsqu'un technicien externe intervient sur une imprimante, celui-ci est-il accompagné par un employé ?
	- Sur les périmètres sensibles, les imprimantes sont-elles gérées par les moyens généraux, le service informatique ou le département sécurité ?
	- Les imprimantes traitant des données très sensibles sont-elles déconnectées du réseau (connexion USB locale uniquement) ?
	- Lors de la récupération d'un document, l'utilisateur doit-il utiliser un badge ou entrer un mot de passe ?

2.2 Audit avec accès physique

2.2.1 Interface intégrée

La première chose à faire une fois le modèle d'imprimante identifié est de se procurer le manuel d'administration et de sécurisation (parfois scotché dans une pochette derrière l'imprimante). La liste des éléments de durcissement possible, mais aussi des mots de passe par défaut, y sont décrits en général de façon très complète. Par exemple, sur de nombreux modèles RICOH, il est indiqué dans le manuel qu'il est possible de se connecter avec le compte supervisor pour resetter le mot de passe administrateur.

La seconde étape consiste en l'identification des mesures de restriction de l'accès physique (salle fermée à clé, cadenas empêchant l'ouverture du châssis, sceaux d'intégrité, vis spéciales, etc.) et comment la traçabilité est assurée (badge, caméra, etc.).

Il est également important d'évaluer comment les câbles réseaux sont posés (s'ils partent dans un renfoncement où il serait possible de placer un dispositif d'interception physique) et comment sont récupérés les documents (code ou badge). Au-delà de l'audit MFP, il est toujours utile de vérifier les processus de destruction des documents ainsi que le matériel en place (broyeur, etc.) et la réaction du personnel sur place si l'imprimante est démontée et ce sans qu'ils n'en aient été avertis.

Si l'interface d'administration est verrouillée, il est soit possible de tenter des mots de passe par défaut **[DEFPASSLIST]**, soit d'utiliser des fonctions de *recovery* spécifiques au système (comptes type *supervisor*, procédure de reset des mots de passe, redémarrage en mode recovery, etc.).

Une fois l'interface « débloquée », de nombreuses données sont accessibles, telles que le carnet d'adresses, les logs d'impression (contenant la liste des documents et souvent des logins), les logs d'envoi de fax, la configuration pouvant contenir des mots de passe, des documents scannés, la réimpression de documents, etc.

Certaines imprimantes peuvent être administrées via USB et un logiciel spécifique est souvent disponible sur le site de l'éditeur.

Fig. 1 : Exemple d'imprimante RICOH démontée. On distingue aisément le disque dur 3.5'' et la carte mère.

2.2.2 Périphériques de stockage

Selon les modèles, les MFP peuvent être équipés de différents supports de mémoire (disque dur, carte SD, etc.). Il est parfois possible de dumper le contenu de la NVRAM sur une carte SD (en général une fonctionnalité de sauvegarde ou utilisée par le support).

Sur les modèles que nous avons étudiés, les cartes SD servaient surtout de carte d'extension pour charger des modules supplémentaires. Souvent écrits en Java, des informations intéressantes pourraient être obtenues après décompilation **[I]**.

Les disques durs peuvent contenir des données telles que des documents scannés ou des fichiers temporaires. S'agissant en général de disque tout à fait standard, il est possible d'en réaliser une copie avec l'utilitaire `dd` ou `ddrescue` via un adaptateur USB puis de les inspecter avec *autopsy/sleuth kit* ou un *file carver* comme *photorec/foremost*.

Globalement, nous avons rencontré deux types de cas : soit des systèmes facilement lisibles comme sur des Kyocera, mais aucun fichier intéressant n'était contenu sur le disque, soit des systèmes utilisant un format spécifique (a priori un système de fichier particulier faisant appel à un algorithme de compression propre au constructeur). C'est le cas de nombreuses imprimantes RICOH. Dans ce dernier cas, le peu d'informations que nous avions pu obtenir (et datant de 2008) étaient que la « table d'allocation des secteurs disques est embarquée sur la carte mère ». Une autre information contradictoire et très ancienne (2006) indiquait « Les principes de sécurité de base : les informations de gestion des pages (table d'allocation) et les documents sont stockés sur le disque dur dans un format propriétaire RICOH (codage et compression). Ces informations ne sont pas effacées après l'impression du document, après extinction de la machine ou coupure de courant [...] Cet algorithme n'est pas diffusé. ». **[RICOH LB]**

Récupérer un document dans le cas où un codage propre au constructeur est utilisé ne nous semble pas trivial et nécessite soit une coopération de la part de ce dernier, soit d'avoir recours à de la rétro-ingénierie.

2.3 Audit avec un accès réseau

2.3.1 Identification de l'imprimante

La méthode la plus simple pour identifier une imprimante consiste à effectuer un scan réseau en se basant sur les ports ouverts (en général les ports Jetdirect/9100, IPP, des interfaces web), les *banners* renvoyées (Jetdirect, RICOH, Xerox, etc.) et les adresses MAC (nmap est très doué pour ça). L'utilisation d'un scanner SNMP comme Foundstone SNSCAN peut être intéressant, de même que la fonction « discovery » des outils d'administration centralisée comme JetAdmin (HP).

Avec un accès à un poste standard d'un utilisateur du domaine, il est soit possible de lister les imprimantes installées, soit d'accéder à la liste des imprimantes sur un share (la procédure d'aide du master contient souvent l'emplacement dans la partie « mon imprimante a disparu » ou en scannant le réseau Windows).

2.3.2 Exploitation des services réseau

2.3.2.1 Telnet

Une interface d'administration est souvent disponible sur ce port et permet d'accéder à la plupart des paramètres de configuration également accessibles via l'interface web.

Si l'interface web a été verrouillée, l'interface Telnet est souvent un point d'entrée : sur de nombreux modèles, le mot de passe défini sur l'interface web n'est pas automatiquement appliqué à cette interface.

Il arrive également que des administrateurs définissent des ACL (par IP) pour filtrer l'accès à l'interface web, mais celles-ci ne s'appliquent pas toujours sur l'interface Telnet. Par exemple, sur certains modèles RICOH, il est possible d'ajouter une ACL pour permettre l'administration via la commande `access <n° ACL> range <IP début> <IP fin>`, il faut lister les ACL libres via la commande `access range`.

Il est bien évidemment possible de récupérer le mot de passe administrateur par écoute au niveau réseau (par exemple en déclenchant un « incident » : via un MITM, bloquer le port 9100, SNMP et l'interface web tout en laissant l'imprimante répondre aux requêtes ICMP et accessible via Telnet).

2.3.2.2 FTP

Le service FTP permet en général l'impression anonyme de documents ; certains modèles permettent aussi d'obtenir des informations par ce biais. Sur de nombreux modèles RICOH, les fichiers help, info (informations génériques), prnlog (log des impressions récentes), stat et syslog sont accessibles par ce biais.

2.3.2.3 HTTP(S)

L'interface utilisateur et l'interface d'administration sont en général accessibles via le même port. Selon les modèles, il convient d'inspecter les possibilités offertes, en particulier si des scans des documents sont accessibles ou si des authentifiants ont été pré-enregistrés (parfois présents en clair dans le code source de la page ! **[PRINTER TO PWND]**). Des logs d'impression, de fax (en particulier les accusés d'envois) sont souvent accessibles. Il nous est arrivé de retrouver des années de correspondance fax en quelques clics sur l'interface.

Il est toujours intéressant d'auditer l'application web afin de chercher des vulnérabilités classiques (type XSS **[2]**, CSRF, auth bypass, etc.).

Une présentation à la *Shmoocon* 2011 **[PRINTER TO PWND]** présente quelques vulnérabilités intéressantes : des *auth bypass* (l'ajout de &page=faxaddr sur certains modèles HP Officejet permet de bypasser l'authentification ; sur certains modèles de Canon ImageRUNNER, la modification du ACL=1 permet de bypasser l'authentification ; sur certains modèles Xerox, il est possible de faire un clone via http://target:8080/cloning.dlm et d'y accéder) et la présence dans certains cas de mots de passe présents en clair dans le code source de la page.

2.3.2.4 SNMP

La vérification est très classique, dans la mesure où il faut tenter d'accéder aux données avec SNMP walk (snmpwalk -v 1 -c public <IP>) ; si la communauté a été changée, tenter un bruteforce **[3]** avec des outils comme Snmpbrute ou ADMsnmp.

Sur certains modèles **[4]**, il est possible de récupérer le mot de passe via SNMP et de le modifier. **[5] [IRONGEEK]**

2.3.2.5 Jetdirect

Le protocole JetDirect (via des « commandes » PJL - *Printer Job Langage*) est particulièrement intéressant dans la mesure où il permet au-delà de l'impression directe de documents, d'accéder à un grand nombre de variables internes (accès aux objets PML *over jetdirect*, équivalent dans de nombreux cas à du SNMP en lecture/écriture via *jetdirect*, même si le port SNMP est filtré) et aux disques.

Ces commandes peuvent être envoyées via un simple client Telnet (le lecteur peut se référer au document de référence des commandes JetDirect **[PJL REF]**).

Des outils plus conviviaux existent, comme Hijetter ou PFT de Phenoelit **[Phenoelit]** ou PrintFS **[WILD]**. Les sources de Hijetter et de PFT étant disponibles, il est possible d'y récupérer directement les commandes les plus intéressantes (voir `libPJL-1.3-src\commands.h`).

Il est à noter que Hijitter permet de changer le message sur l'écran de nombreuses imprimantes (inutile, mais l'effet de communication dans un rapport ou en réunion est toujours bon ;)). **[6]**

Selon les modèles, il est possible de récupérer les fichiers d'impression, des fax, des logs de fax, des scans ou des codes PIN utilisés pour les impressions « sécurisées ».

D'autres modèles sont vulnérables à un *path traversal over* PJL. Par exemple, la CVE 2010-4107, via une requête PJL **[PJL TR]**, permet d'accéder au système de fichiers de nombreuses imprimantes HP Laserjet MFP printer, HP Color LaserJet MFP printer, Laserjet 4100 series, 4200 series, 4300 series, 5100 series, 8150 series, et 9000 series.

```
$ python -c 'print "\x1b%-12345X () PJL FSDIRLIST NAME=\"0:\\..\\..\\..\\" \
ENTRY=1 COUNT=999999\x0d\x0a\x1b%-12345X\x0d\x0a"' | nc 192.168.0.1 9100
```

Parfois, un mot de passe PJL peut être défini pour restreindre les possibilités d'exécution de commandes PJL par des utilisateurs non autorisés. Il s'agit en général d'un nombre entre 1 et 65535 et un mécanisme antibruteforce est rarement implémenté (pypjlpass permet de faire une attaque par bruteforce **[WILD]**).

Il est également possible d'envoyer des fichiers sur le disque (en RAM ou sur un disque dur) et d'utiliser le MFP comme un media de stockage réseau discret ; ou si le répertoire du serveur web est accessible en écriture, de mettre une page piégée (avec une grande variété de vecteurs : XSS, une iframe vers un *beef/yokoso!*, une iframe vers un *browser autopwn*, etc.).

L'outil d'administration centralisé Jetadmin permet souvent d'accéder à plus de fonctionnalités que celles proposées via l'interface web.

2.3.2.6 Autres services

D'autres services d'impression comme LPD (TCP/515) ou IPP (TCP/631) peuvent être exploités.

Selon les modèles, le port RSH (TCP/514) permet l'impression de documents et l'accès aux logs.

Enfin, sur certains modèles, un *daemon* SMTP ou SMB (utilisé principalement pour le dépôt de fichiers pour impression et la récupération de documents scannés) voire VoIP peut être présent.

2.4 Éléments spécifiques

2.4.1 Vulnérabilités liées aux interfaces d'administration et compromission des MFP

2.4.1.1 Backdoor matérielle

Un MFP est une cachette idéale pour la mise en place d'une *backdoor* physique, celle-ci est d'autant plus discrète que l'alimentation ne nécessite ni batterie ni prise supplémentaire et qu'un système embarqué de la taille d'un Gumstix peut facilement passer inaperçu lors d'une maintenance standard.

Un tel système peut soit être utilisé pour écouter le trafic réseau et donc obtenir une copie des documents, soit comme point d'entrée sur le réseau. On peut imaginer l'utilisation d'une interface Wi-Fi ou 3G pour le canal de C&C et l'exfiltration de données.

2.4.1.2 Backdoor logicielle

Bien sûr, un attaquant peut également mettre en place une backdoor logicielle pour remplir les mêmes objectifs que la backdoor matérielle. La facilité de mise en place d'un tel système diffère grandement d'un système à un autre, mais il n'est pas forcément nécessaire d'écrire un *rootkit* NetBSD très poussé alors que parfois une simple option de configuration permet d'obtenir des informations intéressantes.

C'est par exemple le cas de certaines imprimantes équipées de *pcounter* utilisées en mode *scan & share*, sur lesquelles il est possible de configurer via une seconde interface d'administration (sur un port obscur) la possibilité d'adresser une copie de tous les documents scannés et/ou faxés vers une adresse mail. Cette interface étant spécifique à un produit et peu documentée, elle est souvent ignorée des administrateurs systèmes et est accessible avec un mot de passe par défaut.

D'autres modèles permettent de déployer des *applets* Java, ce qui bien que nécessitant des connaissances spécifiques à l'environnement cible permet à un attaquant de développer des applications spécifiques pour une plateforme donnée, voir les travaux de Phoenoelit à ce sujet (ChaiCrack et ChaiPortScan **[Phenoelit]**).

2.4.1.3 Rebond depuis l'imprimante

De nombreuses imprimantes ayant leur *IP fragmentation ID* prédictible, il est possible de les utiliser comme rebond (« Zombie ») avec nmap (-sI) afin de contourner certains mécanismes de filtrage réseau ou de rendre plus difficile à tracer l'origine d'un scan (un IDS identifiera l'imprimante comme source du scan). **[nmap]**

2.4.1.4 File d'attente et postes locaux

La file d'attente partagée permet d'obtenir des informations sur les documents en cours d'impression.

Sur un poste Windows (XP), les fichiers temporaires d'impression sont stockés dans `C:\Documents and Settings\UTILISATEUR\Local Settings\Temp`.

2.4.1.5 Vulnérabilités interactions avec le SI

Les MFP étant souvent interconnectées au SI pour répondre au besoin utilisateur, une double vulnérabilité est présente : celle liée à la transmission des données et celle liée aux comptes utilisés pour déposer les données.

L'interception des données envoyées entre l'imprimante et les cibles (FTP, Share Windows, Webdav, etc.) peut se réaliser avec Ettercap (pour le MITM) et Wireshark, par exemple. Dans le cas d'un fichier déposé over SMB, le lecteur peut utiliser un patch qui permet d'exporter trivialement les fichiers d'une capture à partir de Wireshark **[TADDONG]**.

Il est très rare que les données soient chiffrées. Les seuls cas que nous avons rencontrés étaient ceux liés à l'utilisation d'une solution centralisée d'impression où les flux étaient chiffrés over SSL entre le client et le serveur central d'impression, mais pas entre le serveur central et l'imprimante elle-même. Il est alors possible d'effectuer un MITM entre le switch/routeur local et l'imprimante afin de récupérer les données.

Cette dernière attaque pouvant rapidement se révéler être limitée à une cible locale, il est beaucoup plus intéressant de récupérer les authentifiants utilisés, soit via une écouté réseau, soit directement sur l'imprimante dans les paramètres de configuration.

Lorsque des badges ne sont pas utilisés pour identifier l'utilisateur (ou lorsque l'implémentation du badge est mal conçue), afin que l'utilisateur n'ait pas à entrer son mot de passe sur l'interface locale, un compte générique aux droits étendus est utilisé.

Une fois ce compte compromis, il permet en général d'accéder à tous les répertoires des utilisateurs en lecture/écriture. Parfois, un compte administrateur est utilisé (souvent dans le cas de *share* Windows), ce qui permet de prendre la main sur le serveur cible et dans certains cas de rebondir sur le domaine (soit via la compromission d'un compte administrateur local **[7]** dont le mot de passe est réutilisé sur tous les serveurs du domaine, soit via le dump des hashs LM/NT d'autres utilisateurs, qui avec un peu de chance ou en rebondissant sur les bons serveurs peuvent se retrouver être un administrateur de domaine).

Mis à part les comptes utilisés pour le dépôt de fichiers, il est courant de rencontrer des authentifiants pour des serveurs mails ou des serveurs LDAP.

Durant la *Shmoocon* 2011, Deral Heiland et Pete Arzamendi ont présenté quatre cas intéressants de rebond sur le SI environnant à partir d'un MFP, les deux cas suivants sont en particulier intéressants :

- (Facilitation d'attaque) Récupération de noms d'utilisateurs valides depuis les logs d'impression puis bruteforce des mots de passe associés avec Medusa, identification d'un compte disposant d'un mot de passe faible, puis rebond sur des postes de travail et des serveurs ; récupération token d'admin de domaine encore valide sur un système.
- Récupération de credentials valides dans l'interface de configuration de l'imprimante permettant un accès en lecture/écriture dans le share utilisé pour déposer les scans ainsi que des documents sensibles (informations RH entre autres).

2.4.1.6 Systèmes de gestion centralisée

Les systèmes de gestion centralisée que nous avons rencontrés se présentaient sous la forme d'interfaces web collectant des statistiques via SNMPv2 et permettant à l'administrateur de se connecter sur les machines via un lien sur l'interface web.

2.4.1.7 Interception et rejeu des jobs

La plupart des infrastructures d'impression utilisent des canaux non sécurisés pour effectuer les demandes d'impression. Le format PCL (*Printer Command Language*) est très souvent utilisé : ce langage de description de pages étant un standard de l'industrie.

Ainsi, il est possible de récupérer l'ensemble du contenu par écoute réseau, la première consiste à intercepter le flux, par exemple avec Ettercap, en effectuant un MITM entre l'imprimante cible et la passerelle par défaut :

```
ettercap -q -w data.dump -T -M arp /ip_passerelle/ /ip_imprimante_cible/
```

L'objectif étant d'écouter le trafic réseau tant que des documents sont envoyés pour impression à notre imprimante cible.

Ce trafic est stocké dans le fichier **data.dump**, que nous analysons ensuite via Wireshark.

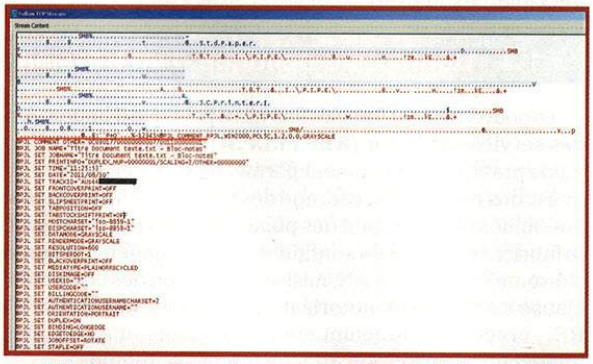


Fig. 2 : Analyse des trames PCL via Wireshark

Une fois le code PCL identifié, il est possible de le sauvegarder dans un fichier et de l'ouvrir avec un outil comme PCL Reader **[PCL READER]**.

Si le format n'est pas facilement lisible, il est toujours possible de rejouer le code enregistré (rejeu réseau ou envoi sur le port FTP).

2.4.1.8 Impression anonyme

De nombreuses imprimantes permettent l'impression directe de documents soit à partir de l'interface web, soit par envoi du fichier sur le serveur FTP/SMB/Jetdirect. Dans ces cas, l'utilisateur est rarement authentifié et l'impression apparaît comme « anonyme » dans les logs. Outre le banal contournement d'une politique de quota, cela pourrait permettre d'exfiltrer des documents en minimisant les traces laissées.

2.4.1.9 Impression « sécurisée »

Certaines imprimantes permettent une impression dite sécurisée : l'utilisateur doit entrer un code PIN sur l'imprimante pour récupérer son document. Ce code PIN ne permet pas en général de chiffrer le document envoyé pour impression. Il ne protège que la récupération du job sur l'imprimante et une écoute réseau permet bien souvent la récupération du document, du nom de l'utilisateur et du code PIN.

Une tentative de récupération d'un document « protégé » de la sorte sur une imprimante HP LaserJet 5550, en récupérant directement le fichier de job via jetdirect (par exemple avec Hijitter) ont systématiquement mis fin à la connexion. Cependant, il est possible de récupérer le code PIN (avec le nom du l'utilisateur et le nom du job) via ces mêmes fonctions en téléchargeant le fichier « Savedevice → SavedJobs → Keepjob → Stored job → JobmgrJobInfo ». Sur la figure 3, on voit le code PIN à côté du nom de l'utilisateur. Avec ce code, il est par exemple possible d'imprimer le document tout en le laissant en mémoire afin que l'utilisateur ne se rende pas compte qu'une copie a été établie.

Fig. 3 : Récupération du code PIN d'une tache « protégée » (accès au filesystem avec Hijitter)

2.4.1.10 Fuite d'information

Il est important d'évaluer les possibilités de fuite d'information présentées par le MFP aussi bien que d'intrusion dans le réseau.

Bien que plus rare de nos jours, certaines imprimantes (principalement des fax) utilisent des rouleaux qui contiennent, une fois utilisés, le négatif de tous les documents transmis.

Une exfiltration de données peut être réalisée via le relais SMTP configuré dans l'imprimante (pour les fonctions *scan to mail*).

Une imprimante connectée sur un réseau IP enclavé (isolée d'Internet) mais interconnectée au réseau PSTN via l'interface téléphonique ou fax peut être utilisée comme pont entre les deux réseaux soit pour l'exfiltration de données, soit comme point d'entrée via l'interface de télémaintenance. **[BA CERTA 2011-03] [AU DOD DSD INFOSEC MAN]**

Dans le cas de télécopieurs utilisés à la fois sur des réseaux « sensibles » et « non sensibles », il convient de vérifier qu'un mode « retransmission automatique en cas d'échec » n'est pas actif. En effet, si le télécopieur est connecté par erreur au réseau PSTN, il peut tenter de retransmettre les données en clair (dans le cas d'un chiffreur externe).

Les informations sur les « statistiques » d'utilisation des imprimantes ou pour la commande automatique des cartouches peuvent représenter une fuite d'information **[8]** tout comme les informations stockées sur les puces de certaines cartouches.

2.4.1.11 Télémaintenance

De nombreux MFP disposent d'un système de télémaintenance à la fois sur l'interface Ethernet mais également sur les interfaces téléphone et fax.

Si d'après les constructeurs elles ne permettent que de modifier certains paramètres du fax (encodage, vitesse de transmission, etc.) et de récupérer quelques informations sur le copieur (état des cartouches, état interne, etc.), il est très difficile d'estimer le risque potentiel lié à ces interfaces (i.e. si elles permettent d'obtenir un *remote root*). À défaut de pouvoir mener une étude par rétro-ingénierie poussée (coûteuse et illégale dans de nombreux pays), la plus grande prudence doit être de mise quant à la connexion d'un MFP au réseau PSTN [DCSSI] [SANS RICOH 450E] [BA CERTA 2011-03].

Nous n'aborderons pas ici le cas de la télémaintenance over IP qui, bien souvent, se fait soit via l'interface web, SNMP ou des mécanismes spécifiques au constructeur (comme JetDirect) et qui permet dans la majeure partie des cas de prendre complètement le contrôle sur le système **[9]**.

2.4.1.12 DOS

Un déni de service peut être réalisé via l'envoi d'un nombre très important de documents à imprimer sur tout le réseau (par exemple à un `ncat /dev/random` sur le port 9100).

2.4.1.13 Détournement des supports d'impression (papier spécial, chèques de paie, etc.)

Outre les aspects purement liés à l'imprimante en soi, il est important de vérifier les mesures mises en place pour assurer le contrôle d'accès et la traçabilité de supports d'impression spéciaux (papier spécial, chèque de paie, etc.) pouvant se trouver à proximité de l'imprimante.

2.4.1.14 Tracking code

Bien que ceci ne concerne pas directement l'audit d'un MFP, rappelons au lecteur que l'EFF a publié un certain nombre de documents relatifs à un code d'identification imprimé sur chaque page par certaines imprimantes afin d'assurer la traçabilité d'un document (par exemple sous forme de minuscules points jaunes). Voir les ressources de l'EFF **[EFF 1]** et une liste non exhaustive de modèles imprimant ou non ces « points » **[EFF 2]**. Des RFID peuvent également être utilisées pour le tracking de documents.

3 Éléments de durcissement

Comme nous venons de le présenter, il existe de nombreux vecteurs d'attaque différents. Dans la suite de cet article, nous proposons un ensemble de mesures organisationnelles et techniques dans le but d'augmenter le niveau de sécurité de l'infrastructure d'impression.

Un écosystème MFP étant hétérogène, nous nous limiterons à donner les grands axes et clés de durcissement, ces éléments devront être déclinés spécifiquement pour chaque modèle.

3.1 Éléments de sécurité opérationnelle

En premier lieu, un cadre organisationnel doit être mis en place pour favoriser une utilisation sécurisée des imprimantes multifonctions.

3.1.1 Définir une politique d'impression

Le gouvernement français fournit sa politique d'impression des services de l'État **[REF M.I.F.A]**. Sous la forme d'un guide pratique, ce document permet de se poser les bonnes questions relatives au cadrage des solutions d'impression, notamment en discutant des points suivants : contrat avec le fabricant, clause de confidentialité, engagement sur le cloisonnement RTC/LAN, mise à disposition des correctifs, clause de fin de vie, autorisation de mener des audit/PT/RE, procédure de maintenance, accompagnement des techniciens/attribution de mots de passe temporaires.

Ce guide rappelle, entre autres, que pour mener à bien un projet visant à refondre l'infrastructure et l'organisation de gestion des impressions, il est nécessaire d'impliquer les responsables hiérarchiques de haut niveau.

3.1.2 Responsabiliser les utilisateurs

« La plus grande menace du Système d'Information, c'est son utilisateur ». Le cas des MFP ne déroge pas à la règle... Qui abandonne (lâchement) ses documents ? Qui laisse les scans de ses fiches de paies sur le serveur de document de la multifonction de l'étage ? C'est encore et toujours cet irréductible utilisateur... La raison principale est que, bien souvent, il ne sait pas comment éviter certains risques. De plus, il considère en général les MFP comme une ressource interne de l'entreprise complètement maîtrisée et ne se pose jamais la question de la sécurité, de la confidentialité des documents imprimés.

En premier lieu, il est ainsi nécessaire de mener des actions de sensibilisation. Du poster affiché devant l'imprimante au « faux vol » de documents imprimés, les idées sont nombreuses pour intégrer la sécurité dans la culture d'entreprise. **[ANSSI SENSIBILISATION]**

Puis, il convient de sécuriser l'accès au document en « forçant » l'utilisateur à être présent lors de l'impression. Presque tous les constructeurs d'imprimantes multifonctions intègrent des options d'impression « sécurisée » : il s'agit de spécifier un nom de tâche et un code PIN permettant de verrouiller la tâche sur l'imprimante. L'utilisateur doit alors se rendre physiquement sur l'imprimante pour déverrouiller la tâche d'impression. D'autres solutions permettent de mettre en place une infrastructure à badge : les tâches d'impression ne s'exécutent qu'à partir du moment où l'utilisateur valide son badge sur l'imprimante.

3.1.3 Audit régulier

Les imprimantes multifonctions doivent être considérées comme un nouvel actif informatique dans le SI. Ainsi, il est nécessaire de réaliser des audits réguliers pour en vérifier la conformité de la configuration et le niveau de sécurité global de l'infrastructure d'impression.

3.1.4 Veille sécurité et patch management

Il est également nécessaire de prendre en compte la sécurité dès les phases en amont des projets de déploiement d'imprimantes.

L'utilisation de ces systèmes et applications « on the shelf » (basés par exemple sur des NetBSD, Linux embarqués avec des applicatifs type Samba, Tomcat, etc.) augmente la surface d'attaque possible pour les individus malveillants. Ces actifs logiciels doivent être intégrés aux différents processus sécurité de l'entreprise, et en particulier à la veille sécurité et au patch management.

3.2 Durcissement technique

Les mesures de sécurité organisationnelles présentées ci-dessus sont des actions d'envergure s'inscrivant dans une démarche globale de sécurité pour l'entreprise.

Des actions techniques rapides et pragmatiques peuvent également être réalisées pour durcir le niveau de sécurité.

Suite à l'expression des besoins de sécurité, il est nécessaire de formaliser une procédure d'installation explicitant l'activation et la configuration des différentes options de sécurité. Cette procédure doit être applicable « off line », c'est-à-dire que l'imprimante n'est reliée au réseau de l'entreprise qu'une fois configurée.

En règle générale, on trouve deux types d'infrastructures d'impression dans les grandes entreprises :

1. Infrastructure décentralisée où tous les postes de travail ont toutes les imprimantes de l'entreprise installées.

   La surface d'attaque est très importante : toutes les imprimantes multifonctions sont accessibles, et très souvent elles n'ont pas été configurées, ou alors pas assez.

2. Infrastructure centralisée avec un serveur d'impression où tous les documents vont transiter.

   Il est souvent facile, avec un simple accès au réseau, de récupérer l'ensemble des documents imprimés par une entreprise : tous ces documents transitent par un SPOF : le serveur d'impression. Et encore une fois, sa sécurisation et celle de ses flux ne sont que très rarement traitées.

3.2.1 Protection contre les attaques physiques

Différentes mesures doivent être prises pour se prémunir des attaques physiques ciblées dont nous avons pu discuter précédemment.

Ces mesures concernent :

- la restriction d'accès physique : en ne mettant pas les imprimantes à disposition de tout public mais en contraignant l'accès aux seules personnes autorisées (e.g. VIP, secrétaires de VIP, etc.).
- le verrouillage du capot pour éviter l'accès au disque dur et à la carte mère : par la mise en place d'un cadenas, d'un sceau d'intégrité, de vis spéciales (sans empêcher une attaque ciblée, ces mesures peuvent ralentir un attaquant).
- la sécurité des câbles réseau : en mettant en place des mesures de contrôle d'accès au réseau évitant à quiconque d'utiliser le câble réseau d'une imprimante pour gagner un accès au reste du SI de l'entreprise.
- le tracking des documents et la protection des supports papiers sensibles (e.g. chèque pré-imprimé) : en mettant en place des toners spéciaux permettant d'imprimer un code de *tracking* des documents et des tiroirs sécurisés (e.g. verrou pour en empêcher l'ouverture).
- la maîtrise des interfaces de l'imprimante : en désactivant celles qui ne sont pas utilisées, généralement les interfaces USB, Firewire, Wi-Fi, Bluetooth, etc.

- la sécurisation de la console d'administration locale à l'imprimante : en désactivant la possibilité d'administrer localement l'imprimante, ou en mettant en place un contrôle d'accès à cette console d'administration.

La plupart de ces mesures n'empêchent pas des vols de documents, mais apportent des éléments permettant de réduire la surface d'attaque et d'augmenter le temps nécessaire pour réaliser ces attaques. De plus, ces mesures améliorent la capacité d'investigation des équipes sécurité suite à un incident.

3.2.2 Désactivation des protocoles inutiles

Nous avons vu l'organisation à mettre en place ainsi que les mesures de sécurité physique. Un attaquant sera donc freiné dans ses tentatives de récupération physique de documents. Toutefois, le réseau, lui, est encore ouvert...

La première action à mener afin de réduire la surface d'attaque est de désactiver les protocoles inutiles (comme AppleTalk ou IPX/SPX). **[HP SEC]**

3.2.3 Adressage statique et vlan dédiés

Idéalement, l'attribution d'une adresse IP statique permet d'augmenter la connaissance et la maîtrise de l'infrastructure d'impression, et diminue la surface d'attaque visant à usurper une imprimante.

Il est également possible de disposer les imprimantes dans une VLAN dédiée afin de mettre en place un premier niveau de cloisonnement.

3.2.4 Restriction des services

Les imprimantes multifonctions sont conçues pour être directement opérationnelles dans des environnements éclectiques. Ainsi, un nombre impressionnant de services sont activés par défaut, comme vu précédemment. **[HP SEC]**

Ils doivent être restreints aux seuls services utiles et nécessaires sur le réseau de l'entreprise. Les services sélectionnés doivent ensuite être durcis par la mise en place d'un contrôle d'accès, par exemple.

Les services les plus souvent présents sont HTTP/HTTPS/SNMP/Telnet pour l'administration ; seule l'administration over HTTPS devrait être utilisée.

En ce qui concerne les protocoles d'impression, ils sont en général variés (LPD, IPP, JetDirect) et il est préférable de n'activer que ceux qui sont utilisés. Il est également recommandé, dans la mesure du possible, de désactiver l'usage de JetDirect (9100) de par ses fonctionnalités avancées (administration).

Enfin, d'autres services utilisés pour l'impression ou l'envoi de documents peuvent être activés (FTP, SMB, Webdav, SMTP), il conviendra de les activer au cas par cas.

Une attention particulière doit être portée sur la gestion des mots de passe : le mot de passe défini sur l'interface web ne sera pas nécessairement répercuté de façon automatique au niveau SNMP, Telnet, JetDirect, etc.

Dans un cadre le permettant, il est également recommandé de limiter les destinataires des fax au carnet d'adresses afin de limiter les possibilités de fuite d'information.

D'autre part, il peut être utile de mettre en place un code de réception pour les fax dans le cas d'échanges confidentiels.

3.2.5 Chiffrement des canaux de communication

Les données confidentielles sont stockées sur des médias chiffrés, transitent chiffrées dans des mails (voire transitent dans des mails chiffrés)... mais sont envoyées à l'imprimante en clair. Rappelons que selon les modèles, l'option « impression sécurisée » ne chiffre pas nécessairement (voire rarement) les documents transmis à l'imprimante.

En ce qui concerne l'interface d'administration, n'autorisez si possible que l'interface HTTPS (et en utilisant de préférence des certificats signés par la PKI de l'entreprise). Si SNMP doit être utilisé, préférez la V3 à la V2. **[SANS]**

Les flux d'impression peuvent soit être chiffrés via des mécanismes natifs s'ils sont supportés par l'imprimante et les postes (e.g. IPP over SSL), soit par un client spécifique ou l'utilisation d'un VPN. **[SANS]**

Si la mise en place du chiffrement de l'ensemble des communications vers les imprimantes ne s'avère pas applicable dans un contexte donné, il est possible de rassembler les imprimantes au sein d'un VLAN, « invisible » depuis les postes utilisateurs et d'utiliser un serveur d'impression comme proxy applicatif. Dans ce cas, il est possible de limiter le chiffrement entre les postes utilisateurs et le proxy.

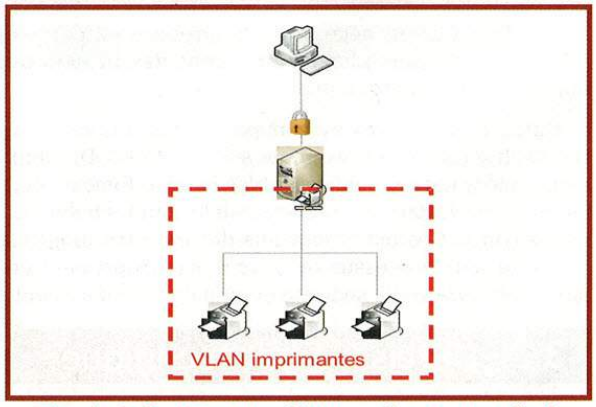


Fig. 4 : Infrastructure d'impression composée de VLAN et avec mise en place du chiffrement des canaux de communication

3.2.6 Chiffrement des médias de stockage

De nombreux médias de stockage différents sont disponibles dans les imprimantes de nos jours : disque dur interne, carte SD, carte mémoire, carte mémoire des cartouches d'encre, rouleau d'impression, bande d'encre, ...

Ces médias doivent être sécurisés pour éviter les détournements vus dans la première partie de cet article.

Le chiffrement des médias apparaît comme la méthode la plus efficace et la moins coûteuse à mettre en place, d'autant que c'est une fonctionnalité communément déployée par les différents constructeurs. Sur le marché, on trouve également des produits réalisant un effacement « sécurisé » entre deux tâches d'impression (e.g. écrasement des fichiers d'impression de la tâche précédente). Ainsi, seul le dernier document traité sera accessible en cas de vol du disque dur de l'imprimante.

3.2.7 Mise au rebut sécurisée

Enfin, lors de la mise au rebut d'une imprimante, il convient de veiller à ce que chacun des médias soit effacé de manière sécurisée (e.g. solution ATA Secure Erase), voire détruit.

En pratique, il est possible de considérer 3 niveaux d'effacement :

- Niveau 1 « base » : utilisation des fonctionnalités d'effacement propre au MFP.
- Niveau 2 « intermédiaire » : effacement manuel des médias. Il convient d'identifier quels sont les médias de stockage présents sur le système :
  - Dans le cas des disques durs magnétiques : un effacement par surimpression de signal (« réécriture » avec **dd** ou tout produit spécifique) ou l'utilisation des fonctions ATA Secure Erase, plus rapide.
  - Dans le cas des mémoires flash/SSD, il est possible de faire un effacement par réécriture, mais étant donné la nature même de la technologie sous-jacente, cet effacement ne sera efficace que contre une tentative de récupération logique (i.e. sans dessouder la puce et tenter une lecture bas niveau).
  - Pour la mémoire RAM, si elle est amovible et n'est pas munie de batterie, la retirer une bonne heure (au chaud ;-)) devrait être suffisant.
  - Pour d'autres médias non amovibles ou spécifiques, il faudra faire confiance aux procédures d'effacement intégrées (nvram, etc.).
- Niveau 3 « sécurisé » : destruction physique des médias. Cette procédure est à appliquer lorsque des données très sensibles sont traitées ou qu'il n'est pas facile de « nettoyer le média » (comme les cartes mémoires des cartouches d'encre, les toners des fax et les bandes d'encre).

Certains médias de stockage sont nativement, ou via des extensions, chiffrés. Dans la mesure où l'implémentation est la plupart du temps une boîte noire et n'a pas pu être auditée, l'effacement des clefs de chiffrement ne peut pas être considéré comme un moyen fiable dès lors que des documents sensibles sont traités (l'utilisation d'algorithmes éprouvés et des clés longues (AES 256/ FIPS, etc.) n'est pas en soi une garantie de solidité tant que l'implémentation n'a pas été éprouvée **[10]**).

Pour plus d'informations sur l'effacement sécurisé de données, l'ANSSI **[ANSSI EFFACEMENT]**, le NIST **[NIST EFFACEMENT]** et le Centre de la sécurité des télécommunications Canadien **[CAN]** ont publié de très bons guides à ce sujet.

3.2.8 Restriction des IP sources

Une autre bonne pratique, mais pouvant s'avérer compliquée à gérer, est de mettre en place un contrôle d'accès au niveau du réseau par la restriction des adresses IP pouvant accéder à l'imprimante.

A minima, la restriction des adresses IP autorisées à effectuer la gestion des imprimantes doit être mise en place. Seuls les postes du réseau des administrateurs pourront se connecter aux interfaces d'administration des MFP.

Cette mesure est cependant applicable dans le cas d'un proxy d'impression, seul ce dernier étant autorisé à communiquer directement avec les imprimantes.

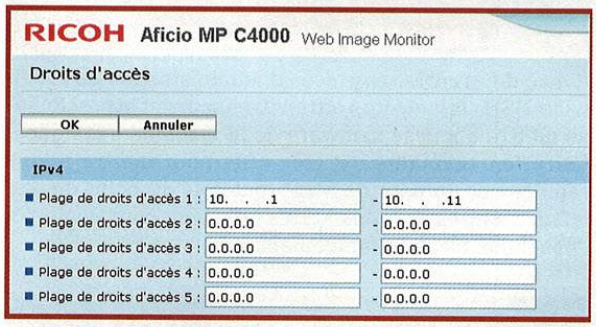


Fig. 5 : Interface de restriction des adresses IP pouvant accéder aux fonctionnalités d'administration des imprimantes RICOH

3.2.9 Durcissement de la configuration SNMP

Afin d'éviter les attaques présentées en première partie de cet article, il est nécessaire de configurer le service SNMP de manière cohérente en :

- changeant les *community string* par défaut (snmp « numéro de communauté » name « nouveau nom ») ;
- désactivant la fonctionnalité « write » de SNMP [SANS] (snmp « numéro de communauté » type « accès ») ;
- utilisant les capacités de chiffrement de SNMP v3 (snmp v3auth sha1).

3.2.10 Verrouillage de la configuration du MFP lors des redémarrages

Pour se prémunir de l'effacement de la configuration après un redémarrage ou une coupure électrique, il convient d'activer les options de persistance de configuration (si elles ne sont pas activées par défaut).

3.2.11 Journalisation

Comme tout matériel, des journaux d'événements sont générés par les imprimantes. Ces derniers peuvent contenir une finesse assez importante, pouvant aller à « qui » a imprimé « quoi », « où » et « quand ».

Une politique de gestion des journaux doit être définie et déployée conformément aux besoins en traçabilité du métier. Cette politique doit tenir compte de la génération des journaux (i.e. de leur contenu), des cas d'accès et de l'exploitation de ces journaux (e.g. stockage centralisé, sauvegarde des journaux, etc.).

3.3 Éléments de durcissement technique dans le cadre de systèmes sensibles

3.3.1 Bloquer la mise à jour du firmware à distance

Les différentes interfaces d'administration des MFP (web, SSH, Telnet, etc.) offrent très souvent la possibilité de mettre à jour le firmware de la machine à distance. Cette fonctionnalité est très utile pour mettre à jour rapidement un parc de MFP, toutefois du point de vue offensif, elle est également très utile pour compromettre l'ensemble du parc rapidement.

3.3.2 Imprimante déconnectée & enclave

Dans le cas d'un environnement très sensible, l'utilisation d'une imprimante « déconnectée » (i.e. raccordée uniquement en USB au poste local) présente une très bonne solution d'un point de vue confidentialité.

Cependant, l'utilisateur ayant un accès direct sur le poste et l'imprimante, la traçabilité peut s'avérer être plus compliquée à assurer, auquel cas il sera nécessaire de passer par un enclavement de l'écosystème MFP (ce qui permet plus facilement l'envoi de logs sur un système tiers, indépendamment du poste client). Le choix entre les deux systèmes devra se faire selon les contraintes métier.

L'enclavement de l'imprimante **[DOD Guide]** (utilisation d'un VLAN dédié et d'un proxy applicatif avec chiffrement natif présenté précédemment) peut être amélioré dans le cas d'un environnement plus sensible en mettant en place une enclave basée sur des technologies maîtrisées par l'entreprise. Par exemple, l'utilisation d'un firewall/VPN maîtrisé plutôt que du chiffrement natif inhérent à l'imprimante et permettant de mettre en place un contrôle d'accès réseau plus poussé. D'autre part, le proxy applicatif devra faire l'objet d'un audit complet.

3.3.3 Points spécifiques

La communication est un des axes majeurs de travail en cas de crise au sein d'une entreprise. La communication passe notamment par les différentes imprimantes déployées sur le SI. Ainsi, une procédure spécifique d'impression en cas de crise doit être définie (e.g. utilisation d'une imprimante déconnectée dans la salle de crise).

De bonnes checklists sont disponibles en ligne **[TEXAS]** **[SANS]** ou à des guides spécifiques au produit concerné **[HP 4345]**.

Note

Cet article ne prend pas en compte les problématiques d'émanations électromagnétiques.

Conclusion

Les imprimantes multifonctions non sécurisées représentent un danger non seulement pour les données qu'elles traitent, mais également pour l'ensemble du SI avec lequel elles interagissent, pouvant dans certains cas aller jusqu'à la compromission du domaine.

Mis à part pour des environnements très sensibles où seule l'utilisation d'une imprimante directement connectée au poste de travail est acceptable, les nombreuses options (chiffrement des liens, utilisation de badges, effacement sécurisé des disques, etc.) et les guides de sécurisation proposés par les constructeurs permettent d'obtenir un niveau correct de sécurisation.

Dans le cas où l'on fait face à une technologie non complètement maîtrisée, et où un niveau de sécurité plus poussé serait nécessaire, la meilleure solution au-delà de la bonne configuration de l'équipement reste l'enclavement des systèmes. Il s'agit de les considérer comme des boîtes noires interagissant via TCP/IP : il faut alors les placer dans des réseaux dédiés, accessibles via un proxy applicatif et un tunnel chiffré maîtrisé tout en assurant un monitoring constant. ■

■ REMERCIEMENTS

Un grand merci à Gérôme Billois, Benoit Marion et Arnaud Soullié pour leurs conseils et leur relecture attentive.

RÉFÉRENCES

[IRONGEEK] Hacking Network Printers, Adrian « Irongeek » Crenshaw, http://www.irongeek.com/i.php?page=security/networkprinterhacking

[TADDONG] http://www.taddong.com/en/lab.html

[EFF 1] http://www.eff.org/issues/printers

[EFF 2] https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots

[SANS RICOH 450E] A Security Assessment of the RICOH Aficio 450E Multifunction Device, David L. Garrard, SANS Institute, 2003

[AU DOD DSD INFOSEC MAN] Australian Government Information Security Manual November 2010, Australian DOD, Defence Signal Directorate

[RICOH LB] Livre Blanc, Informations de sécurité sur les machines RICOH de type GW, Version 1.5, 2006, p 33 & p 38

[BA CERTA 2011-03] Bulletin d'actualité 2011-03, CERTA

[DCSSI] Fiche de recommandation et de bonnes pratiques relatives à la sécurité des [photo]copieurs numériques, SGDN/DCSSI, 27 novembre 2003

[WILD] Printers gone wild ! Shmoocon edition, Shmocoon 2011, TheW1le, http://www.remote-exploit.org/wp-content/uploads/2011/03/Printers-Gone-Wild.pdf

[PRINTER TO PWND] Printer to PWND: Leveraging Multifunction Printers During Penetration Testing (Deral Heiland « PercX » and Pete Arzamendi « Bokojan »), Shmoocon 2011, http://blog.c22.cc/2011/01/29/shmoocon-2011-printer-to-pwnd/ ; video http://www.shmoocon.org/2011/videos/PercX-Printer_to_pwned.m4v et http://www.youtube.com/watch?v=MPhisPLwm2A

[BH 2006 O'CONNOR] Vulnerabilities in Not-So Embedded Systems, B O'Connor, Black Hat USA 2006

[NBS] « Juste une imprimante ? », NBS, JSSI 2011, http://www.ossir.org/jssi/jssi2010/1A.pdf

[M.I.F.A] Politique d'impression des services de l'état, Septembre 2007

[Phenoelit] http://www.phenoelit-us.org/hp/download.html

[USB] http://www.h-online.com/security/news/item/NIST-certified-USB-Flash-drives-with-hardware-encryption-cracked-895308.html

[PJL REF] Printer Job Language Technical Reference Manual, HP, Edition 10, 1997, lprng.sourceforge.net/DISTRIB/RESOURCES/DOCS/pjltkref.pdf

[PJL TR] [http://www.exploit-db.com/exploits/15631

[PCL READER] http://www.pclreader.com/

[TEXAS] Multifunction Device Hardening Checklist, The University of Texas At Austin, http://security.utexas.edu/admin/mfdevice.html

[ANSSI SENSIBILISATION] http://www.ssi.gouv.fr/site_rubrique62.html

[SANS] Auditing and securing Multifunction Devices, C Scott, 2007, http://www.sans.org/reading_room/whitepapers/networkdevs/auditing-securing-multifunction-devices_1921

[DEFPASSLIST] http://www.phenoelit-us.org/dpl/dpl.html

[ANSSI EFFACEMENT] Guide Technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter, DCSSI, 2004 v1.12

[CAN] Conseils en matière de sécurité des TI, Écrasement et déclassification des supports d'information électroniques, Juillet 2006, ISTG-06, centre de la sécurité des télécommunications

[NIST EFFACEMENT] Guidelines for Media Sanitization, SP 800-88 ,NIST, september 2006

[HP 4345] HP LaserJet 4345 MFP Security Checklist, HP, 2006, http://www.hp.com/united-states/business/catalog/nist_checklist.pdf

[HP SEC] http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj05999

[DOD GUIDE] Sharing peripherals accross the network, Security technical implementation guide, 28 july 2005

[nmap] http://nmap.org/book/idlescan.html

NOTES

[1] Attention, le reverse est illégal dans de nombreux pays ;)

[2] http://www.exploit-db.com/exploits/10055/ et http://www.exploit-db.com/exploits/10011/, par exemple

[3] Par exemple sur de nombreux modèles RICOH, les communautés par défaut sont public (R) et admin (RW)

[4] HP JetDirect J3263A, HP JetDirect J3113A, HP JetDirect J3111A [IRONGEEK]

[5] Voir http://www.securityfocus.com/bid/7001/exploit

[6] qui équivaut à l'envoi sur le port 9100 de chaîne suivante : \x1B%-12345X@PJL RDYMSG DISPLAY = \"hello\"\r\n\x1B%-12345X\r\n

[7] Par exemple dump de la base SAM puis récupération du mot de passe avec Ophtcrack ou fastncrack (voir l'article « Rainbow tables à espace probabiliste » d'Alain Schneider paru dans le n°58 de MISC), soit via un pass-the-hash avec PSK Toolkit de Core ou MSF.

[8] Quoiqu'il s'agisse souvent d'un bon moyen de découvrir qu'un pont a été établi entre un réseau cloisonné et Internet.

[9] Dans le cas présent, nous assumons qu'une télémaintenance over IP permet de prendre complètement la main sur le système cible. Afin d'évaluer plus spécifiquement les capacités dans le cas d'un appareil donné, il est soit possible de questionner le constructeur (ce qui apporte en général peu d'informations), soit de simuler/générer une panne suffisamment importante pour qu'une télémaintenance soit effectuée depuis la maison mère (les équipes en France ne disposant pas toujours des bons logiciels).

[10] Sans parler de backdoors (ex : CVE-2009-3200), des « erreurs de conception » peuvent se glisser parmi les lignes de code [USB].

ANALYSER LA GÉOLOCALISATION SUR IPHONE GRÂCE À UN PROXY DE DÉCHIFFREMENT SSL

Alain Pannetrat – Service de l'Expertise Informatique,
Commission Nationale de l'Informatique et des Libertés

mots-clés : *VIE PRIVÉE / GÉOLOCALISATION / IPHONE / INTERCEPTION / MAN-IN-THE-MIDDLE / SSL*

Pendant votre sommeil, votre iPhone raconte parfois à Apple où vous avez passé votre journée. C'est l'intéressante découverte que nous avons faite en étudiant les mécanismes de géolocalisation de ce smartphone. Mais pour en arriver là, il a d'abord fallu déchiffrer les communications SSL de notre téléphone cobaye et en analyser le contenu. Une enquête détaillée pas à pas dans cet article.

1 Les mystères de la géolocalisation sur iPhone

La plupart des smartphones ont une puce GPS, mais cette technologie est lente à démarrer et ne marche pas toujours bien en ville où à l'intérieur de bâtiments. C'est une tout autre approche qui est donc souvent utilisée pour fournir un service de géolocalisation sur ces dispositifs mobiles : la détection de points d'accès Wi-Fi (ou d'antennes GSM). Contrairement au GPS, cette approche nécessite une communication entre le téléphone et un serveur de géolocalisation spécialisé qui détient une base de données recensant la position géographique des points d'accès Wi-Fi. Ceci est possible, car chaque point d'accès Wi-Fi peut être identifié par un numéro unique : son adresse MAC ou « BSSID ».

Cette fonction de géolocalisation offerte par les smartphones entraîne des sentiments ambivalents. Pour beaucoup au quotidien, c'est à la fois un outil fantastique et potentiellement un dispositif de surveillance des déplacements qui inquiète.

Pour en témoigner, il suffit de se rappeler l'énorme *buzz* qu'avaient créé, fin avril 2011, deux universitaires britanniques **[1]** en mettant en lumière une base de données de géolocalisation utilisée par les iPhones d'Apple et sauvegardée sur le PC de l'utilisateur. Étrangement, la découverte initiale de ce fichier, attribuée à Sean Morrissey et Alex Levinson **[2]**, datait de 2010 et était passée inaperçue à l'époque.

Cette base de données, appelée `consolidated.db`, recensait, rappelons-le, plus d'un an d'historique, plus ou moins précis, des déplacements des propriétaires d'iPhone. Apple a depuis corrigé le problème tout en affirmant que le contenu de ce fichier n'était jamais envoyé vers ses propres serveurs.

Une question demeurerait donc : quelles données de géolocalisation sont envoyées vers les serveurs d'Apple et comment ce mystérieux fichier a-t-il été constitué ? Pour tenter de répondre à ces questions, plongeons au cœur des communications de l'iPhone.

2 Déchiffrer des communications SSL/TLS

La première étape de cette expérience consiste à créer un point d'interception des communications entre un iPhone et Internet. Il y a plusieurs canaux pour y parvenir : l'OS de l'iPhone, la 3G/GSM ou le Wi-Fi. L'interception de communications 3G/GSM nécessite un matériel assez lourd, quant à l'installation d'un logiciel d'interception directement sur l'iPhone, cela implique

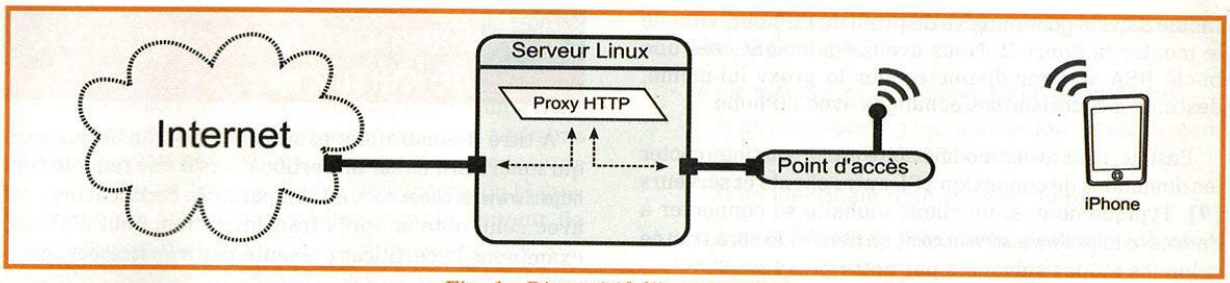


Fig. 1 : Dispositif d'interception

des développements complexes et un « jailbreaking », ce que nous voulions éviter. L'option la plus simple est donc d'exploiter le canal Wi-Fi. Un point d'accès Wi-Fi ordinaire a donc été connecté à une machine Linux, elle-même équipée d'une deuxième carte réseau connectée à Internet par ADSL, comme illustré sur la figure 1.

Sur cette machine Linux, un proxy HTTP à été mis en place pour pouvoir intercepter les communications de l'iPhone. Premier constat : les requêtes de géolocalisation sont sécurisées par SSL/TLS. Ce proxy a donc dû être modifié pour intercepter ce type de communications. Il existait déjà des proxies qui étaient susceptibles de jouer ce rôle, par exemple `mitmproxy` **[3]** ou encore `tcpcatcher` **[4]**. Néanmoins, à l'époque de nos premières investigations, ils souffraient tous de certaines limitations qui nous ont amenés à développer notre propre outil dont le code source est disponible **[5]** sous licence GPL pour les lecteurs qui souhaiteraient répéter les expériences décrites dans cet article.

2.1 Le modèle d'authentification de SSL en question

Dans son utilisation la plus répandue, le protocole SSL/TLS est utilisé pour sécuriser des communications HTTP entre un client et un serveur. Il existe deux grandes familles d'attaques sur SSL/TLS : les attaques qui ciblent les mécanismes assurant la confidentialité des communications et celles qui s'attachent aux problématiques d'authentification des échanges.

Les attaques portant directement sur les mécanismes de confidentialité des communications sont rares, car le protocole SSL/TLS s'appuie sur des primitives cryptographiques éprouvées, même si l'on découvre parfois encore des failles dans la manière dont elles sont mises en œuvre **[6]**. C'est en jouant avec le modèle d'authentification de SSL/TLS que nous avons mis en place un outil susceptible d'intercepter des communications chiffrées entre un iPhone et les serveurs d'Apple.

Fig. 2 : Notre certificat racine installé dans l'iPhone

Rappelons de manière simplifiée les principes d'authentification utilisés par SSL/TLS. Lorsqu'un client se connecte à un serveur **www.serveur.com** en SSL, le serveur lui présente sa clé publique, qui sert alors à initier une communication sécurisée. En effet, si une donnée envoyée par le client est chiffrée avec la clé publique du serveur, seul celui-ci pourra la déchiffrer. Bien sûr, ceci ne fonctionne que si le client est certain que la clé publique appartient bien au serveur **www.serveur.com** et non à un usurpateur. Cette assurance est fournie par un certificat envoyé également par le serveur. Ce certificat contient un lien entre la clé publique du serveur et son identité « www.serveur.com », le tout signé par une autorité de certification. Si le navigateur du client possède lui-même la clé publique de l'autorité de certification, il pourra vérifier la validité de la signature du certificat et par conséquent valider la clé publique du serveur.

Dans ce modèle, la confiance est donc déportée intégralement sur une autorité de certification. Si celle-ci est défaillante, la sécurité des communications n'est plus garantie. Ce fut le cas très récemment lorsque des hackers iraniens ont réussi à obtenir des certificats pour de nombreux sites, dont Google, auprès de l'autorité de certification Diginotar **[7]**. En effet, si l'on peut fabriquer un vrai-faux certificat, alors il est possible de réaliser une interception de type *Man In The Middle*. Nous reprenons ici cette idée : notre proxy intercepte les communications entre le client et le serveur, faisant croire d'une part au client qu'il est le serveur et d'autre part au serveur qu'il est le client. Le client et le serveur n'y verront que du feu !

2.2 Un « Man In The Middle »

Dans notre expérience, nous avons donc créé notre propre autorité de certification appelée « Proxy Certs Master » à l'aide d'OpenSSL **[8]** et nous avons installé son certificat

racine dans le gestionnaire de profil de l'iPhone, comme le montre la figure 2. Nous avons également créé une bi-clé RSA serveur distincte pour le proxy lui-même, destinée à sécuriser ses échanges avec l'iPhone.

Ensuite, nous avons modifié notre proxy pour intercepter les demandes de connexion SSL entre clients et serveurs **[9]**. Typiquement, si un client souhaite se connecter à l'adresse **https://www.serveur.com/**, sa demande sera traitée selon les étapes suivantes par notre proxy :

- Étape 1 : Le client se connecte au proxy – on appellera cette connexion « CONNECTION A ». Le client transmet au proxy une demande de connexion au serveur SSL distant, à l'aide de la requête HTTP **`CONNECT www.serveur.com:443 HTTP/1.1`**. Le proxy répond à cette requête avec un code **`HTTP/1.1 200 Connection established`**, après avoir vérifié qu'une connexion TCP/IP avec le serveur distant était possible sur le port 443 (pas de SSL à ce stade).

- Étape 2 : Le proxy crée une seconde connexion SSL indépendante vers le serveur comme s'il était lui-même un navigateur : on appellera cette connexion « CONNECTION B ». Le proxy récupère et modifie alors le certificat X509 de **www.serveur.com** pour en créer un nouveau en réalisant les manipulations suivantes :

  1) Le descripteur de l'autorité de certification est remplacé par celui de « Proxy Certs Master ».
  2) La clé publique du serveur est remplacée par la clé publique du proxy.
  3) Certaines extensions X509 V3 sont supprimées ou modifiées par souci de cohérence si nécessaire.
  4) Le certificat est reconstruit et signé par la clé privée de l'autorité « Proxy Certs Master ».

- Étape 3 : Le client envoie alors une séquence d'initialisation SSL sur la CONNECTION A. Le proxy y répond en présentant sa propre clé publique et le certificat modifié créé à l'étape précédente. Le client peut vérifier la chaîne de certification à l'aide du certificat racine de notre autorité « Proxy Certs Master » et croit donc dialoguer avec le serveur authentique (et non le proxy).

- Étape 4 : Le client envoie sa requête HTTPS sur la CONNECTION A : **`GET / HTTP/1.1`**. Le proxy la lit et la renvoie sur la CONNECTION B.

- Étape 5 : Le serveur reçoit la requête HTTPS sur la CONNECTION B et renvoie sa réponse **`HTTP/1.1 200 OK`** avec le contenu de la page demandée. Le proxy lit cette réponse et la renvoie vers la CONNECTION A à destination du client.

Les CONNECTION A et B sont alors fermées : l'interception Man-In-The-Middle a été un succès.

2.3 Exemple de modification de certificat

À titre d'illustration, examinons les transformations qui sont réalisées sur un certificat lors d'une requête vers **https://www.facebook.com**, en comparant le certificat original avec celui obtenu après transformation. Tout d'abord, examinons le certificat présenté par **www.facebook.com** :

```
~$ openssl x509 -text -in certificat-original.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0c:6f:c8:59:57:fa:1f:5f:c9:67:2c:9f:e6:5c:db:e6
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert High
        Assurance CA-3
        Validity
            Not Before: Nov 15 00:00:00 2010 GMT
            Not After : Dec  2 23:59:59 2013 GMT
        Subject: C=US, ST=California, L=Palo Alto, O=Facebook, Inc.,
        CN=www.facebook.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c1:df:7d:63:41:bd:c4:e4:fa:65:33:13:78:d5:
                    62:37:96:a7:61:f3:b1:96:bf:23:8e:ba:87:a7:ed:
                    07:f9:de:2d:eb:a8:c7:bc:ad:77:a6:5e:8d:03:03:
                    [... ici le reste de la clé publique de www.facebook.com ...]
                Exponent: 65537 (0x10001)
        X509v3 extensions:
[...]
```

Puis examinons le certificat obtenu après transformation :

```
~$ openssl x509 -text -in certificat-modifie.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0c:6f:c8:59:57:fa:1f:5f:c9:67:2c:9f:e6:5c:db:e6
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=FR, ST=France, O=Proxy Certs, CN=Proxy Certs Master
        Validity
            Not Before: Nov 15 00:00:00 2010 GMT
            Not After : Dec  2 23:59:59 2013 GMT
        Subject: C=US, ST=California, L=Palo Alto, O=Facebook, Inc.,
        CN=www.facebook.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:a9:2f:47:fc:00:99:83:dc:4e:4a:59:55:50:f5:
                    5a:ca:1c:54:fa:0a:cd:cc:40:fe:7a:34:b3:6c:92:
                    b5:c3:8a:98:da:48:d8:da:6f:54:af:a4:50:2b:7b:
                    [... ici le reste de la clé publique du proxy ...]
                Exponent: 65537 (0x10001)
        X509v3 extensions:
[...]
```

On voit clairement le changement d'autorité de certification et de clé publique. Dans les deux cas, les résultats ont été tronqués par souci de simplicité, sinon on pourrait également voir certains changements opérés dans les extensions de ce certificat X509 V3.

3 Analyse des résultats

À l'aide de notre dispositif, nous avons placé un iPhone 3GS sous surveillance. Premier test : nous utilisons une application nécessitant un appel aux services de géolocalisation d'Apple (exemple : la Boussole ou Maps). Le téléphone contacte immédiatement le serveur de géolocalisation d'Apple en SSL à l'adresse **gs-loc.apple.com**. Voici une présentation « brute » de ce premier message :

```
POST /clls/wloc HTTP/1.1
User-Agent: locationd (unknown version) CFNetwork/485.13.9 Darwin/11.0.0
X-Apple-Bundleid: com.apple.Maps
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 148

000000: 00 01 00 05 65 6e 5f 55 53 00 00 00 09 34 2e 33 | ....en_US....4.3
000010: 2e 32 2e 38 48 37 00 00 00 01 00 00 00 76 12 11 | .2.8H7.......v..
000020: 0a 0f 63 3a 36 30 3a 37 36 3a 65 3a 62 38 3a 63 | ..c:60:76:e:b8:c
000030: 33 12 12 0a 10 30 3a 31 66 3a 39 66 3a 66 62 3a | 3....0:1f:9f:fb:
000040: 38 37 3a 31 39 12 12 0a 10 30 3a 31 39 3a 37 30 | 87:19....0:19:70
000050: 3a 34 31 3a 33 61 3a 62 36 12 12 0a 10 32 3a 31 | :41:3a:b6....2:1
000060: 37 3a 33 33 3a 61 61 3a 37 65 3a 62 61 12 11 0a | 7:33:aa:7e:ba...
000070: 0f 30 3a 31 61 3a 32 62 3a 65 3a 36 66 3a 61 63 | .0:1a:2b:e:6f:ac
000080: 18 00 20 00 2a 0e 63 6f 6d 2e 61 70 70 6c 65 2e | .. .*.com.apple.
000090: 4d 61 70 73                                     | Maps
```

Une analyse visuelle rapide fait apparaître la version de l'OS de notre iPhone cobaye (**4.3.2.8H7**) et ce qui semble être des adresses MAC (BSSID), par exemple : **c:60:76:e:b8:c3**. La réponse fournie par le serveur d'Apple est beaucoup plus longue et nous ne la reproduirons pas ici. Elle semble avoir un format similaire, mais elle contient en revanche pas moins de 405 occurrences d'adresses MAC (ce nombre peut varier selon les cas). Reste donc à décoder plus précisément le format de ces échanges.

3.1 Jouer aux devinettes avec le format « protocol buffer »

Lors d'une de nos enquêtes précédentes, nous avions été confrontés à des données encodées dans un format ouvert inventé par Google : les « protocol buffers ». Sans trop croire qu'Apple utiliserait ce type de format, nous faisons tout de même des tests. Bonne pioche : à notre surprise, les requêtes de géolocalisation d'Apple sont presque intégralement encodées dans ce format.

Le format « protocol buffers » (ou simplement « protobuf ») est un mécanisme de sérialisation de données, comme peut l'être ASN.1 **[10]** ou même JSON **[11]**. La meilleure manière de comprendre ce format est de lire la documentation de Google **[12]**. Brièvement, son principe est le suivant :

- Chaque donnée est définie par deux composantes : une clé et une valeur.
- La clé est elle-même composée de deux parties :
  1) un descripteur générique de format (seulement 6 valeurs possibles) ;
  2) un identifiant unique de la donnée.
- La donnée elle-même est encodée de manière variable selon son usage.

Contrairement à un format comme XML qui contient des « tags » textuels normalement destinés à permettre à un humain de deviner le sens des données encodées, le format protobuf nécessite de jouer aux devinettes. En premier lieu, le descripteur générique de format est très vague : par exemple, s'il indique une valeur 32 bits, il reste à savoir s'il s'agit d'un entier signé, d'un entier non signé ou d'un nombre à virgule flottante. De plus, l'identifiant unique de la donnée dépend totalement du contexte.

C'est finalement en recoupant les données collectées avec le contenu de la base de données **consolidated.db** **[1]** dont nous parlions en introduction que nous avons construit une interprétation plausible des requêtes de géolocalisation envoyées vers les serveurs d'Apple, à l'aide d'outils supplémentaires que nous avons également développés.

3.2 Les demandes de géolocalisation

Nous sommes donc en mesure de revisiter la requête de géolocalisation précédente :

```
POST /clls/wloc HTTP/1.1
User-Agent: locationd (unknown version) CFNetwork/485.13.9 Darwin/11.0.0
X-Apple-Bundleid: com.apple.Maps
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 148

000000: 00 01 00 05 65 6e 5f 55 53 00 00 00 09 34 2e 33 | ....en_US....4.3
000010: 2e 32 2e 38 48 37 00 00 00 01 00 00 00 76       | .2.8H7.......v
Block: {
  WifiDetected: {
    BSSID: "c:60:76:e:b8:c3"
  }
  WifiDetected: {
    BSSID: "0:1f:9f:fb:87:19"
  }
  WifiDetected: {
    BSSID: "0:19:70:41:3a:b6"
  }
  WifiDetected: {
    BSSID: "2:17:33:aa:7e:ba"
  }
```

```
  WifiDetected: {
    BSSID: "0:1a:2b:e:6f:ac"
  }
  unknown3: 0
  unknown4: 0
  Service: "com.apple.Maps"
}
```

Cette requête est très simple : elle contient uniquement les adresses MAC de 5 points d'accès Wi-Fi détectés à proximité du téléphone. On notera deux choses intéressantes. Tout d'abord, la requête ne contient aucun numéro identifiant le téléphone de manière unique (comme l'IMEI ou l'UDID). Certes, le serveur d'Apple collecte l'adresse IP de notre connexion ADSL, mais c'est une information plus difficile à exploiter dans ce contexte pour identifier un dispositif mobile comme l'iPhone, car il est susceptible de varier ses méthodes de connexion à Internet pendant une même journée, cela contrairement à un PC fixe. Ensuite, on remarquera que les BSSID sont transmis sans information relative à la force des signaux des points d'accès détectés. Apple ne reçoit donc pas d'information très précise pour géolocaliser le téléphone. On va vite comprendre pourquoi : en effet, ce n'est pas Apple qui géolocalise le téléphone, mais le téléphone qui se géolocalise lui-même...

En effet, voici maintenant la réponse du serveur d'Apple, que nous avons tronquée par souci de simplicité :

```
HTTP/1.1 200 OK
Date: Mon, 02 May 2011 18:06:18 GMT
Content-Length: 14225

000000: 00 01 00 00 00 01 00 00 37 87 12 20 0a 0f 63 3a | ........7.. ..c:
000010: 36 30 3a 37 36 3a 65 3a 62 38 3a 63 33 12 0d 08 | 60:76:e:b8:c3...
Block: {
  WifiInformation: {
    BSSID: "c:60:76:e:b8:c3"
    Location: {
      latitude: 48.86065822
      longitude: 2.38659417
      confidence: 108
    }
  }
  WifiInformation: {
    BSSID: "0:1f:9f:f6:e8:b7"
    Location: {
      latitude: 48.86067944
      longitude: 2.38658750
      confidence: 98
    }
  }
  WifiInformation: {
    BSSID: "0:1a:6b:ca:d1:a1"
    Location: {
      latitude: 48.86068940
      longitude: 2,38657420
      confidence: 72
    }
  }
[...]
```

La réponse contient en tout une liste de 405 points d'accès Wi-Fi. Chacun de ces points est associé à une position géographique précise et ce que nous pensons être une estimation du niveau de confiance que l'on peut accorder à cette information. Si on place ces points sur une carte à l'aide d'un fichier KML **[13]**, on obtient le résultat présenté à la figure 3.

Fig. 3 : Position des points d'accès Wi-Fi dans un quartier de Paris

Avec ces informations et avec la force du signal qu'il a mesuré en provenance des points d'accès environnants, l'iPhone est alors en mesure de calculer lui-même sa position par triangulation. Mieux encore, si le téléphone se déplace dans la même zone géographique, il n'a pas besoin de refaire une requête vers les serveurs d'Apple : il peut puiser dans les informations précédemment reçues pour se géolocaliser. Ces informations peuvent alors être stockées dans une base de données et resservir en cas de connexion défaillante, c'est sans doute le rôle du fameux fichier **consolidate.db** qui avait tant suscité de questions au printemps dernier.

3.3 Des messages nocturnes

Lorsqu'un iPhone est laissé allumé pendant la nuit et connecté à un point d'accès Wi-Fi, il arrive qu'il se connecte à un autre serveur d'Apple : **iphone-services.apple.com**, et cela, sans la moindre intervention de l'utilisateur. Un travail d'analyse nous a permis de déchiffrer en grande partie cet échange, et de découvrir une autre source d'échanges de données de géolocalisation entre l'iPhone et Apple, comme le montre l'exemple suivant :

```
POST /hcy/pbcwloc HTTP/1.1
User-Agent: locationd (unknown version) CFNetwork/485.13.9 Darwin/11.0.0
Connection: close
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 3387
```

Complétez votre collection des anciens numéros de...

Les 4 façons de commander !

Par courrier
En nous renvoyant ce bon de commande.

Par le Web
Sur notre site : www.ed-diamond.com.

Par téléphone
Entre 9h-12h & 14h-18h au 03 67 10 00 20 (paiement C.B.)

Par fax
Au 03 67 10 00 21 (C.B. et/ou bon de commande administratif)

MISC

du numéro...
...au numéro

Bon de commande MISC		
Réf.	**Désignation**	**Prix / N°s**
MISC N°48	Comment se protéger contre la peste spam ?	8,00 €
MISC N°49	Vulnérabilités Web et XSS - Des ennemis que vous sous-estimez !	8,00 €
MISC N°50	La sécurité des jeux	8,00 €
MISC N°51	Sécurité des OS mobiles	8,00 €
MISC N°52	4 Outils indispensables pour tester votre sécurité !	8,00 €
MISC N°53	La sécurité du wi-fi, des paroles en l'air ?	8,00 €
MISC N°54	Anonymat sur internet : Risque ou nécessité ?	8,00 €
MISC N°55	Au coeur des technologies sécurité de MICROSOFT	8,00 €
MISC N°56	Forensics : Les nouveaux enjeux	8,00 €
MISC N°57	Sexe, Drogue et sécurité informatique	8,00 €
MISC N°58	Sécurité et architecture PC : L'impossible confiance ?	8,00 €

du numéro...
...au numéro

Bon de commande MISC Hors-Série		
Réf.	**Désignation**	**Prix / N°s**
MISC Hors-Série N°3	Petit traité de sécurité à l'usage des honnêtes gens ... mais pas seulement !	8,00 €
MISC Hors-Série N°4	À l'assaut du WEB - Nouveaux usages ... Nouveaux enjeux	8,00 €

Bon de commande

à remplir (ou photocopier) et à retourner aux Éditions Diamond - MISC - BP 20142 - 67603 Sélestat Cedex

	Référence	Prix / N°	Qté	Total
EXEMPLE :	MISC N°42	8,00 €	1	8,00 €
		TOTAL :		
		FRAIS DE PORT FRANCE MÉTRO. :		+3,9 €
		FRAIS DE PORT HORS FRANCE MÉTRO. :		+6 €
		TOTAL :		

Voici mes coordonnées postales :
Nom :
Prénom :
Adresse :
Code Postal :
Ville :
Téléphone :
e-mail :

Je choisis de régler par :

- ❑ Chèque bancaire ou postal à l'ordre des Éditions Diamond
- ❑ Carte bancaire n° |_|_|_|_| |_|_|_|_| |_|_|_|_| |_|_|_|_|
  Expire le : |_|_|_|_|
  Cryptogramme visuel : |_|_|_|

Date et signature obligatoire

- ❑ Je souhaite recevoir des infos des Edtions Diamond
- ❑ Je souhaite recevoir des infos des partenaires des Editions Diamond

Retrouvez les sommaires et commandez tous nos magazines sur notre site :
http://www.ed-diamond.com

Complétez votre collection de MISC

Multi-System & Internet Security Cookbook

au tarif promotionnel de 4 € TTC par numéro* !

Les 4 façons de commander !

Par courrier
En nous renvoyant ce bon de commande.

Par le Web
Sur notre site : www.ed-diamond.com.

Par téléphone
Entre 9h-12h & 14h-18h au 03 67 10 00 20 (paiement C.B.)

Par fax
Au 03 67 10 00 21 (C.B. et/ou bon de commande administratif)

Vous recherchez un numéro spécifique ?

Rendez-vous sur www.ed-diamond.com pour consulter le sommaire détaillé de chaque magazine !

Choisissez vos numéros dans le tableau ci-dessous :

- ❑ N°1 Les vulnérabilités du Web !
- ❑ N°2 Windows et la sécurité
- ❑ N°4 Internet un château construit sur du sable? ...ou les protocoles réseaux en question
- ❑ N°6 Sécurité du wireless ?
- ❑ N°7 La guerre de l'information - évaluation, riques, enjeux
- ❑ N°8 Honeypots - Le piège à pirate !
- ❑ N°9 Que faire après une intrusion ?
- ❑ N°10 VPN - Virtual Private Networt - Créez votre réseau sécurisé sur internet
- ❑ N°12 La faille venait du logiciel
- ❑ N°13 PKI - Public Key Infrastructure
- ❑ N°14 Reverse Engineering - Retour au sources
- ❑ N°16 Télécoms - Les risques des infrastructures
- ❑ N°17 Comment lutter contre - Le spam, les malwares, les spywares ?
- ❑ N°18 Dissimulation d'information
- ❑ N°19 Les Dénis de Services - La menace rôd
- ❑ N°20 Cryptographie malicieuse : quand les vers et virus se mettent à la crypto
- ❑ N°21 Limites de la sécurité
- ❑ N°23 De la recherche de faille à l'exploit
- ❑ N°24 Attaques sur le Web
- ❑ N°25 Bluetooth, P2P, Messageries instantanées : Les nouvelles cibles
- ❑ N°26 Matériel, mémoire, humain, multimédia : Attaques tous azimuts
- ❑ N°28 Exploits et correctifs : Les nouvelles protections à l'épreuve du feu
- ❑ N°29 Sécurité du coeur de réseau IP : un organe critique
- ❑ N°30 Les protections logicielles
- ❑ N°32 Que penser de la sécurité selon Microsoft ?
- ❑ N°33 RFID - Instrument de sécurité ou de surveillance ?
- ❑ N°34 Noyau et rootkit
- ❑ N°36 Lutte informatique offensive - Les attaques ciblées
- ❑ N°37 Déni de service
- ❑ N°38 Code malicieux - Quoi de neuf ?
- ❑ N°39 Fuzzing - Injectez des données et trouvez les failles cachées
- ❑ N°40 Sécurité des réseaux - Les nouveaux enjeux
- ❑ N°41 LA CYBERCRIMINALITÉ ...ou quand le net se met au crime organisé
- ❑ N°42 LA VIRTUALISATION : Vecteur de vulnérabilité ou de sécurité ?
- ❑ N°43 La sécurité des web services
- ❑ N°44 Compromissions électromagnétiques
- ❑ N°45 La sécurité de Java en question
- ❑ N°46 Construisez et validez votre sécurité
- ❑ N°47 La lutte antivirale, une cause perdue ?

Numéros MISC épuisés :
N°3, N°5, N°11, N°15, N°22, N°27, N°31 et N°35

* dans la limite des stocks disponibles.

Numéros MISC Hors-Série épuisés : HS N° 1 et 2

Bon de commande

à remplir (ou photocopier) et à retourner aux Éditions Diamond – MISC – BP 20142 – 67603 Sélestat Cedex

Quantité	Prix / N°	Total
	x 4,00 €	=
	FRAIS DE PORT FRANCE MÉTRO. :	+ 3,90 €
	FRAIS DE PORT HORS FRANCE MÉTRO. :	NOUS CONSULTER
	TOTAL :	

Je choisis de régler par :

❑ Chèque bancaire ou postal à l'ordre des Éditions Diamond

❑ Carte bancaire n° |_|_|_|_| |_|_|_|_| |_|_|_|_| |_|_|_|_|

Expire le : |_|_|_|_|

Cryptogramme visuel : |_|_|_|

Date et signature obligatoire

Voici mes coordonnées postales :
Nom :
Prénom :
Adresse :
Code Postal :
Ville :
Téléphone :
e-mail :

❑ Je souhaite recevoir des infos des Édtions Diamond

❑ Je souhaite recevoir des infos des partenaires des Éditions Diamond

```
000000: 00 01 00 05 65 6e 5f 55 53 00 00 00 09 34 2e 33 | ....en_US....4.3
000010: 2e 31 2e 38 47 34 00 00 00 64 00 00 0d 1d 0a 1b | .1.8G4...d....
Block: {
  Header: {
    hardware_version: "N88AP"
    software_version: "iPhone OS4.3.1/8G4"
  }
  WifiMeasurement: {
    BSSID: "0:1a:2b:49:d5:e5"
    channel: 6
    hidden: 0
    signal_strength: -97
    Location: {
      latitude: 48.8356584333
      longitude: 2.38246455
      __32BIT_3: 0x4322f53c
      timestamp: 324742217.051
      __32BIT_5: 0x41ea8bd6
      __32BIT_6: 0x436457fb
    }
  }
  WifiMeasurement: {
    BSSID: "0:11:50:24:6f:9c"
    channel: 6
    hidden: 0
    signal_strength: -96
    Location: {
      latitude: 48.8356584333
      longitude: 2.38246455
      __32BIT_3: 0x4322f53c
      timestamp: 324742217.051
      __32BIT_5: 0x41ea8bd6
      __32BIT_6: 0x436457fb
    }
  }
[...]
```

Cet exemple montre cette fois-ci des données très précises sur des points d'accès Wi-Fi qui ont été vus pendant la journée par le téléphone : latitude, longitude, canal, force du signal et même un horodatage (en secondes écoulées depuis début 2001). Naturellement, la latitude et la longitude correspondent à la position du téléphone au moment de la mesure et pas à la position des points d'accès. Ici encore, cependant, aucune information ne permet d'identifier le téléphone (à part éventuellement l'adresse IP).

La collecte de ces informations permet certainement à Apple d'enrichir sa base de géolocalisation, notamment pour y ajouter de nouveaux points d'accès Wi-Fi détectés. En recoupant les informations fournies tous les jours par des millions de téléphones, Apple est capable petit à petit de faire évoluer sa base cartographique avec une assez grande précision. C'est ce qu'on appelle le « crowdsourcing » : chaque téléphone travaille donc un peu pour Apple.

Conclusion

Cet article a rappelé qu'il est possible d'intercepter une communication SSL à condition de déposer un certificat racine sur les postes informatiques que l'on souhaite surveiller.

Notre analyse montre qu'Apple a utilisé une approche originale pour construire son mécanisme de géolocalisation : ce n'est pas le serveur d'Apple qui géolocalise le téléphone, mais le téléphone qui se géolocalise lui-même à partir des données envoyées par Apple. Ponctuellement, l'iPhone envoie néanmoins des informations détaillées sur les points d'accès Wi-Fi qu'il a vu pendant les heures passées. Une pratique qui mériterait sans doute une meilleure information d'Apple envers ses utilisateurs.

La méthode retenue par Apple semble être plutôt bonne en termes de protection de la vie privée : les données sont sécurisées par SSL/TLS et aucun numéro d'identification n'est présent dans les requêtes, même s'il reste naturellement une possibilité de traçage à partir de l'adresse IP dans certains cas. N'oublions pas cependant que les applications qui utilisent l'API de géolocalisation de l'iPhone peuvent elles-mêmes tracer les individus, même si Apple ne le fait pas.

Si un même téléphone fait une requête de géolocalisation le matin et le soir à partir de deux endroits différents, les serveurs d'Apple ne sont vraisemblablement pas en mesure de savoir qu'elles viennent du même téléphone. Le risque de pistage des personnes par Apple est donc très réduit. Peut-on en dire autant de leurs concurrents ? Vous avez maintenant tous les outils pour mener l'enquête ! ■

RÉFÉRENCES

[1] http://radar.oreilly.com/2011/04/apple-location-tracking.html

[2] Sean Morrissey et Alex Levinson, « iOS Forensic Analysis: for iPhone, iPad, and iPod touch », APress, 2010

[3] http://mitmproxy.org/ : un proxy HTTP/SSL

[4] http://www.tcpcatcher.org/ : un proxy HTTP/SSL

[5] http://code.google.com/p/sslmeat/ : un proxy SSL en C++, GPL V3

[6] http://www.schneier.com/blog/archives/2011/09/man-in-the-midd_4.html

[7] http://en.wikipedia.org/wiki/DigiNotar

[8] http://www.openssl.org/

[9] http://tools.ietf.org/id/draft-luotonen-web-proxy-tunneling-01.txt : la requête HTTP CONNECT

[10] http://fr.wikipedia.org/wiki/ASN.1: le format ASN.1

[11] http://www.json.org/: le format JSON

[12] http://code.google.com/intl/fr-FR/apis/protocolbuffers/docs/encoding.html : Google protocol buffers

[13] http://code.google.com/intl/fr-FR/apis/kml/documentation/kmlreference.html : le format KML

PRISE D'EMPREINTE 802.11

Olivier Heen – olivier.heen@technicolor.com,
Christoph Neumann – christoph.neumann@technicolor.com
et Stéphane Onno – stephane.onno@technicolor.com

mots-clés : 802.11 / PRISE D'EMPREINTE / FINGERPRINT / TESTS D'IMPLÉMENTATION

La prise d'empreinte d'un appareil réseau consiste en la mesure de son trafic afin d'identifier l'appareil lui-même ou certaines de ses caractéristiques techniques.

La prise d'empreinte est une technique bien connue lorsqu'elle est appliquée à la reconnaissance des systèmes d'exploitation, avec des outils populaires comme NMAP ou SinFP. Cette technique est moins connue lorsqu'elle est appliquée à la reconnaissance d'appareils 802.11. Pourtant, depuis 2005, environ trente articles consacrés à ce sujet ont été publiés. Plusieurs outils ont vu le jour, comme BAFFLE [3] ou WiFinger [9].

Dans cet article, nous décrivons diverses méthodes de prise d'empreinte 802.11 : test actif d'implémentation [4], test passif d'implémentation [7], mesure de dérive d'horloge [10, 12]. Nous illustrons le fonctionnement pratique de ces méthodes à l'aide de scripts et nous indiquons les possibilités d'évasion connues.

1 Prise d'empreinte 802.11

La prise d'empreinte d'un appareil 802.11 est la mesure de son trafic dans le but d'identifier l'appareil le plus précisément possible. La prise d'empreinte est généralement effectuée en deux étapes. Première étape, l'apprentissage, qui permet de fabriquer l'empreinte d'une machine particulière et de lui associer un nom. Deuxième étape, la reconnaissance, qui permet au détecteur de vérifier la présence de la machine particulière parmi le trafic d'un ensemble de machines.

La prise d'empreinte idéale permet de reconnaître à coup sûr un appareil 802.11 individuel parmi un ensemble d'appareils quelconques. Peu de méthodes atteignent une telle précision (voir section 4). Plus souvent, la prise d'empreinte se borne à caractériser un *chipset* et un *driver* particuliers (voir sections 2 et 3). Dans ce cas, deux machines ayant exactement le même chipset et le même driver présenteront exactement la même empreinte.

On distingue deux grandes familles de prise d'empreinte : active et passive. Dans la méthode active, le détecteur envoie des trames à la cible. Dans la méthode passive, le détecteur se contente d'écouter le trafic naturel. Dans les deux cas, on peut imaginer que la prise d'empreinte est plus difficile si le réseau est protégé par une clé. En pratique, ce n'est pas plus difficile car 802.11 chiffre essentiellement les données, mais pas les trames de contrôle ni les options. Or ce sont justement les trames de contrôle et les options qui fournissent le plus d'informations sur les particularités d'implémentation des appareils, et donc les meilleures empreintes.

2 Test actif d'implémentation

Dans les méthodes actives, le détecteur envoie diverses trames 802.11 à la cible et analyse les réponses ou l'absence de réponse. Sur certains paramètres, les réponses varient significativement d'un matériel à un autre.

Ces variations révèlent des libertés dans l'implémentation des spécifications, des différences dans les choix de valeurs par défaut, des extensions présentes ou non, etc.

Bratus et al. **[4]** présentent une méthode qui permet la prise d'empreinte active des points d'accès, et à moindre titre des stations. Il s'agit d'envoyer au point d'accès des requêtes utilisant des combinaisons de paramètres atypiques, inutiles ou non définies. Plusieurs paramètres sont utilisés, parmi lesquels :

- les bits **FromDS** et **ToDS,** censés valoir zéro dans un message *Probe Request* ;
- les mêmes bits dans un message *Authorisation Request* ;
- l'absence d'élément attendu dans un message Probe Request, tels que le ESSID et l'information sur les taux de transfert ;
- des bits normalement à zéro dans une trame *Null Data* utilisée pour la gestion de consommation.

Remarque : c'est l'application dans la couche 2 du même principe que celui utilisé dans la couche 3 par un outil comme NMAP pour faire de l'*Operating System Fingerprinting*.

Ici, le nombre de paramètres permet une combinatoire importante qui mène à une méthode de prise d'empreinte assez précise. Une implémentation est disponible sous le nom « Baffle » **[3]**. C'est actuellement la méthode active la plus précise pour les points d'accès. L'utilisation sur des stations est moins efficace. En effet, pour obtenir des réponses intéressantes de la part d'une station, il faut déjà qu'elle soit en mode authentifié ou en mode associé. Or, l'envoi de trames anormales à une station peut aussi provoquer une désassociation ou une désauthentification qui peut à son tour fausser les tests suivants.

2.1 Prise d'empreinte active des points d'accès

Il est possible de généraliser la méthode de Bratus en envoyant toutes les combinaisons d'options possibles et en observant les éventuelles réponses. Pour démontrer cela, nous avons développé un exemple complet de prise d'empreinte active de point d'accès. Pour l'injection de trames en 802.11, on utilise Scapy **[I]**. Tout d'abord, il faut mettre la carte 802.11 en mode *monitor*.

```
# ifconfig wlan0 down
# iwconfig wlan0 mode monitor
# ifconfig wlan0 up
```

Le script Python ci-dessous envoie des trames Probe Request. Une trame est envoyée pour chaque combinaison possible du champ **FCfield**. Il y a huit bits, ce qui donne un total de 256 trames envoyées. Le champ **FCfield** indique un ensemble d'options, telles que **From-DS** ou **To-DS**. Beaucoup de combinaisons de ces options ne sont pas supportées par le standard. Certains points d'accès répondent à un sous-ensemble de ces combinaisons, d'autres pas.

Le script imprime un 1 à chaque fois que le point d'accès cible répond et 0 sinon. Ainsi, une chaîne de 256 bits est retournée. Cette chaîne peut être considérée comme un descripteur précis du point d'accès cible.

```
import sys
from scapy.all import *
fingerprintee=sys.argv[1]
fingerprinter=sys.argv[2]
dot11_frame = Dot11(addr1=fingerprintee, addr2=fingerprinter,
addr3=fingerprintee)/Dot11ProbeReq()
for x in range(256):
    dot11_frame.FCfield=x
    p=srp1(RadioTap()/dot11_frame,iface='wlan0',verbose=0,timeout=1)
    if (type(p) == scapy.layers.dot11.RadioTap) :
        sys.stdout.write("1")
    else:
        sys.stdout.write("0")
    sys.stdout.flush()
```

Ce script s'appelle **activeFP_AP.py**. Il prend pour premier argument l'adresse MAC du point d'accès dont on recherche l'empreinte, noté **fingerprintee** dans le script. Il prend pour second argument l'adresse MAC du détecteur, noté **fingerprinter** dans le script. Avant d'exécuter le script, il faut bien s'assurer d'être sur le même canal 802.11 que la cible (**# iwconfig wlan0 channel XX**). En lançant ce script sur trois points d'accès différents, nous obtenons trois champs de bits très différents.

```
#python activeFP_AP.py 00:06:14:00:33:7f 0c:23:e6:b2:fa:3b
00000000000000000000000000000000000000001100000011000000100000001100
00000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000

#python activeFP_AP.py 00:77:cf:bf:ef:46 0c:23:e6:b2:fa:3b
00000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000100000000000000100000000000000000000

#python activeFP_AP.py 00:0e:25:2b:97:1f 0c:23:e6:b2:fa:3b
11111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111000000
11111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111
```

2.2 Prise d'empreinte active des stations clientes

On peut aussi prendre des empreintes de stations clientes en envoyant un ensemble de trames non supportées par le standard et en observant le comportement de la cible. Bratus propose d'envoyer par exemple des trames de désauthentification/désassocation avec le champ **From-DS** ou **To-DS** à 1.

Dans notre exemple, on envoie des trames de désauthentification. Une trame est envoyée par combinaison possible du champ **FCfield**, ce qui donne un total de 256 trames envoyées. Comme pour notre script testant les points d'accès, le script imprime un 1 à chaque fois que la cible répond par une *Reassociation Request*, et 0 sinon. Ainsi, une chaîne de 256 bits est retournée. Cette chaîne peut être considérée comme un descripteur de la station cliente cible.

```
import sys
from scapy.all import *
fingerprintee=sys.argv[1]
AP=sys.argv[2]
dot11_frame = Dot11(addr1=fingerprintee, addr2=AP, addr3=AP)/
Dot11Deauth()
for x in range(256):
    dot11_frame.FCfield=x
    sendp(RadioTap()/dot11_frame,iface='wlan0',verbose=0)
    ans = sniff(iface='wlan0',timeout=2)
    response=0
    for i in ans:
        if (i.haslayer(Dot11ReassoReq) and string.lower(i[Dot11].
        addr2)==string.lower(victim)):
            response=1
    sys.stdout.write(str(response))
    sys.stdout.flush()
```

Ce script s'appelle **activeFP_STA.py**. Avant d'exécuter le script, il faut s'assurer d'être sur le même canal 802.11 que la station cible (**# iwconfig wlan0 channel XX**). Les traces ci-dessous montrent les résultats d'une prise d'empreinte sur deux stations différentes. La chaîne retournée est bien différente pour les deux équipements. De plus, cette chaîne ne varie pas d'un test à un autre pour une même station cliente. Ce qui est mesuré ici, c'est essentiellement le couple *chipset/driver*. Selon les constructeurs et les configurations, il n'est pas évident de savoir qui du chipset ou du driver a le plus d'influence. En changeant de driver lorsque c'était possible, nous avons pu constater des modifications dans les empreintes mesurées.

```
#python activeFP_STA.py 00:2a:3a:4c:60:34 00:06:14:00:33:7f
10001000000010000000100000001000000010000000100000001000000001000
00000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000

#python activeFP_STA.py 00:29:c3:91:80:16 00:06:14:00:33:7f
00101000001010000010100000101000001010000010100000101000001010000
00000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000
```

Les mesures d'une station peuvent être améliorées de plusieurs manières. Tout d'abord, on constate des réponses différentes selon qu'on envoie des trames de désassociation ou des trames de désauthentificaton. Nous avons constaté que des machines Windows envoient beaucoup plus de réponses sur des trames de désassociation que ne le font les machines Linux. On peut également s'inspirer du *fuzzing* pour améliorer les tests. Par exemple, en ordonnant les tests de manière aléatoire pour limiter les effets de bord d'un test sur l'autre ou moyenner ces effets. Aussi, et au risque de ralentir le processus de prise d'empreinte, le détecteur peut s'assurer avant chaque test que la station cible est bien dans l'état souhaité. Enfin, on peut faire les tests plusieurs fois et ne retenir que les valeurs majoritaires pour les bits à 0 ou à 1.

3 Test passif d'implémentation

Nous montrons maintenant une technique passive. Il s'agit toujours de rechercher des défauts d'implémentation. Mais ici, nous cherchons à constater les défauts plutôt qu'à les provoquer. L'avantage d'une telle technique est qu'elle est indétectable : aucune trame n'est émise sur le réseau. L'inconvénient est le temps d'attente, voire l'absence d'empreinte lorsque les événements attendus ne se produisent pas.

3.1 Algorithme de Probe Request

Franklin et al. **[7]** remarquent d'importantes variations dans l'algorithme d'envoi de trames Probe Request. Cet algorithme est souvent utilisé par les stations pour se connecter, en plus de l'algorithme passif par écoute des Beacon. Sur les centaines de pages de la spécification 802.11, une seule page est consacrée à la description de cet algorithme pourtant non trivial. Les constantes critiques sont nommées, par exemple, **Min_Probe_Response_Time**, mais aucune valeur de référence n'est indiquée.

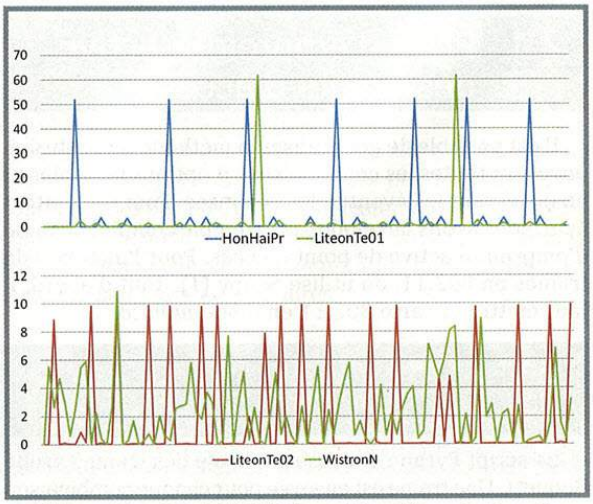


Figure 1 : Variabilité dans l'implémentation du mécanisme de Probe Request. Abscisse : numéro du Probe Request de 1 à 100. Ordonnée : délai en secondes entre deux trames Probe Request.

On retrouve donc naturellement d'importantes variations d'un constructeur à l'autre, comme le montre le graphique 1. Cette méthode est particulièrement discriminante et facile à mettre en œuvre. En revanche, elle est assez facile à contrer : il suffit de supprimer l'envoi de Probe Request. C'est faisable, par exemple, sur Windows en décochant l'option de connexion automatique dans les propriétés du réseau sans fil. Il est plus difficile de supprimer les Probe Request sur les téléphones mobiles.

4 Mesure de dérive d'horloge

Il s'agit d'une méthode passive un peu particulière dont la précision théorique va jusqu'à la machine elle-même et pas seulement le chipset et le driver. Dans le meilleur des cas, on peut reconnaître l'empreinte d'une machine précise parmi toutes les autres, sur différents réseaux.

Toute machine possède une horloge, basée sur la vibration d'un quartz. Le quartz donne le rythme auquel le temps s'écoule. Chaque quartz étant physiquement différent, le temps s'écoule plus rapidement pour certaines horloges que pour d'autres. Ainsi, les horloges ont toutes une dérive différente.

Une méthode de prise d'empreinte consiste donc à mesurer précisément la dérive d'horloge, c'est-à-dire mesurer si le temps de la cible s'écoule plus rapidement ou plus lentement que le temps de la machine de l'observateur. Ceci donne une empreinte « physique » puisqu'elle dépend directement du quartz de la machine. Kohno et al. **[11]** ont démontré qu'on pouvait mesurer la dérive d'horloge d'une machine cible en observant les *timestamps* du protocole TCP. Si les conditions de mesure sont correctes et si la durée de la mesure est suffisante, alors la dérive caractéristique peut être calculée avec précision.

Récemment, il a été démontré qu'on pouvait faire la mesure de la dérive d'horloge en 802.11. En effet, les cartes 802.11 ainsi que les points d'accès ont eux aussi leur propre quartz. Ainsi, deux cartes 802.11 produites par le même constructeur sur la même chaîne de montage auront quand même deux quartz différents : l'une dérivera par exemple de +17µsec/sec, l'autre dérivera de −42µsec/sec. Une dérive de 17µsec/sec veut dire que l'horloge mesurée s'incrémente de 17µsec de plus par seconde que l'horloge de l'observateur.

Remarque

Plusieurs facteurs contribuent à l'efficacité de la méthode en 802.11 par rapport à la méthode de Kohno en IP. Tout d'abord les dérives typiques des cartes 802.11 sont plus grandes que les dérives typiques des horloges principales. En effet, ces horloges nécessitent moins de précision à long terme et peuvent se recaler sur l'horloge principale. Ensuite, les mesures sont effectuées directement en 802.11, qui introduit moins de délai et de variation qu'Internet dans la méthode de Kohno. Ce point a une grande influence sur la mesure des stations clientes (voir 4.2).

4.1 Points d'accès

Jana et al. **[10]** mesurent la dérive d'horloge des points d'accès. La mesure est facilitée par la présence du champ **timestamp** dans chaque trame Beacon envoyée par le point d'accès. Il suffit de comparer la valeur de ce champ et l'heure de réception locale du détecteur. Quelques centaines de Beacon suffisent pour calculer une dérive stable. Les trames Beacon sont envoyées dix fois par seconde, cette valeur étant fixée par la norme. En pratique, une mesure fiable est obtenue en moins de 100 secondes.

Le script ci-dessous montre comment calculer la dérive d'horloge d'un point d'accès. Le script récupère les Beacon du BSSID indiqué en paramètre. Après réception de 1000 Beacon, le script calcule la dérive d'horloge en comparant le temps écoulé selon les Beacon et le temps écoulé selon l'horloge locale.

```
[...]
def sniffAP(p):
    [...]
    if (p.haslayer(Dot11Beacon) and string.lower(BSSID)==string.
    lower(p[Dot11].addr3)):
        ssid = p[Dot11Elt].info
        beacon_timestamp = p[Dot11Beacon].timestamp
        recep_timestamp = p.time*1000000
        receptime_list.append(recep_timestamp)
        beacontime_list.append(beacon_timestamp)
        if (len(receptime_list)==1):
            return
        if ((receptime_list[len(receptime_list)-1] < receptime_
        list[len(receptime_list)-2]) | (beacontime_list[len(beacontime_
        list)-1] < beacontime_list[len(beacontime_list)-2])):
            reference_index=len(receptime_list)-1
            return
        if (len(receptime_list)>1000):
            skew = ((beacontime_list[len(beacontime_list)-1]-beacontime_
            list[reference_index]
-receptime_list[len(receptime_list)-1]+receptime_list[reference_index])
*1000000)/(recep_timestamp-receptime_list[reference_index])
print ssid+"\t"+str(skew)
            exit()

sniff(iface="wlan0", prn=lambda x:sniffAP(x))
```

La méthode de calcul utilisée est très simple. Ainsi, elle ne compense pas les imprécisions de l'horloge de réception dues par exemple à une charge du système. Des méthodes d'interpolation peuvent compenser ces imprécisions.

Un exemple de prise d'empreinte sur un point d'accès est monté ci-dessous.

```
#python timeSkew.py 00:1c:88:88:8c:1a
WLAN1 -10.2885593987
#python timeSkew.py 00:1c:88:88:8c:1a
WLAN1 -9.79307669697
#python timeSkew.py 00:1c:88:88:8c:1a
WLAN1 -10.4997129157
#python timeSkew.py 00:1c:88:88:8c:1a
WLAN1 -9.88750225585
```

4.2 Stations clientes

Les stations clientes n'envoient pas de trames 802.11 contenant un champ **timestamp** ou équivalent. On ne peut donc pas calculer la dérive comme précédemment avec les points d'accès.

Loh et al. **[12]** proposent une méthode alternative. Celle-ci consiste à observer les trames Probe Request sur une longue période, une heure et plus. Ensuite, la méthode regroupe les probes envoyés par rafales et calcule le temps entre les rafales. Celles-ci sont ensuite représentées sur un graphe : un exemple extrait directement du papier **[12]** est montré en figure 2. On remarque que les temps entre rafales dérivent légèrement. En particulier, pour un cluster de rafales donné, le temps entre rafales n'est pas exactement constant : on constate une pente non nulle dans chaque cluster. Cette pente est en fonction directe de la dérive d'horloge. Ainsi, chaque carte 802.11 génère une figure légèrement différente.

Il faut noter que la durée de la mesure, au moins une heure, restreint l'utilisation pratique de cette méthode à des cas particuliers : présence dans une salle de conférence, dans une salle de cours, etc.

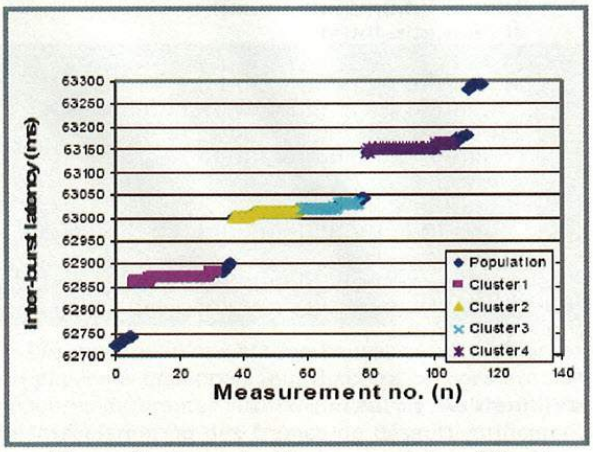


Figure 2 – Exemple d'une empreinte reflétant la dérive d'horloge en observant les trames Probe Request de stations clientes. Abscisse : numéro d'index des rafales. Ordonnée : temps en millisecondes entre les rafales.

4.3 Méthode d'évasion

Une méthode pour tromper la prise d'empreinte par dérive d'horloge des points d'accès est décrite dans **[2]**. Il s'agit de créer un point d'accès ayant la même dérive d'horloge qu'un autre point d'accès. Pour cela, l'attaquant crée deux interfaces virtuelles pour une même carte 802.11. Une de type station et une de type AP. Cela peut être fait avec les commandes suivantes :

```
#iw dev phy0 interface add mystation type station
#iw dev phy0 interface add myap type __ap
```

L'interface virtuelle *mystation* s'associe alors avec le point d'accès à répliquer. L'interface virtuelle *myap* crée un point d'accès en utilisant par exemple **hostapd**. Or, et c'est le point clé, le standard spécifie qu'une station cliente associée à un point d'accès doit se synchroniser à chaque Beacon reçu. L'interface virtuelle mystation synchronise donc l'horloge de sa carte 802.11. Comme l'interface virtuelle myap partage la même carte 802.11, elle partage aussi la même horloge physique. Au final, l'interface virtuelle myap est synchronisée avec l'horloge du point d'accès à répliquer. Et le détecteur mesure une dérive nulle puisqu'il mesure une réplique (presque) parfaite de sa propre horloge.

5 Autres techniques et usages

Il existe plusieurs autres techniques de prise d'empreinte, peut-être moins précises que celles décrites précédemment. Nous les évoquons rapidement avant de montrer quelques applications typiques de la prise d'empreinte.

5.1 Autres techniques

Dès 2006, Gopinath et al. **[8]** ont observé, selon les constructeurs, des variations de paramètres tels que les temps d'attente avant l'envoi de trames (*random back-off timers*), les valeurs du champ **duration**, l'utilisation de champs réservés, etc. Une mesure de l'ensemble de ces particularités peut conduire à une empreinte.

La même année, Johnny Cache **[6]**, dans son projet de fin d'étude, propose deux méthodes pour prendre l'empreinte d'une carte. La première méthode est passive et consiste à observer les valeurs du champ **duration**. Ce champ indique combien de temps la carte émettrice souhaite réserver le canal 802.11 pour émettre une trame. Chaque carte sans fil calcule la valeur **duration** différemment. Certaines cartes produisent même des valeurs non supportées par le standard. Johnny Cache propose un ensemble de calculs statistiques qui, appliqués indépendamment à chaque type de trame envoyé, permet d'obtenir une empreinte pour la carte émettrice. Ces tests

montrent que ce champ permet à lui seul de différencier le chipset de la carte sans fil. Une implémentation non maintenue est disponible **[5]**.

Johnny Cache propose aussi une méthode active. Il détecte des différences de comportement entre stations vis-à-vis du mécanisme de redirection d'association. Ce mécanisme permet normalement à un point d'accès de rediriger dynamiquement des stations vers un autre point d'accès. Pour cela, le point d'accès change juste le BSSID dans le message Association Reply. En pratique, certains chipsets obéissent à l'ordre de redirection, d'autres non. De plus, un ordre de redirection contient plusieurs paramètres comme l'adresse source et le BSSID. En faisant varier ces paramètres et en itérant les tests, J. Cache différencie plusieurs catégories de stations. Là encore, il est difficile de différencier l'effet précis du chipset de l'effet précis du driver. Cette méthode offre un grand nombre de combinaisons possibles, mais peu ont été observées en pratique (cf. pages 47à 50 dans **[5]**) parce que la méthode n'a pas été testée sur beaucoup de machines.

5.2 Usages

Le premier usage est la reconnaissance de point d'accès pour éviter les *rogue access points* (cf. *evil twin attack*). L'attaquant forge un faux point d'accès, semblable au vrai, puis attend que des stations légitimes se connectent et il contrôle alors leur trafic réseau. Avec une méthode de prise d'empreinte, une station vérifie d'abord l'empreinte du point d'accès et agit en conséquence.

Symétriquement, le point d'accès peut vérifier les empreintes des stations. C'est utile sur des réseaux effectuant un contrôle d'accès par adresse MAC. En effet, si un attaquant peut facilement forger une adresse MAC (`C:\tmac -n Local -m 00:01:02:03:04:05 -re`, `# ifconfig wlan0 hw ether 00:01:02:03:04:05`, ...) pour passer outre le contrôle d'accès, il lui sera plus difficile de forger une empreinte 802.11 valide.

On trouve des usages de la prise d'empreinte liés à la localisation des machines. Un ordinateur portable peut mesurer les empreintes 802.11 environnantes et en déduire sa localisation. Localisé dans le domicile, l'ordinateur ne demande pas de mot de passe au login, partout ailleurs, il en demande un.

Des empreintes suffisamment stables, différenciées et nombreuses, pourraient en théorie caractériser un utilisateur précis. Ce cas deviendra préoccupant si le nombre d'appareils 802.11 mobiles continue d'augmenter. Par exemple, la combinaison de trois empreintes : un téléphone professionnel (802.11 activé), un téléphone personnel (802.11 activé) et un ordinateur portable, sert de signature pour un utilisateur nomade. On peut alors détecter cette combinaison unique et marquer des points de présence sur une carte...

La prise d'empreinte est aussi utilisée pour l'appariement d'appareils ayant temporairement des déplacements similaires : téléphones portés par une même personne, station 802.11p d'un véhicule et téléphone mobile du conducteur, etc. Ces deux appareils utilisent les empreintes 802.11 environnantes et leurs variations au cours des déplacements comme une source d'information corrélée. Sur cette base, ils décident d'un secret partagé, difficile à forger pour un attaquant n'ayant pas suivi le même trajet au même moment. ■

■ REMERCIEMENTS

Merci à SID pour ses remarques éclairées et éclairantes !

■ RÉFÉRENCES

[1] Scapy, http://www.secdev.org/projects/scapy/

[2] C. Arackaparambil, S. Bratus, A. Shubina and D. Kotz, « On the reliability of wireless fingerprinting using clock skews », in Proceedings of ACM WiSec 10, March 2010

[3] S. Bratus, Baffle, http ://baffle.cs.dartmouth.edu/

[4] S. Bratus, C. Cornelius, D. Kotz and D. Peebles, « Active behavioral fingerprinting of wireless devices », in Proceedings of ACM WiSec'08, March 2008

[5] J. Cache, Publications of Johnny Cache, http://www.802.11mercenary.net/johnycsh/publications/

[6] J. Cache, Fingerprinting 802.11 Devices, Master Thesis, 2006

[7] J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. V. Randwyk and D. Sicker, « Passive data link layer 802.11 wireless device driver fingerprinting », in Proceedings Usenix Security 06, August 2006

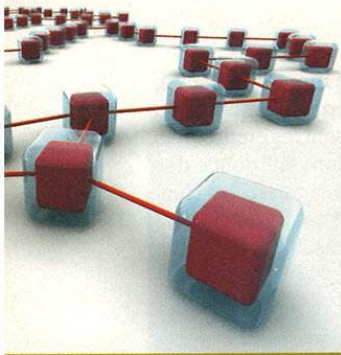
[8] K. Gaopinath, P. Bhagwat and K. Gopinath, « An empirical analysis of heterogeneity in ieee 802.11 mac protocol implementations and its implications », in Proceedings of ACM WiNTECH'06, September 2006

[9] C. Heffner, WiFinger, http ://www.sourcesec.com/2009/05/09/wifingerpassive-wireless-fingerprinting-tool/

[10] S. Jana and S. K. Kasera, « On fast and accurate detection of unauthorized wireless access points using clock skews », in Proceedings of ACM MobiCom 08, September 2008

[11] T. Kohno, A. Broido and K. C. Claffy, « Remote physical device fingerprinting », IEEE Trans. Dependable Secur. Comput., 2 :93–108, April 2005.

[12] D. C. C. Loh, C. Y. Cho, C. P. Tan and R. S. Lee,« Identifying unique devices through wireless fingerprinting », in Proceedings of ACM WiSec'08, March 2008.



LES CONFIGURATIONS DES ÉQUIPEMENTS RÉSEAU NE SONT PLUS STATIQUES

Cédric Llorens (cedric.llorens@wanadoo.fr) et Denis Valois (denis.valois@laposte.net)

mots-clés : RÉSEAU / SÉCURITÉ / CONFIGURATION / PROGRAMME

Cet article décrit comment les configurations des équipements réseau sont devenues dynamiques grâce à la possibilité d'embarquer de véritables programmes pouvant les modifier à la volée. De plus, il décrit aussi les dangers de sécurité associés et donne quelques recommandations.

1 Introduction

Grâce aux évolutions technologiques, Cisco offre maintenant la possibilité d'embarquer et d'exécuter des scripts au sein de ces équipements réseau.

Ainsi, et via son offre « Embedded Event Manager (EEM) », il est possible d'associer à des événements réseau une action ou un script/programme : une configuration qui était statique auparavant devient dynamique maintenant. En effet, un tel script peut en effet modifier la configuration actuelle en une nouvelle configuration lors de son exécution.

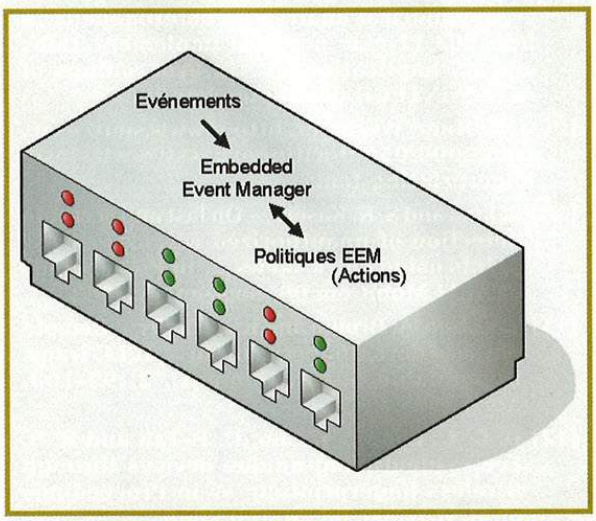


Figure 1 : Gestion des événements par EEM

Les enjeux de la sécurité liés à cette nouvelle fonctionnalité sont importants si une telle pratique n'est pas fortement encadrée. Après une description du « Embedded Event Manager (EEM) », nous décrirons ensuite les risques de sécurité associés et quelques recommandations de sécurité.

2 Embedded Event Manager (EEM)

Cisco « Embedded Event Manager » est une technologie permettant de développer et d'exécuter des actions pour automatiser des tâches associées à un équipement réseau, comme l'illustre la figure 1.

Pour simplifier, il y a trois composants dans le cadre EEM :

- Les événements : ils sont de natures diverses telles que des événements de type syslog, les événements liés à des données snmp, les événements liés à des protocoles de routage, etc.
- EEM *(Embedded Event Manager)* : associé à des politiques EEM, il permet d'exécuter les politiques en fonction des événements reçus.
- Les politiques EEM définissent de manière précise les actions à faire pour des événements particuliers.

Il y a deux moyens d'écrire des politiques EEM, soit en mode *applet* CLI (*Command Line Interface*), soit en mode TCL (*Tool Command Langage*). Quel que soit le mode choisi, il est possible d'appeler via ces politiques des scripts écrits en langage TCL.

2.1 Le langage TCL (Tool Command Langage)

TCL est un langage interprété intégré dans le système d'exploitation de Cisco IOS ou IOS-XR. Proche du langage C, on peut exécuter des commandes TCL de manière interactive ou via un script stocké en mémoire **[TCL]**.

Pour rentrer en mode interactif et passer des commandes TCL, on lance les commandes suivantes pour afficher, par exemple, les interfaces d'un routeur :

```
routeur#tclsh

routeur(tcl)#set test [exec "show ip int brief"]

routeur(tcl)#foreach line [split $test "\n"] {puts $line}
      Interface       ip address
      GigabitEthernet 0/0  10.0.0.1
      GigabitEthernet 0/0.1  10.0.0.2
      GigabitEthernet 0/0.2  10.0.0.3
      GigabitEthernet 0/0.3  10.0.0.4

routeur(tcl)#
```

Pour lancer un script TCL, il suffit de lancer la commande suivante en prenant l'hypothèse que le script est en mémoire flash ou NVRAM (non volatile RAM) :

```
routeur#tclsh flash:script.tcl
```

Le langage TCL permet d'écrire de véritables programmes complexes contenant des boucles conditionnelles, scripts hiérarchiques, etc. La procédure suivante, écrite en TCL, permet d'afficher de manière indentée les interfaces de type Ethernet :

```
proc get_bri {} {
    set check ""
    set int_out [exec "show interfaces"]
    foreach int [regexp -all -line -inline "(^Ethernet\[0-9]/\[0-
    9])" $int_out] {
        if {![string equal $check $int]} {
            if {[info exists bri_out]} {
                append bri_out "," $int
            } else {
                set bri_out $int
            }
            set check $int
        }
    }
    return $bri_out
}
```

Avec un script TCL, vous pouvez donc faire tout ce que vous voulez, écrire une nouvelle configuration, établir une session avec l'extérieur, envoyer des emails, lancer des requêtes snmp, etc. ; bref, le parfait couteau suisse pour le meilleur et pour le pire.

2.2 Politique EEM en mode Applet CLI

Cette méthode permet de définir une politique avec trois types de commandes :

- La commande **event** permet de définir sur quel événement l'applet doit être exécutée.
- La commande **action** définit les commandes à exécuter.
- La commande **set** permet de stocker une valeur dans une variable liée à l'applet.

Une politique EEM s'écrit en exprimant l'événement que l'on souhaite détecter et en y associant les actions à mener. Par exemple, pour une configuration Cisco :

```
event manager applet OSPF
  event syslog pattern "Neighbor Down: Dead timer expired"
  action 1.0 cli command "enable"
  action 1.1 cli command "sh proc cpu | append flash:cpu_info"
  action 1.2 cli command "show interface | append flash:interface_info"
  action 1.6 syslog msg "OSPF NEIGHBOR DOWN"
```

Cette politique détecte les événement de type syslog « Neighbor Down: Dad timer expired » et exécute alors une série de commandes sauvant dans sa mémoire flash des informations liées au processeur et aux interfaces.

Il est aussi possible de lancer des scripts de type TCL de la manière suivante :

```
event manager applet OSPF
  event syslog pattern "Neighbor Down: Dead timer expired"
  action 1.0 cli command "tclsh flash:script.tcl"
```

2.3 Politique EEM en mode TCL

Une politique EEM s'écrit en exprimant l'événement que l'on souhaite détecter et en y associant les actions à mener. Par exemple, pour une configuration Cisco :

```
event manager policy script.tcl type system
```

Le script TCL associé suit alors une structure (de codage) précise pour correspondre à une telle politique EEM :

- Définition des événements à détecter.
- Définition des variables d'environnement utilisées dans le script TCL et liées à la commande *event manager* dans la configuration de l'équipement.
- Import des commandes à des librairiesbibliothèques EEM, etc.
- Variable liée au statut d'entrée indiquant si une politique s'est exécutée avant celle-ci pour le même événement et donnant le statut de son exécution (statut de succès, etc.).

- Le corps du script TCL.
- La valeur du statut de sortie utilisée par le processus EEM.

De nombreux sites existent, où l'on peut trouver des scripts gratuits similaires à des bibliothèques de fonctions.

3 Les risques de sécurité

Manuel Humberto Santander Pelaez **[Santander]** a décrit deux types d'utilisation de script TCL pour créer des trojans sur des routeurs Cisco. Ces deux utilisations supposent que l'attaquant a pu pénétrer un routeur Cisco via une faiblesse de sécurité liée au système d'exploitation IOS ou par un accès légitime provenant de l'interne **[Santander]**.

La preuve de concept de ces deux exemples illustre qu'il est possible, via des scripts TCL, de mettre en place des trojans rendant leur détection difficile. En effet, savoir si un script TCL est ou n'est pas un trojan en définitif est équivalent à la détection de virus dans un programme **[Cohen]**.

Quelle que soit la méthode d'accès au routeur, les scripts sont téléchargés dans la mémoire flash ou NVRAM (non volatile RAM) via des protocoles tels que sftp, ftp, etc.

3.1 Trojan connectant l'équipement à un serveur

Dans cet exemple, l'attaquant utilise EEM pour définir une politique afin de lancer le trojan pour chaque démarrage de l'équipement par la commande de configuration suivante (détection de l'événement lié au démarrage) :

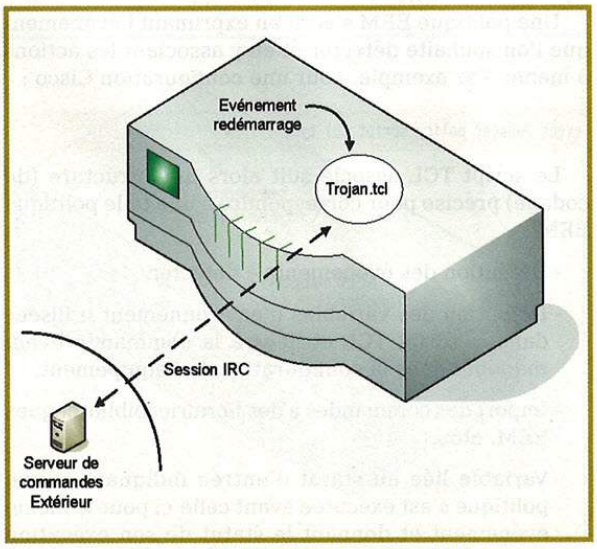


Figure 2 : Trojan et session IRC

```
event manager applet Trojan1
  event syslog pattern "SYS-5-RESTART"
  action 1.0 cli command "enable"
  action 1.0 cli command "tclsh bootflash:trojan1.tcl"
```

Une fois le programme **trojan1.tcl** lancé, le script établit une connexion avec un serveur distant via le protocole IRC et se met en boucle dans l'attente de commande du dit serveur, comme l'illustre la figure 2.

Comme évoqué en préambule, tous les outils sont là (présents sur l'équipement) pour gérer une gestion de socket réseau via le langage TCL.

3.2 Trojan se substituant au CLI de l'équipement

Le deuxième exemple est encore plus bluffant dans le sens où le trojan (script TCL) se substitue littéralement au CLI du routeur *(Command Line Interface)*. Ainsi, lorsqu'un utilisateur se connecte à l'équipement, il croit parler au CLI du routeur, mais interagit en fait directement avec le trojan, comme l'illustre la figure 3.

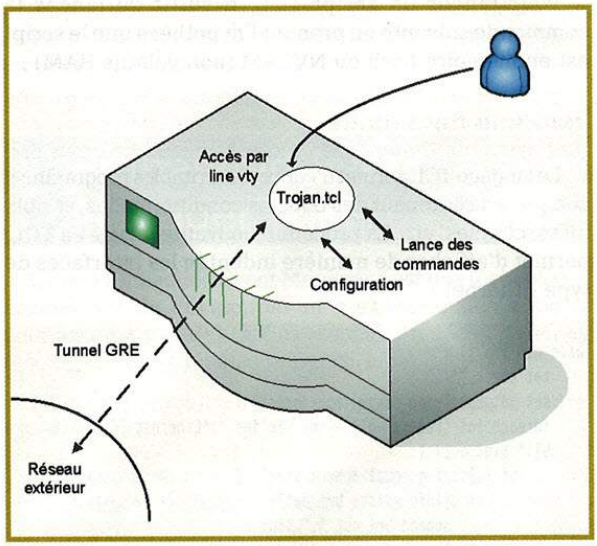


Figure 3 : Trojan et masquage du CLI

Prenons les choses dans l'ordre, la première étape consiste donc à lancer le trojan chaque fois qu'un utilisateur se connecte. Dans un contexte Cisco et pour un utilisateur distant, celui-ci se connecte via une « line vty ». Pour lancer notre trojan, il suffit d'associer une commande qui s'exécute automatiquement et à chaque accès utilisateur, comme l'illustre le code suivant :

```
Line vty 0 4
 login
 autocommand tclsh nvram:trojan2.tcl
```

Une fois lancé, le script réalise plusieurs actions :

- Il modifie la configuration pour y configurer un tunnel GRE (*Generic Routing Encapsulation*) et un utilisateur pour authentifier cette connexion. La connexion s'établit et permet de créer ainsi une porte dérobée. Malgré la présence de ces instructions de configuration, on verra comment le trojan masque à un utilisateur la configuration réelle de l'équipement.
- Le trojan émule une interface CLI en détournant certaines commandes qui pourraient montrer à l'utilisateur qu'une *backdoor* existe sur l'équipement. Ainsi et pour la commande `show interfaces`, qui montre toutes les interfaces du routeur, l'interface GRE serait donc dévoilée à l'utilisateur. Le trojan exécute donc la commande réelle, mais ne montre à l'utilisateur qu'un résultat filtré (sauvegarde du résultat de la commande éelle en mémoire) censurant l'interface GRE.

Grâce aux détournements de plusieurs autres commandes, qui pourraient dévoiler la backdoor, le trojan interdit aussi des commandes qui pourraient lancer une session `tclsh` pouvant compromettre le trojan.

Reconfiguration, connexion à l'extérieur et masquage du mode CLI sont mis en œuvre par cette preuve de concept dont le code TCL fait 342 lignes. Le code complet et les explications détaillées sont disponibles sur le site de l'auteur **[Santander]**.

Enfin, la détection d'un tel trojan est potentiellement aussi complexe que la détection d'un trojan sur n'importe quel système. Cependant, la fuite de trafic réseau par la porte dérobée peut être un moyen de détection ainsi que l'utilisation de commandes avancées sur Cisco. Un anti-virus sur l'IOS Cisco verra peut-être le jour !!

4 Quelques recommandations de sécurité

Voici quelques recommandations liées à l'utilisation de script TCL au sein d'un réseau :

- Il est préférable d'utiliser EEM en mode applet sans appel de script TCL (rappel : un appel de script TCL via EEM se fait dans une configuration Cisco par la commande `tclsh script.tcl`). La raison est que tous les éléments/instructions apparaissent alors directement dans la configuration et sont visibles à la lecture de la configuration (via la commande `show run`). Rappelons que le contenu d'un script TCL n'apparaît pas dans la configuration de l'équipement (seul son appel apparaît : `tclsh script.tcl`). Pour voir le script en soit (c'est-à-dire le code), il faut alors regarder directement le fichier `script.tcl` stocké dans la mémoire de l'équipement.
- Mettre en œuvre des contrôles de configuration approfondis **[MISC 52]**.
- Limiter au maximum l'usage des scripts TCL pour gérer, par exemple, des bugs temporaires. Un script TCL est un vrai programme qui peut induire des effets de bord importants sur un équipement ou sur un réseau.
- Il faut mettre en œuvre un système de contrôle d'authentification, autorisation et de traçage afin de limiter/contrôler l'accès aux commandes EEM et de limiter l'accès au shell `tclsh`.
- Les actions liées à une politique EEM doivent être contrôlées en définissant un utilisateur et un profil d'autorisation. Ainsi, lors de l'exécution des commandes, les serveurs centraux AAA (*Authentication Authorisation Accounting*) valideront alors l'exécution des commandes lancées par une politique EEM donnée.
- Cisco permet, grâce au support cryptographique (utilisation de la bibliothèque OpenSSL et de certificat pour la signature), de signer des scripts TCL afin d'assurer leur provenance. La procédure complète de création de scripts TCL est disponible à cette référence **[TCL SIGNED]**.
- Cisco offre aussi un environnement fermé TCL appelé *safe-tcl* dans lequel la protection du système est renforcée et les fonctions/applications offertes sont réduites.

Conclusion

Une nouvelle ère s'ouvre avec des équipements dont la configuration peut être modifiée de manière dynamique par des scripts TCL. Le temps des configurations statiques est révolu, apportant ses améliorations techniques ainsi que ses problématiques sécurité. ■

▪ RÉFÉRENCES

[Cohen] Site de référence de F.Cohen : Computer Viruses - Theory and Experiments : http://en.wikipedia.org/wiki/Fred_Cohen

[MISC 52] D.Valois, C.Llorens, « Une approche intégrée pour l'analyse des configurations – partie1 », journal MISC no52, novembre-décembre 2010.

[TCL] http://fr.wikipedia.org/wiki/Tool_Command_Language

[TCL SIGNED] Procédure de Cisco pour créer des scripts TCL signés : http://www.cisco.com/en/US/docs/ios/12_4t/netmgmt/configuration/guide/sign_tcl.html

[Santander] Site personnel de l'auteur contenant le code et explications des trojans, http://manuel.santander.name/

LE CLOUD COMPUTING : UN NUAGE D'ENJEUX JURIDIQUES

Garance Mathias – Avocat à la Cour

mots-clés : *DONNÉES / CONTRAT / EXTERNALISATION / CNIL / TRANSFERTS, SÉCURITÉ / CONFIDENTIALITÉ / RÉVERSIBILITÉ / RESPONSABILITÉ*

Du fait de l'apparition de l'infogérance, de l'externalisation dans les années 1980, puis de l'accessibilité de l'informatique dans les années 1990, et durant la dernière décennie, de la généralisation de l'Internet ; nous assistons aujourd'hui à l'explosion du cloud computing. Ce concept fait référence à l'utilisation des capacités de mémoire et de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. L'accès aux données et aux applications peut ainsi se faire à partir de n'importe quel périphérique connecté. En d'autres termes, le cloud computing permet de s'affranchir des contraintes traditionnelles et d'avoir une approche modulaire selon le besoin. Dans ce contexte international mutualisé, ces services nécessitent donc la rédaction de contrats afin d'appréhender les responsabilités de chacun des intervenants ainsi que la prise en compte des formalités imposées par la CNIL.

Le *cloud computing* ou traduction littérale, l'informatique dans les nuages **[1]**, est une nouvelle forme dématérialisée de fourniture de services et de ressources informatiques. L'accès aux données et aux applications est réalisé entre l'utilisateur et la multiplicité de serveurs distants, ce qui permet à celui-ci de générer des fichiers, de communiquer en ligne avec d'autres utilisateurs. Toutefois, la mutualisation et la délocalisation des serveurs multiplient les risques juridiques. Le cloud computing peut donc se définir comme une accessibilité à des « services » qui permettent d'accéder à des applications, une puissance de calcul, des moyens de stockage, etc.

De manière générale, les solutions cloud computing reposent sur des technologies de virtualisation et d'automatisation. Ainsi, le cloud computing peut être représenté en trois composantes principales dont il est indifféremment l'une, les deux ou encore les trois combinées :

- SaaS (*Sofware as a Service*) : il s'agit de la mise à disposition d'un logiciel, non pas sous la forme d'un produit que le client installe en interne sur ses serveurs, mais en tant qu'application accessible à distance comme un service, par le biais d'Internet et du Web. Les clients payent pour utiliser ces applications. L'utilisation reste transparente pour les utilisateurs qui ne se soucient ni de la plate-forme, ni du matériel qui sont mutualisés avec d'autres entreprises. Les principales applications actuelles de ce modèle sont la relation client (CRM), la vidéoconférence, la gestion des Ressources Humaines, etc.

- PaaS (*Plateform as a Service*) :il s'agit de la mise à disposition pour une entreprise d'environnements techniques pour développer des applications qui fonctionneront à distance comme pour le Saas. Toutefois, cet environnement inclura des outils de personnalisation et une intégration à d'autres programmes hébergés. L'objectif est ainsi de proposer un environnement modulaire capable de combiner plusieurs fonctions et processus métiers, voire plusieurs technologies en provenance de divers éditeurs.

- IaaS (*Infrastructure as a Service)* : il s'agit de la mise à disposition, à la demande, de ressources d'infrastructures dont la plus grande partie est localisée à distance dans des *data centers*. Les serveurs, postes de travail et imprimantes peuvent être facturés en fonction de leur utilisation.

En outre, il peut également coexister différents modèles de cloud :

- Cloud privé : il s'agit d'un cloud entièrement dédié et accessible via des réseaux sécurisés, hébergés chez un tiers. Ce cloud peut être interne à l'entreprise ou externalisé chez un prestataire.
- Cloud public : il est externe à l'organisation accessible via Internet, géré par un prestataire externe, propriétaire des infrastructures avec des ressources partagées entre plusieurs sociétés.

Pour résumer, trois caractéristiques clés du cloud le différencient des solutions informatiques traditionnelles, à savoir :

- des services à la place de produits technologiques avec mise à jour en continu et automatique ;
- un self-service et un paiement à l'usage (en fonction de ce que l'on consomme), ce qui induit des économies budgétaires conséquentes ;
- une mutualisation et une allocation dynamique de capacité (indépendant de toutes contingences matérielles, logicielles).

Le cloud computing constitue donc globalement une nouvelle forme d'informatique à la demande, à géométrie variable, que l'on pourrait placer d'un point de vue juridique à la croisée des services d'externalisation et des services d'ASP. Les utilisateurs des solutions de cloud computing restent propriétaires des données qui y sont hébergées, mais non des applications ou de l'architecture qui permettent leur utilisation ou leur hébergement.

Ainsi, le cloud computing pose de nombreux enjeux, notamment ceux du contrôle, de la sécurité et de la traçabilité des données. Dès lors, il s'agit de bien mettre en place des procédures d'habilitation et de contrôle d'accès aux données. En effet, on peut voir de nombreux exemples dans l'actualité faisant état de véritables défaillances des processus de sécurité, des fuites de données, comme pour Sony ou Amazon Web Services. Les entreprises doivent donc définir clairement leur rôle et responsabilité, tout en recherchant des solutions leur permettant de sécuriser l'externalisation de leurs données. Comme on le verra, ce conflit entre les responsabilités et le partage des tâches en ce qui concerne notamment la sécurité ne se résume pas à une simple relecture des contrats d'externalisation.

Le contrat cloud doit aborder la responsabilité de chaque partie et définir le périmètre de la prestation. Faute de contrat formalisant les partages de responsabilité, les procédures en cas de litige peuvent être longues et laborieuses dans un domaine où la jurisprudence est rare. En outre, le marché du cloud computing représente un enjeu économique majeur du secteur informatique : 6 milliards d'euros au niveau européen avec une croissance annuelle de l'ordre de 20 % **[2]**.

Dans ce contexte, il convient de mieux cerner les risques juridiques, pour ensuite appréhender les principales clauses contractuelles dans le cadre d'un projet cloud.

1 Les risques juridiques

Comme nous l'avons exposé, l'externalisation est un choix stratégique de l'entreprise. Ce choix doit prendre en compte les règles juridiques applicables, notamment celles concernant les données à caractère personnel **[3]**.

En effet, cette problématique des données personnelles est d'autant plus importante que les nouvelles dispositions issues de l'ordonnance du 24 août 2011 transposant le paquet télécoms impliquent une protection renforcée de la vie privée et, plus précisément, de ces données personnelles. Désormais, l'article 38 de l'ordonnance prévoit une procédure spécifique de notification à la CNIL et à l'utilisateur en cas de « faille de sécurité » **[4]**.

De prime abord, il est indispensable d'identifier les parties et de les qualifier en termes de responsabilité, à savoir le prestataire de cloud computing doit-il être considéré comme un sous-traitant ou comme le responsable du traitement **[5]** ? En effet, cette qualification complexe va entraîner un engagement de responsabilité différent pour le prestataire ou pour l'utilisateur. Si des services supplémentaires sont fournis par l'hébergeur, lui donnant ainsi la faculté de contrôler la manière dont les données personnelles sont traitées, cela pourrait avoir pour conséquence de modifier son statut de sous-traitant au profit de celui de responsable de traitement.

La responsabilité première en matière de données personnelles (sécurité, confidentialité, etc.) pèse sur le responsable du traitement et non sur le sous-traitant. Le sous-traitant, en application de l'article 35 de la loi n°78-17 du 6 janvier 1978 **[6]**, n'est tenu que par des obligations contractuelles de confidentialité et de sécurité visant à protéger les données personnelles contre la destruction accidentelle ou illicite, l'altération, la diffusion ou l'accès non autorisés.

Le droit français **[7]**, à l'instar de la majorité des lois nationales relatives à la protection des données personnelles au sens de la directive n°95/46/CE du 24 octobre 1995 **[8]**, considère en principe ce prestataire tiers (hébergeur du système de cloud computing) comme un sous-traitant des données agissant conformément aux instructions d'un responsable des données.

Cependant, compte tenu des difficultés de qualification, plusieurs critères ont été dégagés par le groupe de travail de la CNIL **[9]** afin de faciliter l'appréciation de la fonction de prestataire. Le faisceau d'indices élaboré par la CNIL repose sur les critères suivants :

- le niveau des instructions préalables données par le responsable du traitement. Il s'agit d'apprécier si le niveau d'instructions donné par le client au prestataire dans le cadre du contrat d'externalisation est général ou précis.
- le niveau du contrôle de l'exécution des prestations. Il s'agit de vérifier le degré de supervision du client en tant que responsable de traitement sur la prestation de son prestataire.

- la transparence. Il s'agit d'apprécier le degré de transparence du responsable de traitement au niveau de la prestation de service.

- l'expertise. Il s'agit d'apprécier le degré d'expertise du prestataire par rapport au client.

Ces critères doivent être appréciés dans leur ensemble : seule la réalisation de plusieurs de ces critères permettra de qualifier le prestataire.

Il convient d'aborder plus particulièrement la question du transfert des données personnelles dans le cloud. En effet, l'article 5 **[10]** de la loi de 1978 modifiée soumet à la loi française les traitements de données à caractère personnel dont le responsable du traitement est établi sur le territoire français ou dont les moyens de traitement sont situés sur le territoire français.

Dans le cadre de l'externalisation, le responsable du traitement devra donc s'assurer que le transfert de ses données dans ou via un pays s'effectue dans un pays ayant un niveau de protection adéquat. Ce transfert doit s'opérer dans le cadre des grands principes prévus par la loi Informatique et Libertés :

- Les transferts en dehors de l'Union européenne sont interdits **[11]**.

- Les exceptions à cette interdiction sont prévues par l'article 69 de la loi : ainsi, les transferts en dehors de l'Union européenne sont autorisés si le pays ou l'entreprise destinataire assure un niveau de protection adéquat aux données transférées. Cette protection adéquate peut être apportée de plusieurs manières :

  - légalement, si le pays destinataire des données personnelles a une législation reconnue par la commission européenne comme offrant une protection adéquate ;

  - de manière contractuelle, par la signature de Clauses Contractuelles Types, adoptées par la Commission européenne, entre l'entité exportatrice et l'entité importatrice de données personnelles, ou par l'adoption de Règles Internes d'entreprises (*Binding Corporates Rules*), qui constituent un code de conduite en matière de transferts de données personnelles depuis l'Union européenne vers des pays tiers ;

  - lorsque l'entité importatrice est basée aux États-Unis et qu'elle adhère aux principes du Safe Harbor **[12]**.

L'article 69 **[13]** permet également d'opérer des transferts dans des situations exceptionnelles. Ces autres dérogations s'opèrent néanmoins avec un contrôle strict de la CNIL qui délivre, le cas échéant, une autorisation. À titre d'illustration, l'exception en cas de consentement exprès de la personne est prévue dans le cadre de l'article 69. Toutefois, la CNIL, se fondant sur la définition posée par la directive, rappelle que ce consentement exprès doit être une manifestation positive de volonté (ce qui exclut, par exemple, de recueillir le consentement des personnes sur un site avec une case pré-cochée). Ce consentement doit également être donné et pouvoir être retiré librement, ce qui a pour conséquence d'invalider, en principe, le consentement de salariés donné à l'employeur, compte tenu de la dépendance hiérarchique dans laquelle ils se trouvent.

Le consentement de la personne doit enfin être spécifique. Ainsi seront considérés comme non valables les consentements donnés par anticipation à des transferts futurs non définis. Par ailleurs, l'intégralité des informations disponibles concernant le niveau de protection assuré par le pays destinataire devra être communiquée aux personnes concernées.

Étant précisé que ces procédures de transfert doivent préalablement recueillir l'autorisation de la CNIL et être soumises pour information aux institutions représentatives du personnel.

Toutefois, indépendamment de respecter les procédures, des réglementations sectorielles peuvent permettre à des autorités nationales locales d'accéder aux données. Ainsi, aux États-Unis, le Patriot Act permet au gouvernement américain d'accéder à toute donnée stockée sur son territoire, en cas d'urgence ou en cas de nécessité pour la sécurité nationale.

En outre, citons l'article 97 du Code de Procédure Pénale **[14]** qui indique que l'hébergeur doit être en mesure d'extraire de son cloud les éléments recherchés ou l'ensemble des informations concernant un client particulier.

Nonobstant le respect de normes techniques telles que l'ISO 27001 à l'ISO 27005, fixant les méthodes et pratiques en matière de système de management et de sécurité d'information, la rédaction du contrat est la clé pour une bonne gestion d'un projet de cloud afin de créer un climat de confiance entre les différents acteurs y contribuant.

2 Une solution : la contractualisation

Le contrat de cloud devra avant tout fixer les frontières de la responsabilité de chacun. Cette répartition sera définie notamment au regard des documents réalisés en amont du projet comme le cahier des charges ou l'expression des besoins tant fonctionnels que techniques du client (responsable du traitement).

En outre, des contrats dits « miroirs » devront être mis en place avec les sous-traitants. Au sein de ces contrats, les contraintes et les engagements assumés par le prestataire devront être repris dans leur intégralité. Les sous-traitants devront également assister aux réunions des différents comités pilotant le projet cloud.

De prime abord, l'engagement de disponibilité et de performance du prestataire est un enjeu conséquent en termes de responsabilité. Plus précisément, cet engagement permet de mettre en place des niveaux de service (délais d'intervention, garantie de service, etc.) avec des éventuelles pénalités à la charge du prestataire en cas de manquement à son obligation. Ces niveaux de service sont également considérés comme des outils permettant, au fil de la relation contractuelle, d'améliorer le service fourni par le prestataire.

De même, l'entreprise (responsable du traitement) devra mettre en place des outils nécessaires au bon suivi du projet afin de ne pas perdre le contrôle des données dont elle demeure responsable. Dans ce cadre, il est nécessaire d'insister sur le fait que le prestataire (hébergeur) est soumis à une obligation de conseil envers son client et doit l'informer de tout manquement par rapport au projet initialement défini. Cette obligation de transparence doit se retrouver quant à l'information sur la localisation des données.

La sécurité et la confidentialité des données, comme on a pu le constater précédemment, emportent des enjeux considérables. Il s'avère donc nécessaire de les aborder dans le contrat, notamment pour ce qui est de la confidentialité des données personnelles et du secret médical ou bancaire, puisque dans ces hypothèses particulières, il s'agit d'obligations imposées par la loi. Le responsable du traitement devra donc s'assurer via les clauses contractuelles – et il en va de sa responsabilité – que le prestataire de cloud respectera son obligation de confidentialité et de sécurité. Il sera également nécessaire de délimiter strictement les cas de force majeure (à titre d'illustration, un prestataire peut souhaiter inclure les pannes de réseaux, d'électricité, etc.). De même, une clause prévoyant l'obligation pour le prestataire de cloud de contracter une assurance pourra s'avérer intéressante en cas de pertes d'exploitation pour le responsable du traitement.

La propriété intellectuelle occupe également une place importante. En effet, la titularité des droits de propriété devra être clairement précisée dans le contrat. De même, il sera nécessaire d'intégrer une clause de cession des droits de propriété sur les développements spécifiques réalisés par le prestataire pour les besoins de l'entreprise décidant de recourir au cloud. Cette cession pourra également concerner les modalités effectives d'accès par le responsable du traitement aux codes sources des applications mises en place par le prestataire à l'occasion d'éventuelles défaillances de ce dernier.

Un autre aspect fondamental de ce type de contrat est la réversibilité. Cette clause de réversibilité doit organiser la possibilité de revenir à une situation antérieure si celle-ci est toujours viable. La conception de la réversibilité doit être envisagée largement, notamment en prévoyant, le cas échéant, le transfert du système chez un autre prestataire. De manière usuelle, la clause de réversibilité est fonction de la durée du contrat ou de ses modes de résiliation. À titre d'illustration, cette clause peut être définie sur le plan technique dans le cadre d'une annexe qui précisera, indépendamment du coût, le format des données et applications qui seront restituées.

Enfin, le droit choisi et le tribunal compétent doivent être expressément mentionnés au contrat. À défaut, en cas de litige, la juridiction compétente et le droit applicable seront déterminés par application des règles de droit international privé. Ces règles sont d'une grande complexité et leur application peut difficilement être anticipée, ce qui génère une insécurité juridique.

Le droit applicable au contrat revêt en effet une grande importance, souvent non prise en compte par les opérateurs chargés de négocier le fond du contrat. Même si le bloc européen tend à s'harmoniser, pour autant, chaque système de droit conserve ses spécificités. En effet, les lois impératives, c'est-à-dire celles qui se superposent aux dispositions du contrat, sont différentes d'un pays à l'autre. Aussi, une disposition valable par exemple en droit anglo-saxon comme une exclusion de responsabilité se révélera non conforme au droit français. En outre, la jurisprudence varie d'un pays à l'autre et sa prise en compte permet de mieux appréhender l'interprétation du contrat.

Quant à la juridiction compétente, dès lors que les parties n'optent pas pour l'arbitrage, il est indispensable de la mettre en cohérence avec le droit choisi. Le choix du droit et de la juridiction résulte d'une véritable réflexion stratégique, qui commande de prendre en compte la taille respective des contractants, l'existence ou non d'implantations de l'un ou de l'autre dans le pays où la décision sera rendue et la facilité d'obtention de l'exequatur de la décision dans le pays de l'autre partie.

En conclusion, la négociation contractuelle est impérative et requiert l'intervention du juriste dès la phase de conception du projet cloud, et ce, afin de circonscrire le périmètre de responsabilité. Néanmoins, compte tenu de la complexité de ces projets, de l'évolution des menaces, de la dissémination des données et des informations, il convient d'anticiper sur ces nouveaux risques. En effet, les menaces sur les infrastructures sont déjà bien connues et l'entreprise est actuellement confrontée à la protection de ses informations qui constituent une valeur patrimoniale et donc la convoitise de ses concurrents. La nouvelle menace vise également l'intégrité et l'authentification de l'identité **[15]**. Dans ce contexte, outre la négociation du contrat, l'entreprise doit sensibiliser son personnel à ces nouveaux risques. Le cloud computing devenant une solution incontournable au sein de l'entreprise, la protection des données, de quelque nature qu'elles soient, passe obligatoirement par une responsabilisation et une formation des utilisateurs. En effet, dans ce domaine, la prévention s'avérera beaucoup plus constructive pour l'entreprise que des éventuels contentieux. ■

NOTES

[1] Selon la traduction qui a été donnée par la Commission Nationale de terminologie et de néologie, JO du 6 juin 2010

[2] http:www.cnil.fr, Le cloud computing : la Cnil engage le débat – 17 octobre 2011

[3] La loi n°78-17 du 6 janvier 1978 dispose en son article 2 que « Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

[4] Il est inséré, après l'article 34 de la loi du 6 janvier 1978, un article 34 bis ainsi rédigé :

« Art. 34 bis.-I. — Le présent article s'applique au traitement des données à caractère personnel mis en œuvre dans le cadre de la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public, y compris ceux prenant en charge les dispositifs de collecte de données et d'identification.

Pour l'application du présent article, on entend par violation de données à caractère personnel toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques.

II. — En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit, sans délai, la Commission nationale de l'informatique et des libertés.

Lorsque cette violation peut porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique, le fournisseur avertit également, sans délai, l'intéressé.

La notification d'une violation des données à caractère personnel à l'intéressé n'est toutefois pas nécessaire si la Commission nationale de l'informatique et des libertés a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation.

À défaut, la Commission nationale de l'informatique et des libertés peut, après avoir examiné la gravité de la violation, mettre en demeure le fournisseur d'informer également les intéressés.

III. — Chaque fournisseur de services de communications électroniques tient à jour un inventaire des violations de données à caractère personnel, notamment de leurs modalités, de leur effet et des mesures prises pour y remédier et le conserve à la disposition de la commission. »

[5] Le responsable du traitement se caractérise par son autonomie dans la mise en place et la gestion du traitement, c'est la personne qui détermine les finalités et les moyens du traitement et ce conformément à l'article 3 de la loi du 6 janvier 1978.

[6] Article 35 de la loi du 6 janvier 1978 : « (...) Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement. »

[7] La loi dite Informatique et Libertés du 6 janvier 1978, modifiée par la loi n°2004-801 du 6 août 2004

[8] JOCE n°L281

[9] www.cnil.fr en date du 11.10.2010 et intitulé « Les questions posées pour la protection des données personnelles par l'externalisation hors de l'Union européenne des traitements informatiques »

[10] Article 5 modifié par la loi n°2004-801 du 6 août 2004 : « I - Sont soumis à la présente loi les traitements de données à caractère personnel : 1° Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ; 2° Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre État membre de la Communauté européenne. II - Pour les traitements mentionnés au 2° du I, le responsable désigne à la Commission nationale de l'informatique et des libertés un représentant établi sur le territoire français, qui se substitue à lui dans l'accomplissement des obligations prévues par la présente loi ; cette désignation ne fait pas obstacle aux actions qui pourraient être introduites contre lui. »

[11] Article 68 de la loi Informatiques et Libertés : « Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un État n'appartenant pas à la Communauté européenne que si cet État assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.

Le caractère suffisant du niveau de protection assuré par un État s'apprécie en fonction notamment des dispositions en vigueur dans cet État, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées. »

[12] Il s'agit d'un ensemble de principes de protection des données personnelles, publié par le Département du Commerce Américain, auxquels des entreprises établies aux États-Unis adhèrent afin de pouvoir recevoir des données en provenance de l'Union européenne. Le Safe Harbor permet donc d'assurer une protection adéquate pour les transferts de données en provenance de l'Union européenne vers des entreprises établies aux États-Unis.

[13] L'article 69 dispose que « Toutefois, le responsable d'un traitement peut transférer des données à caractère personnel vers un État ne répondant pas aux conditions prévues à l'article 68 si la personne à laquelle se rapportent les données a consenti expressément à leur transfert ou si le transfert est nécessaire à l'une des conditions suivantes : (...) 5° À l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ;

6° À la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers. (...) »

[14] Article 97 du Code de procédure pénale : « Lorsqu'il y a lieu, en cours d'information, de rechercher des documents ou des données informatiques et sous réserve des nécessités de l'information et du respect, le cas échéant, de l'obligation stipulée par l'alinéa 3 de l'article précédent, le juge d'instruction ou l'officier de police judiciaire par lui commis a seul le droit d'en prendre connaissance avant de procéder à la saisie. (...) Il est procédé à la saisie des données informatiques nécessaires à la manifestation de la vérité en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition. »

[15] Le délit d'usurpation d'identité est défini à l'article 226-4-1 du Code pénal : « Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne. »

GÉREZ VOS SOURCES & PROJETS PROPREMENT !

LM 145 Actuellement en kiosque !

N°145 JANVIER 2012

L 19275 - 145 - F: 6,50 €

GNU LINUX MAGAZINE / FRANCE

Administration et développement sur systèmes UNIX

France Métro : 6,50 € / DOM : 7 € / TOM Surface : 950 XPF / POL. A : 1400 XPF / CH : 13,80 CHF / BEL,PORT.CONT : 7,50 € / CAN : 13 $CAD / TUNISIE : 8,80 TND / MAR : 75 MAD

DISPONIBLE CHEZ VOTRE MARCHAND DE JOURNAUX JUSQU'AU 27 JANVIER 2012 ET SUR :

www.ed-diamond.com