- http://lepouvoirclapratique.blogspot.fr/
- Cédric BERTRAND

- Juin 2012

Etat de l’art des malwares

Qu’est-ce qu’un malware ? Pourquoi sont-ils créés ? Qui sont leurs auteurs ? Zoom sur leurs modes de fonctionnement et de propagation. Exemple d’une infection

Sommaire

1. Etat de l'art des malwares 4
1.1. Qu'est-ce qu'un malware 4
1.2. Comment fonctionnent les malwares 4
1.3. Pourquoi y'a-t-il des malwares ? 5
1.4. Comment sont diffusés les malwares ? 8
1.4.1. Les exploits 8
1.4.2. Les exploits pack 8
1.4.3. Social engineering 9
1.4.4. Les périphériques USB 10
1.4.5. Réseaux sociaux 10
1.4.6. Les courriels 11
1.4.7. Cracks / Keygens 11
1.4.8. Fausses applications 12
1.5. Qui sont les auteurs de malwares ? 12
1.6. Un exemple d'infection : le malware ZeuS 13
2. Conclusion 16

Table des illustrations

Figure 1 Schéma général d'un botnet 5
Figure 2 Quelques exemples de botnet 5
Figure 3 Ventes de malwares sur Internet 7
Figure 4 Malwares se diffusant par l'intermédiaire d'exploits 8
Figure 5 Quelques exploits packs sur les marchés underground 9
Figure 6 Exemples de techniques de Social engineering utilisées par les malwares 9
Figure 7 Applet Java malicieux 10
Figure 8 Lancement d'un malware sur clé USB par le fichier autorun.inf 10
Figure 9 Quelques attaques sur les réseaux sociaux 11
Figure 10 Diffusion de malwares par courriel 11
Figure 11 Diffusion par les faux cracks 12
Figure 12 Malwares diffusés par de fausses applications 12
Figure 13 Des malwares de plus en plus complexes 13
Figure 14 La russe domine la cybercriminalité 13
Figure 15 Pillage des comptes bancaires avec ZeuS 13
Figure 16 Diffusion du malware ZeuS 14
Figure 17 Exemple de campagne de diffusion de ZeuS - Extrait du site VirusList 14

Glossaire

Adware	Logiciel publicitaire
Backdoor	Outil permettant de contrôler un ordinateur à distance
Blindage	Procédé permettant de ralentir l'analyse d'un malware
Botnet	Ensemble de machines infectées reliées entre elles
Cheval de troie	Idem que Backdoor
Cryptographie	Techniques permettant d'assurer la confidentialité des données
DDos	Technique qui consiste à saturer un service pour le rendre indisponible
Exploit	Programme permettant d'exploiter une vulnérabilité
Exploits pack	Outil permettant d'infecter un ordinateur de manière automatique par la simple consultation d'un site web
Exploit/faille 0-Day	Vulnérabilité pour laquelle il n'existe pas encore de correctif
Honeypot	Simulation d'une machine vulnérable afin de pouvoir étudier les attaques de malwares ou des pirates
Malware	Logiciel malveillant (vers, virus, backdoors, etc.)
Obfuscation	Procédé consistant à rendre un code viral plus compliqué à comprendre
Packer	Logiciel utilisé pour rendre un malware indétectable aux antivirus
Phishing	Technique utilisée pour soutirer des informations à un utilisateur
Ransomware	Logiciel malveillant bloquant l'ordinateur
Reverse engineering	Technique consistant à décompiler un programme afin de l'analyser
Rootkit	Ensemble de techniques permettant de masquer la présence
Sandbox	Procédé consistant à exécuter une application dans un environnement sécurisé
Spams	Courriel indésirable
Tracker	Logiciel de suivi

Documents de référence

[MALEKAL]	Projet Antimalwares
[MISC]	Recherche « à froid » de malwares sur support numérique
[MISC]	Analyse de documents malicieux : Les cas PDF et MS Office
[MISC]	Analyse de malwares sans reverse engineering
[SecurityVibes]	Analyse de malware à la sauce maison

1. Etat de l'art des malwares

1.1. Qu'est-ce qu'un malware

Nous pourrions définir un malware par un programme qui exécute des actions sans le consentement de l'utilisateur. Cette définition volontairement vaste permet d'inclure de nombreux programmes aux fonctionnalités et aux fonctionnements très différents mais qui ont en commun l'objectif de réaliser un certain nombre d'actions en général non souhaitées par l'utilisateur : prise de contrôle à distance, espionnage, vol de données, etc. Les malwares se classent principalement en 3 catégories :

- **Les virus/vers** : ces programmes ont la capacité de se propager et d'infecter de nouvelles cibles (infection de fichiers exécutables, diffusion sur le réseau local, etc.). Parmi les virus/vers les plus connus, nous pouvons par exemple citer *CIH*[1], *IloveYou*[2], *Conficker*[3].
- **Les chevaux de troie / backdoors / Rat** : Contrairement aux virus/vers, ceux-ci ne peuvent pas se propager par eux-mêmes. Ils sont souvent utilisés pour contrôler des ordinateurs à distance pour des opérations de vol de données ou d'espionnage par exemple. Parmi les *chevaux de troie* les plus connus, nous pouvons citer *Subseven*[4] qui était utilisé pour contrôler un ordinateur à distance, *ZeuS*[5] créé pour dérober des données bancaires ou encore *Rustock* un malware créée pour envoyer du *spam*.
- **Les programmes divers** : Dans cette catégorie, nous pourrions y mettre tous les programmes malveillants, qui ont des fonctionnalités très spécifiques (ne se propagent pas et ne se contrôlent pas à distance). Nous pourrions citer dans ces programmes par exemple les *adwares* (logiciels publicitaires), les *ransomwares*[6] (logiciels débloquant un ordinateur contre une somme d'argent), les *dialers* (programmes composeur de n° surtaxés), les faux anti-virus[7], etc.

La plupart des malwares sont souvent écrits soit en langage assembleur[8], soit en C. Les spécificités de ces langages sont qu'ils sont assez proches de la machine et permettent de générer des programmes efficaces et rapides ce qui est souvent recherché par les auteurs de malwares.

1.2. Comment fonctionnent les malwares

Un point commun à la plupart des malwares est le fait que ceux-ci doivent pouvoir être contrôlés à distance (récupération d'informations, actions à exécuter, etc.) par leurs auteurs. Cette définition permet d'introduire le terme de *botnet*. Un botnet est un ensemble de postes infectés (bot ou zombie) contrôlés sur Internet par un cybercriminel (le botmaster). Un schéma simple permet de représenter cette idée :

[1] http://fr.wikipedia.org/wiki/Tchernobyl_(virus)
[2] https://fr.wikipedia.org/wiki/I_love_you_%28ver_informatique%29
[3] http://www.secuser.com/alertes/2008/conficker.htm
[4] http://fr.wikipedia.org/wiki/SubSeven
[5] https://en.wikipedia.org/wiki/Zeus_%28Trojan_horse%29
[6] http://fr.wikipedia.org/wiki/Ransomware
[7] http://www.cnetfrance.fr/news/les-faux-antivirus-scareware-de-plus-en-plus-repandus-39760903.htm
[8] https://fr.wikipedia.org/wiki/Assembleur

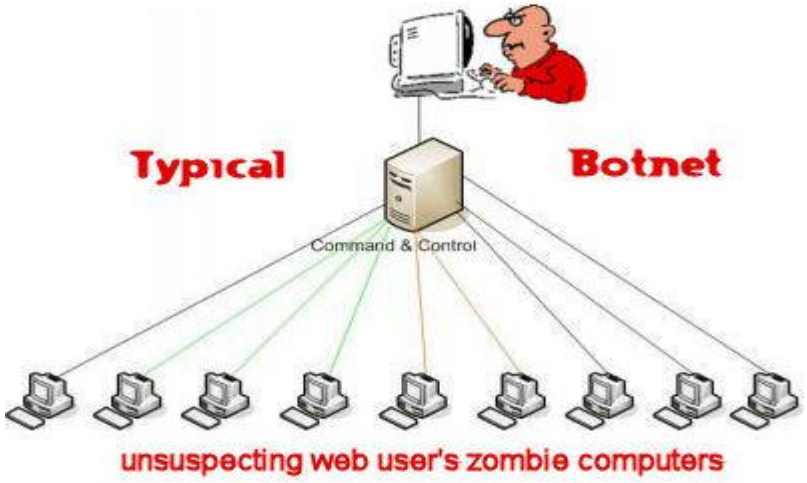

Figure 1 Schéma général d'un botnet

Plus un *botnet* compte de machines infectées, plus ses capacités de nuisance et son profit seront grands. C'est le nombre qui fait la force des *botnets*. Depuis des années, on découvre ainsi fréquemment des *botnets* composés de millions d'ordinateurs infectés.

Un **botnet** Russe infecte 6 **millions** d'ordinateurs ~ Cr@zy WS
www.crazyws.fr/.../un-**botnet**-russe-infecte-**millions**-ordinateurs-2FNI...
25 juin 2012 – Les autorités policières Russes disent que le **botnet** d'un hacker de 22 ans, qu'ils ont arrêté jeudi dernier, a infecté plus de 4.5 **millions** ...

Ghost Click : **botnet** à 4 **millions** d'ordinateurs démantelé
www.generation-nt.com/**botnet**-fbi-ghost-click-dns-changer-actualite...
10 nov. 2011 – Le FBI annonce le démantèlement d'un **botnet** criminel qui a infecté jusqu'à 4 **millions** d'ordinateurs. L'opération Ghost Click a abouti à ...

Figure 2 Quelques exemples de botnet

Parmi les botnets les plus connus, nous pourrions citer *Storm*[9], *Rustock*[10], *Srizbi*[11]. Maintenant voyons quels sont les objectifs des malwares.

1.3. Pourquoi y'a-t-il des malwares ?

L'argent motive sans conteste les auteurs de malwares. Ce n'était pas le cas des premiers créateurs de virus dans le milieu des années 80. À cette époque, c'était plutôt par défi, pour montrer qu'ils en étaient capables, par provocation ou par jeu tout simplement. Les infections se contentaient de se dupliquer elles-mêmes, d'afficher un message, et détruisaient parfois (rarement) des données. Désormais les malwares sont crées pour des objectifs financiers et sont source de revenus par divers moyens :

- Attaque en masse (*DDOS*) à partir d'ordinateurs détournés,

Des **botnets** et des attaques DDoS à la demande en vente à bon ...
www.undernews.fr/.../des-**botnets**-et-des-attaques-ddos-a-la-demande...
8 janv. 2012 – Tous les programmes ont été réalisés par des codeurs **professionnels**. » Ce site est dédié à la vente de **Botnet**, IRC **Botnet**, Web **Botnet** et ...

[9] http://fr.wikipedia.org/wiki/Botnet_Storm
[10] http://fr.wikipedia.org/wiki/Rustock
[11] http://fr.wikipedia.org/wiki/Botnet_Srizbi

11/01/2012

Le blocage de The Pirate Bay conduit les Anonymous à lancer une attaque DDOS

Anonymous a frappé les sites de deux associations qui militent contre le piratage, un jour après le blocage de l'accès au moteur d (...)

- Envois de publicités à partir d'ordinateurs détournés (spam),

Un botnet Android capable de générer du **spam**

PC Inpact - il y a 5 jours

La découverte a commencé avec la réception de certains **spams** qui ont attiré le regard de Zink. Parmi leurs points communs, on en trouvait un ...

- Affichage de publicités,

L'opération "Ghost Click" met fin à une cyberarnaque de 14 millions de dollars

- Arnaques avec de faux logiciels de sécurité (rogues),

Les faux antivirus : un business à 300 millions de d'euros

14:20 - vendredi 19 novembre 2010 - Par Nicolas Aguila - Source : Tom's Guide FR

- Vol de données, de mots de passe, de numéros de série de logiciels...

Des pirates russes détournent un million d'euros de comptes bancaires français

- Redirection vers des sites frauduleux (phishing),
- Espionnage,

21/06/2012

Les outils numériques facilitent la surveillance de son conjoint

"En moyenne, plus d'un Français sur cinq (21%) avoue avoir déjà regardé dans le portable ou l'ordinateur de son conjoint. Mais hom (...)

- Chantage (*ransomware*),

07/05/2012

Un malware exige un paiement pour débloquer les PC

Une vague de logiciels malveillants bloque les ordinateurs et exige le paiement d'une dîme pour les déverrouiller, alléguant à to (...)

- Envoi de sms surtaxés,

Un Trojan envoie des SMS surtaxés depuis des mobiles Android

- Etc.

De plus, les malwares sont de plus en plus utilisés aussi par les états, gouvernements, et polices pour des opérations de cyber-guerre, d'espionnage économique ou encore de surveillance généralisée :

Après Stuxnet et Duqu, le malware Flame cyberespionne Etats et entreprises

Bull a fourni la **surveillance** électronique de la Libye de Kadhafi - RFI
www.rfi.fr/.../20110831-**bull**-fourni-**surveillance**-electronique-libye
31 août 2011 – Selon le Wall Street Journal, le groupe informatique français **Bull** et sa **filiale** Amesys auraient fourni des systèmes de **surveillance** électronique ...

17/10/2011
La police suisse a aussi eu recours à un logiciel d'espionnage
Le département fédéral de justice et police (DFJP) a confirmé jeudi soir une information de la télévision alémanique SF et du quot (...)

L'espionnage des personnes sur Internet : nouveau cheval de bataille de WikiLeaks

Le FBI réclame des "backdoors" aux fournisseurs d'outils de communication IP

Loin d'être utilisés uniquement par les cybercriminels pour se faire de l'argent, **les malwares sont aussi des armes numériques**.

Sur internet d'ailleurs, les malwares se vendent désormais comme un simple produit :

et représentent un business à part entière sur Internet[12] :

Mpack : un logiciel de piratage vendu 700 dollars sur le Net.
www.01net.com/.../des-logiciels-de-piratage-vendus-cles-en-main-sur...

Un site propose l'achat de malwares en toute impunité

Un RAT qui s'infiltre dans les terminaux d'hôtel, vendu sur des forums illégaux

Figure 3 Ventes de malwares sur Internet

[12] http://tjrlapourtaider.superforum.fr/t7-projet-antimalware-by-malekal

Dans de nombreux cas, il est aussi par exemple d'acheter son malware à la demande…

1.4. Comment sont diffusés les malwares ?

Les malwares utilisent de nombreux moyens pour se propager. Avant dans la grosse **majorité** des cas, c'était **l'utilisateur** lui-même qui invitait sans le savoir ces compagnons indésirables par un excès de confiance. Simplement en **exécutant** des programmes téléchargés. Actuellement ce n'est plus le cas et les malwares utilisant de plus en plus des méthodes d'exploitation automatisées.

Voici les principaux vecteurs d'infection passés & actuels:

1.4.1. Les exploits

Un *exploit* est un programme qui utilise une vulnérabilité dans un programme. Les malwares utilisent les exploits afin d'infecter d'autres cibles de manière silencieuse et automatique sans nécessiter d'intervention de l'utilisateur. Il y a d'ailleurs tout un marché autour des exploits dont certains peuvent se vendent quelques dizaines de milliers de dollars.

Certains malwares utilisent des exploits pour se propager sur les réseaux locaux (ex : Stuxnet[13], Conficker[14])

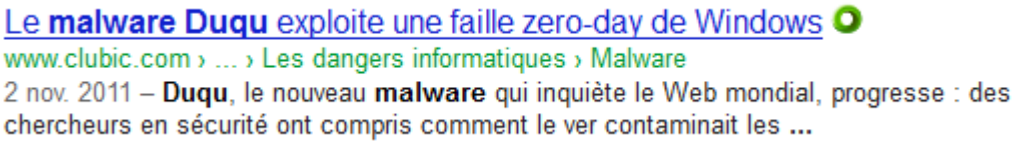

Figure 4 Malwares se diffusant par l'intermédiaire d'exploits

Avec ces exploits, les cybercriminels ont crée des outils permettant leur utilisation de manière automatique et plus massive : *les exploits pack*.

1.4.2. Les exploits pack

C'est actuellement la méthode d'infection la plus utilisée (plus de 90% des cas). Un *exploit pack* est un outil utilisé pour télécharger des malwares sur des ordinateurs distants en exploitant plusieurs vulnérabilités (*exploits*). Ils permettent de réaliser des attaques de type « *drive-by download* [15]», c'est-à-dire une attaque où un utilisateur est infecté en visitant un

[13] https://fr.wikipedia.org/wiki/Stuxnet
[14] https://fr.wikipedia.org/wiki/Conficker
[15] https://www.ebas.ch/index.php?option=com_content&view=article&id=75&Itemid=0&lang=fr

simple site web. Les exploits packs se vendent sur les forums underground pour quelques milliers d'euros.

Figure 5 Quelques exploits packs sur les marchés underground

Afin de diffuser les pages malveillantes, les cybercriminels piratent des sites web à forte audience ce qui leur permet de pouvoir infecter en quelques heures des dizaines de milliers d'utilisateurs.

27/09/2011

MySQL.com piraté pour injecter des logiciels malveillants

Le fournisseur de services de sécurité Armorize Technologies a relevé le problème sur le site MySQL.com le lundi 26 septembre à en (...)

1.4.3. Social engineering

Pour diffuser leurs malwares, les cybercriminels ont une grande imagination : fausses cartes d'anniversaire, mises en scène d'événements d'actualité, St-Valentin, fausses mises à jour de logiciels, etc. La moindre actualité est reprise afin d'infecter de nouvelles victimes.

Diffusion de **malwares** sur la **mort de Ben Laden** - News sur la ...
cybersecurite.over-blog.com/article-diffusion-de-**malwares**-sur-la-**mo**...
6 mai 2011 – Comme à chaque évènement mondial, les cyberpirates réagissent immédiatement à l'actualité, c'est encore le cas avec la **mort de Ben laden**, ...

Zidane inspire aussi les auteurs de **malwares** - Actualité PC INpact
www.pcinpact.com/.../30102-Zidane-inspire-aussi-les-auteurs-de-**mal**...
17 juil. 2006 – Le **coup** de tête de Zidane durant la finale de la **coupe** du **monde** ... est de télécharger plusieurs autres **malwares** aux effets divers et variés.

Saint-Valentin: Attention aux **malwares** - Chloé-sécurité
chloe-securite.over-blog.fr/article-**saint-valentin**-attention-aux-**malwa**...
12 févr. 2012 – La **saint-Valentin** approche à grands pas et comme tous les ans cet évènement ne manquera pas d'être exploité par les piratespour tenter de ...

Figure 6 Exemples de techniques de Social engineering utilisées par les malwares

Ces derniers mois, de nombreux malwares se diffusaient par des pages web malicieuses en proposant l'installation d'un applet java.

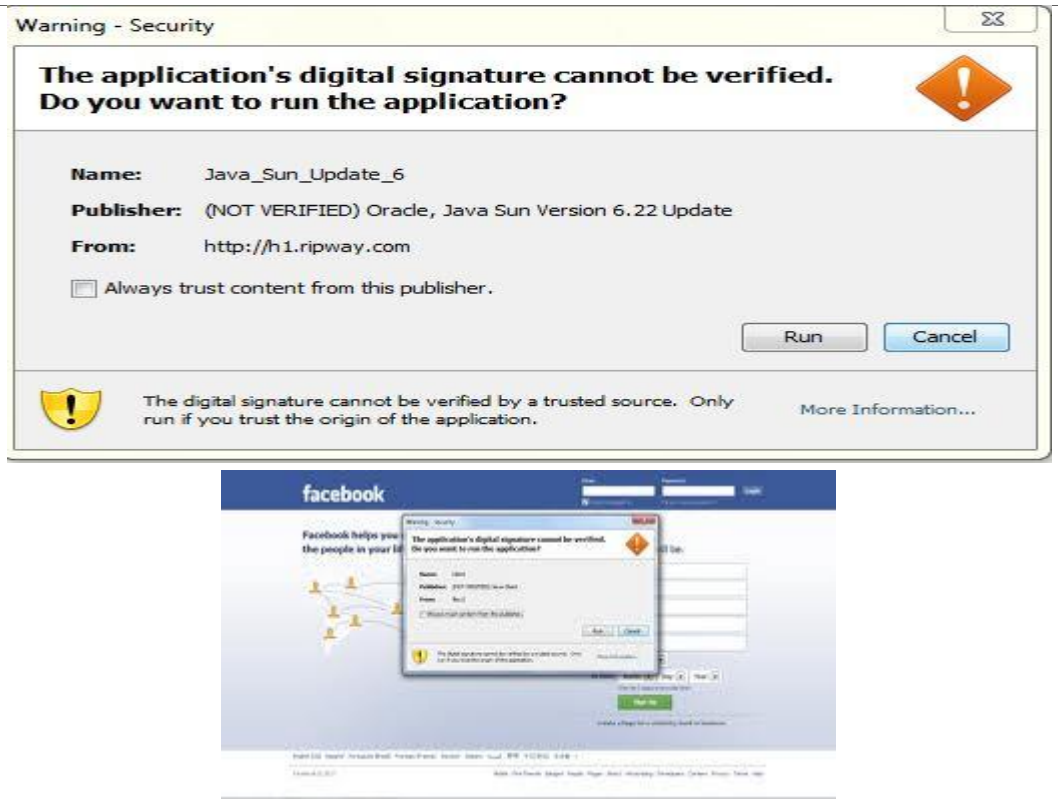

Figure 7 Applet Java malicieux

1.4.4. Les périphériques USB

Beaucoup moins utilisés depuis que l'exécution automatique des périphériques USB a été désactivée par défaut, de nombreux dangers y encore sont liés. Néanmoins les malwares par clé USB sont toujours utilisés dans le cadre de certaines attaques plus ciblées (ex : *Stuxnet*). En général les malwares utilisant les clés USB se propagaient soit par un exploit, soit se lancer par le fichier <autorun.inf>

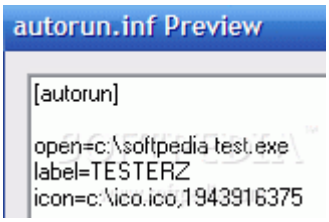

Figure 8 Lancement d'un malware sur clé USB par le fichier autorun.inf

Qui a peur de **StuxNet** ?
www.zdnet.fr › Blogs
4 oct. 2010 – **StuxNet** se propage via des **clefs USB** infectées. Mais en dehors de ce moyen de diffusion, aucune propagation autonome n'a été relevée ...

1.4.5. Réseaux sociaux

De plus en plus présents et de plus en plus utilisés, les réseaux sociaux deviennent une des portes préférées des malwares : fausses applications, fausses vidéos, fausses actualités, etc. Les réseaux sociaux sont une mine d'or pour les pirates car ils permettent de mieux cibler les utilisateurs.

Figure 9 Quelques attaques sur les réseaux sociaux

1.4.6. Les courriels

Très utilisé il y a quelques années et remplacé peu à peu par les exploits pack, les courriels représentent actuellement un vecteur d'infection encore utilisé à part dans le cas d'attaques dites « ciblées » (attaques visant un objectif précis ou/et un utilisateur particulier) ou des arnaques à la nigériane[16].

Figure 10 Diffusion de malwares par courriel

1.4.7. Cracks / Keygens

Pour utiliser des **logiciels payants** sans débourser le moindre centime, nombreux sont ceux qui **enlèvent** les protections à l'aide d'un programme appelé communément *crack* ou **inscrivent** un numéro de série généré par un *keygen*. Toutes ces applications facilitant le piratage ne sont pas forcément contaminées, mais les auteurs de *malwares* font maintenant passer leurs créations **malignes** comme étant ce type de programme.[17]

[16] http://bigbrowser.blog.lemonde.fr/2012/02/10/spam-arnaque-nigeriane/
[17] http://forums.futura-sciences.com/securite-malwares-desinfectez-machine/204436-projet-antimalware-etes-infectes.html

Diablo III : Les faux **cracks** deviennent légion, prudence ! | UnderNews
www.undernews.fr/**malwares**.../diablo-iii-les-faux-**cracks**-deviennent-...
28 mai 2012 – Avant de pouvoir télécharger le fameux **crack** pour Diablo III, vous devez **...** à répandre de de faux **cracks** infectés par des **malwares**. **...** les **cracks** et autres générateurs de clés (**keygens**) qui peuvent (ou pas) fonctionner.

Malekal's forum • Le danger des **cracks** ! : Sécurité : Prévention **...**
forum.malekal.com/danger-des-**cracks**-t893.html
4 messages - 1 auteur - 9 sept. 2011
Les **cracks** sont un vecteur de **malwares** et d'infections très important **...** Voici une liste de **faux** sites de **cracks** - tous les **cracks** proposés sur ces sites sont identiques et **...** Code: Tout sélectionner: **keygen**.name A 85.142.1.66 **...**

Figure 11 Diffusion par les faux cracks

Sachez que les auteurs de malwares créent de faux sites de cracks où tous les cracks proposés sont infectieux, d'autres sites eux contiennent des exploits, si votre navigateur est pas à jour, c'est l'infection. En outre, certaines infections issues de cracks proposées sur les réseaux P2P, une fois installées mettent à disposition des cracks piégés sur le réseau P2P pour que d'autres internautes les téléchargent et s'infectent.

1.4.8. Fausses applications

L'engouement pour de nombreuses applications n'échappe pas aux pirates qui en tirent profit en diffusant ces applications infectées par un malware.

03/05/2012
De fausses applis Instagram et Angry Birds apparaissent sous Android
L'éditeur de solutions antivirus Trend Micro alerte sur la mise en ligne de liens vers de fausses applications Instagram et Angry (...)

20/06/2012
Le malware Zeus se cache dans une app antivirus pour Android
L'application trouvée par les chercheurs de Kaspersky Lab s'appelle Android Security Suite Premium. Elle est capable de voler des (...)

Figure 12 Malwares diffusés par de fausses applications

Nous pouvons constater que les auteurs de malwares sont très créatifs et innovants en ce qui concerne la façon de diffuser leurs malwares. Voyons maintenant qui sont leurs auteurs.

1.5. Qui sont les auteurs de malwares ?

Les auteurs de malware peuvent être divers (personne isolée, équipe, crime organisé, état, etc.), néanmoins au fil des années, force est de constater leur professionnalisation ainsi que la complexité des malwares.

Malware Duqu : du travail de pros
www.linformaticien.com/.../id/.../**malware-duqu**-du-travail-de-pros.as...
20 mars 2012 – On s'en doutait mais Kaspersky Labs aidé par la communauté de programmeurs le confirme : Le **malware Duqu**, lui-même inspiré ...

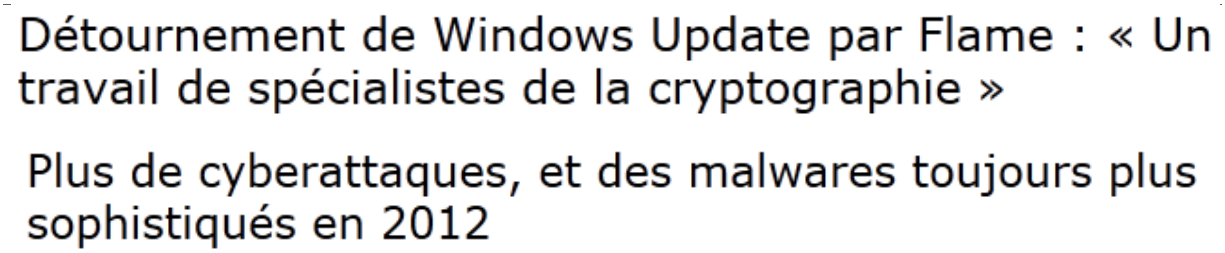

Figure 13 Des malwares de plus en plus complexes

Parmi les pays les plus actifs dans le domaine, les russes ainsi que les chinois tiennent une place assez prépondérante dans le classement.

Figure 14 La russe domine la cybercriminalité

Dans le chapitre suivant, nous allons voir un exemple d'infection par un des malware qui a beaucoup fait parler de lui ces dernières années : ZeuS.

1.6. Un exemple d'infection : le malware ZeuS

Créé en Russie, ZeuS est un cas typique des nouveaux malwares actuels. Spécialisé dans la récupération d'informations sur un poste infecté (informations bancaires, personnelles, mots de passe, etc.), il est activement utilisé par les cybercriminels afin de piller des comptes bancaires :

Figure 15 Pillage des comptes bancaires avec ZeuS

Afin de le diffuser au plus grand nombre possible, les cybercriminels ont utilisé de nombreux moyens de propagation :

Le malware Zeus vous dévalise via Facebook, Gmail

06 juillet 2012

Le malware **Zeus** se cache dans une app antivirus pour Android
www.lemondeinformatique.fr/.../lire-le-malware-**zeus**-se-cache-dans-...
20 juin 2012 – Le malware **Zeus** se cache dans une app antivirus pour Android ... **Zeus** classique pour détourner de l'argent des **comptes bancaires** en ligne.

Sécurité IT : le **malware Zeus** chasse sur les terres de LinkedIn ...
www.itespresso.fr/securite-it-le-**malware-zeus**-chasse-sur-les-terres-de...
10 juin 2011 – Le réseau social professionnel LinkedIn est victime d'une importante attaque de phishing permettant d'installer sur le PC le **malware Zeus** pour ...

ZBot se propage via des documents scannés | UnderNews
www.undernews.fr/**malwares**.../zbot-se-propage-via-des-documents-s...
11 févr. 2011 – Quatre vulnérabilités **PDF** sont exploitées dans une nouvelle ... Voici comment cela se passe : les auteurs de **malwares** utilisent le modèle d'e-mail propriétaire des imprimantes et des scanners professionnels pour **diffuser** du spam. ... de ZBot : également appelé **Zeus**, ZeusBot ou WSNPoem, ce cheval de ...

Figure 16 Diffusion du malware ZeuS

Voici un exemple d'une opération de diffusion utilisée par ZeuS :

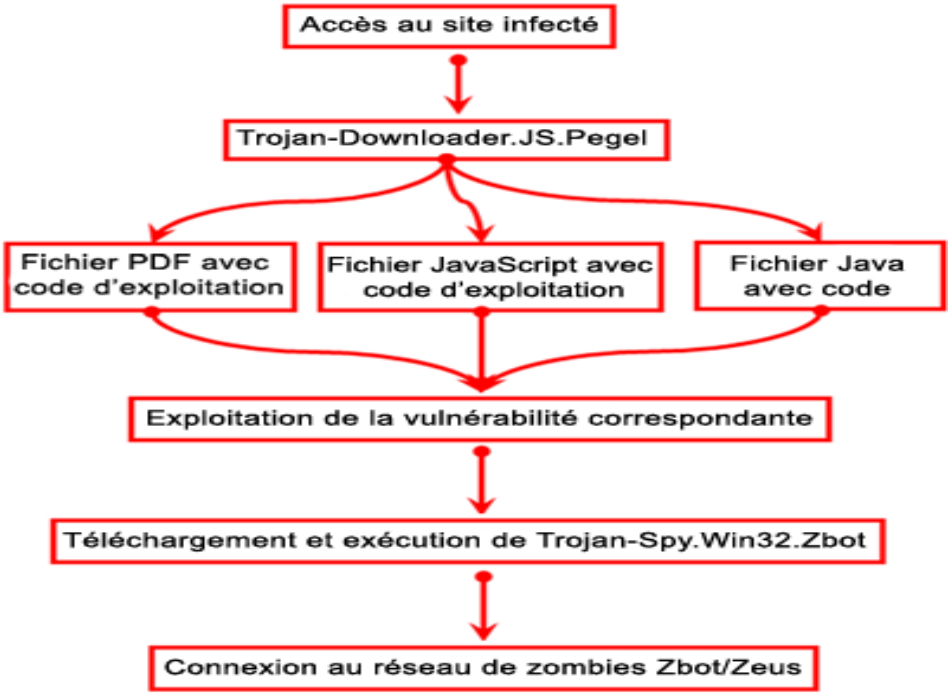

Figure 17 Exemple de campagne de diffusion de ZeuS - Extrait du site VirusList

Voici l'analyse de cette campagne extraite du site Viruslist :

La première étape de l'infection est l'accès de l'utilisateur à un site infecté par Trojan-Downloader.JS.Pegel. Ensuite, Pegel redirige l'internaute vers une page contenant le pack de codes d'exploitation. Puis la tentative de téléchargement et d'installation directe du bot. La toute dernière étape est la connexion de l'ordinateur infecté au centre de contrôle du réseau de zombies et son inclusion dans le réseau de zombies.

L'ingénierie sociale est une autre méthode largement employée pour diffuser les codes d'exploitation. Par exemple, l'utilisateur peut recevoir un lien vers un « nouveau message personnel » qui aurait été envoyé par Facebook ou un message de la banque invitant le client à accéder à une page où il pourra « débloquer son compte ». Au moment de cliquer sur un tel lien, il est tout à fait probable que l'utilisateur télécharge un code d'exploitation sur son ordinateur.

Sur les ordinateurs déjà infectés par un Trojan-Downloader, le téléchargeur peut télécharger et installer différents programmes malveillants, y compris des programmes qui exploitent les vulnérabilités.

Mais la méthode de diffusion la plus efficace est celle qui consiste à diffuser les codes d'exploitation depuis un ordinateur infecté du réseau local. Une requête réseau spéciale est générée et diffusée à tous les ordinateurs du réseau. Cette requête entraîne l'exploitation de la vulnérabilité. Les dangereux vers de réseau Kido et Lovesan se propagent principalement de cette manière. Cette méthode permet d'infecter l'ensemble du réseau local en un laps de temps assez court. La poursuite de l'infection ne pourra pas être interrompue tant que la vulnérabilité du composant n'aura pas été supprimée.

Vous pouvez consulter l'article suivant pour avoir plus d'informations sur le fonctionnement et la diffusion de Zeus : [FR – MALEKAL] Zbot/ZeuS. Si vous désirez voir comment fonctionne un botnet sous ZeuS, vous pouvez aussi consulter l'article suivant : [FR] Inside a ZeuS Botnet.

ZeuS est un des malwares emblématique de notre époque : complexe, créé et maintenu par une équipe de développeurs professionnels, utilisé pour récolter des comptes bancaires, utilisant de nombreuses techniques pour être diffusé au plus grand nombre. A travers cet exemple, nous pouvons constater le professionnalisme affiché des cybercriminels.

2. Conclusion

Les malwares sont devenus une réalité pour la majorité des utilisateurs et bien peu d'entre eux y échappent (en particulier sous les systèmes Windows & Android). Créé au départ par jeu ou par défi, ils sont vite devenus au fil des années de véritables armes numériques. Connaître leur mode de fonctionnement ainsi que méthodes de propagation restent le meilleur moyen de s'en protéger.

Les documents suivants traitent de l'analyse des malwares ainsi des différentes façons de s'en protéger.