Les pièges de l'Internet

par Pierre Therrode (Espace de Pierre Therrode)

Date de publication : 10 Juin 2010

Dernière mise à jour :

« Arrêtez le mal avant qu'il n'existe ; calmez le désordre avant qu'il n'éclate.»Lao-tseu, VI siécle av.J.C

I - Introduction....3
II - Les risques....3
II-A - La motivation des pirates....3
II-B - En énoncer le principe pour mieux s'en protéger....6
II-B-1 - Les rogues....6
II-B-1.2 - Contre les rogues....8
II-B-2 - Les faux codec....8
II-B-2.2 - Contre les faux codecs....9
II-B-3 - Les vers informatiques....9
II-B-3.2 - Contre les vers informatiques....10
II-B-4 - Les machines "Zombies"....10
II-B-5 - Le spam....11
II-B-5.2 - comment est-on spamé et comment lutter ?....13
II-B-6 - Le phishing....14
II-B-6.1 - Le phishing de "bas niveau"....14
II-B-6.2 - Le phishing de "haut niveau"....16
II-B-6.3 - Contre le phishing....16
II-B-7 - Conclusion....17
III - La détection....17
III-A - (E;5)...Touché!!....17
III-B - Jouer les "Sherlock Holmes"....18
III-C - Les sites Web suspects....19
III-C-1 - Les "recherches passives"....19
III-C-2 - Étude plus approfondie....22
IV - Les solutions....24
IV-A - Vérifier les programmes lancés au démarrage et vérifier la mémoire....24
IV-A-1 - Les programmes qui se lancent à chaque démarrage....24
IV-A-2 - Vérifier la mémoire....25
IV-B - Voyage au centre du système: le noyau....27
IV-C - "Élémentaire mon cher Watson !" : la suppression des malwares....28
V - Comment éviter les problèmes....29
V-A - Outils élémentaires d'un poste sécurisé....29
V-B - Technique de cryptage....29
V-B-1 - Le réseau et cryptographie....30
V-B-2 - Quelques procédés de chiffrement....30
VI - Conclusion générale....31
VII - Liens annexes....31
VIII - Remerciements....33

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

I - Introduction

A l'heure actuelle, un nombre incalculable de données transitent tous les jours sur la toile de l'internet, données qui sont d'ordre personnel, financier, culturel, audio et visuel. Nous autres, utilisateurs du World Wide Web ou plus communément appelé Internet, nous utilisons ce réseau afin de communiquer avec nos proches, effectuer des recherches, consulter ses finances, c'est-à-dire pouvoir naviguer simplement et tranquillement sur le net. Certains individus possèdent des connaissances et un savoir-faire exceptionnel dans ce milieu.
Ils sont définis comme des Hackers. (1)

Certains Hackers de philosophie White-hat (c'est-à-dire ayant le sens de l'éthique) participent à l'élaboration et au perfectionnement de l'utilisation d'Internet, d'autres, les Black-Hat, utilisent leurs connaissances afin d'en tirer un bénéfice financier avec la création de logiciels malveillants (malware en anglais) tels que les virus, les trojans, les vers, etc.. afin de compromettre une ou des entreprises, ou de simples internautes. Dès lors, et dans l'optique de pouvoir répondre à ces attaques, les éditeurs d'antivirus n'hésitent pas à livrer bataille aux créateurs de malwares en proposant des solutions de sécurité toujours plus innovantes, à ceux qui veulent se prémunir contre ce type de désagréments. En échange d'une protection optimale et face à la recrudescence de la cybercriminalité, les éditeurs n'hésitent pas à proposer des solutions payantes (compter environs 40 euros pour une solution complète), mais rassurez-vous, l'article proposera des outils entièrement gratuits afin de répondre au problème sécuritaire auquel se heurtent bon nombre d'utilisateurs de chez Windows. Outre cela, l'article tentera par la même occasion de montrer certains vecteurs d'attaques, qui ne sont pas forcement liés aux faiblesses du système, mais à l'utilisateur lui même.

II - Les risques

II-A - La motivation des pirates

Comme énoncé dans l'introduction, les pirates ont pour motivation deux vecteurs:
-Le premier est indiscutablement celui de l'argent. En effet, il n'est pas rare de trouver des "kits de piratage" afin de pirater des utilisateurs d'un système bien particulier qui sont liés à une vulnérabilité du moment. A cela, on peut citer "le couteau suisse" Mpack, créé par des pirates de L'EST en 2007 et qui était alors vendu aux alentour de 80 à 500 euros suivant la spécification du produit (Attaque DDOS, Spam, Trojan, Phising etc...). Depuis quelques temps, la vente de malwares est devenu pratique courante sur le net, au même titre que celle d'antivirus ou de pare feux, car bon nombre de black-hat ont compris les bénéfices financiers qu'ils pourraient en tirer en créant des logiciels malveillants afin de satisfaire leur compte en banque ou tout simplement la commande d'un "client". En effet, cette pratique tend à se populariser, avec des notices d'utilisations accompagnant la version bêta du malware. Se rajoutent aussi les chantages numérique.

L'exemple suivant est un aperçu de la notice d'utilisation du programme malvaillant Agobot (2) , contenant un descriptif des différents prix suivant l'obtention de la version:

[5.3] What's the price for the private version ?
Minimum:
** No updates, but bugfixes if they are requested*
** Price: 50$*
** Update price: 10$*
Standard:
** All updates and new scanners*
** Price: 100$*
Premium:
** Linux scanners, all updates and new scanners*
** Price: 250$*

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

I accept payment through paypal.
I might also be willing to sell/rent/share bots but I don't have a price set, contact me and we can negotiate one.

-Le second, est celui de la notoriété. Cela est une particularité bien spécifique dans le milieu du piratage, car chaque "Team" cherche à égaler le ou les concurrents en s'attaquant à des sites bien spécifiques tels que les Casinos en ligne, les sites d'antivirus,etc... de telle sorte que cela touche le plus de cibles possibles -ici la notion de cible représente les utilisateurs d'un système ou d'une application-. Vous l'aurez donc compris, leur but est de faire la une des médias par tous les moyens mis en place pour arriver à leur fin.

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

zone-h
unrestricted information

ws Archive Archive ★ Onhold Notify

FILTERS]

acks: **1856** of which **1856** single ip and **0** mass defacements

epage defacement
defacement (click to view all defacements of this IP)
facement (click to view all defacements of this site)
cial defacement (special defacements are important websites)

	Attacker	H	M	R	★	Domain	OS
/28	NobodyCoder	H				www.ashley-t.com	Win 2003
/28	1923Turk	H		R		cheapcarsinamarillo.com	Win 2003
/28	1923Turk	H		R		cheapcarsinabilene.com	Win 2003
/28	1923Turk	H		R		cheapcarsinaustin.com	Win 2003
/28	1923Turk	H		R		cheapcarsinbrownsville.com	Win 2003
/28	1923Turk	H		R		cheapcarsincorpus.com	Win 2003
/28	1923Turk	H		R		cheapcarsindallas.com	Win 2003
/28	1923Turk	H		R		cheapcarsinelpaso.com	Win 2003
/28	Bela!	H		R		www.tahribat.com	Win 2003
/28	Persian Boys Hacking Team	H				www.jis8.com	Win 2003
/28	Persian Boys Hacking Team	H				www.hhaosf.com	Win 2003
/28	CrazyHacker16					circledmetalart.com/home.asp	Win 2003
/28	YaRaLi_1985			R		ironworkers712.com/portals/0/d...	Win 2003
/28	YaRaLi_1985					huntingworkshop.com/portals/0/...	Win 2003
/28	YaRaLi_1985					heathermendler.com/portals/0/d...	Win 2003
/28	YaRaLi_1985					hbbafla.com/portals/0/dbx.txt	Win 2003
/28	YaRaLi_1985					huntingtutor.com/portals/0/dbx...	Win 2003
/28	YaRaLi_1985					harrisonkakos.com/portals/0/db...	Win 2003

zone-h, sorte de panthéon numérique où les pirates affichent leurs exploits

Le deuxième vecteur d'attaque ne concerne pas cet article. En revanche, rien ne vous interdit de visiter le lien suivant, qui traite des méthodes de protections des sites web. (3)

Afin de réaliser le premier vecteur, les pirates n'hésitent pas à utiliser divers moyens d'attaques tels que les:
-Rogues
-Faux codec

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

-Vers informatiques
-DDOS
-Ransonware
-Phishing
Ces termes peuvent paraître barbares pour celui qui ne s'y connaît pas trop, mais ne vous inquiétez pas ils seront détaillés plus loin. Enfin il est bon de souligner que ce genre d'infection est généralement discret et utilisent dans la majorité des cas les derniers exploits, c'est-à-dire les dernières vulnérabilités lié à un système ou une application afin de rester le plus longtemps possible sur le système corrompu.

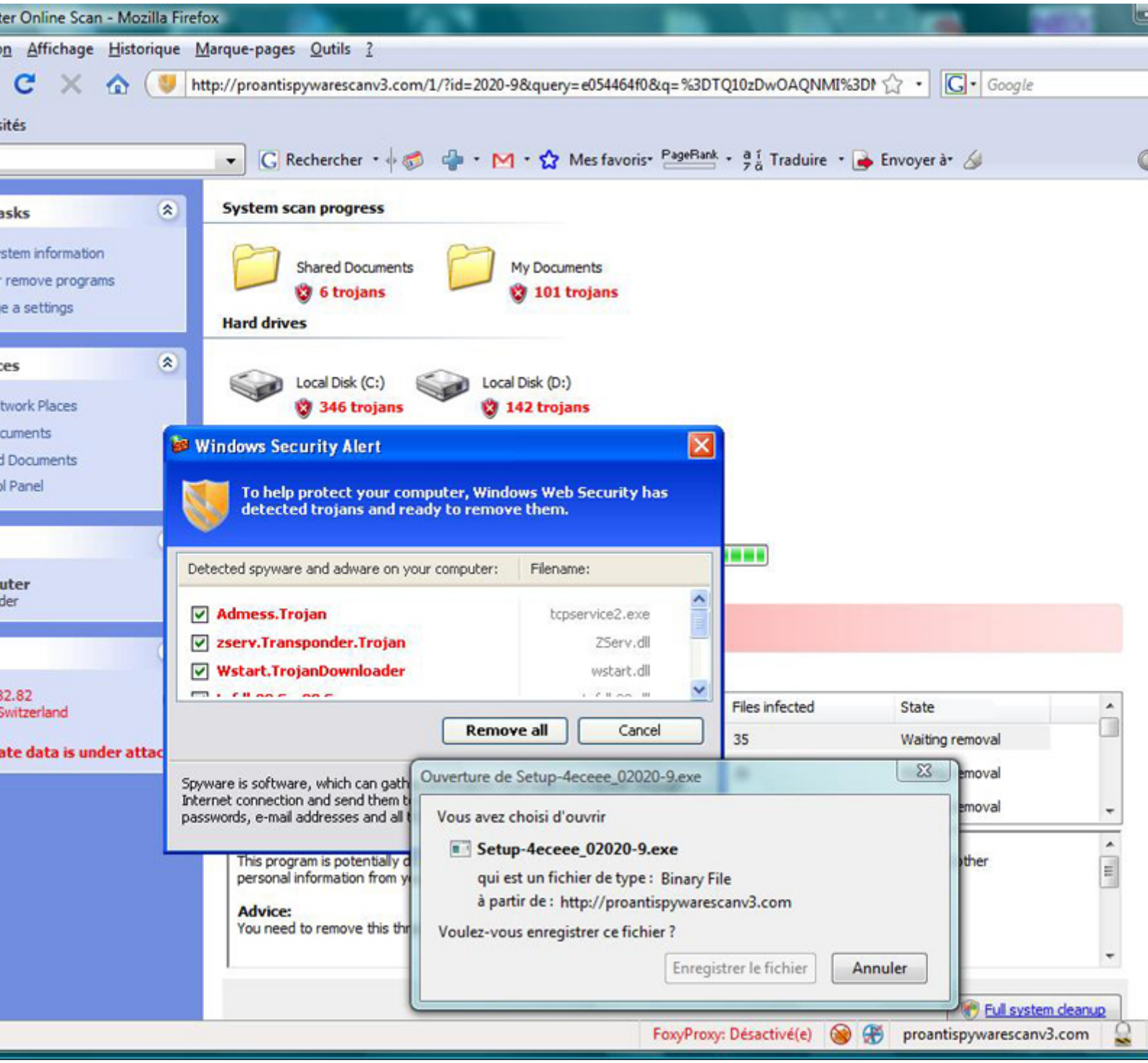
II-B - En énoncer le principe pour mieux s'en protéger

Neuf fois sur dix, une infection est due à la négligence de l'utilisateur, à crédulité et/ou à cupidité. En effet, la plus grande faiblesse de tout système reste l'utilisateur lui même (4) ...

II-B-1 - Les rogues

Lorsqu'on navigue sur Internet, il nous arrive de parfois de tomber par hasard sur de faux sites d'antivirus faisant l'éloge d'un nouveau système de protection ultra performant. Le rogue est un terme anglais désignant un escroc ou un voyou. En informatique, cela désigne un faux logiciel de protection mit en place par des pirates afin d'infecter les utilisateurs d'un système bien spécifique. Les rogues qu'on trouve sur le net ont pour but de simuler une recherche de menaces potentielles présentes sur l'ordinateur et d'alerter l'utilisateur en lui annonçant que son système d'exploitation est -faussement- infesté de virus. Parfois, les pirates n'hésitent pas à venter les mérites de leur pseudo antivirus en citant des noms d'antivirus connus, en reprenant l'ergonomie de certains éditeurs d'antivirus afin d'accentuer la crédibilité du produit et ainsi berner un visiteur qui n'y connait rien. D'autre, comme le montre l'exemple, font preuve d'imagination en recréant l'espace de travail de Windows.

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.



Aperçu d'un rogue simulant la recherche de fichiers malvaillants sur notre disque dur

De plus, il n'est pas rare que le rogue force le visiteur à télécharger le logiciel en question (à l'aide de scripts) et à l'acheter par carte bancaire en le redirigeant vers un lien soi-disant sécurisé. (Il est à noter que les faux sites d'antivirus, ainsi que les alertes sont généralement en Anglais). Parfois, et à la suite d'un téléchargement non réfléchi, il arrive que ce genre de malware arrive à s'installer sur notre système et là commencent d'interminables rappels nous annonçant que notre logiciel de protection n'est pas mis à jour et que nous encourront de graves dangers. Là encore, les pirates ont pour motivation de récupérer des numéros de cartes bancaires (afin de les utiliser ou de les revendre) et de continuer l'infection de façon discrète une fois que l'utilisateur s'est délesté de quelques euros. Ces infections serviront par la suite aux pirates afin de réaliser des attaques DOS (Denial Of Service), relayer des envois de spam et/ou récupérer des informations personnelles...

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

II-B-1.2 - Contre les rogues

Rappelez-vous qu'un véritable site d'antivirus proposant un "scan Online" ne peut pas réaliser le scan de votre disque dur en direct, il faut avant tout que l'utilisateur signe numériquement une charte en acceptant les conditions d'utilisations. De ce fait, l'éditeur d'antivirus ne force jamais l'installation de son logiciel de protection. Une fois l'installation et le scan terminés, l'antivirus vous signale les malwares présents sur votre système d'exploitation et peut vous proposez un bref aperçu de son encyclopédie virale en ligne. Pour connaître les scanners Online officiels, ainsi que des antivirus officiels, reportez-vous en fin d'article à la rubrique liens annexes.

II-B-2 - Les faux codec

Quelques fois, en naviguant de site en site, il nous arrive de tomber sur des vidéos humoristiques ou pornographiques qui sollicitent notre curiosité. Mais généralement, pour visualiser le contenu, le site nous invite à télécharger un codec ou un ActiveX en usurpant dans la plupart des cas le logo de Microsoft Windows, ou l'ergonomie d'un lecteur média connu. Ces codecs ou ces ActiveX ne sont ni plus ni moins que des malwares qui ont pour but d'infecter le système d'exploitation du visiteur.

Les fausses alertes de codecs ressemblent le plus généralement à ceci:

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

II-B-2.2 - Contre les faux codecs

Face à cela, des moteurs de recherche comme Google indexent automatiquement les sites qui présentent un danger potentiel pour les internautes. Afin d'être averti d'un site potentiellement dangereux, il suffit de cocher dans Mozilla FireFox les deux cases "Signaler....." et la case "Prévenir.... qui se situe dans Outils > Options > Sécurité. Il en va de même pour Internet Explorer, avec un curseur mis sur "Haute" pour ce qui concerne la navigation Web; le chemin à suivre est: Outils > Options Internet > Sécurité.

Exemple d'avertissement lié à une politique de sécurité stricte du navigateur FireFox

De plus, pour être sûr de pouvoir lire toutes sortes de fichiers multimédia sans que cela puisse poser problème, il existe des sites officiels qui proposent des packs regroupant un nombre important de codecs, et ceci de façon totalement gratuite et non dangereuse (lien bas).

II-B-3 - Les vers informatiques

Cependant, même si vous n'êtes pas sur le net, il est possible d'être infecté par une pièce jointe que l'on peut recevoir depuis sa boite mail ou tout simplement en utilisant une messagerie instantanée. En effet, comme bon nombre d'utilisateurs nous recevons beaucoup de mails ; certains dont nous ne connaissons pas l'expéditeur, contiennent parfois une pièce jointe avec dans le corps du message un descriptif nous invitant à l'ouvrir, jouant ainsi sur le curiosité du lecteur. Quelques fois, il arrive que l'un de vos contacts soit lui même infecté et vous envoie sans le vouloir/savoir un message qui vous invite à ouvrir cette pièce jointe contenant un fichier "exe". Dans le meilleur des cas, il vaut mieux supprimer le message si l'envoyeur ne vous confirme pas que celui-ci a bien été envoyé par lui même et si votre antivirus ne détecte rien...

Il est bon de rappeler aussi que les grands noms tels que Orange, Microsoft ainsi que d'autres sociétés, n'invitent jamais leurs utilisateurs à télécharger des pièces jointes contenues dans les mails et que les fichiers texte (en .txt) - ou image (en .jpg ou .gif) ne peuvent propager de virus (sauf, bien sûr, si le virus est caché dans l'image...). De plus,

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

certains utilisateurs sur les messageries instantanées véhiculent (sans le vouloir) à travers leurs connections des fichiers malveillants ou des liens qui renvoient vers des sites à haut risque. Généralement, ces demandes ont lieux de manière inhabituelle et spontanée, c'est à dire qu'elles interviennent alors même que l'on ne discute pas avec la personne ou lors d'une communication entre elles, celle-ci se fait de façon incohérente... Avec l'ère des réseaux sociaux tels que Facebook,Twitter, etc... les pirates ont comprit l'influence que peut avoir un compte piraté dans la diffusion de malwares et l'extention de leur(s) réseau(x) de machines zombies.

Exemple d'un compte piraté servant à la prolifération d'un malware

II-B-3.2 - Contre les vers informatiques

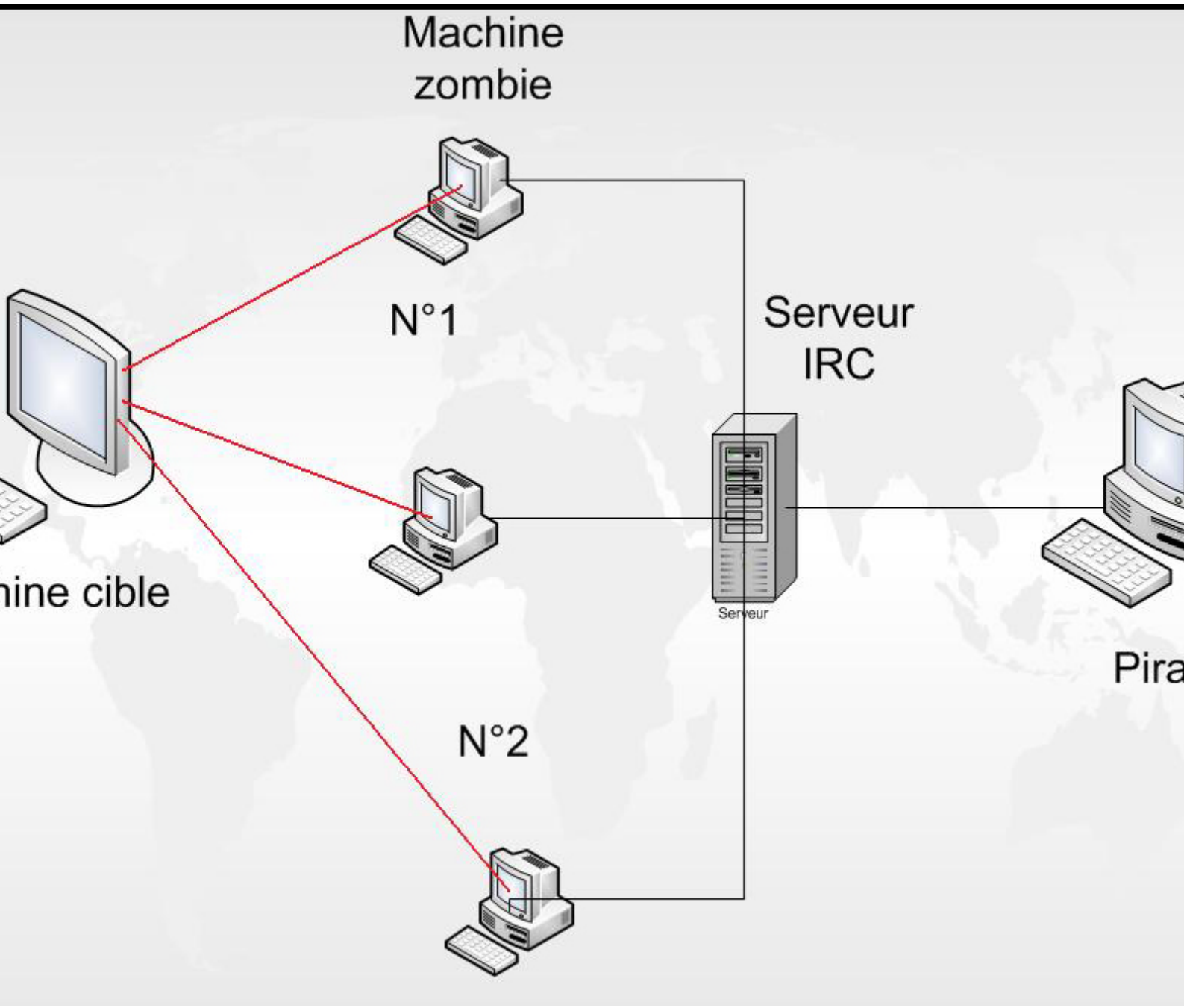
Ayez toujours un regard critique la prochaine fois que l'un de vos contact envoie sans le vouloir un tel message ou que vous tomber sur un lien suspect. Demandez lui confirmation avant toute tentative de manipulation. Si le ver se diffuse à travers un réseau, c'est alors à l'administrateur de mettre en place un "honey pot" (5) afin de pouvoir le capturer et l'étudier.

II-B-4 - Les machines "Zombies"

Au point où nous en sommes, il semble opportun d'expliquer ce que deviennent les machines qui ont été infectées. Comme dit plus haut, les motivations diffèrent selon le pirate. Cela peut couvrir la récupération des données personnelles, la récupération de données bancaires, le ransomware, c'est-à-dire que des fichiers sensibles se trouvant sur le système ciblé vont être chiffrés ou détruits si l'utilisateur de paye pas une rançon (une sorte de chantage des temps modernes)...Cependant la motivation la plus importante reste l'emprise que peut avoir un pirate sur la toile ou/et sur un réseau, et pour mener à bien cette ambition, les machines ainsi infectées vont devenir des machines zombies, c'est-à-dire quelles deviendront ses esclaves afin de mener à bien ses intentions.

Cela peut donner lieu à l'envoi de millions de spam à travers le monde, à des attaques de types DOS (Denial of Service ou déni de service), c'est-à-dire que le pirate va utiliser son réseau dans le but de rendre une application informatique incapable de répondre aux requêtes de ses utilisateurs.

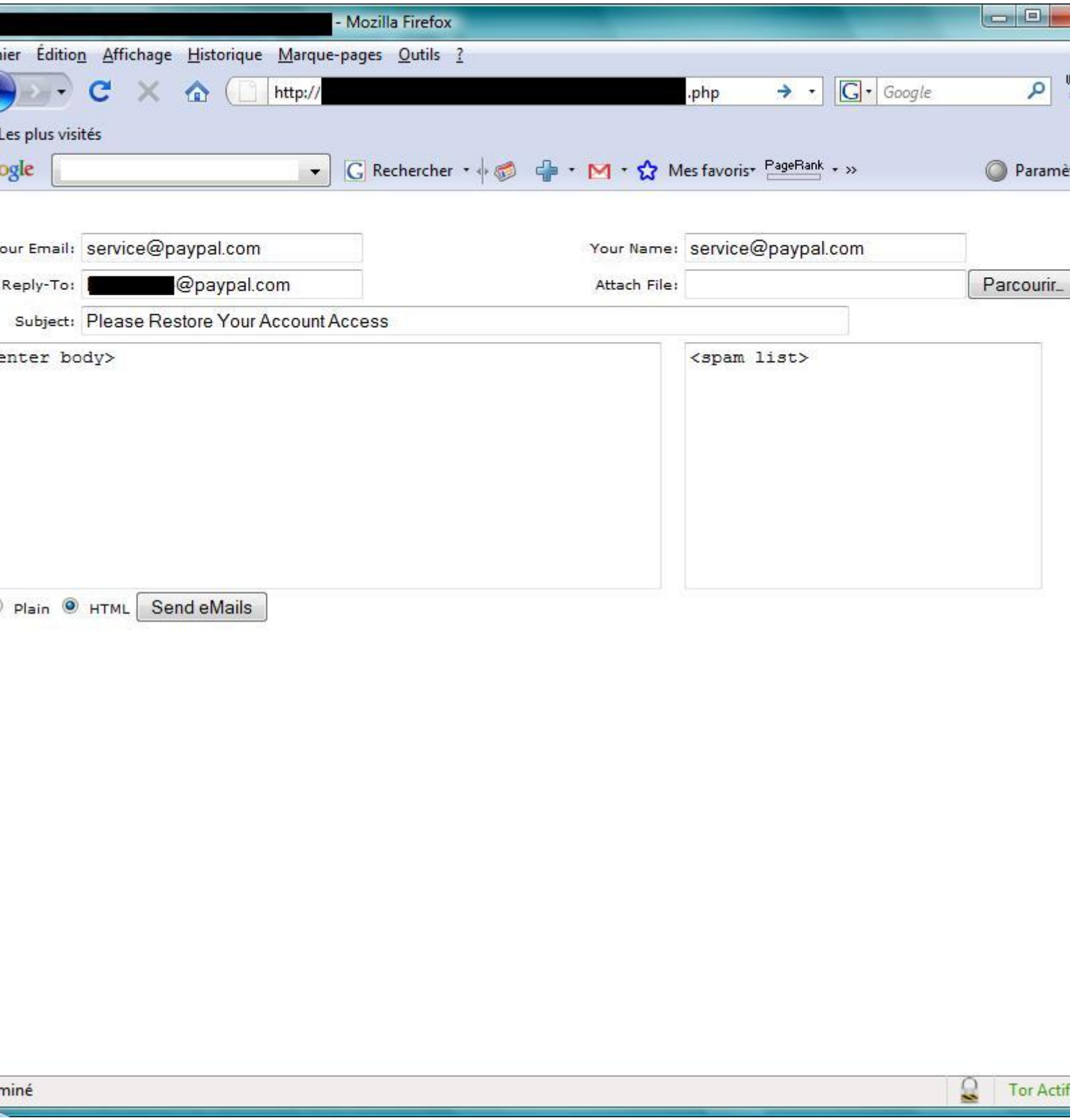
Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.



II-B-5 - Le spam

Le Spam ou pourriel, désigne l'envoi de courriers non sollicités par les destinataires qui est envoyé en masse par un pirate à des fins publicitaires. Généralement, un pirate utilise deux méthodes pour pouvoir réaliser l'attaque:
-soit il passe par un réseau de botnet;
-soit il exploite un ou des sites web mal protégés (d'un particulier ou d'une entreprise).

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.



Aperçu d'un site zombi permettant l'envoi de spam

Le contenu de ces pourriels est multiple. En effet, cela peut correspondre à l'incitation d'utilisation de médicaments (viagra, DHEA), de casinos en ligne, de (faux) crédits à la consommation, de passeports... Certains pirates n'hésitent

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

pas à promouvoir les mérites de chaines financières promettant un enrichissement rapide et efficace (bien entendu tout cela est faux !!) (6)

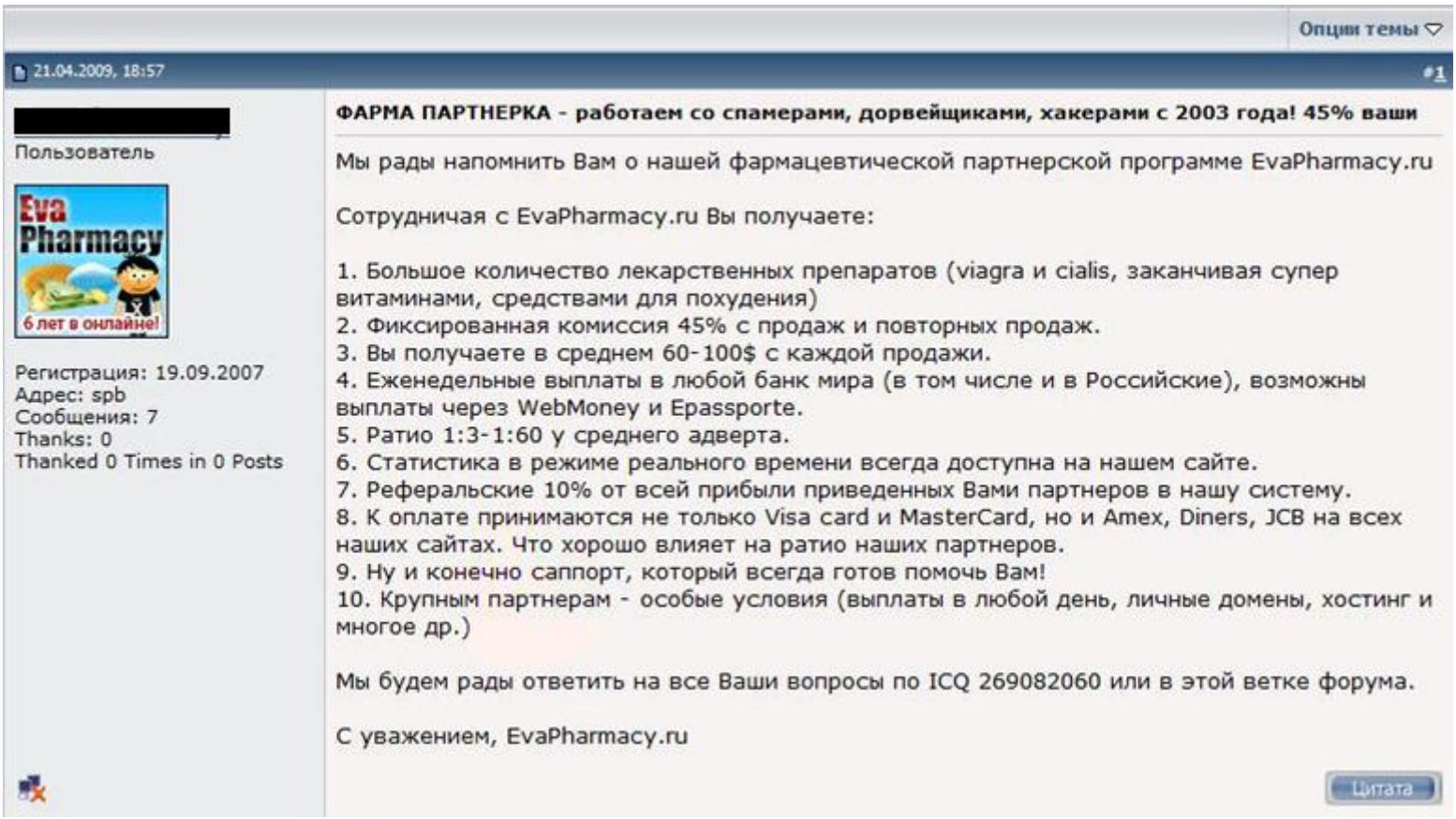
II-B-5.2 - comment est-on spamé et comment lutter ?

Toutes les adresses mails sont glanées par le pirate sur internet en utilisant le ou les moteur(s) de recherche qui sont à sa portée tout en utilisant des programmes crées généralement par ses soins. S'il estime avoir un nombre assez important d'adresses mail, il peut les revendre sur des sites "Pirate" afin d'en tirer un bénéfice (généralement cela se vend par des lots de mille pour quelques euros). Dans le cas contraire, il peut les garder pour lui et les utiliser pour infecter des utilisateurs.

Échantillon d'une liste de mails fonctionnels

Parfois, il arrive que ce soit des entreprises malveillantes qui font appel à des services de spam afin d'augmenter leurs visites, et/ou d'obtenir un éventuel client. Ces techniques sont utilisées dans le domaine de la revente de faux médicaments, tel que la vente de viagra ou de protéines musculaires, comme le montre la capture d'écran suivante (traduction: (7))

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.


Опции темы
21.04.2009, 18:57 #1
[redacted]
Пользователь
Eva Pharmacy
6 лет в онлайне!
Регистрация: 19.09.2007
Адрес: spb
Сообщения: 7
Thanks: 0
Thanked 0 Times in 0 Posts

ФАРМА ПАРТНЕРКА - работаем со спамерами, дорвейщиками, хакерами с 2003 года! 45% ваши

Мы рады напомнить Вам о нашей фармацевтической партнерской программе EvaPharmacy.ru

Сотрудничая с EvaPharmacy.ru Вы получаете:

1. Большое количество лекарственных препаратов (viagra и cialis, заканчивая супер витаминами, средствами для похудения)
2. Фиксированная комиссия 45% с продаж и повторных продаж.
3. Вы получаете в среднем 60-100$ с каждой продажи.
4. Еженедельные выплаты в любой банк мира (в том числе и в Российские), возможны выплаты через WebMoney и Epassporte.
5. Ратио 1:3-1:60 у среднего адверта.
6. Статистика в режиме реального времени всегда доступна на нашем сайте.
7. Реферальские 10% от всей прибыли приведенных Вами партнеров в нашу систему.
8. К оплате принимаются не только Visa card и MasterCard, но и Amex, Diners, JCB на всех наших сайтах. Что хорошо влияет на ратио наших партнеров.
9. Ну и конечно саппорт, который всегда готов помочь Вам!
10. Крупным партнерам - особые условия (выплаты в любой день, личные домены, хостинг и многое др.)

Мы будем рады ответить на все Ваши вопросы по ICQ 269082060 или в этой ветке форума.

С уважением, EvaPharmacy.ru

Цитата

Annonce de relayeur de spam sur un forum de L'Est

Il existe diverses techniques pour ne pas voir sa boîte mail spamée :
-La première consiste à écrire son adresse mail en langage humain ou de façon "masquée" (en utilisant des "[" ou des "]"). Par exemple, l'adresse JeanDupond@ladresse.com devient : "JeanDupond[arobase]ladresse [point/dot(en Anglais)]com", ou tout simplement "JeanDupond a l'adresse point com"
-La seconde consiste à écrire son adresse mail dans une image en y ajoutant en début et en fin d'adresse des éléments de ponctuations ou tout autre chose et ceci afin que l'adresse ne soit pas aspirée par un robot.

Enfin, il existe des sites permettant de référencer le contenu des spams ainsi que leur origine. En voici quelques-uns: :
-**http://www.stopforumspam.com**
-**http://www.spamhaus.org**
-**http://fspamlist.com**

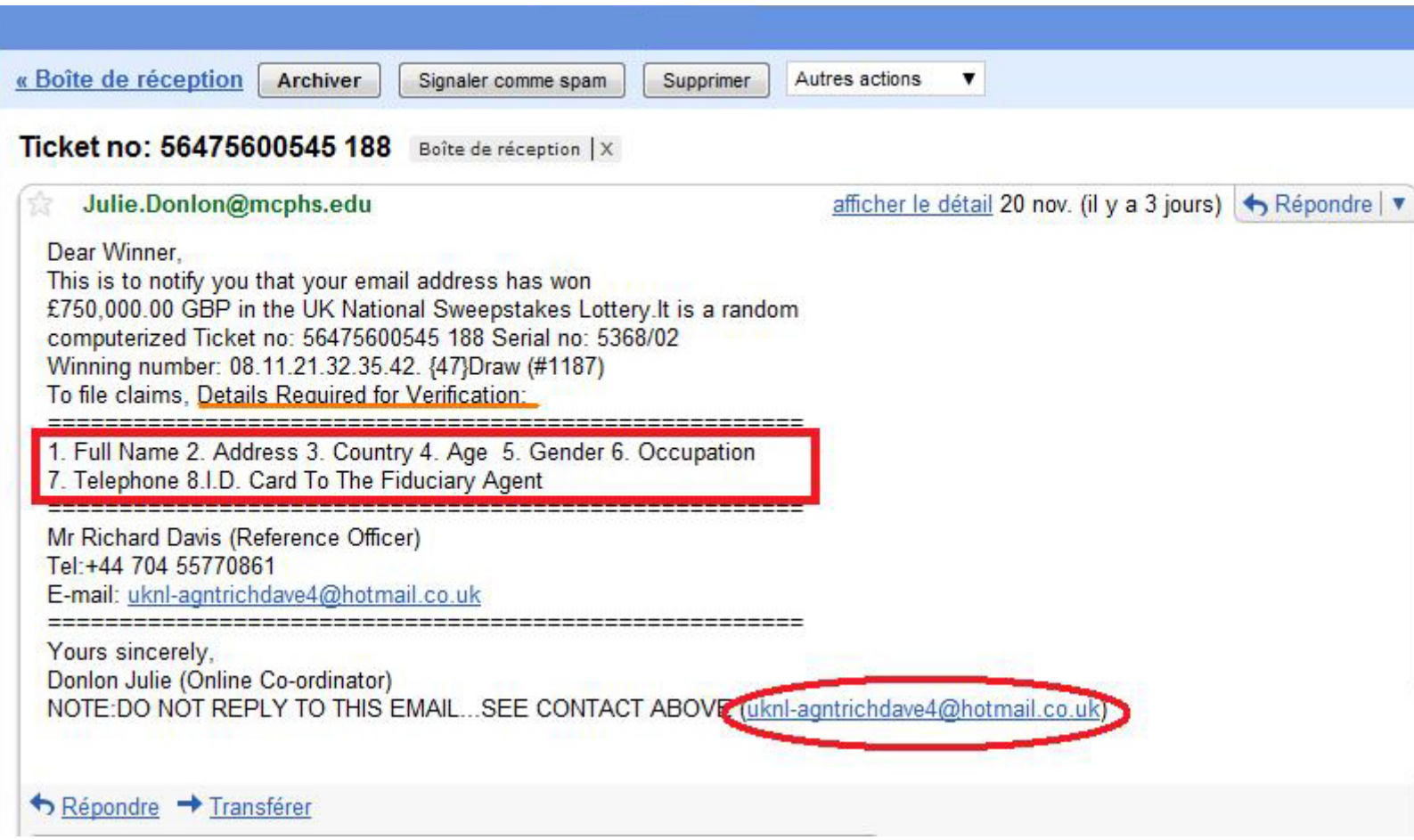
II-B-6 - Le phishing

II-B-6.1 - Le phishing de "bas niveau"

Enfin, pour clore cette partie, il est important d'énoncer un type d'attaque qui se base entièrement sur la naïveté humaine, à savoir le phishing (ou l'hameçonnage en français). Cette attaque consiste à faire croire à la victime qu'elle converse avec un site ou une entreprise de confiance, afin de lui soutirer des informations personnellesEnfin, pour clore cette partie, il est important d'énoncer un type d'attaque qui se base entièrement sur la naïveté humaine, à savoir le phishing (ou l'hameçonnage en français). Cette attaque consiste à faire croire à la victime qu'elle converse à un site ou une entreprise de confiance, afin de lui soutirer des informations personnelles (numéro de carte bancaire,

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

mots de passe) ou tout simplement à lui faire croire qu'elle est l'heureuse gagnante d'une loterie ou d'un héritage quelconque. Cela peut passer par le biais de mails ou la redirection vers un site vitrine.



Attaque de type phishing par mail

Dans la même idée, cela consiste à envoyer un mail aux victimes potentielles en usurpant l'adresse mail de leur(s) banque(s) ou de toutes autres sociétés auxquelles elles sont rattachées. Le contenu du mail leur annonce qu'elles ont perdues leur identifiants et que cela risque d'être définitif. Dès lors, la seule alternative annoncée par les pirates est celle de la re-confirmation des identifiants sur une vitrine par l'intermédiaire d'un lien.

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

Cher client de **Crédit Agricole Centre France**,

Le département technique de Crédit Agricole procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

http://www.cantal.credit-agricole.fr/id73001733411/modext

Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

© Crédit Agricole 2007

Exemple de tentative de phishing sur les clients du Crédit Agricole en 2007

Vous l'aurez donc compris, le pirate avancera toujours des arguments réalistes prônant une amélioration des services de sécurité, une panne technique qui a compromis la base de données des clients, supprimant par la même occasion les identifiants, une mise à jour qui a besoin d'être aidée par le client...

II-B-6.2 - Le phishing de "haut niveau"

Le phishing de "haut niveau", qui est plus avancé que les attaques de phishing normal, est appelé Pharming. Cela consiste à falsifier des adresses IP appartenant à des domaines et à introduire ces informations dans la mémoire cache du serveur DNS. De ce fait, si une victime potentielle tape les mots clés spécifiques à sa banque dans son navigateur web, celle-ci sera automatiquement redirigée vers la page vitrine du pirate. Il faut comprendre que le pharming est une attaque très dangereuse car elle ne force aucunement la victime à cliquer sur un lien ou à exécuter un fichier, elle redirige simplement l'individu vers un lien spécifique sans que celui-ci ne s'en rende compte.

II-B-6.3 - Contre le phishing

Contre ce type de désagrément, il est bon de toujours garder à l'esprit que votre banque, votre fournisseur d'accès à Internet, ainsi que divers types de jeux en ligne ne vous demanderons jamais vos différents identifiants suite à une pseudo panne technique ou à une mise a jours qui à mal tourné. Les Banques, ainsi que différentes sociétés, ont de quoi se prémunir face à ce genre de problème, donc les clients n'ont pas de soucis à ce faire de ce côté-là. En revanche, il est vrai qu'un mot de passe trop faible augmente les risques de voir son compte piraté. Pour éviter ce genre de problème concernant les mots de passe trop faibles, reportez-vous à la rubrique liens. Enfin, concernant les attaques de types phishing sur le net, les "vitrines" mises en place par les pirates sont généralement vite détectées par les moteurs de recherche puis indexées dans la liste noire (la fameuse Google Black-list). Dès qu'un internaute tente d'accéder à une page contre-faite, celui-ci est automatiquement alerté par un "écran" lui annonçant le plagiat ou le site malveillant.

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

II-B-7 - Conclusion

En conclusion, il semble bon de rappeler qu'il est parfois dangereux de naviguer sur des sites de Warez, sur des sites de "Super-Hacker" vous montrant comment devenir le maître du monde avec 3 commandes MSDOS (bien sûr cela est ironique), sur des sites pornographiques et plus encore sur des sites où l'on peut trouver des keygens et des cracks, car généralement ces programmes apparemment inoffensifs cachent les 3/4 du temps un virus ou un trojan (8) ...
Si vous ne pouvez ou si vous ne voulez pas payer des logiciels, il existe l'alternative des logiciels open source ainsi que d'autres logiciels qui peuvent être utilisés gratuitement. Enfin, il faut toujours garder à l'esprit de ne jamais divulguer ses informations personnelles sur des forums ou des chats, plus encore si Internet est utilisé par des enfants. Dans ce cas là, il faut veiller à utiliser un contrôle parental tout en limitant les installations.(cf:"liens annexes")

III - La détection

III-A - (E;5)...Touché!!

Suite à une infection, il faut se poser quelques questions, à savoir:
-Comment cela a été possible ?
-Par quel moyen le malware a-t-il réussi à s'installer ?

A ces deux questions, on peut émettre l'éventualité que le programme malveillant ait réussi à s'installer en exploitant diverses vulnérabilités, comme une application configurée par défaut (voire mal configurée), un oubli de mise à jour d'un élément de sécurité, un mot de passe trop court ou pas assez complexe, etc... A cela, on peut aussi rajouter "le clic de trop" qui a fait s'installer le malware avec un nom alléchant, une confiance trop aveugle en l'expéditeur d'une pièce jointe, une installation faite par ingénierie sociale.

La deuxième partie de cet article ne prétend pas détecter tous les malwares, mais simplement vous aidez dans la recherche puis la suppression de malwares, grâce à de simples événements qui vont trahir la ou les présence(s) de logiciel(s) malveillant(s), à savoir:

-L'écran bleu, cela résulte d'un bug dans le fonctionnement du système Windows. Ce genre d'erreur se produit généralement lorsqu'il manque le driver d'une carte graphique ou de tout autre composant de l'ordinateur, mais si cela se produit assez fréquemment et depuis quelques temps, il se peut que ce soit un malware (ou un rootkit) qui soit à l'origine de ce problème.

-Message d'erreurs récurant.

-Activation du matériel tel que l'ouverture et la fermeture du lecteur de cédérom, message provenant de la barre des tâches annonçant la désactivation d'un élément de sécurité, ou le déplacement non voulut de la souris. Ces symptômes trahissent la présence de trojans sur votre système d'exploitation.

-La présence de fichiers inconnus tels que des musiques, des parties de film ou des fichiers avec une extension non reconnue. Si la présence de ces fichiers ne n'est pas dûe à l'utilisation de votre entourage, cela signifie que le système sur lequel vous travaillez est compromis et qu'il est vraisemblablement utilisé comme machines zombies servant aux téléchargement ou à l'hébergement de fichiers illégaux. Cela peut être dangereux si ces fichiers ont un caractère pédo-pornographique, et en cas de constat avéré, il est sage d'alerter les autorités compétentes (liens).

-L'apparition répétitive de la boîte de dialogue UAC (User Account Control) qui est propre au système d'exploitation de Windows Vista (et ses successeurs). Cette boite de dialogue apparaît à chaque fois qu'il y a besoin des droits d'administrateurs pour installer un programme (9) .

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

-Un fort ralentissement du système d'exploitation, qui se traduit par une utilisation du processeur qui tend vers les 100% et/ou une mémoire qui est saturée après un certain laps de temps d'utilisation. Ces symptômes trahissent la présence d'un malware qui est trop gourmand en ressource.

-Une connexion internet lente; cela peut être dû à une connexion physique mal entretenue ou un malware qui exploite la connexion Internet.

III-B - Jouer les "Sherlock Holmes"

Lorsqu'un des symptômes énoncé plus haut est présent sur votre système d'exploitation, la première chose à faire est d'essayer de lancer un rapport du logiciel Hijackthis (10) . Le logiciel Hijackthis permet de détecter les installations malveillantes sur les navigateurs web et les malwares qui se lancent à chaque démarrage de Windows. Pour cela, une fois Hijackthis lancé, il faut sélectionner l'onglet "Do a system scan and save a logfile". A la suite du scan, le programme fournit un log qui peut être interprété par le site web du créateur de hijackthis, à savoir: **http://www.hijackthis.de/fr**. Lors de l'interprétation du log, il faut faire attention aux fausses alertes et porter une attention toute particulière aux points d'interrogations jaunes, ainsi qu'aux croix rouges.

O16 - DPF: {17492023-C23A-453E-A040-C7C580BBF700} (Windows Genuine Advantage Validation Tool) - http://go.microsoft.com/fwlink/?linkid=39204	✓	Sûr	Cet élément a été classé comme bonne par no
O17 - HKLM\System\CCS\Services\Tcpip\..\{4D82B0BA-B585-4FA7-9D2B-5FB2C97ECB9B}: NameServer = [redacted]	?		Effacer si l'IP ou le domaine '[redacted]' ne vous est pas connu.
O23 - Service: Ad-Aware 2007 Service (aawservice) - Lavasoft - C:\Program Files\Lavasoft\Ad-Aware 2007\aawservice.exe	✓	Très sûr	Ce service (aawservice.exe) a été identifié co légitime.
O23 - Service: Google Updater Service (gusvc) - Google - C:\Program Files\Google \Common\Google Updater\GoogleUpdaterService.exe	✓	Sûr	Ce service (GoogleUpdaterService.exe) a été étant légitime. Cet élément a été classé comm visiteurs.
O23 - Service: Network helper Service (MSDisk) - Unknown owner - C:\WINDOWS \System32\irdvxc.exe (file missing)	✗	Nasty	Ce service (irdvxc.exe) semble être méchant.
O23 - Service: last version (msn messengers) - Unknown owner - C:\WINDOWS \msgmrs.exe	?		Service inconnu. (msgmrs.exe)
O23 - Service: NOD32 Kernel Service (NOD32krn) - Eset - C:\Program Files\Eset \nod32krn.exe		Sûr	Ce service (nod32krn.exe) a été identifié com légitime.
O23 - Service: Program Learning Management System (PLMS) - Unknown owner - C:\WINDOWS\System32\plms.exe (file missing)	?		Service inconnu. (plms.exe)

Aperçu d'un rapport Hijackthis

Une fois l'origine de l'infection ciblée, il suffit de se pencher sur le problème en recherchant d'éventuels détails..... A l'heure actuelle, le meilleur outil permettant la recherche de renseignements sur un fichier (et sur tout autre caractère) reste sans aucun doute le moteur de recherche Google. En effet, il suffit de taper dans la barre de recherche le nom du fichier suspect pour tomber sur des analyses qui ont eu lieu et/ou sur des commentaires divers (forum, éditeurs d'antivirus,etc...). Dès lors, l'utilisation du moteur recherche permet de confirmer les suspicions d'un ficher malveillant.

Viruslist.com - Backdoor.Win32.Rbot.bni
%System%**irdvxc.exe**. Après quoi, la backdoor exécute cette copie toutes les deux secondes avec les paramètres de ligne de commande suivants : **...**
www.viruslist.com/fr/viruses/encyclopedia?virusid=141920 - 23k - En cache - Pages similaires

Exemple de recherche concluante sur un fichier suspect

Il existe aussi sur la toile des sites spécialisés qui permettent l'étude d'un fichier suspect (lien). On peut citer le site d'analyse dynamique Virus Total qui, une fois le fichier suspect uploadé, le soumet à une trentaine d'antivirus. Cependant, il faut rester vigilant aux fausses alertes qui peuvent être émisses par le moteur de recherche (un patch

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

officiel d'un élément sécurité peut être vu par un antivirus comme un élément néfaste, cela est rare mais ça arrive quelques fois).

Fichier **LiteVideocodec.exe** reçu le **2008.11.29 19:49:48 (CET)**
Situation actuelle: **terminé**
Résultat: **9/37 (24.33%)**

Antivirus	Version	Dernière mise à jour	Résultat
AhnLab-V3	2008.11.28.2	2008.11.29	-
AntiVir	7.9.0.36	2008.11.29	TR/Crypt.XPACK.Gen
Authentium	5.1.0.4	2008.11.28	-
Avast	4.8.1281.0	2008.11.28	-
AVG	8.0.0.199	2008.11.29	-
BitDefender	7.2	2008.11.29	MemScan:Trojan.FakeAlert.APF
CAT-QuickHeal	10.00	2008.11.29	(Suspicious) - DNAScan
ClamAV	0.94.1	2008.11.29	-
DrWeb	4.44.0.09170	2008.11.29	Trojan.DownLoad.13276
eSafe	7.0.17.0	2008.11.27	-
eTrust-Vet	31.6.6234	2008.11.28	-
Ewido	4.0	2008.11.29	-
F-Prot	4.4.4.56	2008.11.28	-
F-Secure	8.0.14332.0	2008.11.29	-
Fortinet	3.117.0.0	2008.11.29	-
GData	19	2008.11.29	MemScan:Trojan.FakeAlert.APF

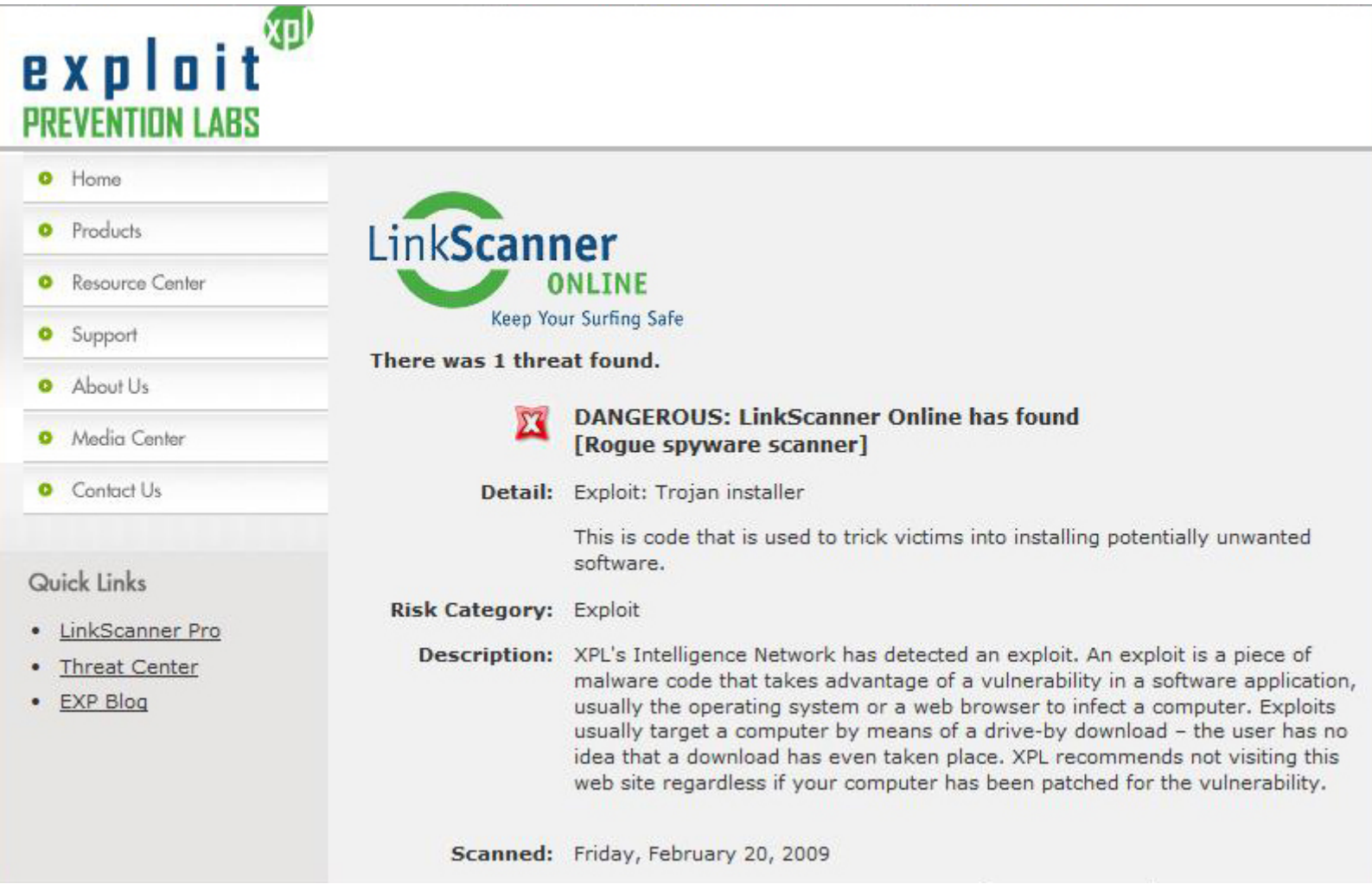
Extrait d'un rapport d'analyse d'un faux codec vidéo à partir du site Virus Total

III-C - Les sites Web suspects

III-C-1 - Les "recherches passives"

Lorsqu'on est sur le web, il nous arrive parfois de douter sur l'authenticité d'un site. Afin de pallier ce doute, il existe sur la toile quelques sites proposant le scan online d'une page web (lien bas). Il faut comprendre ici par scan online le fait que le site dynamique va scanner la page ciblée en vérifiant le code source de la page douteuse. Généralement, les codes sources qui sont utilisés par le pirate pour permettre des infections, ne sont que guère modifiés.

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.



Résultat du site LinkScanner concernant une page frauduleuse

De plus, si l'on souhaite obtenir d'avantage d'informations sur un site suspect, il est alors possible d'utiliser des outils de collecte d'information dite "passive". A cela, on peut citer le site **ripnet.com** ou encore "le couteau de suisse" l'internet **Robtex.com**. Il rassemble à lui tout seul bon nombre d'outils permettant la collecte de différents types, tels que:
-RBL
-DNS
-IP-number
-route
-AS numbers
-BGP annoucements
-AS macros

à l'heure de la publication, l'exemple suivant est périmé.

Par exemple, si nous recherchons des informations sur la localisation géographique d'un site qui nous paraît suspect (ici ? adresse ?), on peut utiliser l'un des outils proposés pour connaître l'adresse IP du serveur qui héberge le site, leurs noms, l'AS (11) ainsi que l'adresse mail qui a servi à enregistrer le site. Si l'on creuse un peu plus, on apprend que le serveur en question est localisé en Russie, et plus particulièrement à Saint-Petersburg. On remarque également le (faux) nom personnel utilisé par le pirate, qui a permi d'enregistrer le nom de domaine.

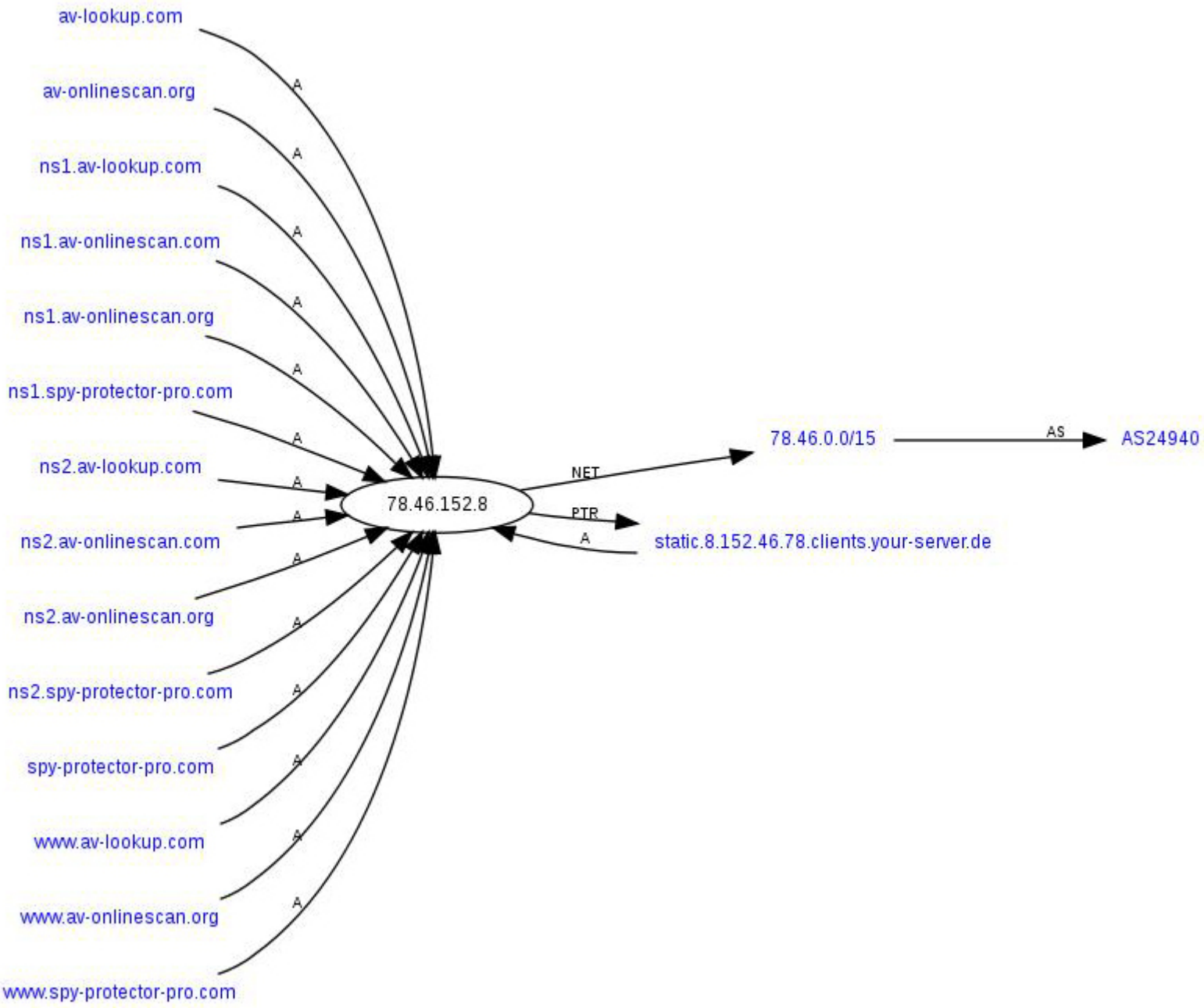
% This is the RIPE Whois query server #1.

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

```
% The objects are in RPSL format.
% % Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html
% Note: This output has been filtered.
% To receive output for a database update, use the "-B" flag.
% Information related to '78.46.152.0 - 78.46.152.63'
inetnum:      78.46.152.0 - 78.46.152.63
netname:      FASTVPSRU
descr:        FastVPS.ru
country:      DE
admin-c:      OL203-RIPE
tech-c:       OL203-RIPE
status:       ASSIGNED PA
mnt-by:       HOS-GUN
source:       RIPE # Filtered
person:       Oleg Lyubimov
address:      Leninskiy pr. 96-1-128
address:      198332 Saint-Petersburg
address:      RUSSIAN FEDERATION
phone:        +79219707212
fax-no:       +79219707212
e-mail:       oleg.lyubimov@gmail.com
nic-hdl:      OL203-RIPE
mnt-by:       HOS-GUN
source: RIPE # Filtered
% Information related to '78.46.0.0/15AS24940'
route: 78.46.0.0/15
descr: HETZNER-RZ-NBG-BLK5
origin: AS24940
org: ORG-HOA1-RIPE
mnt-by: HOS-GUN
source: RIPE # Filtered
organisation: ORG-HOA1-RIPE
org-name: Hetzner Online AG
org-type: LIR
address: Hetzner Online AG
Attn. Martin Hetzner
Stuttgarter Str. 1
91710 Gunzenhausen
Germany
phone: +49 9831 610061
fax-no: +49 9831 610062
e-mail: info@hetzner.de
admin-c: GM834-RIPE
admin-c: HOAC1-RIPE
admin-c: MH375-RIPE
admin-c: RB1502-RIPE
admin-c: SK2374-RIPE
mnt-ref: HOS-GUN
mnt-ref: RIPE-NCC-HM-MNT
mnt-by: RIPE-NCC-HM-MNT
source: RIPE # Filtered
```

De plus, grâce aux fonctionnalités de robtex, il est possible de visualiser l'arborescence des noms de sites qui composent l'enregistrement de domaine.

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.



Visualisation de l'arborescence

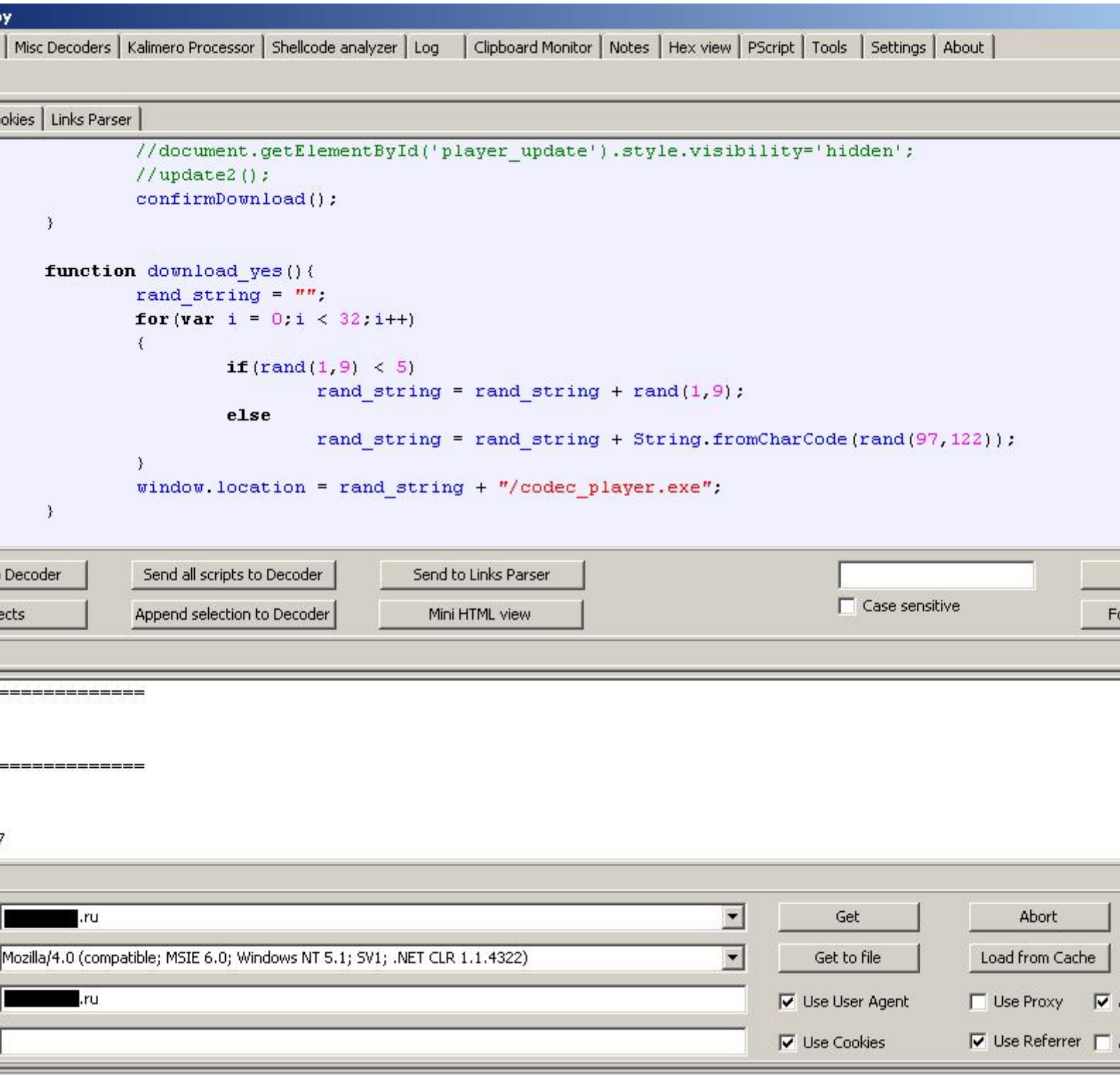
Enfin, si l'on étudie la source de l'une de ces pages vitrines, on remarque que les malwares ne sont pratiquement jamais hébergés sur le même serveur; ils sont téléchargés à partir d'un lien annexe. C'est ce que nous allons voir tout de suite dans le chapitre suivant.

III-C-2 - Étude plus approfondie

Malzilla est un utilitaire bien utile lorsqu'il s'agit d'analyser en profondeur une page suspecte. En effet ce petit logiciel permet de décoder bon nombre de fonctions qui sont parfois utilisées dans des applications web, comme l'encodage

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

en base 64. Il permet aussi d'afficher la page en format texte ou hexadécimal et prend en charge l'analyse des cookies, des logs,



Aperçu du programme Malzilla

Dans l'exemple précédent, nous pouvons voir distinctement que le site héberge un malware (dans mon cas, le logiciel s'est avéré être un ransomware) intitulé "codec_player.exe".

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

IV - Les solutions

IV-A - Vérifier les programmes lancés au démarrage et vérifier la mémoire

IV-A-1 - Les programmes qui se lancent à chaque démarrage

Pour être toujours actifs, les malwares ont besoin d'être lancés à chaque démarrage du système et, pour cela, ils vont devoir modifier la base de registre, ainsi que les divers paramètres qui son liés au démarrage des fichiers. L'outil Autoruns de chez Microsoft liste tous les programmes et bibliothèques qui sont automatiquement exécutés à chaque démarrage de Windows. L'avantage majeur de cet outil est qu'il permet de voir les programmes qui se lancent pour tous les utilisateurs, ainsi que ceux lancés par l'utilisateur lui même. Les programmes lancés au démarrage sont classés par type (Logon, Explorer, Internet Explorer, etc□). Afin de ne pas surcharger l'affichage, il faut veiller à cocher les paramètres suivants : Verifiy Code Signature et Hide Microsoft Signed Entries, se trouvant dans l'option du menu. Il est à noter que l'onglet Logon liste tous les programmes exécutés à l'ouverture d'une session.

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

Sysinternals: www.sysinternals.com

Options Help

KnownDLLs | Winlogon | Winsock Providers | Print Monitors | LSA Providers | Network Providers | Side
ng | Logon | Explorer | Internet Explorer | Scheduled Tasks | Services | Drivers | Codecs | Boot Execute

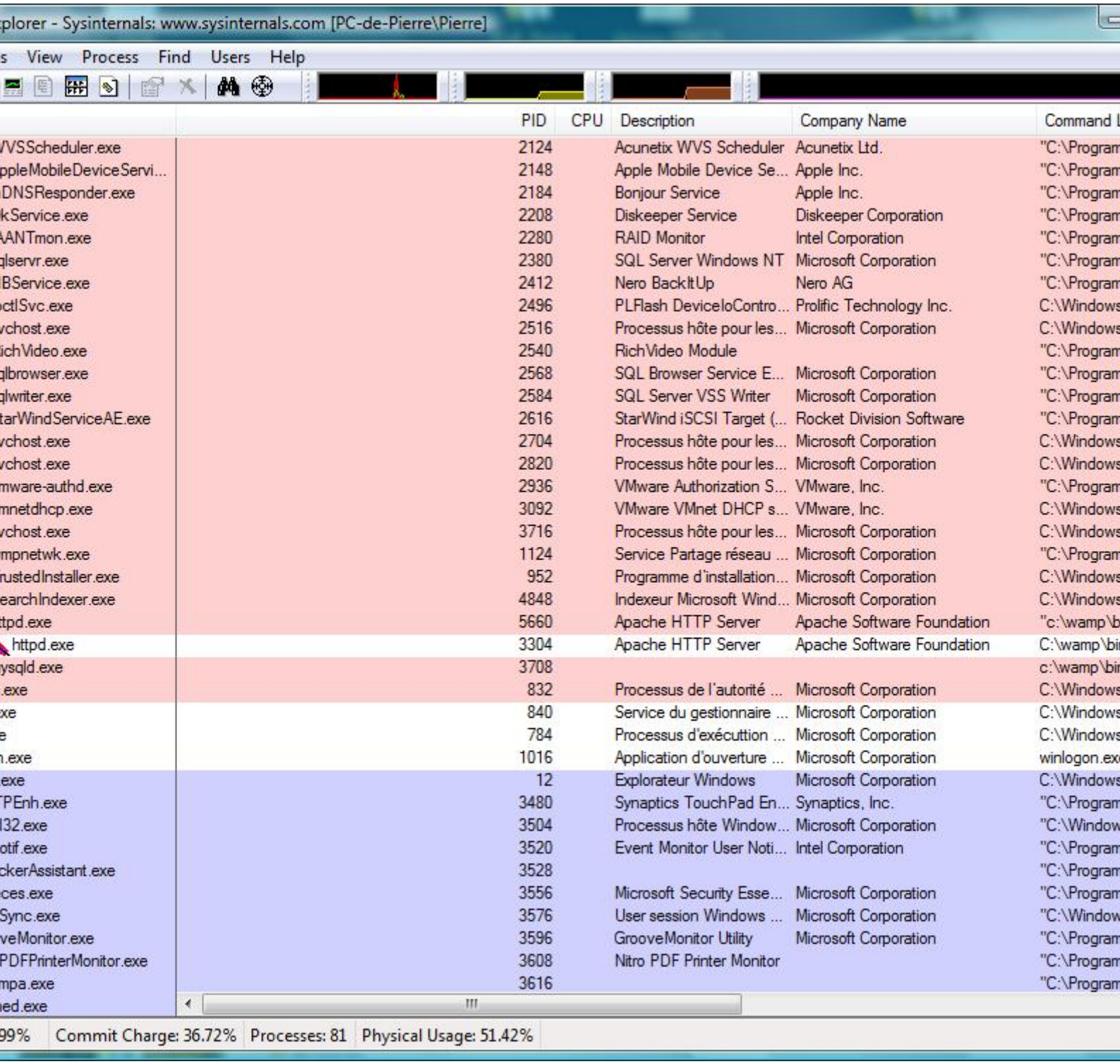
	Description	Publisher
DFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit		
\Windows\system32\userinit.exe	Application d'ouverture de session Userinit	(Verified) Microsoft Windows
DFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell		
plorer.exe	Explorateur Windows	(Verified) Microsoft Windows
DFTWARE\Microsoft\Windows\CurrentVersion\Run		
dobe Reader Speed Launcher	Adobe Acrobat SpeedLauncher	(Verified) Adobe Systems, Incorporated
ooveMonitor	GrooveMonitor Utility	(Verified) Microsoft Corporation
Anotif	Event Monitor User Notification Tool	(Verified) Intel Corporation
SNavgnt		(Not verified) ABC
SSE	Microsoft Security Essentials User Interface	(Verified) Microsoft Corporation
tro PDF Printer Monitor	Nitro PDF Printer Monitor	(Verified) Nitro PDF Software
vCplDaemon	NVIDIA Display Properties Extension	(Verified) Microsoft Windows Hardware Com
vMediaCenter	NVIDIA Media Center Library	(Verified) Microsoft Windows Hardware Com
vSvc	NVIDIA Driver Helper Service, Version 167.62	(Verified) Microsoft Windows Hardware Com
DVD8LanguageShortcut	Language Application	(Verified) CyberLink
VRISOVM.EXE	PowerISO Virtual Drive Manager	(Not verified) PowerISO Computing, Inc.
uickTime Task	QuickTime Task	(Not verified) Apple Inc.
emoteControl8	PowerDVD RC Service	(Verified) CyberLink
unJavaUpdateSched	Java(TM) Platform SE binary	(Verified) Sun Microsystems, Inc.
nTPEnh	Synaptics TouchPad Enhancements	(Verified) Microsoft Windows Hardware Com
olbar_eula_launcher		(Not verified)
hlockerAssistant		

Aperçu de l'outil Autoruns

IV-A-2 - Vérifier la mémoire

Après avoir listé les programmes qui se lancent au démarrage, il est bon de continuer l'investigation dans l'analyse du système.Pour ce faire, on peut utiliser l'outil Process Explorer, et ceci afin de lister les processus tout en donnant les caractéristiques, les bibliothèques utilisées, port utilisé,....

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.



Aperçu du logiciel Process Explorer

Afin de faciliter l'exploration, il faut avant tout configurer le logiciel. Pour cela il suffit d'aller dans l'onglet View de sélectionner "Select Columns" pour cocher les cases suivantes: Compagny Name, Command Line, Description, Version et Verified Signer. Toutes ces options permettent de nous renseigner sur l'origine du programme (cf: Company Name), sur son chemin d'accès (cf:Command Line) qui, s'il est différent des chemins habituels peut être considéré comme un programme suspect. Dès lors, il suffit d'utiliser le moteur de recherche pour en savoir plus sur un fichier suspect...

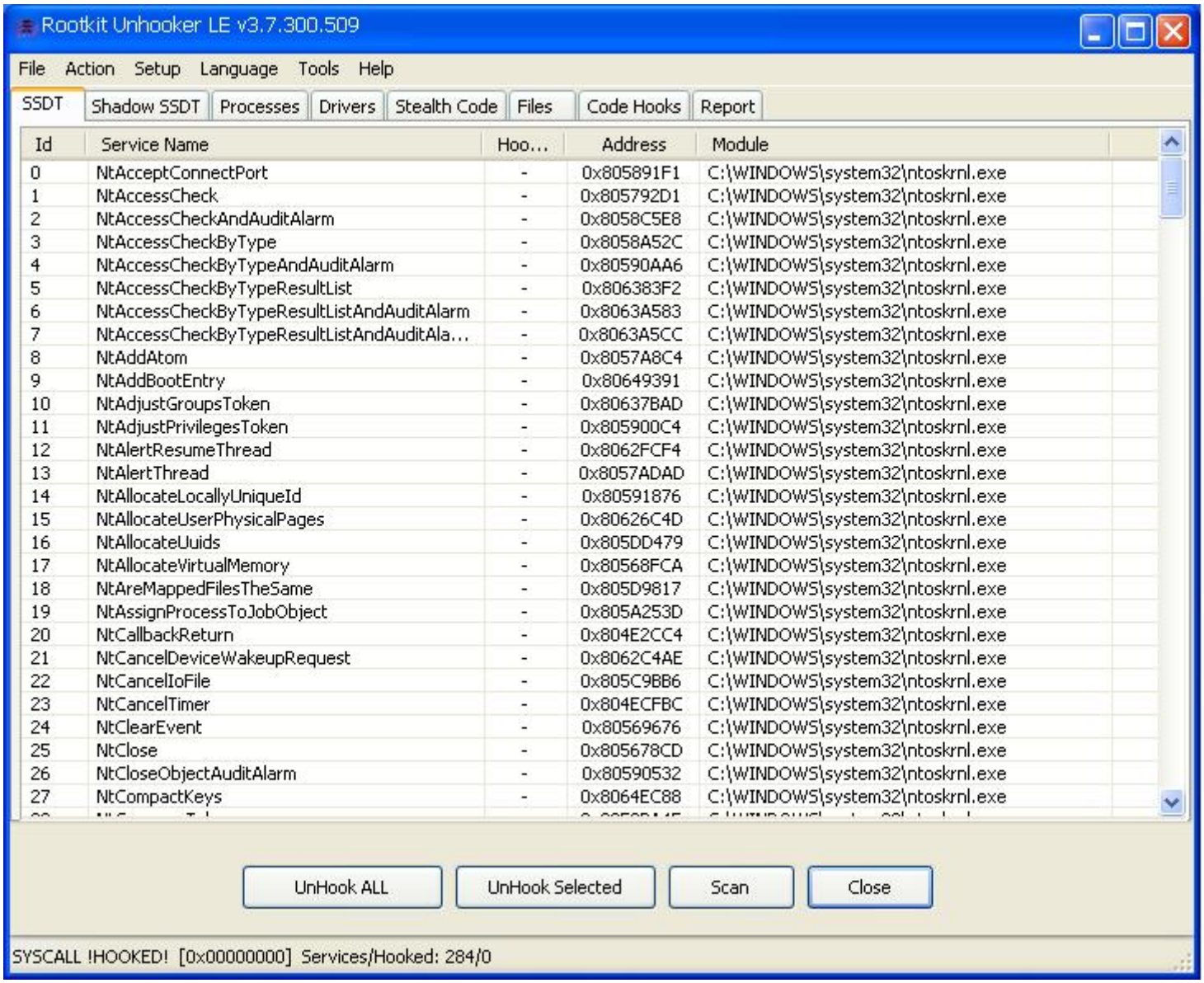
Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

IV-B - Voyage au centre du système: le noyau

Le noyau est la pièce maîtresse de tout système d'exploitation.
En effet, il gère les ressources de l'ordinateur et permet aux différents éléments qui composent l'ordinateur de communiquer entre eux; il est par exemple responsable du bon déroulement des programmes qui sont en cours d'exécution. De ce fait, lorsqu'un malware ou plus particulièrement un rootkit arrive à compromettre le fonctionnement du noyau, il est alors possible que celui-ci dissimule des informations à l'utilisateur du système compromis. Il peut en effet cacher un accès à une porte dérobée ou cacher un programme en cours d'exécution, ce qui rend particulièrement difficile la détection de ce genre de malwares, car les antivirus ont une confiance aveugle en tout ce qui concerne les appels système ou plus particulièrement les pilotes de périphérique (cf: "Liens annexes:Revue, MISC").

A l'heure actuelle, il n'existe aucun moyen fiable pour détecter la présence d'un rootkit, mais certaines compromissions du noyau trahissent la présence de malwares. De ce fait, le site **antirootkit.com** recense un nombre important de rootkits et présente de nombreux logiciels permettant de détecter et de les supprimer. On peut citer le logiciel "Aries Rootkit Remover" permettant de supprimer les rootkits de la société Sony, suite à l'écoute de l'un de leur CD musicaux, ou encore "RootKit UnHooker" qui permet de détecter les processus cachés ainsi que les Hooks....

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.



Aperçu du logiciel Rootkit UnHooker

Le logiciel Rootkit UnHooker présente la particularité d'être assez simple d'emploi pour tous ceux qui désirent vérifier la présence d'éventuels rootkits sur leur système d'exploitation.

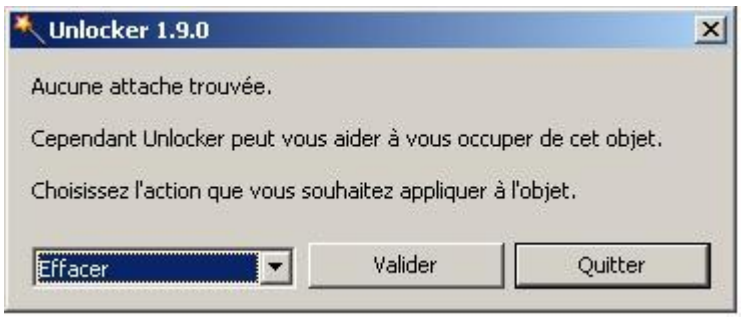
Il faudra veiller à rester vigilant sur les chemins des exécutables dans les onglets "Drivers" et "Processes", principalement si les chemins soulignent un répertoire temporaire ou qui est caché, il est alors bon de faire une recherche plus approfondie.

IV-C - "Élémentaire mon cher Watson !" : la suppression des malwares

Suite à une étude approfondie d'un poste compromis, il est bon de prendre en note le chemin du malware. Face à cela, il convient de supprimer au plus vite le malware afin qu'il ne puisse plus se relancer aux prochains redémarrages du système, cependant et outre la propre protection du fichier malveillant, Windows bloque à chaque fois la suppression d'un fichier lorsque celui est en cours d'exécution.

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

Ces deux méthodes combinées offrent aux pirates l'opportunité de voir leur malware persister sur le système compromis. Toutefois, il existe un outil de suppression nommé Unlocker qui passe outre ces restrictions.



Aperçu de l'outils Unlocker

Parfois, il arrive que Unlocker et/ou l'antivirus ne puissent supprimer un malware car le pirate qui a codé le programme a fait en sorte de pallier ce genre de suppression. Il est alors bon se tourner vers Linux(8), en démarrant l'ordinateur à partir d'un Live CD, et de le supprimer depuis ce système d'exploitation.

V - Comment éviter les problèmes

V-A - Outils élémentaires d'un poste sécurisé

Un poste sécurisé est synonyme de logiciels de sécurité et de mises à jours.
En effet, cela doit absolument passer par l'utilisation d'un antivirus qui jouera le rôle de détecteur de malwares ainsi que d'un pare-feu permettant de restreindre l'accès à un système d'exploitation depuis l'Internet. Bien évidement, tous ces éléments doivent régulièrement être mis à jours lorsque le logiciel ou le système le rappellent. Il est bon d'éviter d'installer des logiciels de peer to peer car généralement ils recèlent des publicités que l'on ne souhaite pas forcement recevoir lorsque l'on est sur le net (ex: Kaza), il en va de même pour les pseudos logiciel permettant de personnaliser notre messagerie instantanée, etc... De plus, il est souhaitable de nettoyer de temps à autre le système d'exploitation avec des logiciels appropriés tels que Ccleaner .

V-B - Technique de cryptage

L'analyse du trafic réseau est une activité qui plait énormément aux spécialistes de la sécurité ainsi qu'aux Hackers. Grâce à des logiciels spécialisés dans l'écoute du trafic réseau (exemple: **wireshark**), ils peuvent alors stocker les paquets du trafic pour par la suite, lire le contenu des communications. Il est à noter que la plupart de ces outils se basent sur le fait que certains protocoles font transiter des informations en clair sur le réseau. Dès lors, si le réseau est partagé par un HUB, alors de simples outils d'écoutes suffisent pour sniffer et déchiffrer le contenu. Cependant si le réseau commuté est configuré avec un switch, le pirate ou le spécialiste mettra alors en place une attaque de type MAC flooding ou un ARP spoofing. Afin de pallier ces faiblesses, il existe des protocoles qui utilisent une stratégie cryptographique.

Avant de rentrer dans le vif du sujet, je vous suggère l'article suivant, écrit par l'un des membres de site: **Introduction aux réseaux TCP IP**

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

V-B-1 - Le réseau et cryptographie

OSI	TCP/IP	Protocoles
7-Application	HTTP, FTP, Telnet	PGP, GnuPG, SET, S-HTTP,S/MINE
6-Présentation		
5-Session		
4-Transport	UDP, TCP	SSL, TLS,STLP, PCT, IPSEC
3-Réseau	Interconnexion de réseau IP ICMP	IPsec - IP MPLS couche 3 (BGP)
2-Liaison de données	Interface réseau Ethernet, Frame Relay, ATM, PPP	
1-Physique		

V-B-2 - Quelques procédés de chiffrement

PGP (Pretty Good Privacy):
PGP est une combinaison des meilleures fonctionnalités de la cryptographie de clé publique et de la cryptographie conventionnelle.
C'est aussi un système de "cryptographie hybride". Lorsqu'un utilisateur utilise la cryptographie PGP pour chiffrer un texte, les données sont d'abord compressées. Cela permet de réduire le temps de transmission, d'économiser l'espace sur le disque et, surtout, de renforcer la sécurité cryptographique.
Il s'ensuit, une opération de chiffrement qui se déroulent en deux étapes :
-PGP crée une clé secrète IDEA de manière aléatoire, et chiffre les données avec cette clé.
-Ensuite, PGP crypte la clé secrète IDEA et la transmet au moyen de la clé RSA publique du destinataire.
Lors de la phase de décryptage, cela se passe également en deux étapes :
-PGP déchiffre la clé secrète IDEA grâce à la clé RSA privée
-PGP déchiffre les données avec la clé secrète IDEA obtenue précédemment.

SSH (Secure Shell):
Mit au point en 1995 par le Finlandais Tatu Ylönen, ce protocole permet à un client d'ouvrir une session sur une machine distante afin d'envoyer des commandes ou des fichiers de manière sécurisée.
Les données qui circulent entre le client et la machine distante sont chiffrées, permettant ainsi une grande confidentialité et rendant impossible l'écoute de la communication.

IPSec (Internet Protocol Security):
C'est un ensemble de RFC (**Request For Comments**) destinées à utiliser des algorithmes permettant l'acheminement de données sécurisées au sein d'un réseau IP.
Cela permet donc d'authentifier et de chiffrer les données, ce qui aura pour conséquence de rendre le flux de données que par le destinataire final tout veillant à l'intégrité de celle-ci.

SSL (Secured Socket Layer):
Élaboré au début par Netscape, le protocole SSL offre une communication sécurisée au niveau de la 4éme couche (transport).
IL se base sur les algorithmes RSA et utilise des certificats pour identifier l'émetteur et le récepteur.

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

TLS (Transport Layer Security):
Basé sur SSLv3, il permet de remplacer le SSL. Ne dépendant pas des algorithmes déposés par la RSA, il comporte beaucoup de problèmes légaux.

VI - Conclusion générale

Bon nombre d'éditeurs de système de protections vendent leur produit pour répondre à une demande des utilisateurs ainsi que pour pallier le nombre croissant des menaces liées à Internet. Cependant, il ne faut pas se croire entièrement en sécurité derrière un simple antivirus (12) , car celui-ci n'est qu'un maillon parmi tous les éléments de sécurité (pare-feu, filtre, accès restreint par mot de passe, etc...). Si le matériel informatique est à disposition de tierces personnes, comme dans les bibliothèques, dans les lycées avec le CDI,.... il est alors bon de rappeler les bonnes pratiques d'une utilisation d'Internet en y affichant des rappels d'utilisation (post-it), à travers les écrans de veille ou sur le fond d'écran de l'ordinateur et d'en limiter leur utilisation (ex: filtrage des adresses MAC si cela est dans un réseau wifi, droit d'administrateur restreint, téléchargement interdit, logiciel de contrôle à distance pour l'administrateur, etc...). Ces rappels passent aussi par une sensibilisation de l'utilisation de l'ordinateur et d'internet dans les écoles ou les lycées. Les chats ouverts à tout publiques sont fortement à proscrire, surtout lorsque l'ordinateur est utilisé par des enfants. Enfin, il est intéressant de se tenir informé des dernières vulnérabilités en visitant des sites comme Zataz.com, Vulnérabilite.com, voire Developpez.com.

VII - Liens annexes

-Club des développeurs: **http://www.developpez.com**
-Portail de la Sécurité: **http://fr.wikipedia.org/wiki/Portail:Sécurité_informatique**
-Journal de l'actualité informatique et multimédia: **http://www.zataz.com**
-Site regroupant les dernières vulnérabilité afin de se tenir à jours des découvertes: **http://www.vulnerabilite.com**

Microsoft:
-Qu'est-ce que Microsoft ?: **http://fr.wikipedia.org/wiki/Microsoft**
-Site officiel: **http://www.microsoft.com/downloads/search.aspx?displaylang=fr**
-Microsoft TechNet: **http://technet.microsoft.com/fr-fr/sysinternals/default.aspx**
-FAQ Windows sur Developpez.com: **http://windows.developpez.com/faq/**

Linux:
-Qu'est-ce que Linux ?: **http://fr.wikipedia.org/wiki/Linux**
-Distribution Linux: **http://www.livecdlist.com**
-FAQ Linux sur Developpez.com: **http://linux.developpez.com/faq/**

Protections:
-Débat sur les meilleurs antivirus:
http://www.developpez.net/forums/d294988/hardware-systemes-logiciels/windows/securite/s-antivirus-trouvez-efficace
-Débat sur les meilleurs par-feux:
http://www.developpez.net/forums/d294994/hardware-systemes-logiciels/windows/securite/firewall-s-trouvez-efficace-s
-L'ABC de la sécurité, fait par l'un des membres de developpez.com (Shoky):
http://www.developpez.net/forums/d356579/hardware-systemes-logiciels/windows/securite/labc-securite
-FAQ Sécurité de developpez.com: **http://securite.developpez.com/faq**
-Vulgarisation de la sécurité informatique: **http://www.securite-informatique.gouv.fr/gp_mot4.html**

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

Scanner Online:
-Trend Micro: **http://housecall.trendmicro.com/fr**
-BitDefender: **http://www.bitdefender.com/scan8/ie.html**
-Kaspersky lab: **http://www.kaspersky.com/virusscanner**

Sites web dynamiques proposant d'analyse d'un fichier suspect:
-UploadMalware: **http://www.uploadmalware.com**
-VirusTotal: **http://www.virustotal.com**
-Anubis: **http://analysis.seclab.tuwien.ac.at**
-Jotti's malware scan:**http://virusscan.jotti.org**
-ThreatExpert (13) : **http://www.threatexpert.com/default.aspx**
-VirSCAN Online AV Scanner: **http://virscan.org**
-Filterbit: **http://www.filterbit.com**

Logiciels Utiles:
-Les meilleurs outils gratuits pour Windows: **http://windows.developpez.com/freewares/**
-Malzilla:**malzilla.sourceforge.net/**
-codec video pour pouvoir lire tous les formats video: **http://www.01net.com/telecharger/windows/Multimedia/codecs/fiches/26950.html**

Protection de l'enfance:
-Protection des mineurs: **http://www.delegation.internet.gouv.fr/mineurs/index.htm**
http://www.actioninnocence.org/suisse/index.aspx
http://www.internet-mineurs.gouv.fr
-Contrôle parental: **http://www.aig-filtra.org/web/resultats.aspx?nav=3**
http://www.orange.fr/bin/frame.cgi?u=http%3A//assistance.orange.fr/755.php
-Signaler un site: **https://internet-signalement.gouv.fr**
-spots publicitaires: **http://www.youtube.com/watch?v=FtuOpNy4Bj4**
http://www.youtube.com/watch?v=Q8sMcHZD4D0
-Internet sans craintes: **http://www.internetsanscrainte.fr**

Pour aller plus loin:
-The New York Times, 20 Octobre 2008, John Markoff, "A Robot Network Seeks to Enlist Your Computer":
http://www.nytimes.com/2008/10/21/technology/internet/21botnet.html
-Google Black-list: **http://fr.securityvibes.com/mcafee-france-press-601.html**
-Anti-phishing et vie privée: **http://blog.developpez.com/adiguba?title=anti_phishing_et_vie_privee**
-Interview de Eric Filliol :**"L'Etat doit s'appuyer sur les hackers"**
Reportage:
-National Geographic, Hackers
-ARTE, Cyber Guérilla
-Envoyé Spécial, Cybercriminalité
-ARTE, Tous fichés
Livres:
-La Taz, Peter Lamborn Wilson dit Hakim Bey, pour comprendre en partie comme fonctionne la mentalité des pirates.
-Tsun zu, l'art de la guerre
-Sécurité informatique, principe et méthode à l'usage des DSI, RSSI et administrateur
-Chaines d'exploits, sénarios de Hacking avancé et prévention
Revue:
-Science et vie, Décembre 2008, n° 1095, Internet au bord de l'explosion
-Misc n°41, Dossier: La cybercriminalité..ou quand le net se met au crime organisé
-Misc n°47, Dossier: La lutte antivirale, une cause perdue ?

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

-Hakin9 n°31, Secrets de cybercriminels, Phisers, spammeurs, voleurs d'identité
-Courrier International, 2 au 22 Aout 2007, n°874-875-876, rubrique Europe > Russie, Les Hackers investissent le champ politique
-Courrier International, 5 au 11 Mars 2009, n°957, rubrique Europe > Multimédia, Hackers en uniforme
-Courrier International, /////////// 2009, n°///, rubrique Science, cyberguerre

VIII - Remerciements

Je tiens à remercier :
-**Alain Defrance** pour ses bonnes idées.
-**Jean-Philippe Dubbé** pour sa patience.
-**Ced**, **Bovino**, **jacques_jean** pour leur rigoureuse relecture orthographique ;)
-**Djug** pour avoir relancer la rédaction.
-**ram-0000** pour ses conseils.
-**spawntux** pour ses remarques.
Ainsi qu'à tous ceux que je n'ai pas cité, mais qui se reconnaitront ;).

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

1 : Un Hacker est un terme Anglais désignant un technicien passionné très compétent qui maitrise comme par don les ordinateurs et uvre pour la bonne cause. Malheureusement ce terme est trop souvent repris à tort par les médias, qui amalgament les crackers à des Hackers.
2 : Agobot est un virus réticulaire (botnet) qui permet à un pirate d'avoir une prise de contrôle totale sur le système infecté. Il permet en outre de pouvoir relayer des envois de spam, récupérer des informations personnelles... (source:**http://www.sophos.fr/security/analyses/viruses-and-spyware/w32agobotnz.html**)
3 : -Discution concernant la sécurité des sites web face aux pirates informatiques (**http://www.developpez.net/forums/d74061/webmasters-developpement-web/general-conception-web/securite/meilleures-pratiques-securite-proteger-site-hackers/**) -Site officiel de l'OWASP
4 : "Deux choses sont infinies : l'Univers et la bêtise humaine. Mais, en ce qui concerne l'Univers, je n'en ai pas encore acquis la certitude absolue", Albert Einstein.
5 : Exemple de honey pot: **http://goldkey.developpez.com/tutoriels/linux/installation-configuration-honeypot/**
6 : Certains sites web (blogs, forums, sites personnels) mettent à la disposition des visiteurs des techniques prétendant pouvoir de gagner au casino en ligne. Généralement, ces sites appartiennent aux mêmes escrocs (source:**http://www.zataz.com/news/19184/casinos--rouge--noir--hawks.html**)
7 : Bonjour, chers webmasters et les optimiseurs, je tiens à vous proposer la coopération avec le programme d'affiliation EvaPharmacy.ru Nous sommes sur le marché depuis plus de 6 ans et possèdent une vaste expérience dans Pharma-convertir du trafic en ligne gastronomique. Avec la filiale pharmaceutique EvaPharmacy.ru vous obtenez: 1. Un grand nombre de médicaments (Viagra et Cialis, terminant avec un super vitamines, amaigrissement) 2. Fixe 45% de commission sur les ventes et les ventes répétées. 3. Vous obtenez une moyenne de 60-100 $ par vente. 4. Les paiements hebdomadaires à toutes les banques du monde (y compris en Russie), mai payer par WebMoney et ePassporte. 5. Ratio 1:3-1:60 les publicités à la moyenne. 6. Statistiques en temps réel est toujours disponible sur notre site Web. 7. 10 Décision% de tous les profits étant donné vos partenaires dans notre système. 8. Le paiement peut être faite non seulement une carte Visa et MasterCard, et Amex, Diners, JCB, à tous nos sites. Comme pour influer sur le ratio de nos partenaires. 9. Et bien sûr un support, qui est toujours prêt à vous aider! 10. Les grands partenaires - les conditions particulières (paiement en une journée, personnels des domaines, hébergement, et bien d'autres)
8 : Etude réalisée par la société Kaspersky Lab en 2007 (source: **http://www.viruslist.com/fr/analysis?pubid=200676132**)
9 : La chercheuse en sécurité informatique, **Joanna Rutkowska**, a réussi à démontrer qu'il était possible d'infecter Windows Vista en outrepassant cette sécurité (source: **http://blog.ifrance.com/webinpocket/post/292435-vista-a-deja-son-rootkit**)
10 : Descriptif et utilisation du logiciel: **http://www.developpez.net/forums/d530859/systemes/windows/securite/hijackthis-lutiliser/**
11 : AS: mettre def (source:**http://fr.wikipedia.org/wiki/Autonomous_System**)
12 : Constat fait par éric Filiol, expert français en virologie informatique: **"Les éditeurs d'antivirus confondent le business et le besoin des utilisateurs "**, **Le pire cauchemar, c'est le décideur qui écoute les messages marketing des éditeurs d'antivirus**
13 : ThreatExpert:Site developpé par une équipe de professionnels qui sont à l'origine du site PC Tools'

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2009 - Therrode. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.