Réflexions pour un plan d'action contre les botnets

SSTIC

Rennes, 09-11 juin 2010

Lieutenant-colonel Éric FREYSSINET, DGGN/SDPJ

Plan

- Constat
  - La menace
  - Les actions menées
- Plan d'action ?
  - Prévention
  - Détection
  - Réaction
- Faire évoluer la législation

Nota: les extraits d'articles de presse en ligne sont © leurs auteurs.

Licence pro NTECH
Master SSI

Partenaires:
- PN: OCLCTIC, BEFTI, DCRI
- Douanes: SNDJ, DNRED
- CNIL, HADOPI, ARJEL,...

AFSIN: enquêteurs, experts, magistrats (www.afsin.org)

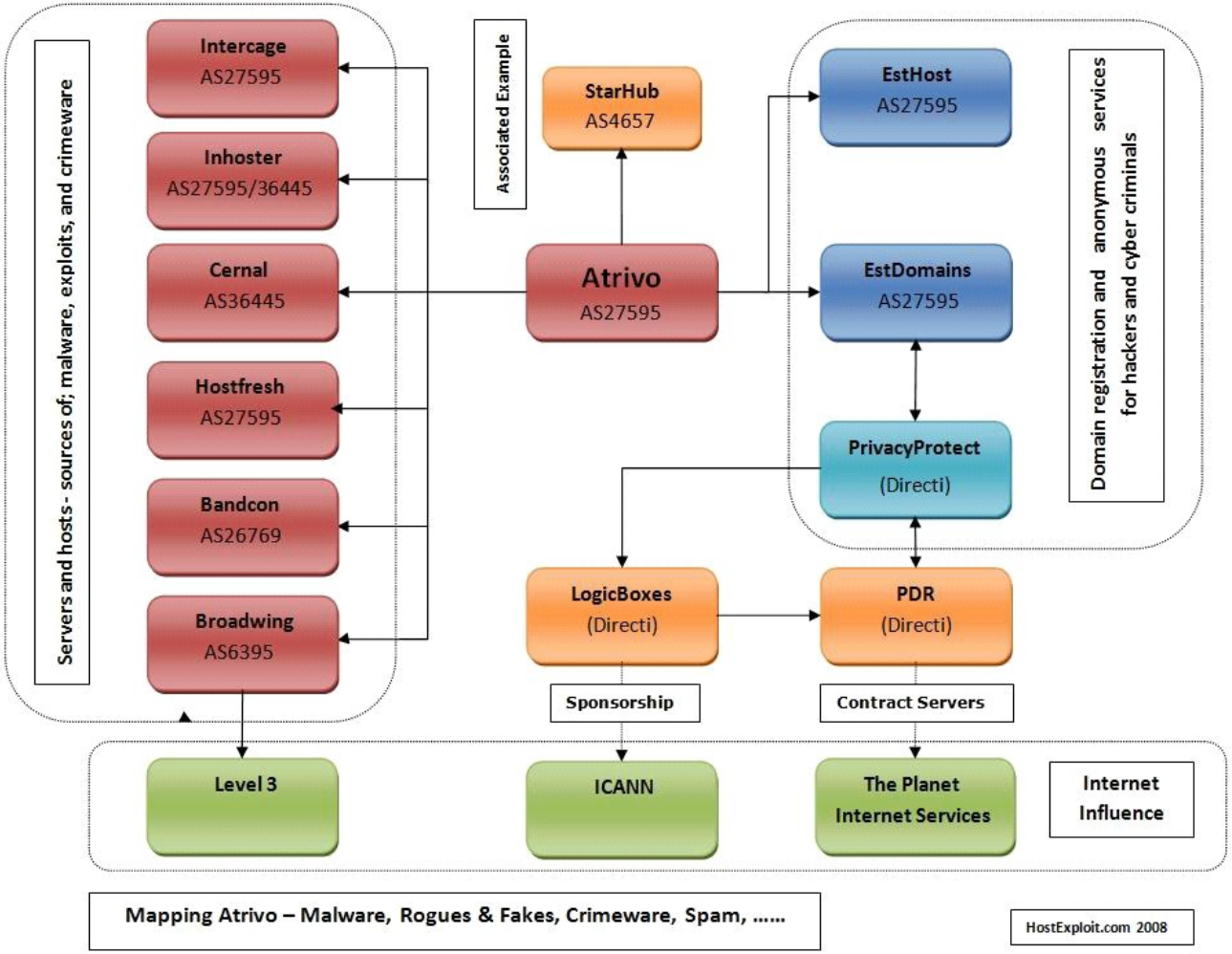
Europe:
- Services spécialisés
- Europol, Interpol, Eurojust
- ENFSI, ECTEG

Académique
- 2CENTRE (UTT, UCD, UM...)
- Projets ANR,...

La menace

- Botnets:
  - 85 à 90 % du spam selon les sources
    - Y compris le spam « commercial », cf. Soloway
  - Campagnes de phishing
  - Distribution de logiciels malveillants
  - Collecte de données personnelles
  - Attaques en déni de service, évidemment
  - Et on peut tout imaginer

Atrivo



Connu depuis de nombreuses années comme hébergeant des activités malhonnêtes en grand nombre

Liens avec de nombreuses autres entités qui assurent la résilience du système.

« Fermé » sous la pression en septembre 2008, mais...

(Jart Armin - http://hostexploit.com/downloads/view.download/4/12.html)

McColo

http://blog.fireeye.com/research/2008/10/mccolo-hosting-srizbi-cc.html

FireEye Malware Intelligence Lab

Threat research, analysis, and mitigation | www.fireeye.com

« McColo hosting W32/Dedler C&C | Main | McColo (still) hosting Rustock C&C »

2008.10.28

McColo hosting Srizbi C&C

We've written about McColo hosting the Srizbi Cc
wrinkle that I haven't seen before.

After my machine got infected, it went through t
send SPAM?" test that Bots do - ie, the outbound
the test domain is also hosted by McColo!

EHLO pur3.pwnag3.com
MAIL From:<a_fake_address@pickedbysrizbi.com
RCPT To:<[blocked]@bestyounggirls.com>
DATA

Above you see Srizbi sending a blank message to
208.72.168.85. A quick 'dig' of bestyounggirls.cc
explaination is that Srizbi wanted to see if the Bl
to a domain that was controlled by the group whc
there's no need for it to try and possibly be detec

After it does the SPAM test, you can see the nori
headers to take away identifyable information)

POST /r/A1412B-12F1E6-A55215 HTTP/1.1
Host: 208.72.169.212

SECURITY FIX

Brian Krebs on Computer Security

About This Blog | Archives | XML RSS Feed (What's RSS?)

Major Source of Online Scams and Spams Knocked Offline

A U.S. based Web hosting firm that security experts say was responsible for facilitating more than 75 percent of the junk e-mail blasted out each day globally has been knocked offline following reports from **Security Fix** on evidence gathered about suspicious activity emanating from the network.

For the past four months, Security Fix has been gathering data from the security industry about **McColo Corp.**, a San Jose, Calif., based Web hosting service whose client list experts say includes some of the most disreputable cyber-criminal gangs in business today.

On Monday, Security Fix contacted the Internet providers that manage more than 90 percent of the company's connection to the larger Internet, sending them information about badness at McColo as documented by the security industry.

http://voices.washingtonpost.com/securityfix/2008/11/major_source_of_online_scams_a.html

Waledac

// Microsoft fait fermer le botnet de spam Waledac

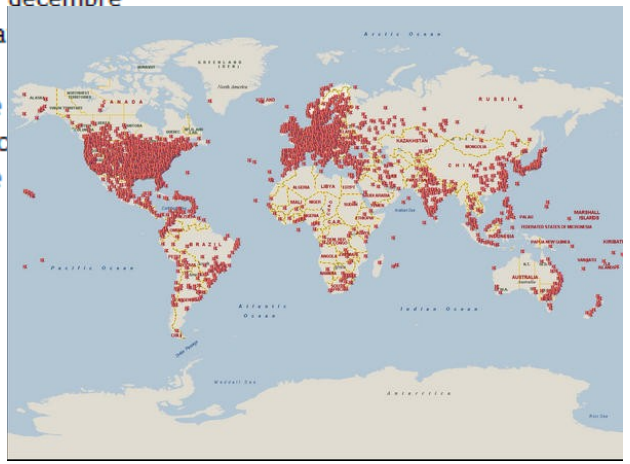
Publiée par Guillaume Belfiore le Jeudi 25 Fevrier 2010

Sur le blog officiel de Microsoft le conseiller *Tim* Cranton explique que la société de Redmond a réussi à mettre fin aux activités du botnet Waledac. Ce réseau d'ordinateurs infectés était utilisé par des hackers pour envoyer du spam. Ces actions ont pu être mises en oeuvre grâce à plusieurs dépôts de plainte et mais aussi aux efforts techniques des partenaires de la firme au sein du groupe Botnet Task Force. Cette équipe de choc est notamment constituée de Shadowserver, l'Université de Washington et *Symantec*.

M. Cranton ajoute que la fermeture de Waledac est le fruit de plusieurs mois d'investigation sur un projet baptisé en interne *Operation b49*. « *C'est l'un des 10 plus gros botnets aux Etats-Unis et l'un des distributeurs majeurs de spam* », affirme le conseiller. Il ajoute : « *On estime que Waledac a infecté plusieurs centaines de milliers de machines autour du monde (...) et envoyé 1,5 million de spams par jour* ». D'après une récente étude menée par Microsoft, entre les 3 et 21 décembre 2009, ce sont 651 millions de courriers indésirables qui auraient été envoyés sur la messagerie Hotma

Trois jours après l'injonction judiciaire du 22 février dernier, la plupart des systèmes de commande ont été désactivées même si « *l'opération n'a pas nettoyé les ordinateurs infectés* ». Microsoft rec donc de suivre les conseils de son *site* dédié à la sécurité sur Internet et de télécharger son *outil* de de malware.

http://www.clubic.com/actualite-327092-microsoft-fermer-botnet-waledac.html



Business as usual...

http://news.cnet.com/8301-1009_3-10462103-83.html

cnet news

Latest News | CNET River (BETA) | Webware | Crave | Business Tech | Green Te

Home > News > Security

Security

March 2, 2010 6:46 AM PST

Botnets cause surge in February spam

by Lance Whitney

Font size | Print

68 retweet | Share 12

Spam now accounts for close to 90 percent of all e-mail worldwide due to a s
Symantec.

Two botnets named Grum and Rustock helped push spam levels up 5.5 perc
according to the security firm's report (PDF). After doing business as usual o
sprar
to bla

Rusto
for th
Syma
of all

http://www.allspammedup.com/2010/03/rustock-botnet-spam-surges/

AllSpammedUp

anti spam in a business environment

search

Home | Links | Anti-spam

More on anti-spam

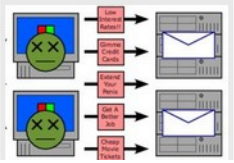
Rustock Botnet Spam Surges

by Sue Walsh on March 31, 2010

A new surge in spam being pumped out by the Rustock botnet has been detected,

and it's got a new twist – it's encrypted. The spam is
Transport Layer Security, which is a successor to Secure
ts Layer and usually used for emails. Up to 77% of
ck's resources are devoted to this new encrypted spam.

set up a node in our Labs with TLS and confirmed that
ne Rustock botnets were indeed using TLS," said Phil



Google: Botnet Takedowns Not Reducing Spam Levels

By: Geoff Duncan • April 15, 2010

6 retweet | Share

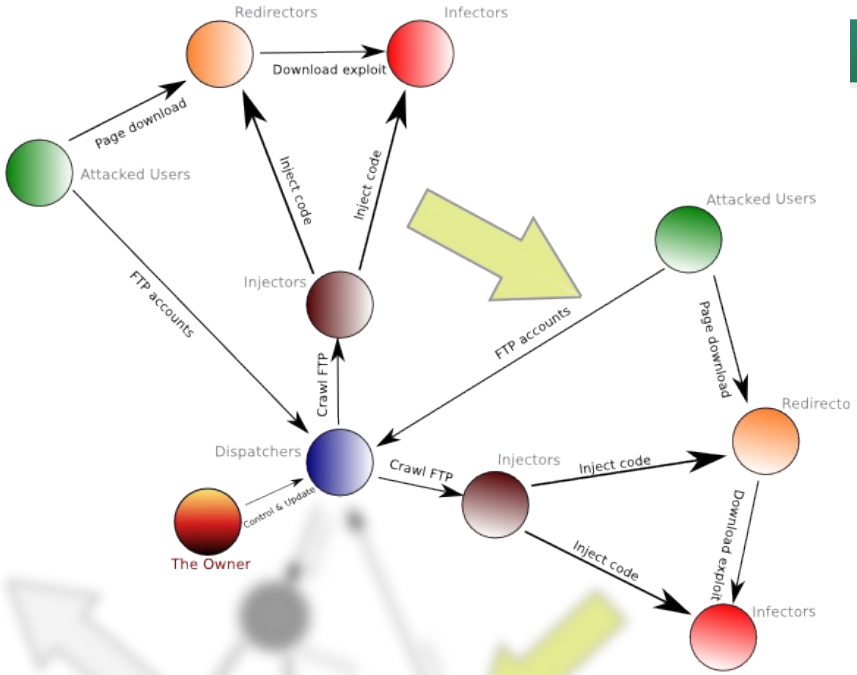
Recent high-profile takedowns of botnets are wins for security pros, but Google says spam levels are holding pretty steady anyway.

The battle against spam seems like it will never end, and in recent months security professionals and government agencies have shifted their efforts from taking down spam-friendly ISPs like McColo and 3FN to actions against specific botnet networks like ZeuS and Waledac. While these actions at least keep the bad guys on their toes and chalk up some victories for Internet users everywhere, Google says they don't really seem to be having much of an impact on overall levels of spam. In a post to its enterprise blog, Google says that while the volume of spam it measures dropped 12 percent from the fourth quarter of 2009 to the first quarter of 2010, the first quarter of 2010

http://www.digitaltrends.com/computing/google-botnet-takedowns-not-reducing-spam-levels/

De plus en plus complexes

- Gumblar



SECURELIST

Internet threat level: 1

Threats | Analysis | Blog | Descript

Home → Blog → Research → November 11 2009 → The Gumblar system

The Gumblar system

0

VitalyK
Kaspersky Lab Expert
Posted November 11, 10:20 GMT
Tags: Botnets, Gumblar

We've been looking at the infrastructure of the Gumblar malware and found some curious facts on how Gumblar operates which we would like to share to make hosting owners aware of the Gumblar threat.

Analysis of some infected websites showed that the only way to inject the infection of Gumblar was by using FTP access, because those websites have no server-side scripting. Later this was proved by an analysis of FTP log files.

The malicious code injection in HTML pages (which is a simple insertion of <script> tag in every file having HTML) was done by downloading all files from the server that could have HTML, changing them and uploading back. We call the websites modified in this way "redirectors", because they simply redirect browsers to the website spreading malware.

http://www.securelist.com/en/blog/208187897/The_Gumblar_system

(Vitaly Kamluk, Kaspersky)

Mariposa (02/2010)

PANDALABS blog

Home | About PandaLabs

About PandaLabs

Mariposa botnet

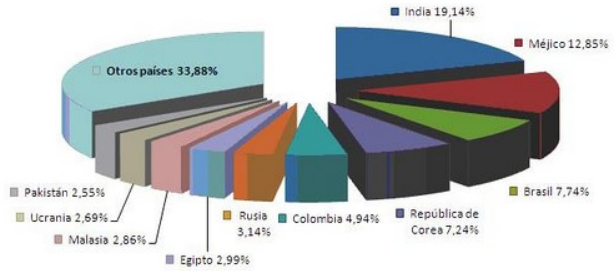
Mar 3

Posted on 03/3/10 by Luis Corrons

J'aime 18 personnes aiment ça. Soyez le premier parmi vos amis.

PANDA SECURITY

IPs comprometidas por el bot Mariposa por país



http://pandalabs.pandasecurity.com/mariposa-botnet/

In May 2009, Defence Intelligence ann
a new botnet, dubbed "Mariposa". This
by months of investigation, aimed
criminal network behind what was
largest botnets on record.

Initial steps involved the creation of
Group (MWG), comprising Defence I
Tech Information Security Center and
with other international security exper
agencies. The aim was to set up a task force to eradicate the
botnet and bring the perpetrators to justice.

Plan d'action ?

- Prévention
- Détection
- Réaction

Millefeuille des cibles potentielles

- Développeurs
  - De bots
  - De serveurs de commande
  - De charges utiles
- Revendeurs
- Pasteurs (*herders*)
- Mûles

- Commanditaire
- Hébergeurs
- Clients de services malhonnêtes
- Victimes...
- etc.

Prévention

- Sensibilisation
  - Des utilisateurs
- Mesures de sécurisation
  - Sur les réseaux des opérateurs
  - Sur les réseaux des entreprises
  - Dans les protocoles essentiels
  - Dans les OS

Détection

- Travail déjà réalisé par de nombreux groupes:
  - Lutte contre le spam (MAAWG, Signal-Spam,...) et le phishing (APWG)
  - Sociétés de sécurité (Anti-Virus, Sécurité réseaux)
  - CERTs
  - Groupes dédiés
- Quelques exemples .../...

Team Cymru

(Image brouillée, cf. http://www.team-cymru.org/ pour plus d'infos)

Report Types

Each of these reports as a different source and format. While we have attempted to keep them some what similar, that is not always possible based on the data.

Report	Alternative Report Name	Description	Source	Interval
ASN Summary Report		Top 25 ASN's summarized by number of Command and Control systems that were within that ASN, by the highest closed C&C's, and lowest closed of C&C's	Summary from all data sources	Weekly (Sunday)
Botnet URL Report		Any URL that was seen in a botnet channel is reported. The URL could be an update, complaint, or information related to the criminals. Everything is included in case there is something of value in the URL	Botnet Monitoring	24-Hours
Compromised Host Report		Specific hosts that were seen to be compromised from a botnet. These are usually seen when another infected system reports on each host that had been compromised	Botnet Monitoring	24-Hours
Click-Fraud Report		This is used as a source of fraud and possible revenue when a botnet is used to select links that are used for tracking or monetary purposes. The specific URL's are targeted are listed	Botnet Monitoring	24-Hours
Command and Control Report		A list of all the currently known active C&C's	Tracking System	7-Days
Conficker HTTP Drone Report		Any host connecting to any of the Conficker Working Group Sinkholes	Conficker Sinkholes	24-Hours
DDoS Report		Any attack is reported whether the recipient is the target or the source of the attack	Botnet Monitoring	24-Hours

FI.R.E

http://www.maliciousnetworks.org/

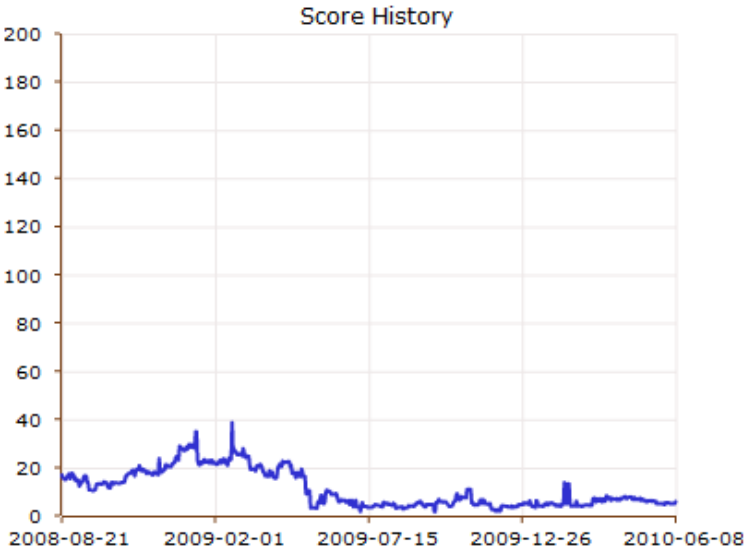
FIRE: FInding RoguE Networks

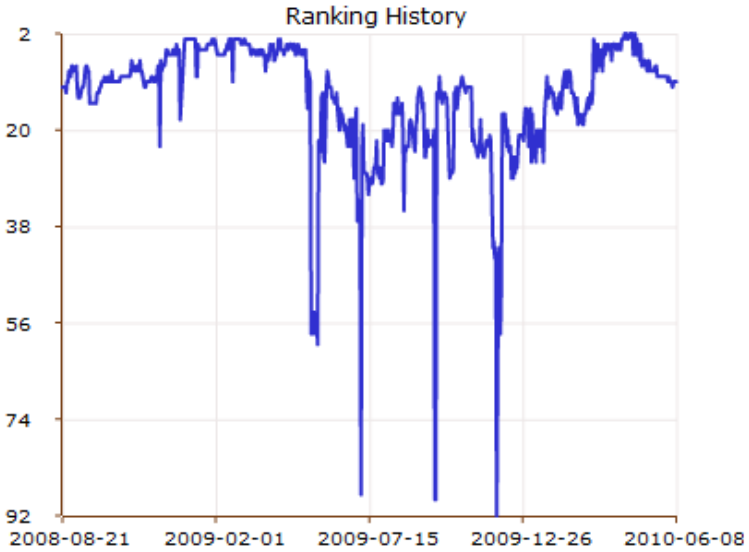
Home | ASN History | Host Info | Country Info | Global Map | About

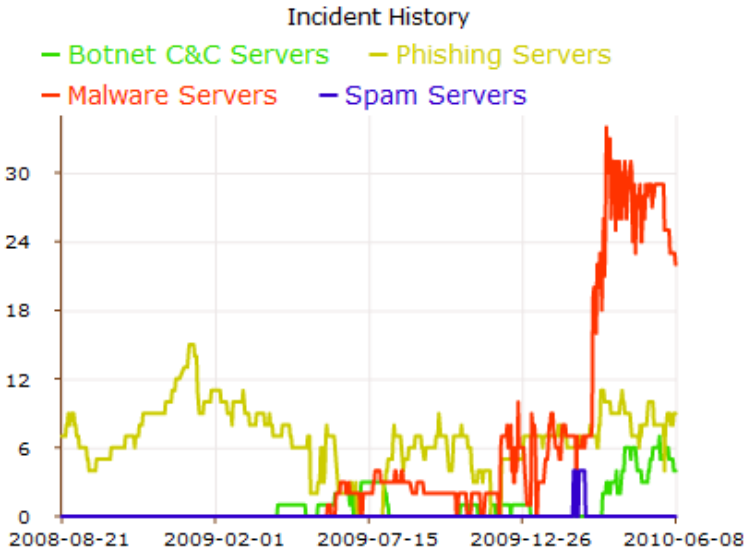
Top 20 Malicious Autonomous Systems

Rank	Rank Change	ASN						
1	✖	AS21844	THEPLANET-AS - ThePla					
2	✖	AS21740	ENOMAS1 - €					
3	✖	AS26496	PAH-INC - C					
4	⬆	AS4134	CHINANET-BACKBC					
5	⬇	AS23650	CHINANET-JS-AS-AP AS Number f					
6	⬆	AS46475	LIMESTONENETWORK					
7	⬇	AS36057	WEBAIR-AMS Webai					
8	⬇	AS21788	NOC - Network (					
9	⬆	AS24940	HETZNER-AS Hetzner Online AG RZ	DE	5.59	11	11	19
10	⬇	AS27715	LocaWeb Ltda	BR	5.27	15	0	8

History for OVH OVH







http://www.maliciousnetworks.org/chart.php?as=AS16276

Collationner

- Sources très nombreuses
- Pas de réel langage commun
  - IODEF ? (Incident object description exchange format, RFC 5070)
- Pas toujours d'objectif commun
- Identifier des cibles intéressantes
- Groupes de travail opérationnels à créer

Réaction

- Détection, analyse
- Coordination
- Opération policière et technique coordonnée
- Analyse des preuves collectées
- Partage de l'information et rémorçage

Groupe de travail Interpol

- Working party on IT Crime – Europe
  - Créé en 1990, services d'enquête spécialisés
  - 3 réunions par an
  - Europe au sens d'Interpol Portugal → Russie
    - Nous ont rejoint récemment: Suisse, Turquie, Russie
  - Groupes de projet, Manuel du cybercrime
    - Mondes virtuels
    - Live forensics

http://www.interpol.int/Public/TechnologyCrime/WorkingParties/default.asp

Interpol – Botnet project

- Mai 2010 – Mai 2011
- Objectif: identifier et démanteler de façon coordonnée un ou plusieurs botnets
- Participent au projet:
  - Des membres du groupe
  - Des invités
- Prouver que c'est possible, sensibiliser, communiquer

Évolutions législatives souhaitables ?

- Actions maîtrisées sur les réseaux
  - Bloquer la propagation des menaces
  - Prendre le contrôle de botnets et forcer le nettoyage
- Courriers électroniques non sollicités
  - Aujourd'hui
    - Collecte de données personnelles
    - Escroquerie, atteintes aux STAD (phishing)
    - Messages commerciaux non sollicités (LCEN)
  - Demain ?
    - Étendre LCEN à spam non commerciaux...
    - Diffusion de pourriels comme délit (seuil)

Gendarmerie nationale

Une force humaine

www.gendarmerie.interieur.gouv.fr

Conclusion

Eric Freyssinet, lieutenant-colonel
Direction générale de la gendarmerie nationale
Sous-direction de la police judiciaire
35 rue Saint Didier
F-75775 PARIS Cedex 16

Mél: eric.freyssinet@gendarmerie.interieur.gouv.fr
http://blog.crimenumerique.fr/

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR, DE L'OUTRE-MER ET DES COLLECTIVITÉS TERRITORIALES