Les Botnets

S'informer pour mieux se protéger

Source :www.welivesecurity.com

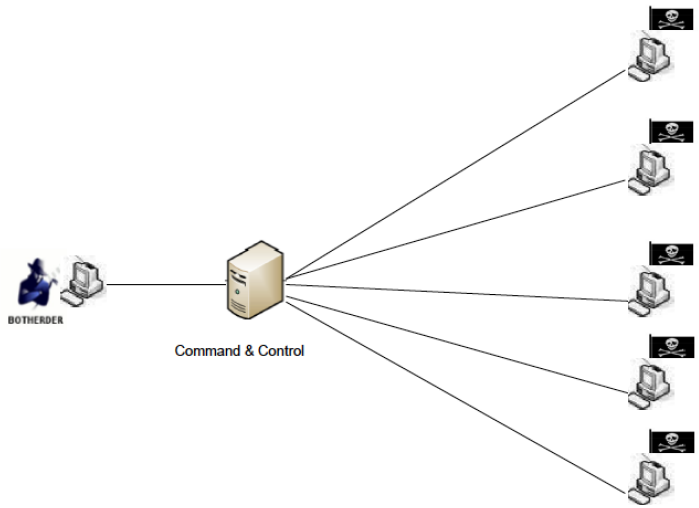
Mohamed Mejri, Ph.D.
Université Laval
Québec, Canada

Plan

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
- **Verre (Warm) ∼1980 (1ère génération) :** pouvoir d'autoréplication... consomm des ressources (mémoire, CPU, bande passante réseau) ... DOS
- **Cheval de Troie et porte dérobée (Trojan and backdoor) ∼1998 (2éme 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 loue ou à vendre)

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

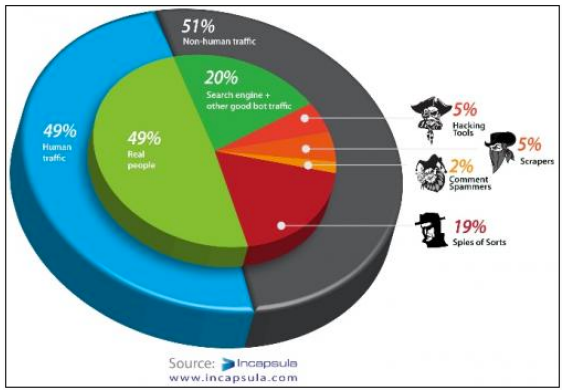
Situation actuelle

Que disent les optimistes et les pessimistes ?

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

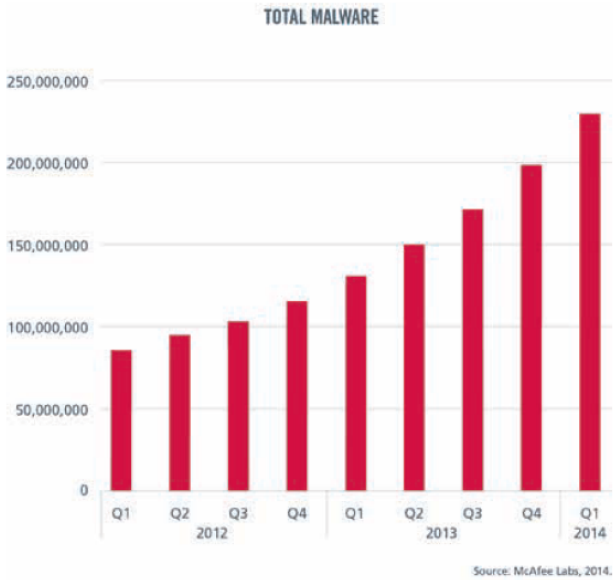
  source : www.sidn.nl/en/news/news/article/abuse-ix-takes-on-botnets

- 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



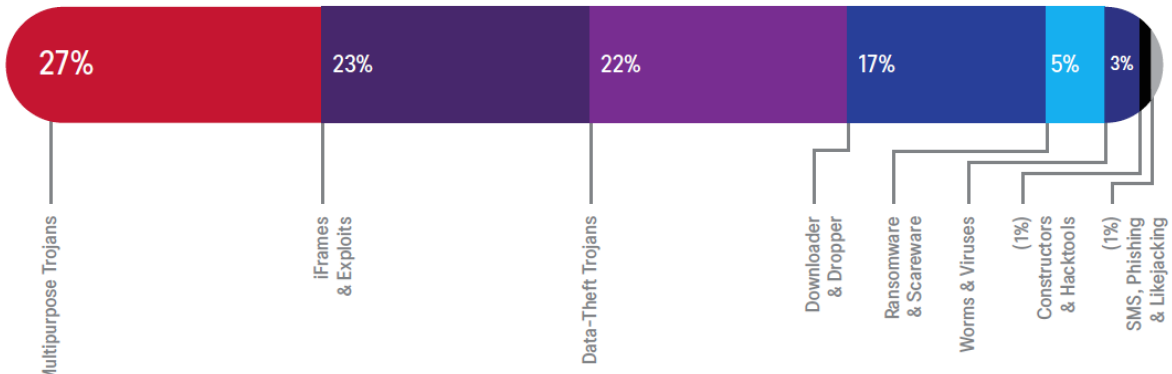
Vecteurs d'attaques

Programme mal veillant (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



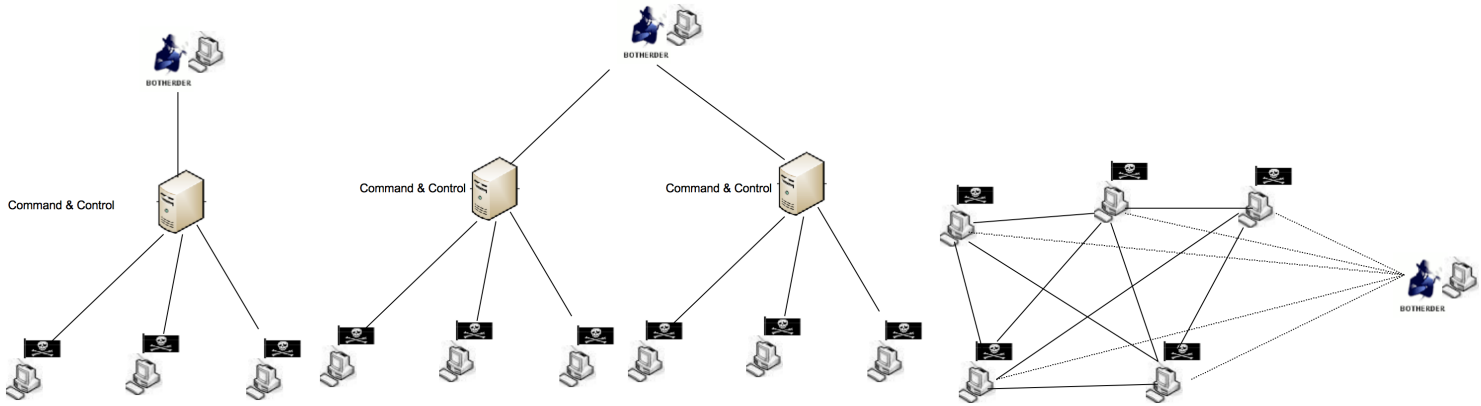
Situation actuelle

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

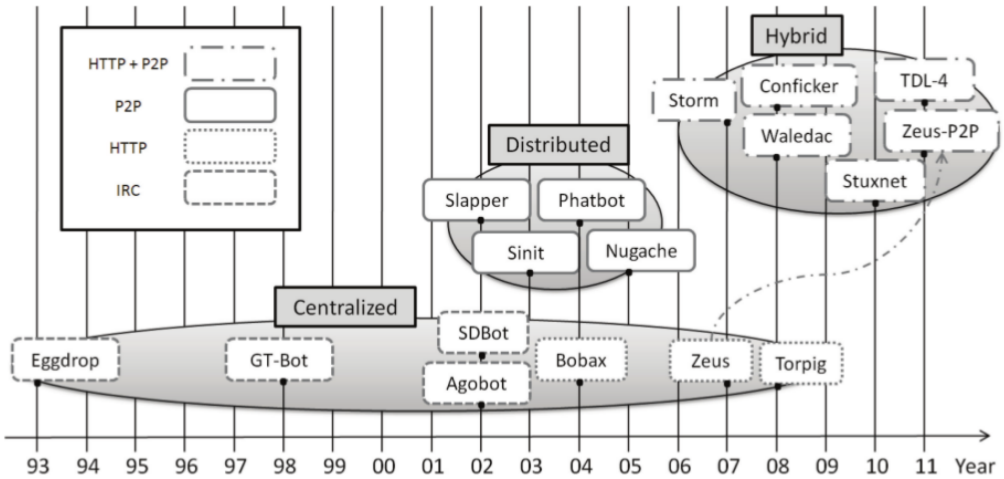
source : http ://en.wikipedia.org/wiki/Botnet

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 : 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

Wrapper

Hacker

Connexion avec l'exterieur.

- Courriel
- HTTP
- IRC
- DNS
- Etc.

Cheval de Troie (Trojan)

Cheval (Over)

- Jeux
- Antivirus
- Etc.

Soldat (Cover, payload)

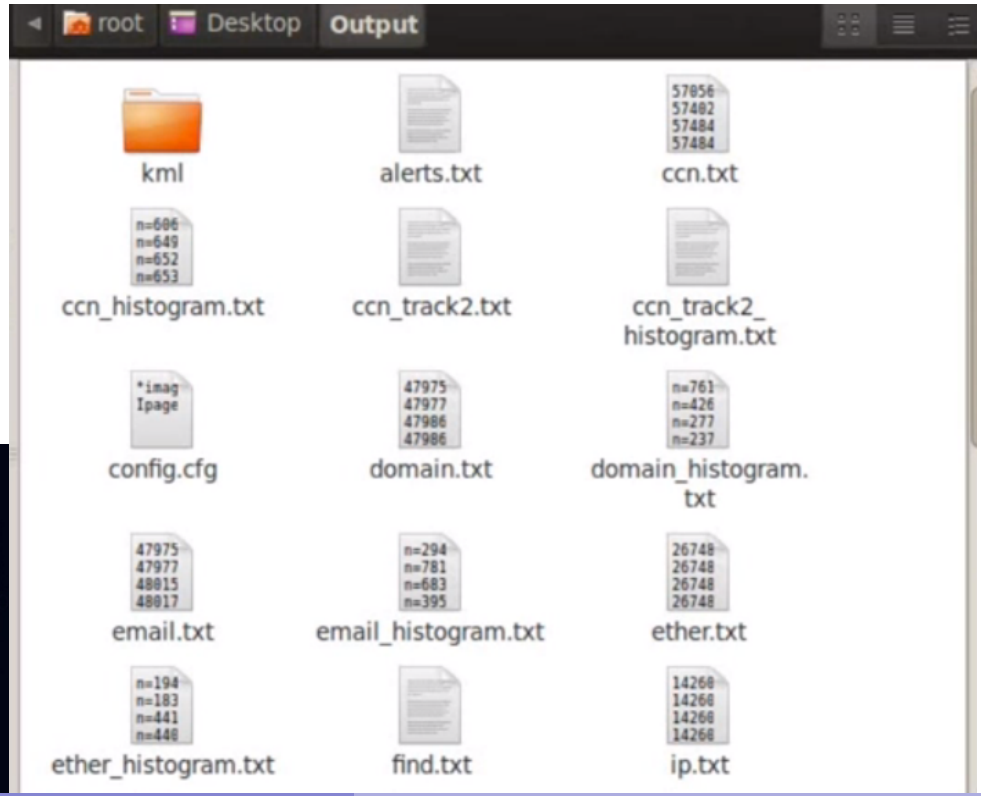
- Backdoors
- Spywares
- Keyloggers
- Rootkits
- RansomWare
- Etc.

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

Examples

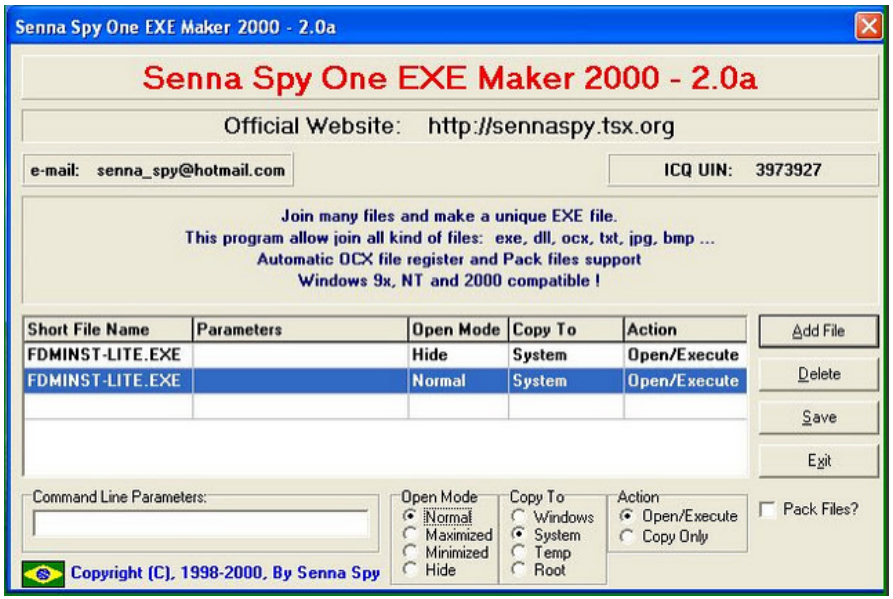
- tini.exe (3Kb), iCmd (mot de passe) netcat, etc.
- ProRAT, Beast, NetBus, Mosucker, Net-Devil, VNC-Trojan : des outils avec interface graphique permettant souvent un contrôle complet

- 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

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 personne (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 (voir des millions) de cibles
- Une fois une cible est 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.

Cheval de Troie

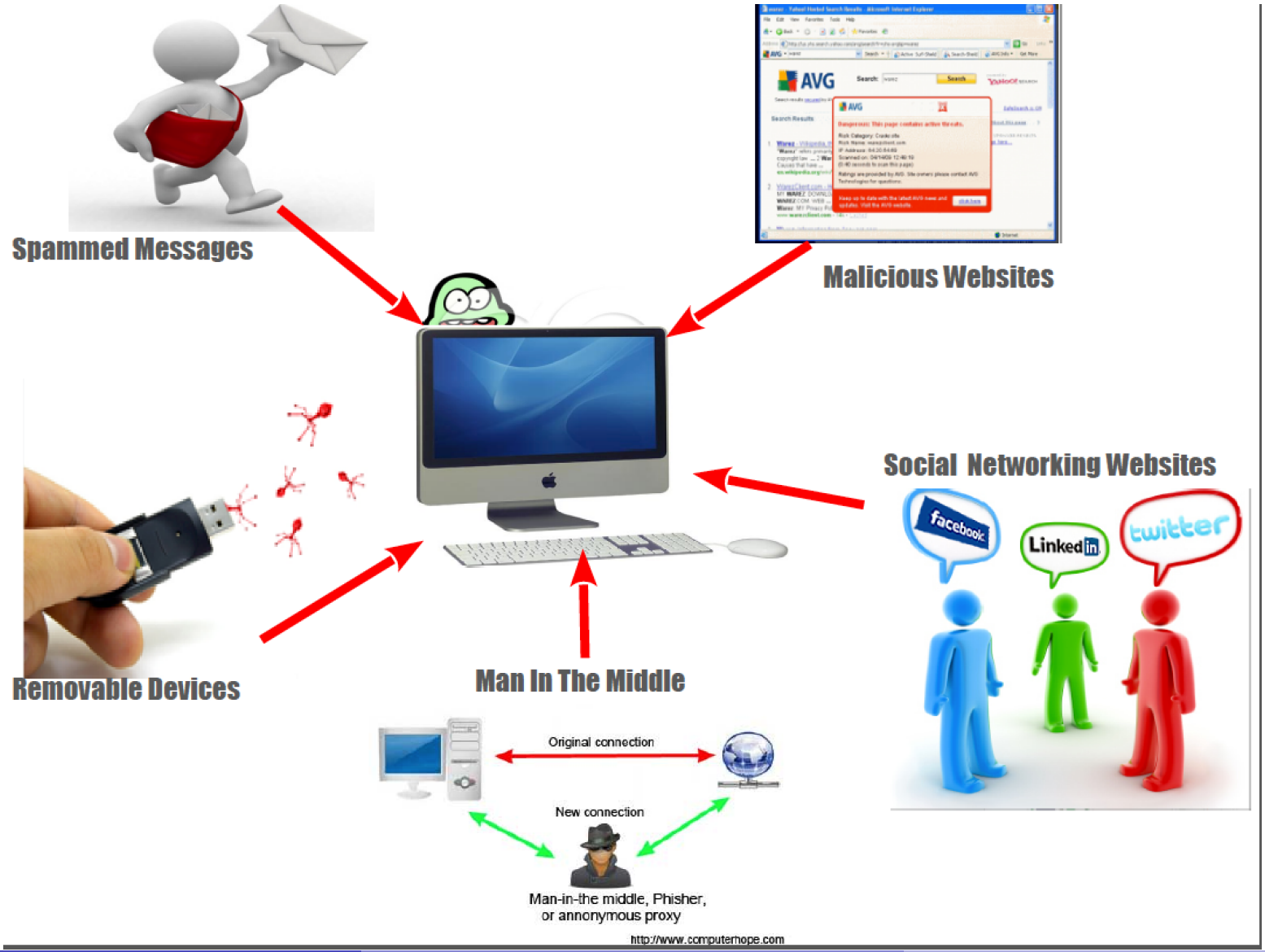
Démonstration

Botnet : techniques d'infection

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

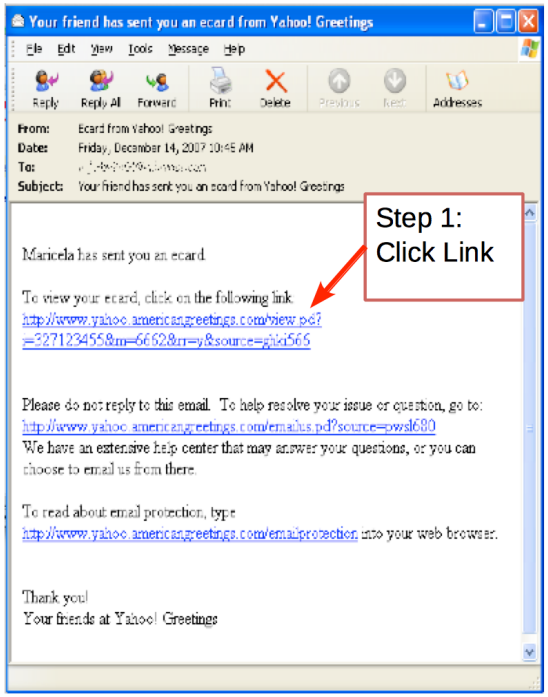
Botnet : techniques d'infection

Principales méthodes d'infection

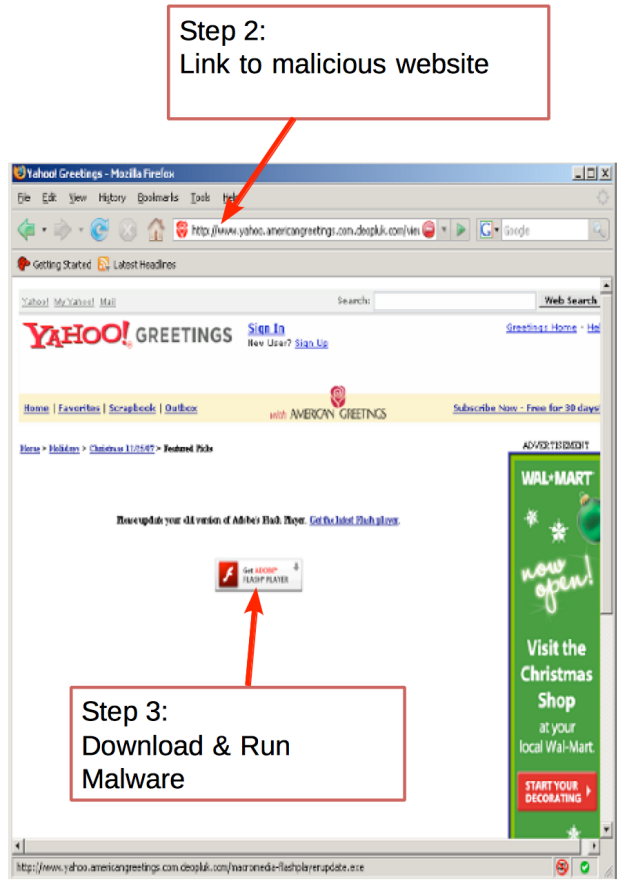


Botnet : techniques d'infection

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)



Botnet : techniques d'infection

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

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)

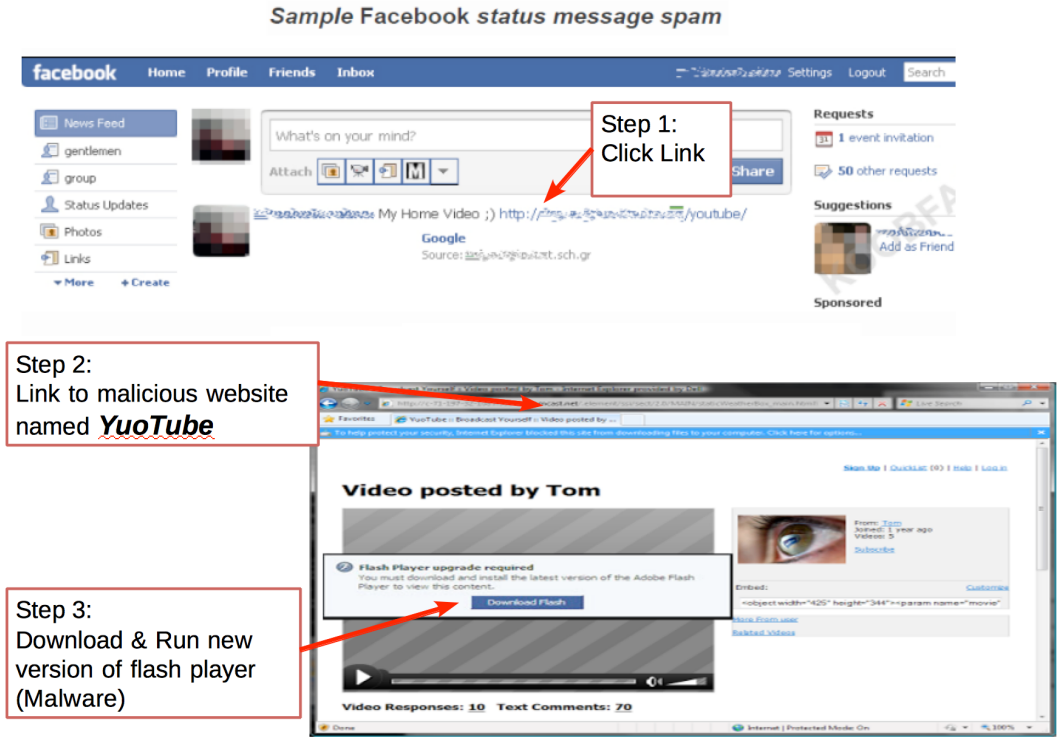
Botnet : techniques d'infection

Infection via SPAM  **: Sujet intéressant + attachement**


- **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

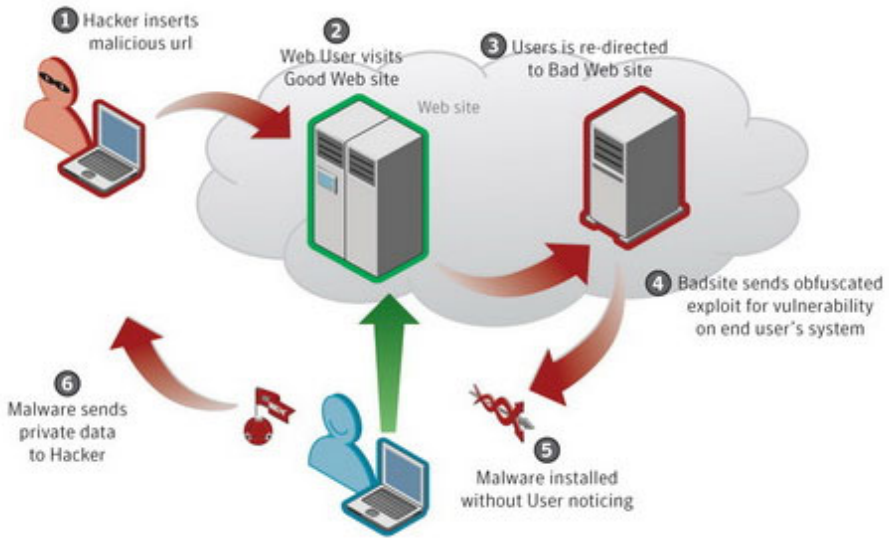
Botnet : techniques d'infection

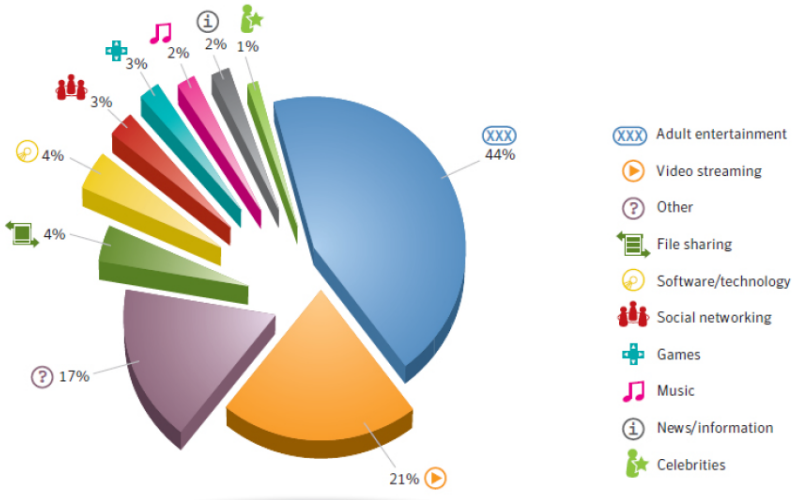
Infection via des réseaux sociaux (exemple : le botnet Koobface, 2009 : 2 millions de dollars de profits à ses gestionnaires) :
Propagation : Envoyer des message aux amis facebook des ordinateurs infectés pour les inciter à ouvrir une vidéo



Botnet : techniques d'infection

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





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

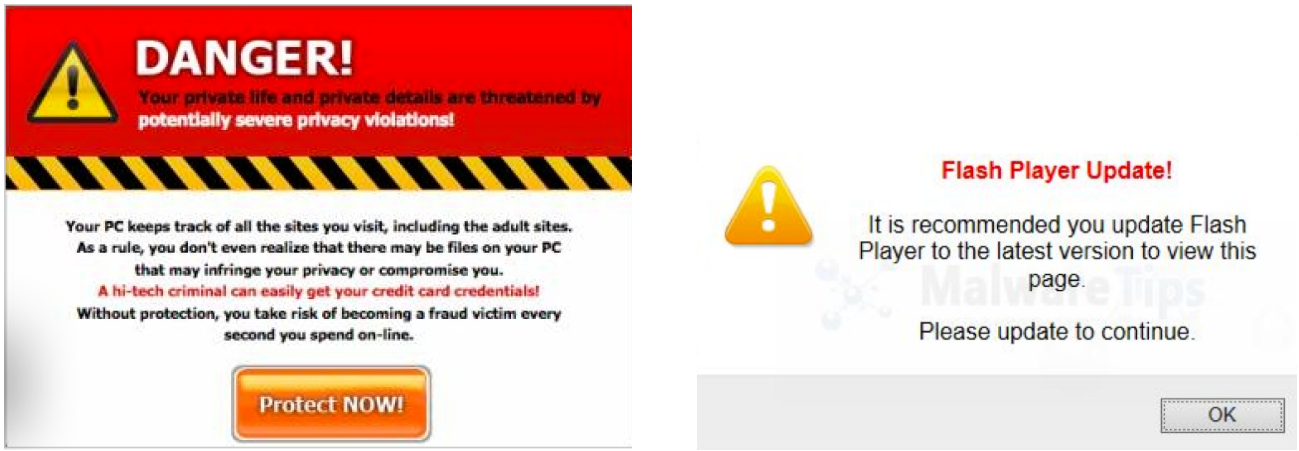
Driven by-download : exploite souvent des vulnérabilités dans un navigateur ou un add-in (Flash Player, Adobe Reader, Java ou Microsoft Silverligh) pour exécuter un code

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:// 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 utilisateur à installer leur code malveillant

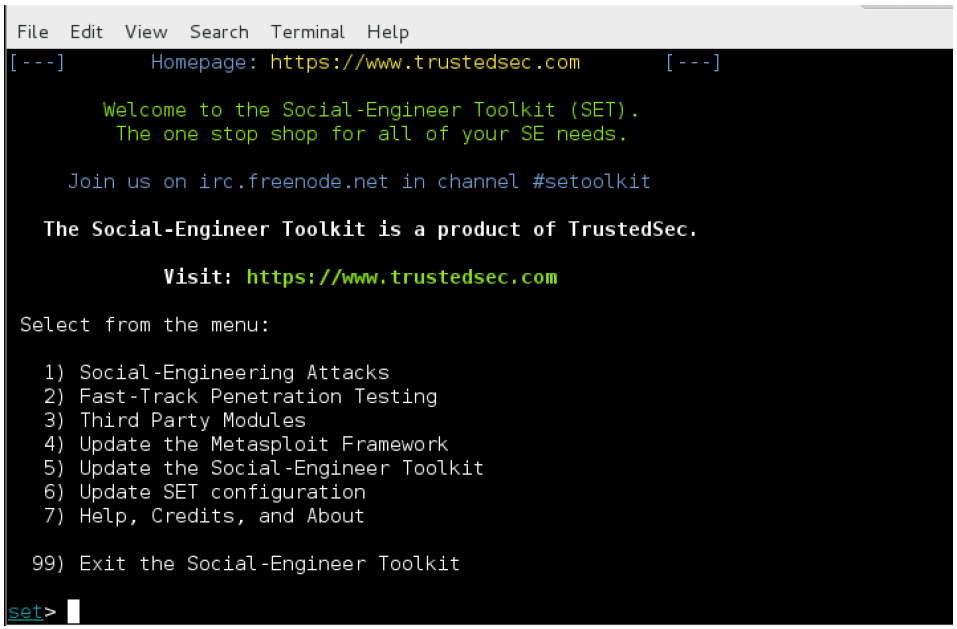


(source : www.spywarevoid.com)

Botnet : techniques d'infection

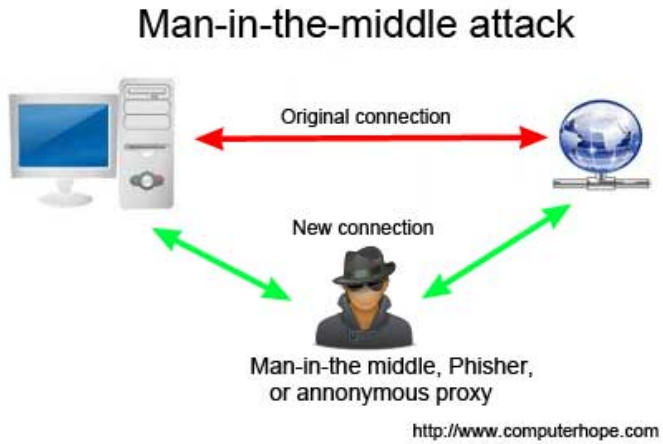
Sites web malicieux http:// (Utilisation de l'outil SET)

- 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



Botnet : techniques d'infection

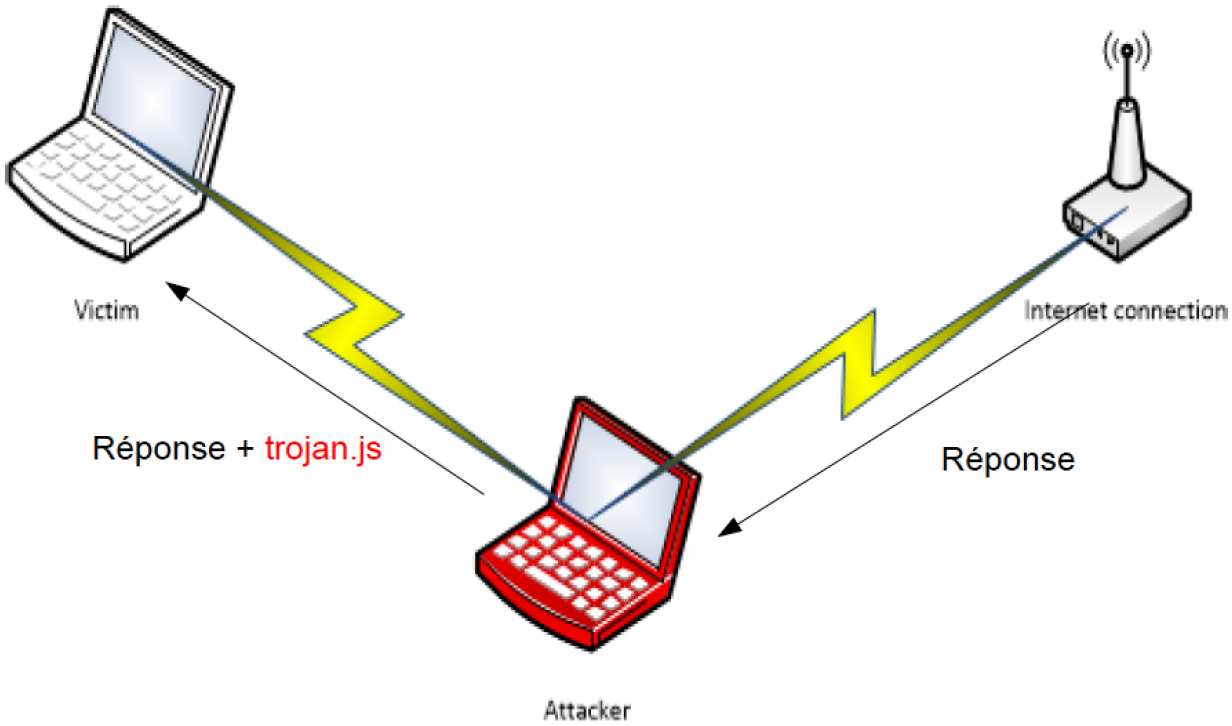
Man In The Middle



- 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 grand 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.

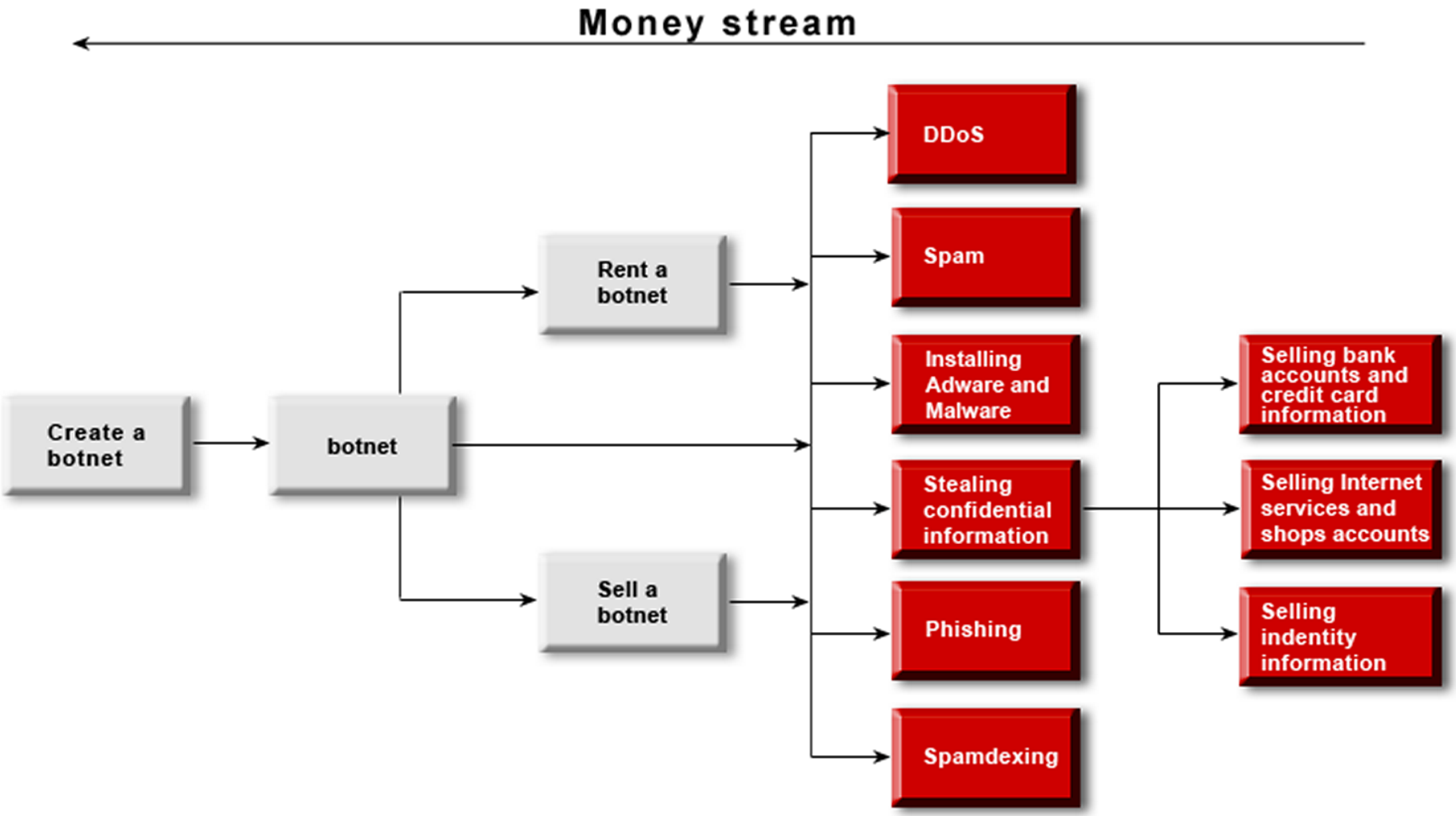
- (TS//SI//REL TO USA, FVEY) Influence policies, standards and specification for commercial public key technologies.

- 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]

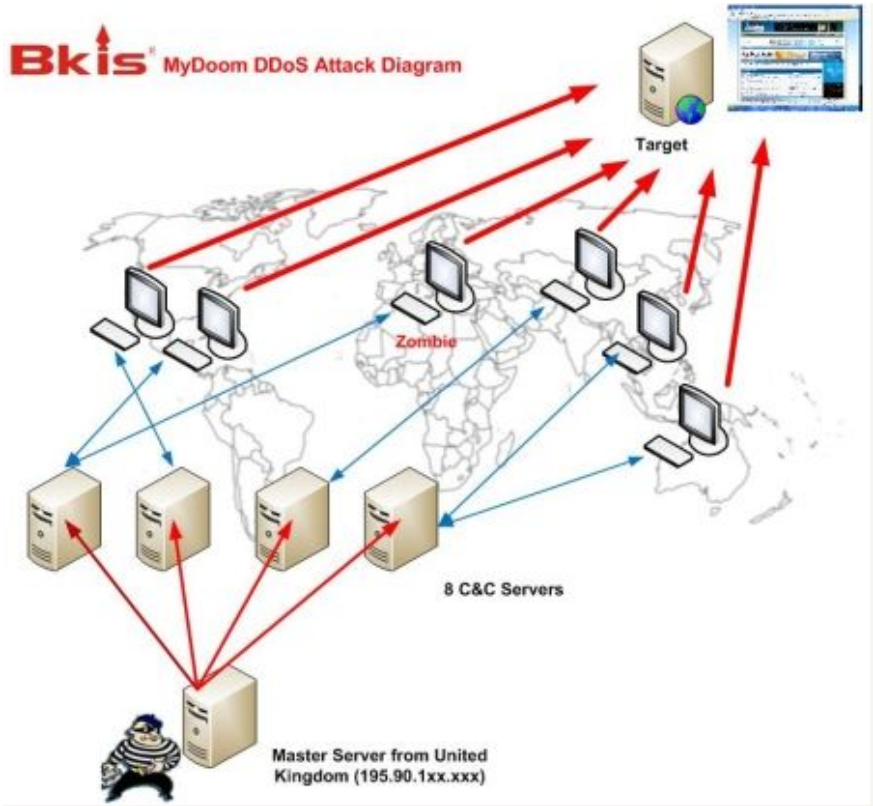
Botnet et Business : l'économie souterraine

Botnet et Business : l'économie souterraine



source :http ://bizsecurity.about.com

Attaques DDOS



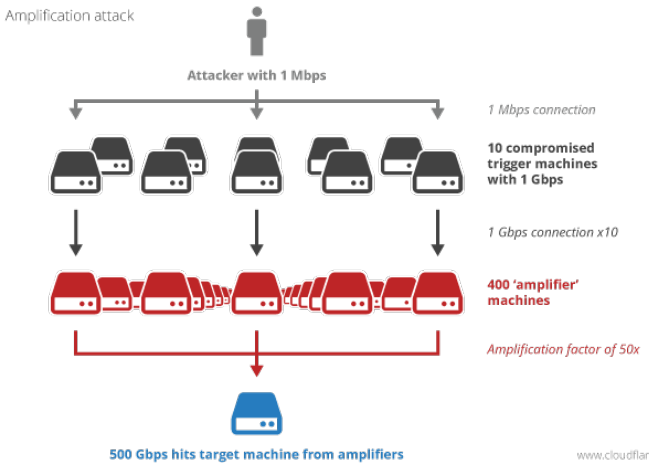
source : http ://www.sott.net/article/

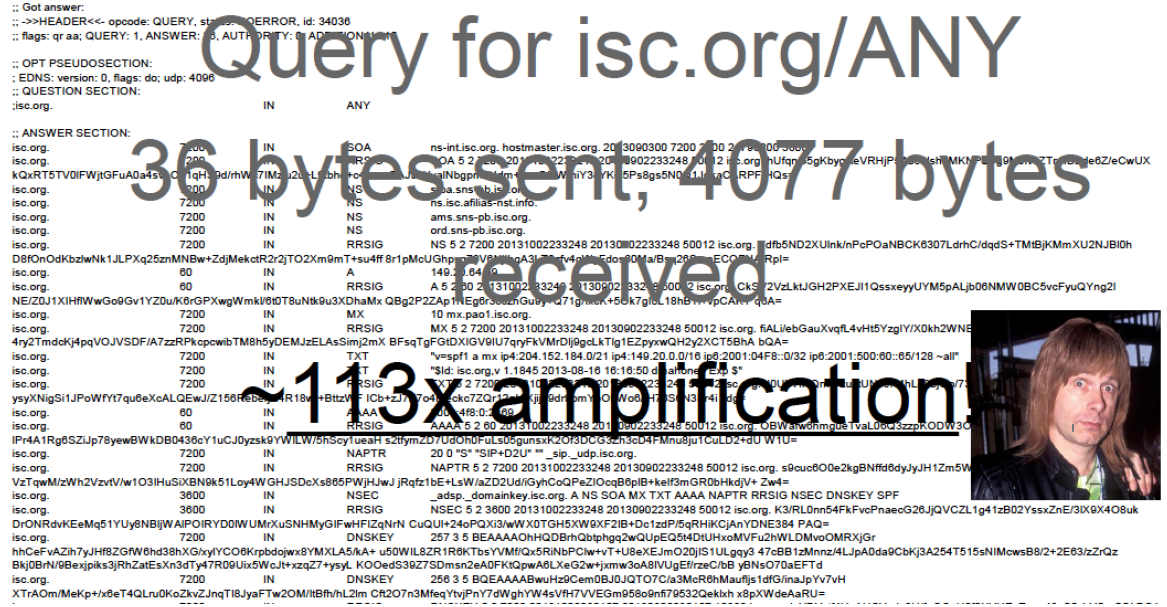
- Louer un botnet pour une attaque DDoS : $30-$70 par jour, $1,200 par mois

  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

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





Query for isc.org/ANY

36 bytes sent, 4077 bytes received

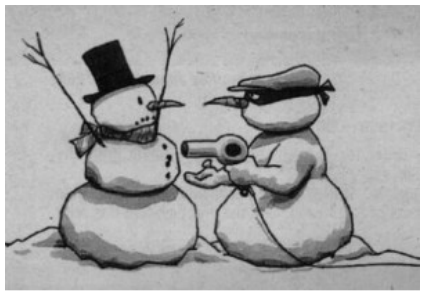
~113x amplification!

Un peu de mathématique...

- Chaque bot a une connexion de 1Mbs =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 $113x28000 \approx 913Mbs$
- 11 bots génèrent 1 Gbs.

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 : insuremekevin.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/

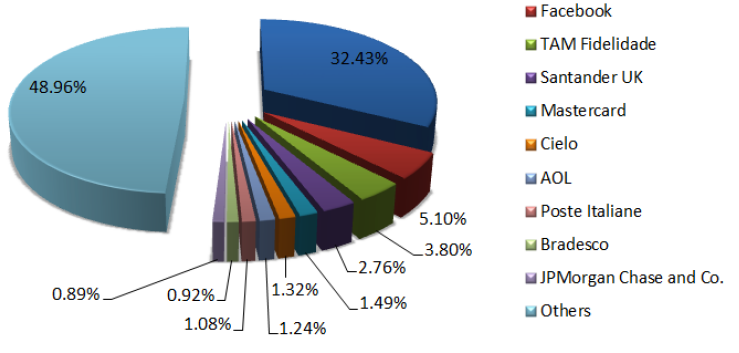
- En février 2007, de nombreux serveurs DNS racines ont été touchés par une attaque DDoS. Il s'agit d'une **preuve de puissance**.
- En 2007, attaque russe contre l'Estonie : le pays est complètement paralysé (La majorité des sites gouvernementaux, les serveurs de banques, les sites de journaux sont 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)



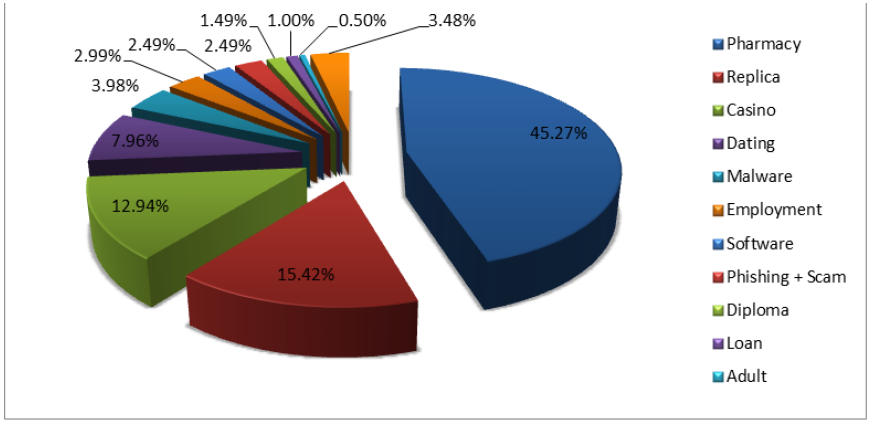
source : www.generation-nt.com

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.

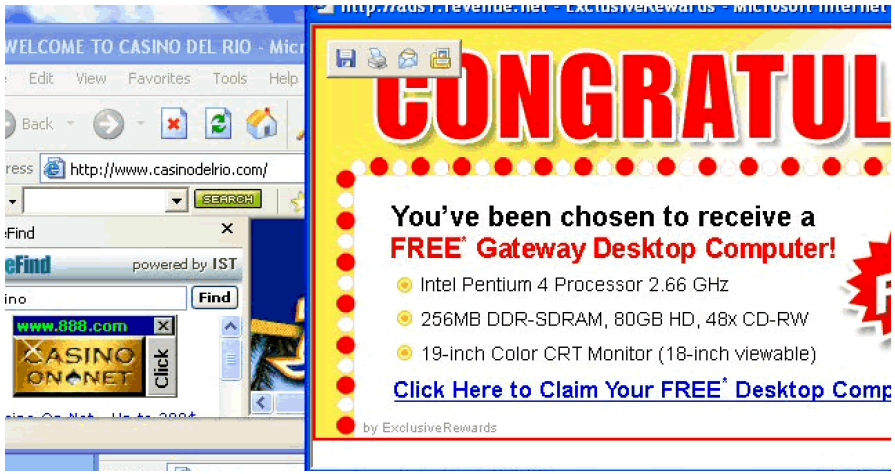
source : http://bizsecurity.about.com

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

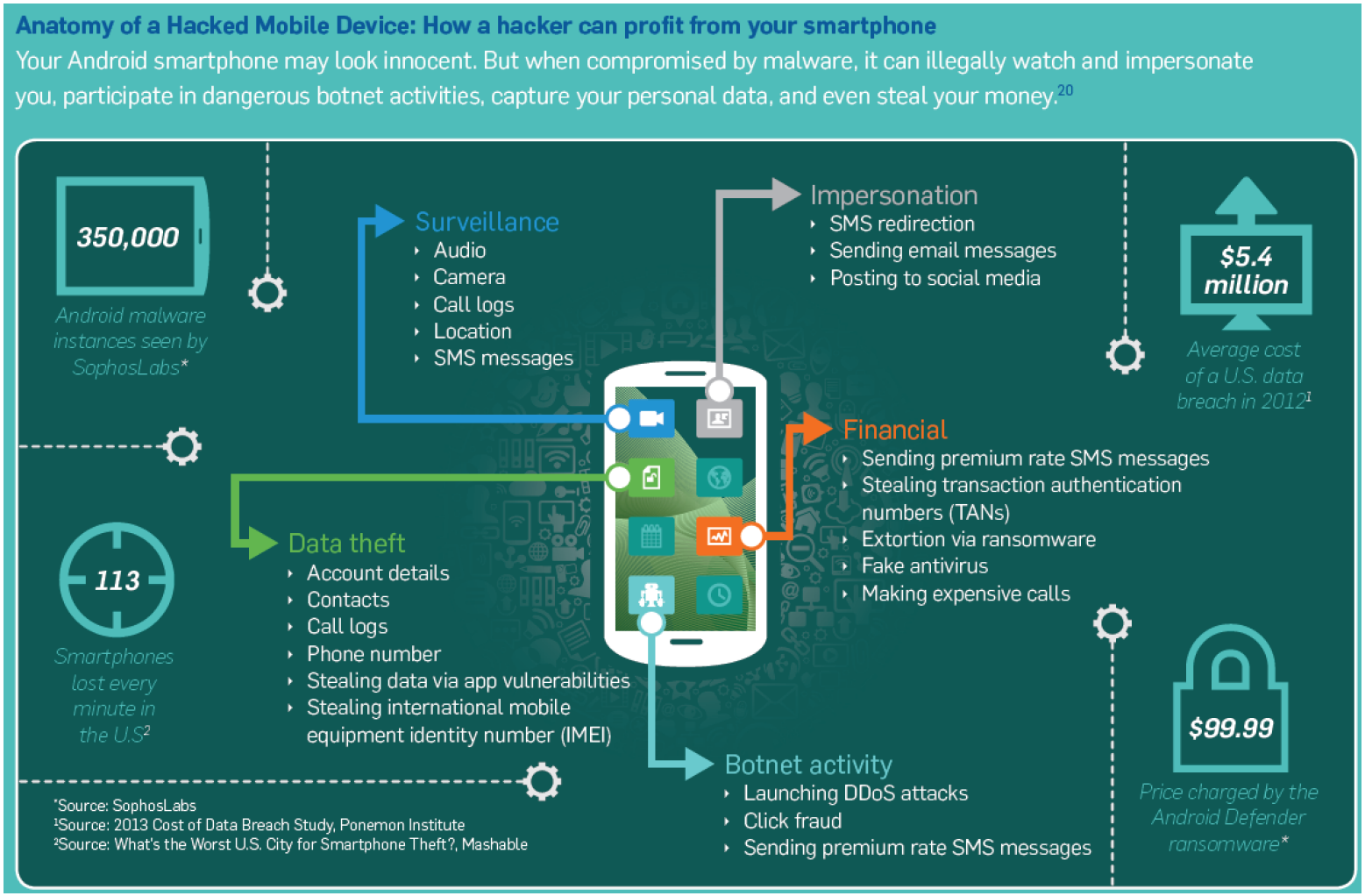


- Un adware est un programme qui affiche automatiquement les fenêtres de publicités sans notre intervention.
- Beaucoup d'entreprises qui offrent des services de publicité en ligne payent pour ce type de service.
- Le prix varie entre 30 cents et $ 1,50 pour chaque programme installé
- Les prix dépendent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

source : http ://bizsecurity.about.com

Installation de *adware* et de malware

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



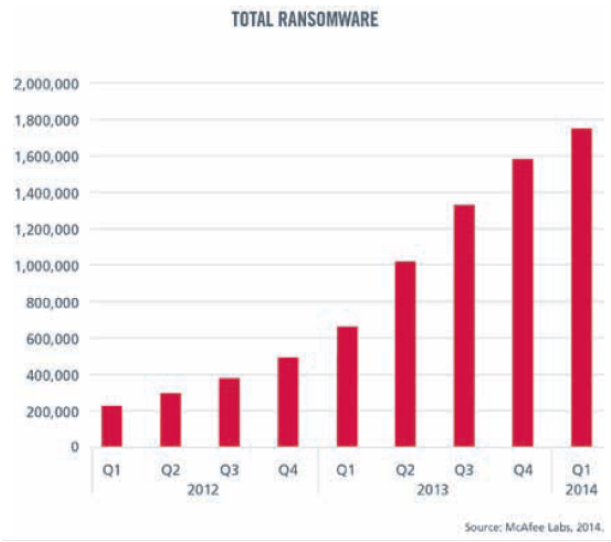
Source : Security Threat Report 2014, SOPHOS

Installation de *adware* et de malware

- **Ransomware**

Ransom Instructions from CryptoLocker

Source : Cisco 2014 Annual Security Report

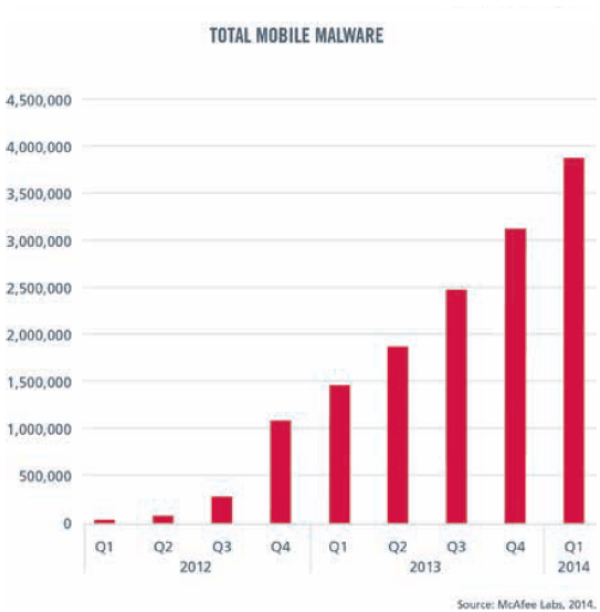


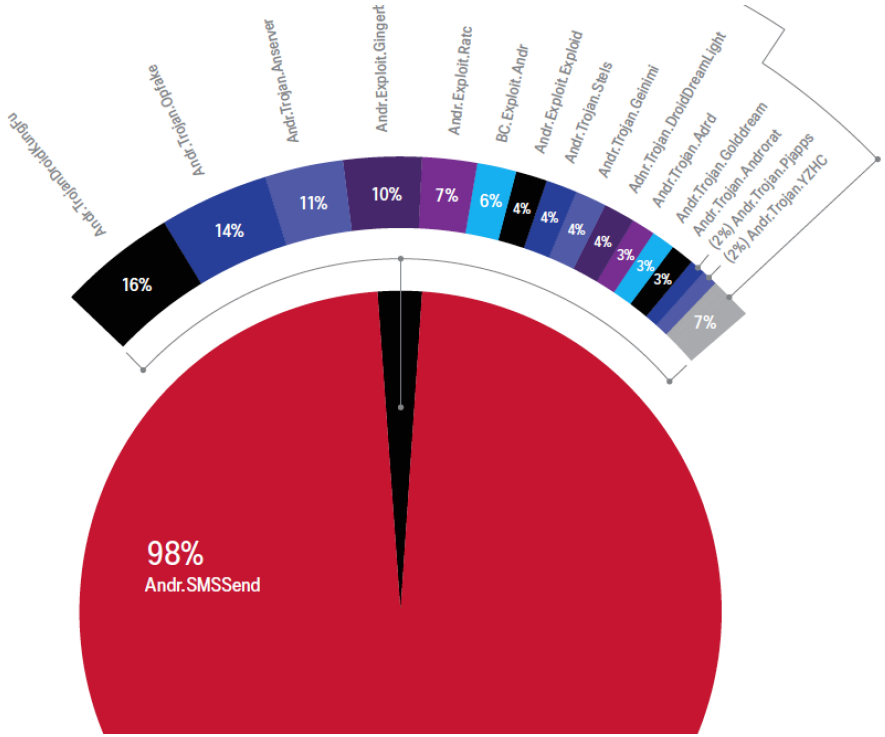
Source : McAfee Labs Threat s Report, June 201

- 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

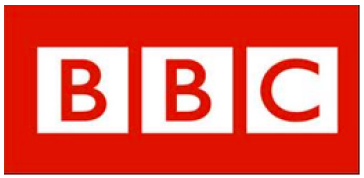
Installation de *adware* et de malware

Programme mal veillant (Malware) : $\approx$ 400 millions de malware pour le mobile. Une grande partie fait des SMS.





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

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

Surveiller l'ordinateur

- Les processus, les ports, les registres, les processus qui s'exécutent au démarrage, etc.

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
- ...

Botnet : Défense

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

- Détecter et neutraliser les serveurs C&C
  - Infiltrer un botnet via un *honeypot* pour l'analyser et localiser ses serveurs C&C
  - Détecter 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 ...

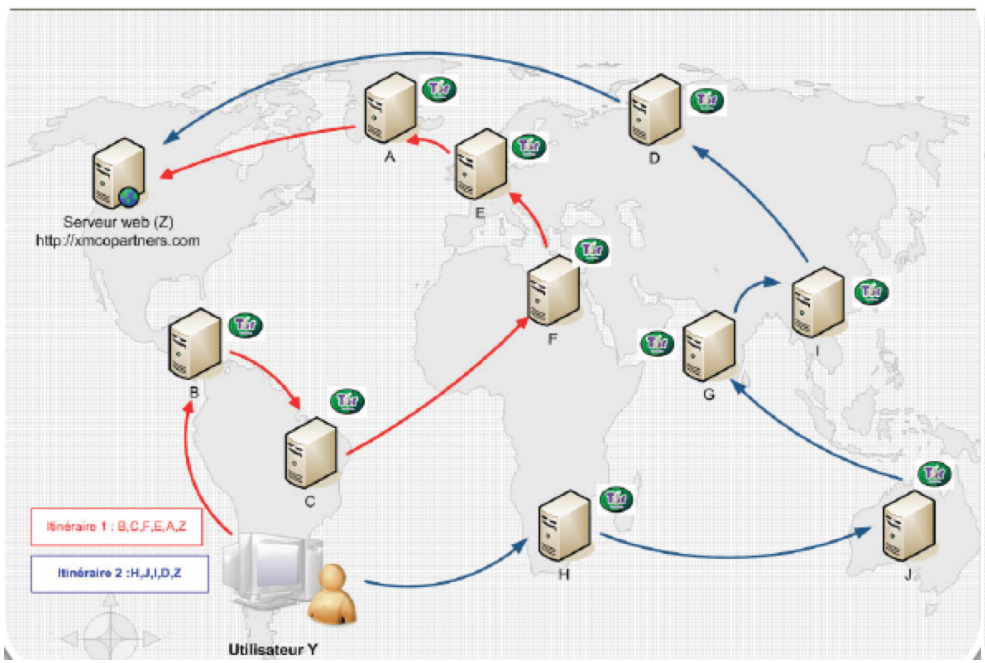
Outils de défense de pirate

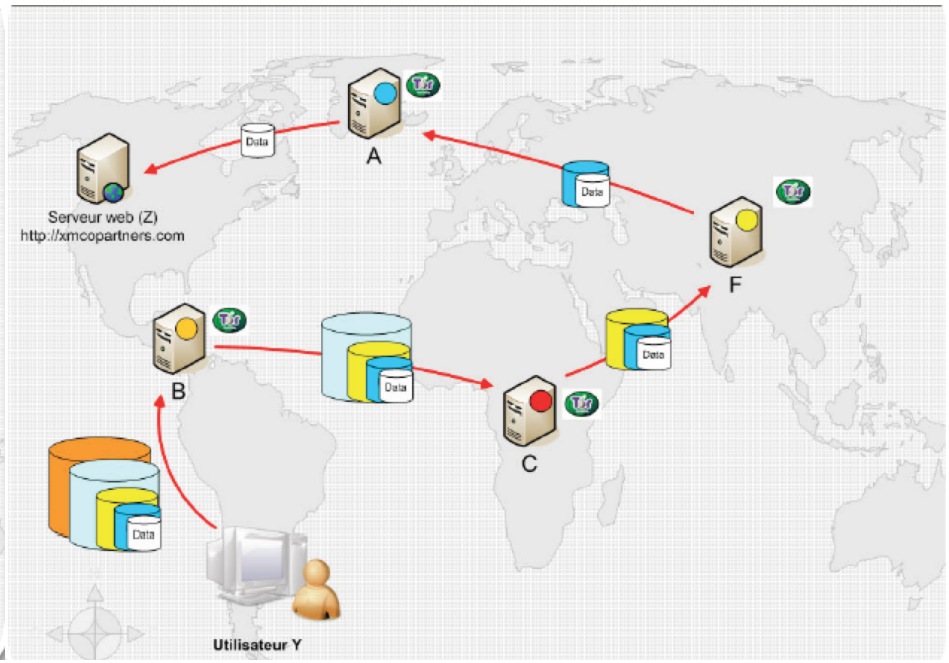
- Code difficile à comprendre ou lui trouver une signature : obfuscation du code, code polymorphes, etc.
- Anonymat : TOR, proxy, etc.
- Cible en constante mouvement : "Fast Flux" (simple et double) :
- Non-décidabilité de la détection virale (Travaux de Fred Cohen (1984 - 1988))

Catch me if you can ...

: (The Onion Router)

$$
\begin{array}{lcll}
Y & \longrightarrow & B: & [To\ C, [To\ F, [To\ A, [To\ Z,\ M]_{Pk(A)}]_{Pk(F)}]_{Pk(C)}]_{Pk(B)} \\
B & \longrightarrow & C: & [To\ F, [To\ A, [To\ Z,\ M\}_{Pk(A)}]_{Pk(F)}]_{Pk(C)} \\
C & \longrightarrow & F: & [To\ A, [To\ Z,\ M]_{Pk(A)}]_{Pk(F)} \\
F & \longrightarrow & A: & [To\ Z,\ M]_{Pk(A)} \\
A & \longrightarrow & Z: & M
\end{array}
$$





source : http ://www.xmco.fr

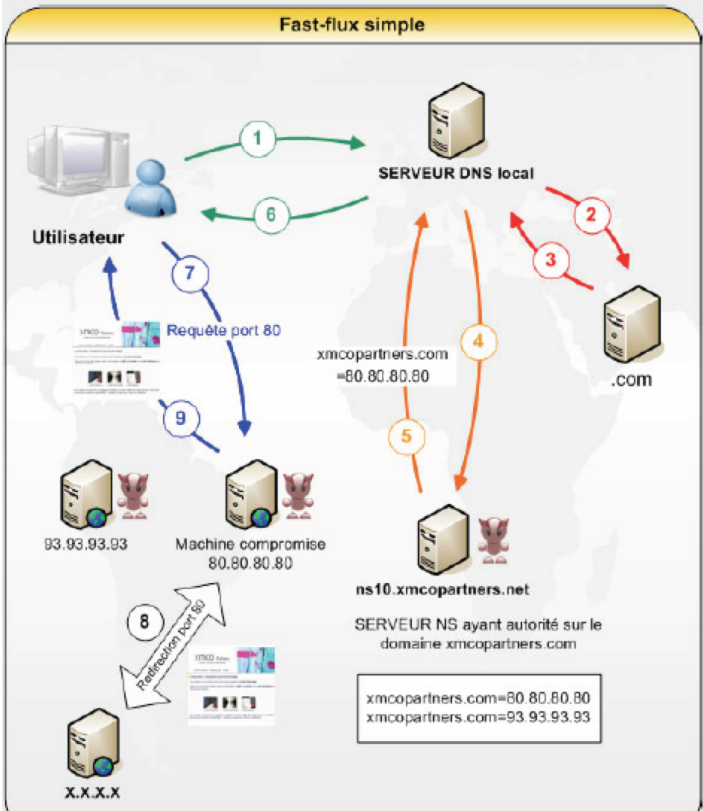
Catch me if you can ...

Fast Flux (Flux=changer)

- IP Fluxing : changement rapide d'@ IP associées aux domaines (TTL petit)
- Domain Fluxing : changement rapide de noms domaines
- Domain Name Generation Algorithm (DNGA)

Protéger les serveurs C&C

- Idée : les robots générer 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 bootmasters opèrent toujours

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 poxy (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 ...

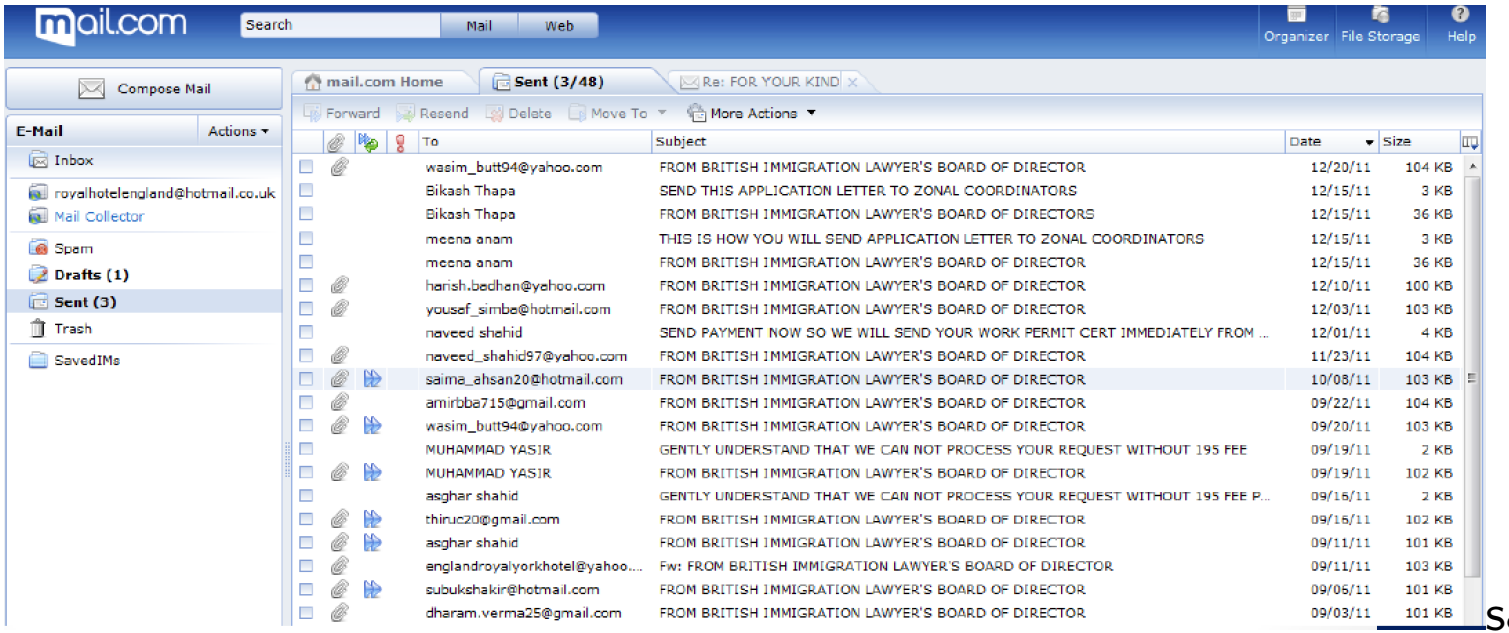
Un javascript botnet qui rattrape les "méchants"...hacking the hackers !

- Expérience : Chema Alonso & Manu " The Sur" en 2012
  1. 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 !

- Expérience : Chema Alonso & Manu " The Sur" en 2012
  1. Victimes : Fraudeurs Nigérians. Promesse de visa de travail à UK



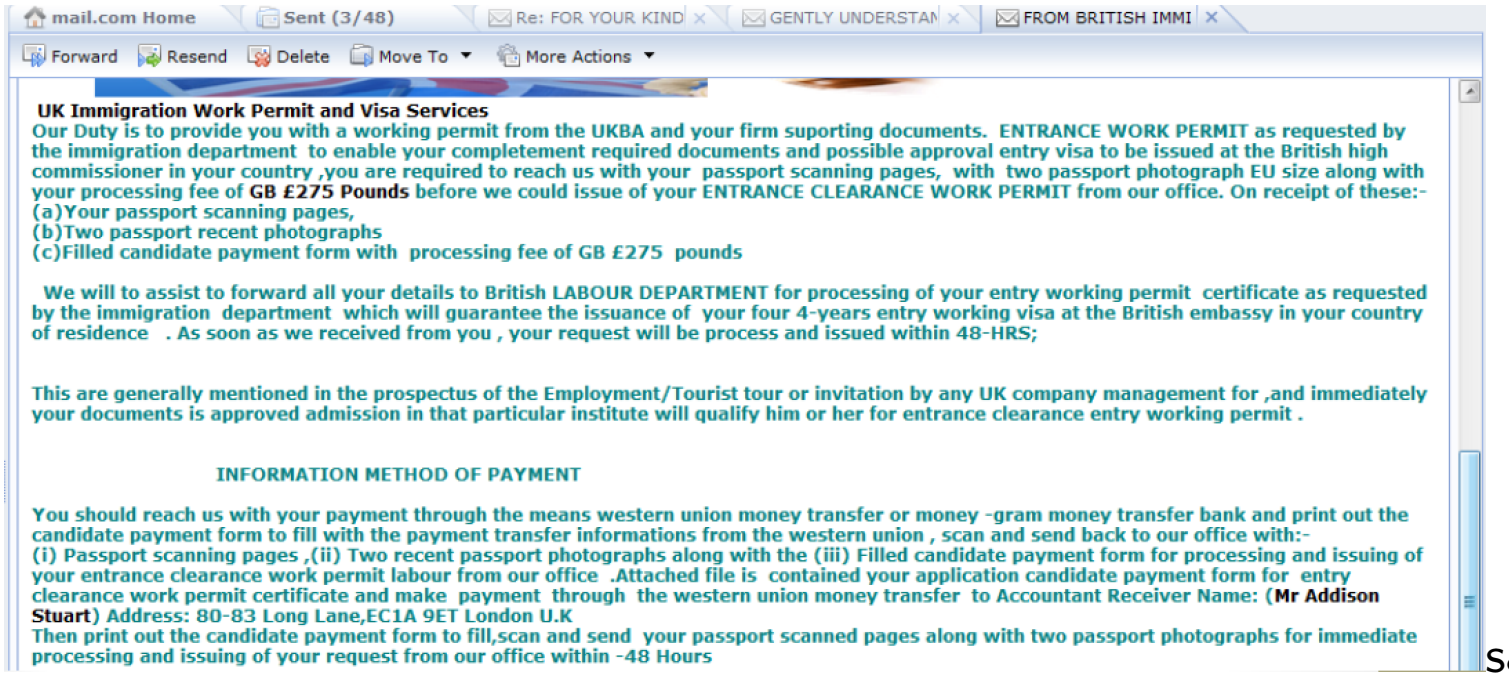
Source :

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
  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 !

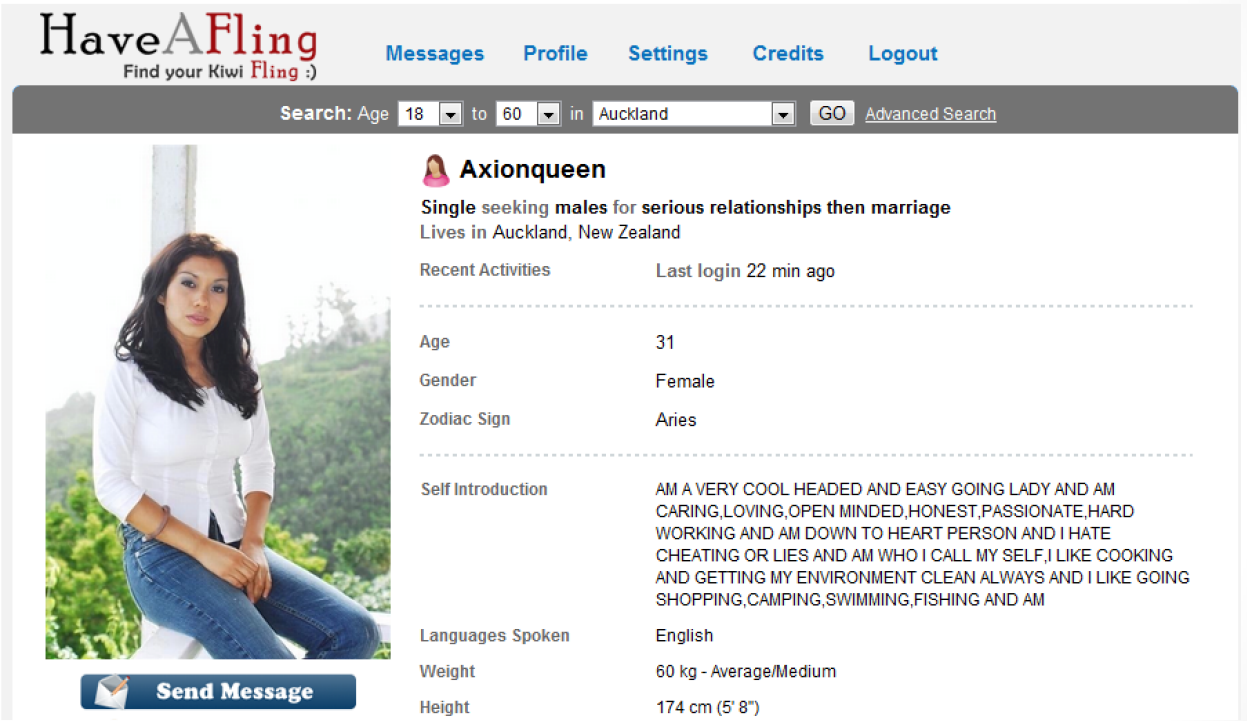
- Expérience : Chema Alonso & Manu " The Sur" en 2012
  1. Victimes : Fraudeurs Nigérians. Promesse de visa de travail à UK

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

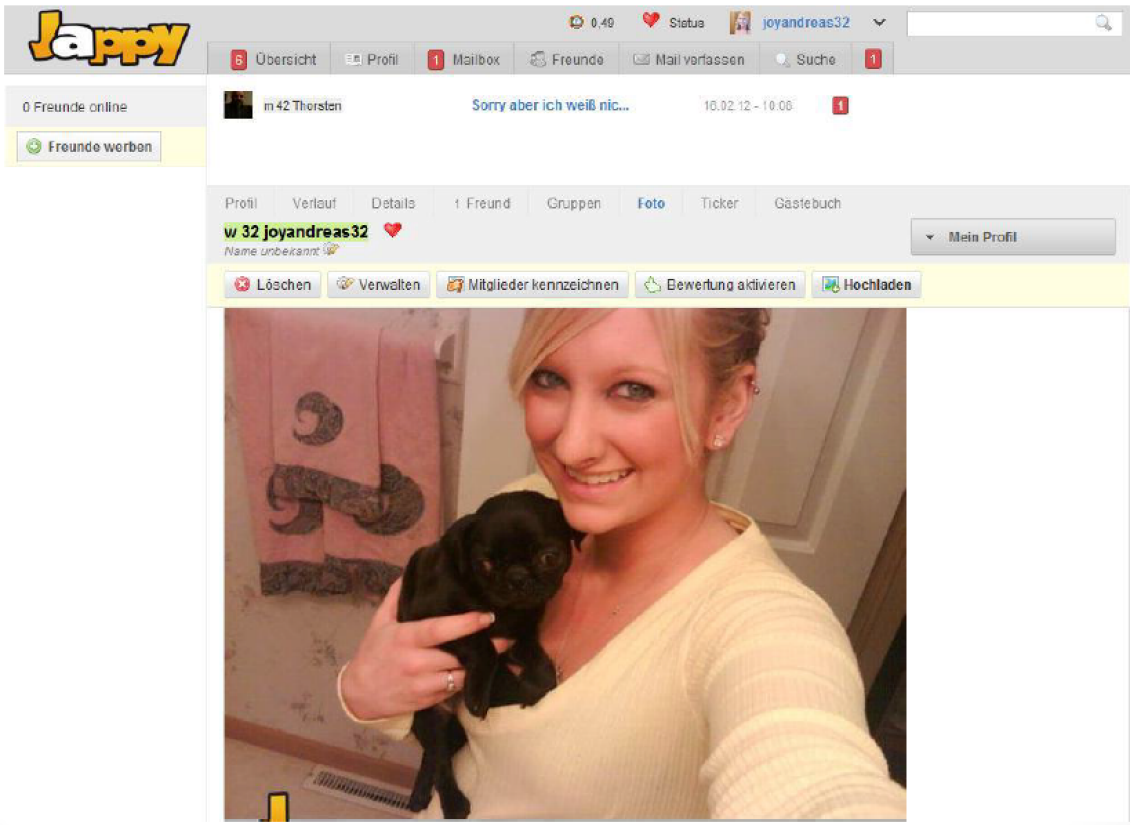


Source : Owning Bad Guys & Mafia with JavaScript Botnets

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.

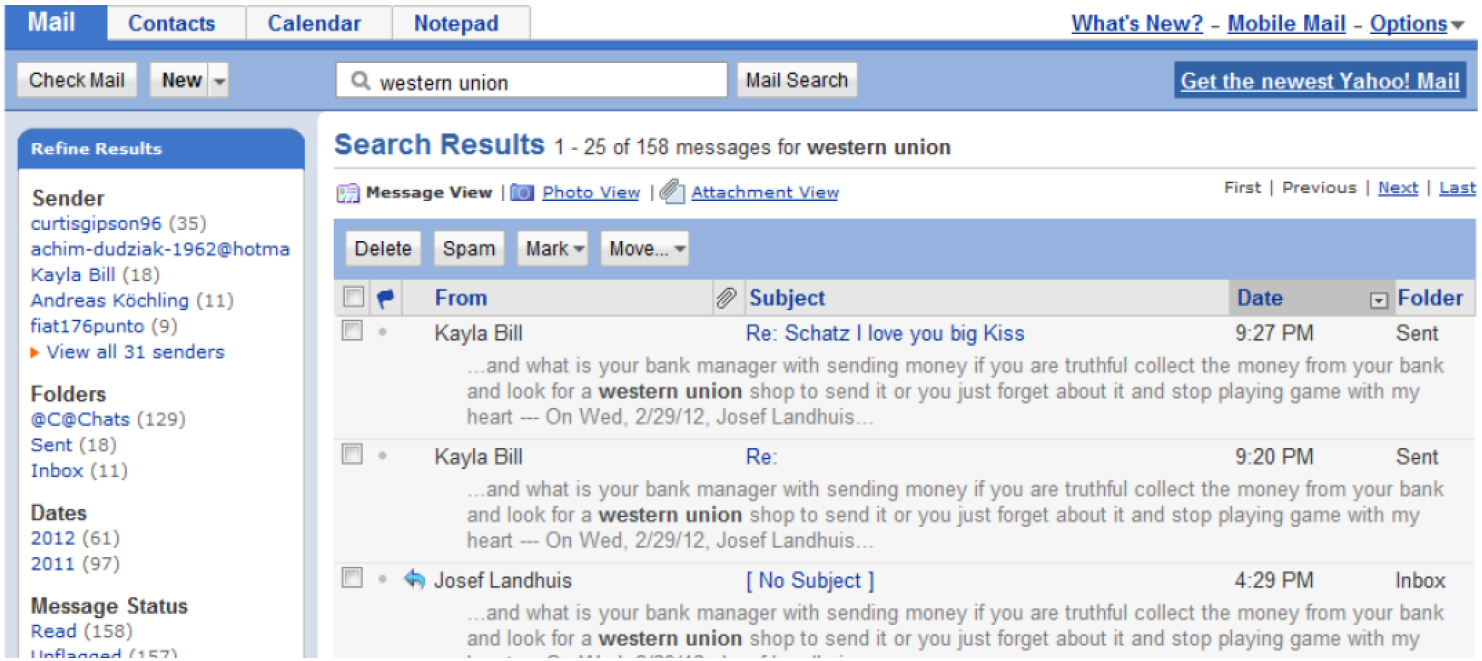


Source : Owning Bad Guys & Mafia with JavaScript Botnets

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

Conclusion

- Botnet : menace grandissante
- Tout le monde est concerné : individus, entreprises, infrastructures, etc.
- Impact : vie privée, argent, identité, secret technologique, etc.
- Technique d'infection : USB, courriel, site web, réseaux sociaux, WiFi, etc.
- Facilité d'attaque et difficulté de défense
- Appliquer les règles d'hygiène de la sécurité informatique

Références

- Security Threat Report 2014, SOPHOS
- McAfee Labs Threats Report, June 2014
- Cisco 2014 Annual Security Report
- OWASP : Open Web Application Security Project
- SANS : (SysAdmin, Audit, Network, Security)
- The Hacker News (facebook)
- Chema Alonso) and Manu "The Sur" : Owning Bad Guys & Mafia with JavaScript Botnets