CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Cybercrime Overview 2008

January 15 2009

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF : *Committed to information security*

A **Non-profit** association (created in the early 1980s)

> 600 members (50% suppliers and goods and/or service providers, 50% CISO, CIO, managers)

To share information

Exchanges among officially recognized experts, collective know-how, documentary resources

Develop its positioning

Feedback, increased visibility, Directory of Offering Members

Anticipate trends

The "network", inform offerers of expectations

Promote IS security

Join…

CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Working group dynamics

Free access to documents (English, German translations…)

Public stands taken on issues and requests for proposals

Permanent **exchange spaces**: MEHARI, threats, CISO

Active groups in 2009

- **Botnet**
- **Design of Secured IS Center**
- **Forensics**
- **MEHARI™ Documentation**
- **PC Security Sheets**
- **Problems Management**
- **Facilities Management**
- **MEHARI™ Integration**
- **CLUSIF training label**
- **Phreaking**
- **MEHARI 2007**
- **Cybercrime Overview**
- **PCI-DSS**
- **Web application security**
- **27000 serie / Metrics**

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Regional initiatives and international joint efforts

CLUSIB (Club de la sécurité informatique belge)
8, Rue des Sols
1000 Bruxelles
Contact :
Tel : + 32 2 515 08 57
Fax : + 32 2 515 09 85
Secrétariat : Jan Steenlant
Web : https://www.belcliv.be/clusib/index.html?&lang=fr.

CLUSSIL (Club de la sécurité des systèmes d'information Luxembourg)
c/o CRP Henri Tudor
29 rue John F. Kennedy
L-1855 Luxembourg - Kirchberg
Contact :
Tel : + 352 42 59 91 206
Fax : + 352 42 48 99
Secrétariat : Anne Gaspard
Web : http://www.clussil.lu/tiki-view_articles.php.

CLUSIS (Club de la sécurité informatique suisse)
Case postale 9
CH 1026 Lausanne
Contact :
Tel : + 41 21 636 32 39
Fax : + 41 21 636 32 38
Secrétariat : Nathalie Drevet-Rosenthal.
Web : http://www.clusis.ch/.

CLUSIT (Associazione Italiana per la Sicurezza Informatica)
Università degli Studi di Milano
Dipartimento di Scienze dell' Informazione
Via Comelico 39, 20135 MILANO
Contact :
Tel : + 39 349 776 8882
Fax : + 39 02 700 440 566
Secrétariat.
Web : http://www.clusit.it/.

CLUSI Burkina Faso
Adresse Postale: 01 BP 521 Ouagadougou 01 Contact :
Tel : (226) 70 27 36 86 ou (226) 70 28 48 48
M. Youn SANFO.
Web : http://www.clusibf.org/.

Club de la Sécurité des Systèmes d'Information du Languedoc-Roussillon

Club de la Sécurité des Systèmes d'Information de la Région Midi Pyrénées

Club de la Sécurité des Systèmes d'Information de la Région Est

Club de la Sécurité des Systèmes d'Information de la Région Provence-Alpes-Côte-d'Azur

Club de la Sécurité des Systèmes d'Information de la Région Rhône-Alpes

Club de la Sécurité des Systèmes d'Information de la Région Nord Pas de Calais Picardie

Club de la Sécurité de l'Information de Poitou-Charentes

Club de la Sécurité de l'Information Région Aquitaine

Objectives of the Overview

Evaluate the emergence of new risks and determine current trends in existing risks

Put into perspective events that have made headlines

Place "high-tech" crime in the same category as more traditional felonies

Contributions to the 2008 Overview

Selected by a diverse working group: insurers, scientists, journalists, law enforcement officers, goods and services providers, CISO

- AIG Europe
- Best Practices-SI
- HSC
- Kroll Ontrack
- McAfee
- Orange
- SNCF
- Websense
- National Criminal Investigation Directorate (OCLCTIC)
- National Gendarmerie
- Office of the public prosecutor of the Appeal Court of Versailles
- Québec Provincial Police

Choice of topics/ contributions do not reflect the opinions of businesses and organizations that participated in the working group

Selection of media events

Presentation of:

- emerging risk,
- a trend,
- a volume of incidents.

Specific cases:

- impact or stakes,
- case study.

CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

2007 in review

- Virtual worlds: the lure of profits
  - ☺ Woman arrested for 'killing ' virtual husband
  - ☺ Real divorce following virtual adultery
- Disturbances
  - Defamation
    - ☺ CastleCops conviction
    - ☺ F1 president in S&M video
    - ☺ Testing of carding via charity donations
  - Hacking to attract attention?
    - ☺ Deforestation in Brazil (hacking and altering of felling permits)
  - Industrial espionage
    - ☺ Executive at a French tire manufacturing firm tries to sell information to a competitor
    - ☺ Emergence of B2B cyber spying
    - ☺ Sale of trade secrets belonging to a French aircraft manufacturer
  - Social networking sites, potential for fraud/information theft
    - ☺ MySpace trial for teenager's suicide (over rejection by fake "Josh Evans" persona)
    - ☺ Confer Infra

2007 in review

- Sophistication of the attacks
  - ☺ Kraken even more effective than Storm
  - ☺ ICANN takes action on domain tasting
  - ☺ Another 6 ,000 web sites corrupted by iFrame attacks
- E-Commerce fraud
  - Internet credit card fraud
    - ☺ Multiple arrests in Romania
  - Scams *via* auction sites
- Notable events
  - "Cyber war" in Estonia
    - ☺ Lithuania, Tibet, Radio Free Europe, GSM blackout in Afghanistan, etc.
  - " Chinese " cyber attacks
    - ☺ India accuses China
  - Security stakes for SCADA infrastructures
    - ☺ CIA links blackouts to cyber attacks
    - ☺ Hacking of FEMA (Federal Emergency Management Agency) phone system
    - ☺ Traffic engineers found guilty of hacking into traffic light system in Los Angeles

Webography

http://www.independent.co.uk/life-style/gadgets-and-tech/news/woman-jailed-after-killing-virtual-husband-972457.html
http://technology.timesonline.co.uk/tol/news/tech_and_web/article5002721.ece
http://uk.reuters.com/article/lifestyleMolt/idUKTRE4AD39G20081114
http://www.networkworld.com/news/2008/061008-hacker-pleads-guilty-to-attacking.html
http://www.theregister.co.uk/2008/10/13/castlecops_attacker_sentenced/
http://www.theregister.co.uk/2008/04/18/mosley_sues_again/
http://blogs.iss.net/archive/RainforestHackers.html
http://www.lefigaro.fr/societes-francaises/2008/01/16/04010-20080116ARTFIG00338-un-espion-presume-chez-michelin.php
http://www.infoworld.com/article/08/01/15/Cyber-espionage-moves-into-B2B_1.html
http://fr.reuters.com/article/technologyNews/idFRMAN56193920080125
http://news.zdnet.co.uk/security/0,1000000189,39292445,00.htm
http://www.usatoday.com/news/nation/2008-11-14-327594069_x.htm
http://www.theregister.co.uk/2008/04/07/kraken_botnet_menace/
http://www.theregister.co.uk/2008/01/30/icann_to_stamp_out_domain_tasting/
http://www.theregister.co.uk/2008/01/23/booby_trapped_web_botnet_menace/
http://www.zataz.com/news/17130/Demantelement--reseau-international--hameconnage--phishing.html
http://www.7sur7.be/7s7/fr/1503/Multimedia/article/detail/332300/2008/06/30/La-Lituanie-se-plaint-d-avoir-subi-des-cyberattaques.dhtml
http://www.upi.com/Emerging_Threats/2008/05/02/US-Belarus_row_escalates_after_cyberattack_expulsions/UPI-24681209747593/
http://uk.reuters.com/article/latestCrisis/idUKISL8417720080315
http://www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=1670
http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=205901631
http://www.theregister.co.uk/2008/08/21/dhs_phonesystem_hacked/
http://www.theregister.co.uk/2008/11/06/traffic_control_system_sabotage/

Overview 2008

- Web 2.0 and social networking: further evidence of threats…
- Hardware security and network trust
  Spreading problem of chip hacking
  Internet routing: errors, fraud, opportunities…
- Organized crime in the digital world
- Media hype and unexploited security flaws: how real are the threats?
- From internal sabotage to attacks on infrastructure security

Speakers

Mr François Paget

Senior Virus Research Engineer – McAfee Avert Labs

Francois_Paget@avertlabs.com

M. Franck Veysset

Senior Expert – Orange Labs

franck.veysset@orange-ftgroup.com

LCL Eric Freyssinet

Cybercrime project coordinator – Direction Générale Gendarmerie Nationale

eric.freyssinet@gendarmerie.defense.gouv.fr

M. Hervé Schauer

Computer systems security consultant – HSC

Herve.schauer@hsc.fr

M. Pascal Lointier

IS Risks Advisor – AIG Europe

Pascal.lointier@aig.com

Overview 2008

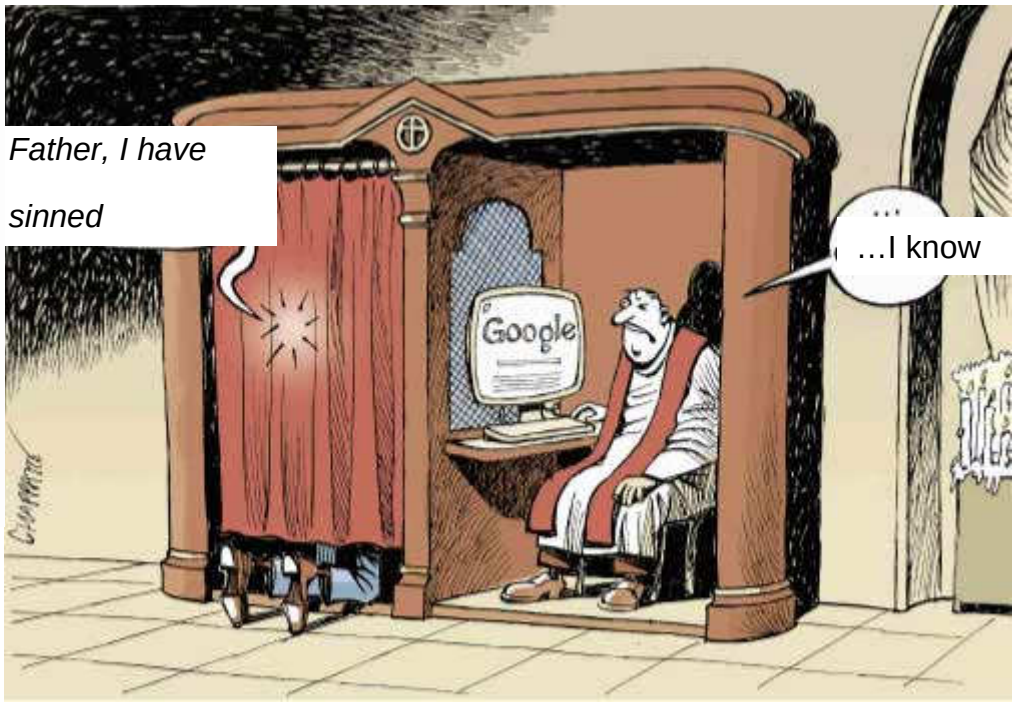
- **Web 2.0 and social networking: new evidence of threats**

- Hardware security and network trust
  Spreading problem of chip hacking
  Internet routing: errors, fraud, opportunities…

- Organized crime in the digital world

- Media hype and unexploited security flaws: how real are the threats?

- From internal sabotage to attacks on infrastructure security



Source: http://www.rezonance.ch/fs-search/download/SKOCH_Rezonance_Reputation_160108-2s.pdf?version_id=1971752

Web 2.0 and social networking: new evidence of threats

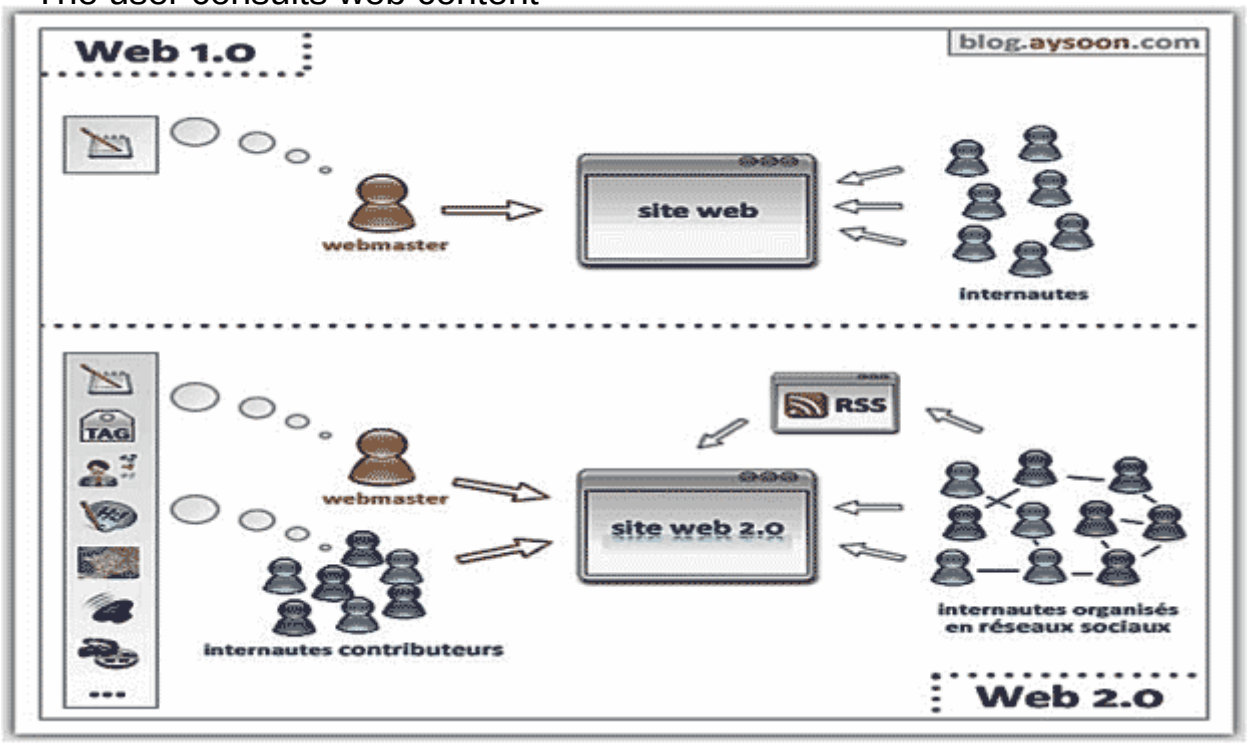
Web 2.0

One definition among many…

"Web 2.0 could be defined as a global social network in which each web site acts plays a role, allowing users to become active participants"

Thierry Gagnaire
http://www.neteco.com/128670-web-tribune-thierry-gagnaire.html

The user consults web content

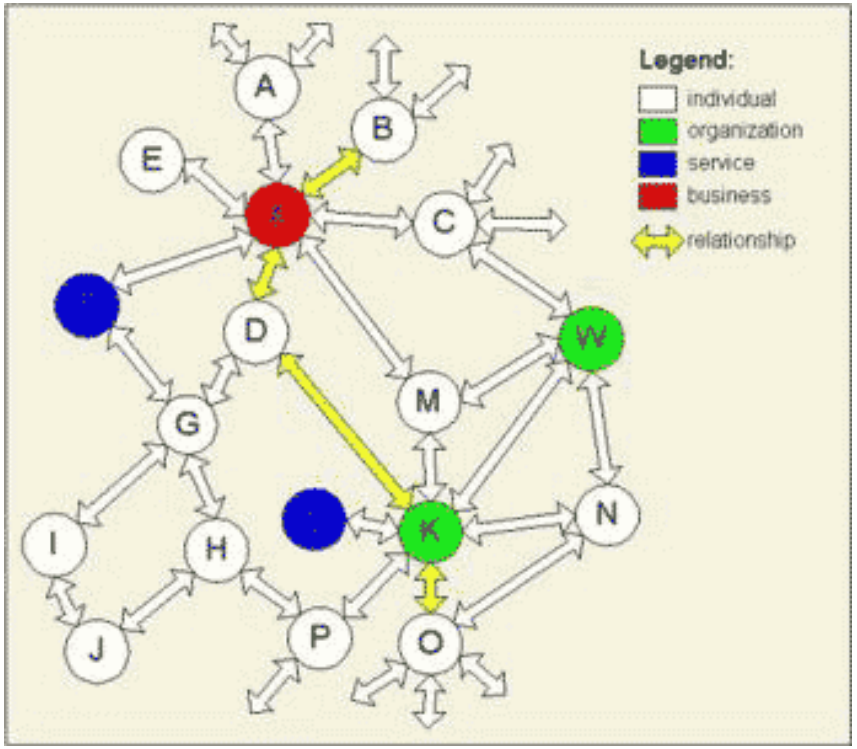


The user interacts

Social networking

Common features:

- User profile
- User-specific search capabilities
- Possibility of establishing contact between users
- Encouragement to provide information



Social networking sites work in the following way: the user creates a profile (providing personal information, pictures, hobbies, etc.) and invites "friends" to join.

The most popular social networking sites are Myspace, Facebook and Skyrock (France).

Social networking = Sharing

Users share everything:

> *"Over 25% of young office workers spend three hours (and sometimes more) on web sites such as You Tube and MySpace during work hours".*
>
> (Source Clearswift - 2007)

Videos

You Tube, DailyMotion

Podcasts (audio files)

Podemus, Radioblog

Pictures and slideshows

Flickr, Fotolia, SlideShare

Résumés, professional networking

General interest networks: Facebook, MySpace, Copainsdavant
Professional networks: LinkedIn, Viadeo
Scientific research network: Scilink

Web bookmarks

Del.icio.us, Blogmarks

Information and knowledge

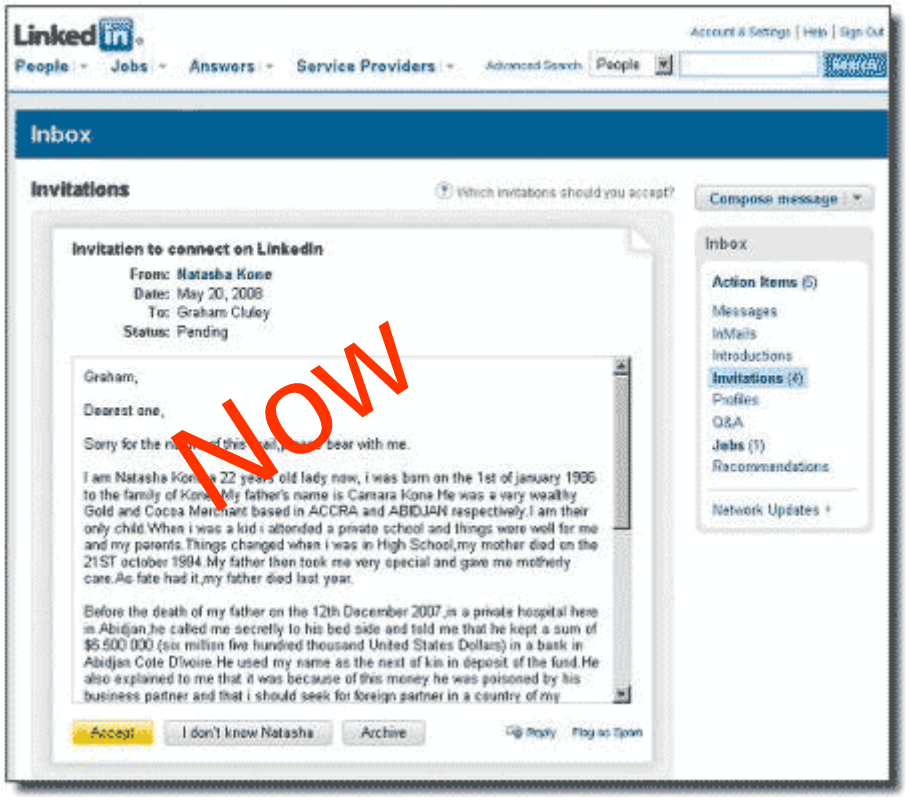
Wikipédia, AgoraVox

Social networking

Evolving risks

In 2005: *"I'm 19 years old, etc."*
(I use e-mail)

In 2008: *"I'm 22 years old, etc."*
(I use LinkedIn)



Example: 419 scam

Social networking

Motivated and opportunistic criminals

Malware, Vulnerabilities, Spam, Phishing

- Worms, Viruses, Trojans, Rogue Widgets
- Wall Spam
- Cross-Site scripting (XSS) attacks, GIFAR files (GIF + JAR)

Information theft, Espionage

- Collection
- Clustering
- Data concatenation

Attacks on the reputation of businesses and individuals

- Manipulation,
- Stalking,
- Bullying

Risk of non-removability

Social networking– Ordinary threats

Malware

W32/Koobface.A.worm (MySpace)

- Spread when a MySpace user logs on to their account
- Creates a list of comments on friends' profiles

W32/Koobface.B.worm (Facebook)

- Targets Facebook users
- Generates spam which is sent to friends

Over 25 variants in 2008

CLUSIF

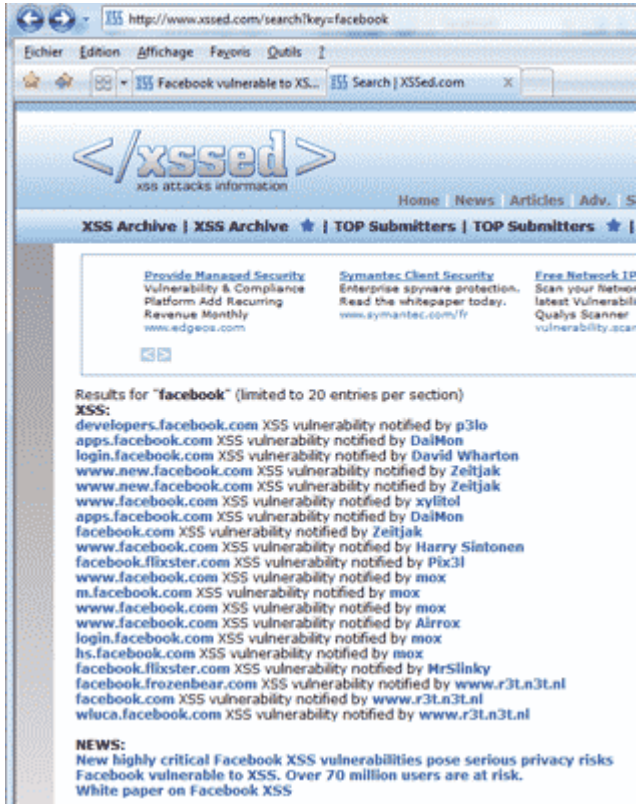
CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Social networking– Ordinary threats

Cross-Site Scripting (XSS) security flaws

XSS flaws can allow a remote attacker to "steal" user session information and carry out phishing attacks.

Colonne1	FIXED	UNFIXED
déc-08		1
déc-08		1
déc-08		1
déc-08		1
oct-08		1
sept-08		1
juil-08		1
juin-08		1
juin-08	1	
mai-08		1
mai-08		1
mai-08		1
mai-08	1	
avr-08		1
avr-08		1
mars-08		1
févr-08		1
févr-08		1
janv-08		1
janv-08		1
Total	2	18



Social networking– Ordinary threats

Spam

- Canadian Adam Guerbuez and his front company Atlantis Blue Capital were sued by Facebook.
- From March – April 2008, he sent over 4 million spam messages to Facebook users after hacking into some accounts.
- Presented as being from friends or other users, the messages contained ads for medicinal marijuana and viagra-type pills.
- On November 28, Guerbuez was sentenced to pay Facebook $873 million.

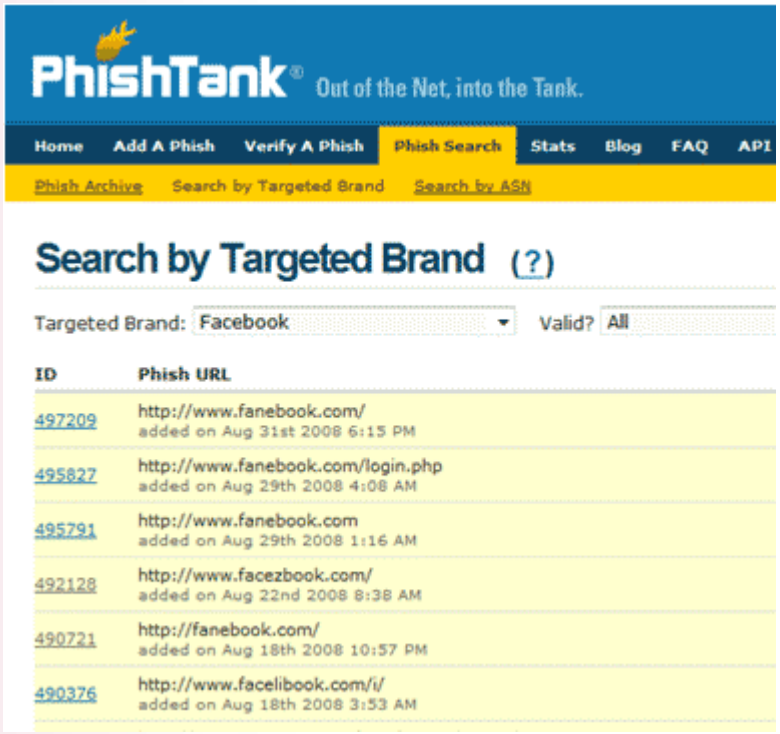
Image source: http://www.alleyinsider.com/2008/8/facebook-s-virus-reappears-but-facebook-s-vaccine-works-as-advertised

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

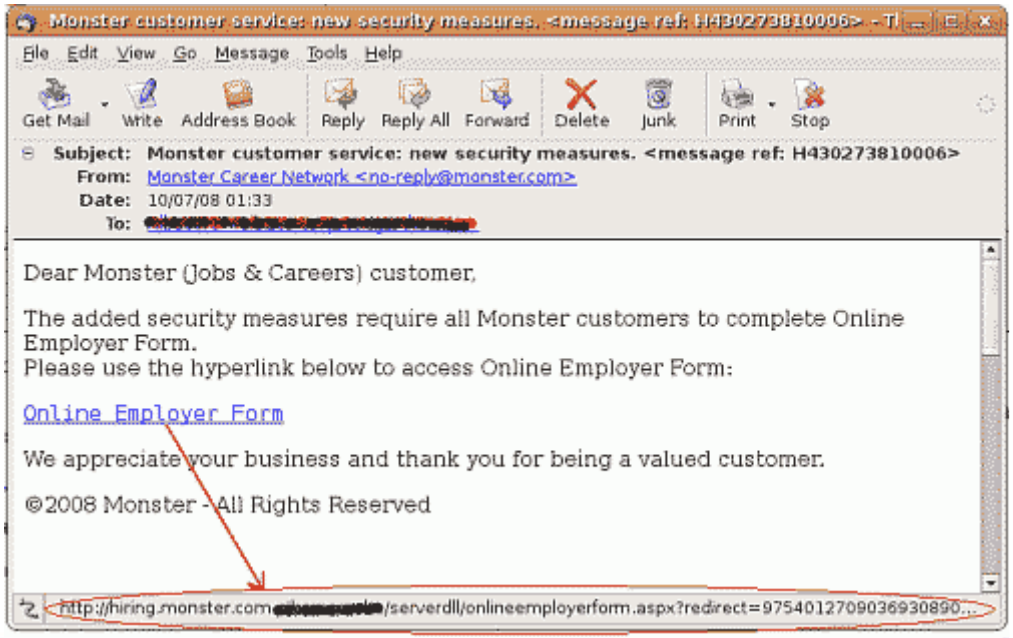
Social networking – Ordinary threats

Phishing and Typosquatting

- Significant increase in fake e-mails and mirror sites.



Typosquatters register domain names that are similar to the ones from which they would like to divert visitors. They hope that a typo error or reading the address too fast will bring the victim to their mirror sites.



Social networking– Ordinary threats

Botnet & Social Engineering - Facebot

Researchers designed a proof of concept (PoC) demonstrating that Facebook can be used for a new type of botnet attack.

Disguised as an application offering daily National Geographic photos, they used IMG image-loading HTML tags to stage a DDoS attack.

With every click and new photo that appeared, HTTP requests were generated towards a victim host.

Even though it was not advertised, a large number of users discovered the application and installed it.

Similar simulated attacks on MySpace were presented at the BlackHat/DEFCON security conference in August 2008.

Social networking– Personal risk

Friends today may not be tomorrow: e-reputation

- A Swiss MP asks his mistress to film him with his cell phone.
- He later breaks up with her.
- She sends the film to a 'friend' who then sends it to a journalist.
- The media picks up the story.
- He loses his position and privileges.

CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Social networking– Personal risk

Bad encounters

Adolescents reveal too much about themselves on social networking sites.

November 2008: a young minor meets up with a man she met online.

A recognized repeat offender, he is accused of kidnapping and sexually assaulting a 15 year-old minor, aggravated by "the use of electronic means of communication".

LE FIGARO.fr Flash

Accueil · France · Politique · International · Economie · Débats
Bourse · Patrimoine · Emploi · Sciences · Culture · Impôts

Rechercher un article | Rechercher

"Pédophile": ni viol, ni séquestration

Source : AFP
20/11/2008 | Mise à jour : 19:21 | Commentaires 4

Le pédophile récidiviste qui avait rencontré sur internet une jeune fille de 14 ans ayant fugué pendant cinq jours pour le retrouver, ne sera pas poursuivi pour viol et séquestration, a indiqué le procureur de la République de La Rochelle, Guy Etienne.

"La séquestration n'a pas été retenue car il n'y avait ni contrainte ni menaces ni chantage. De même pour le viol, la jeune fille ayant été consentante pour avoir des relations sexuelles", a indiqué lors d'une conférence de presse le procureur.

[redacted] 44 ans, sera présenté au juge d'instruction de La Rochelle, Yann Taraud, pour "soustraction de mineur en état de récidive légale" et "atteinte sexuelle sur mineur de 15 ans avec pour circonstance aggravante l'usage de moyens de communication électronique".

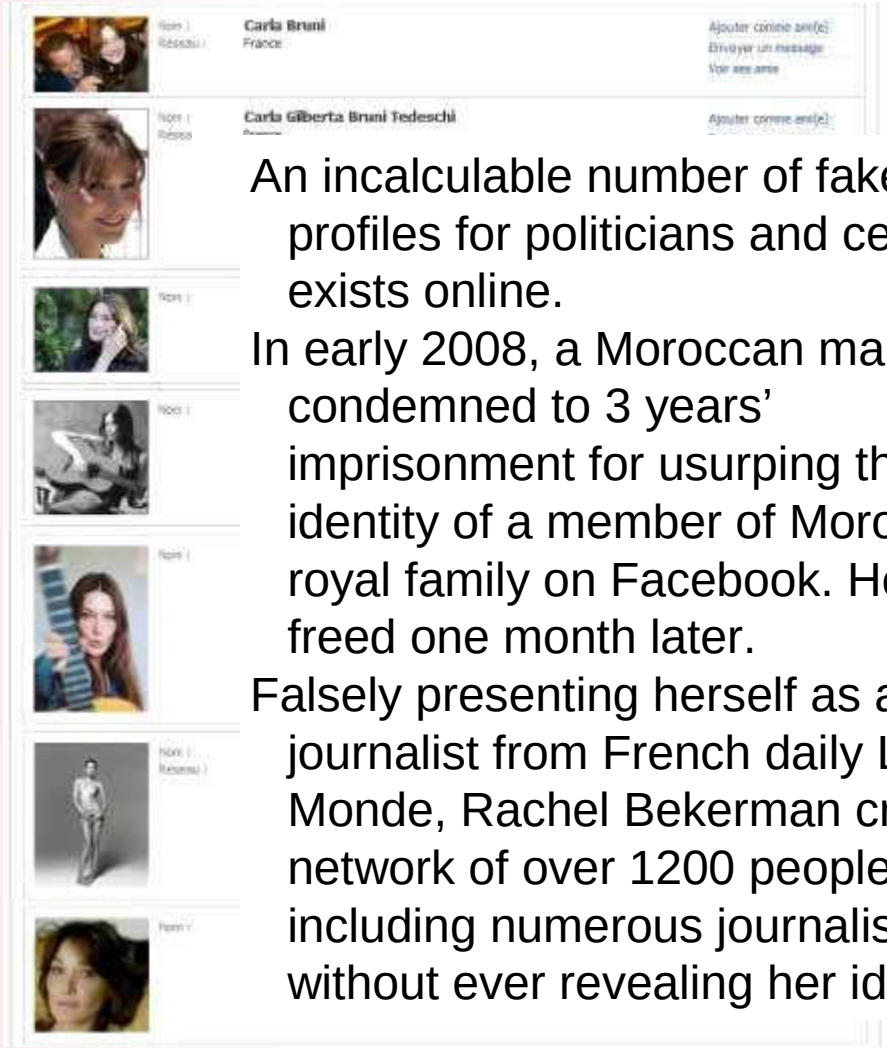
Ces faits sont passibles de 5 ans d'emprisonnement, 10 ans avec la récidive. Le recours aux moyens électroniques porte aussi la peine à 10 ans, a souligné le procureur.

CLUSIF

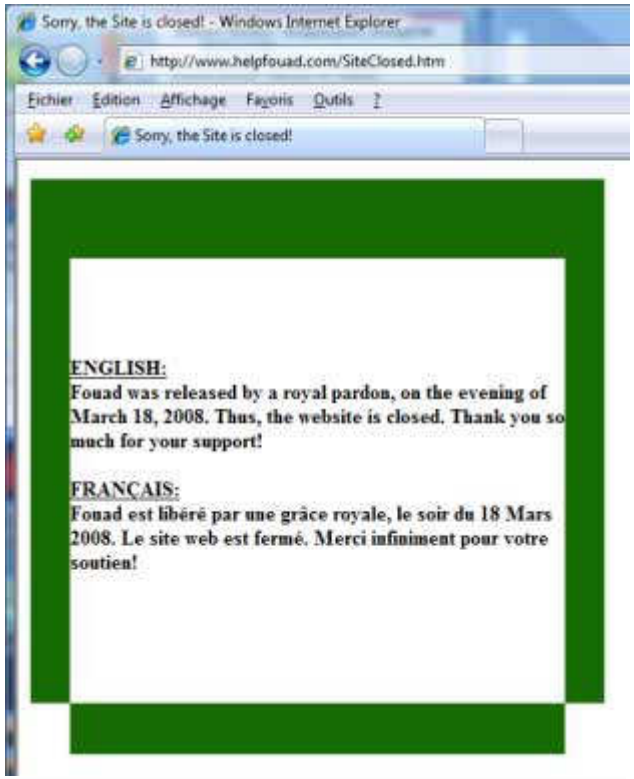
CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Social networking – Personal risks

Fake profiles: from fun to manipulation



- An incalculable number of fake profiles for politicians and celebrities exists online.
- In early 2008, a Moroccan man was condemned to 3 years' imprisonment for usurping the identity of a member of Morocco's royal family on Facebook. He was freed one month later.
- Falsely presenting herself as a journalist from French daily Le Monde, Rachel Bekerman created a network of over 1200 people, including numerous journalists, without ever revealing her identity.

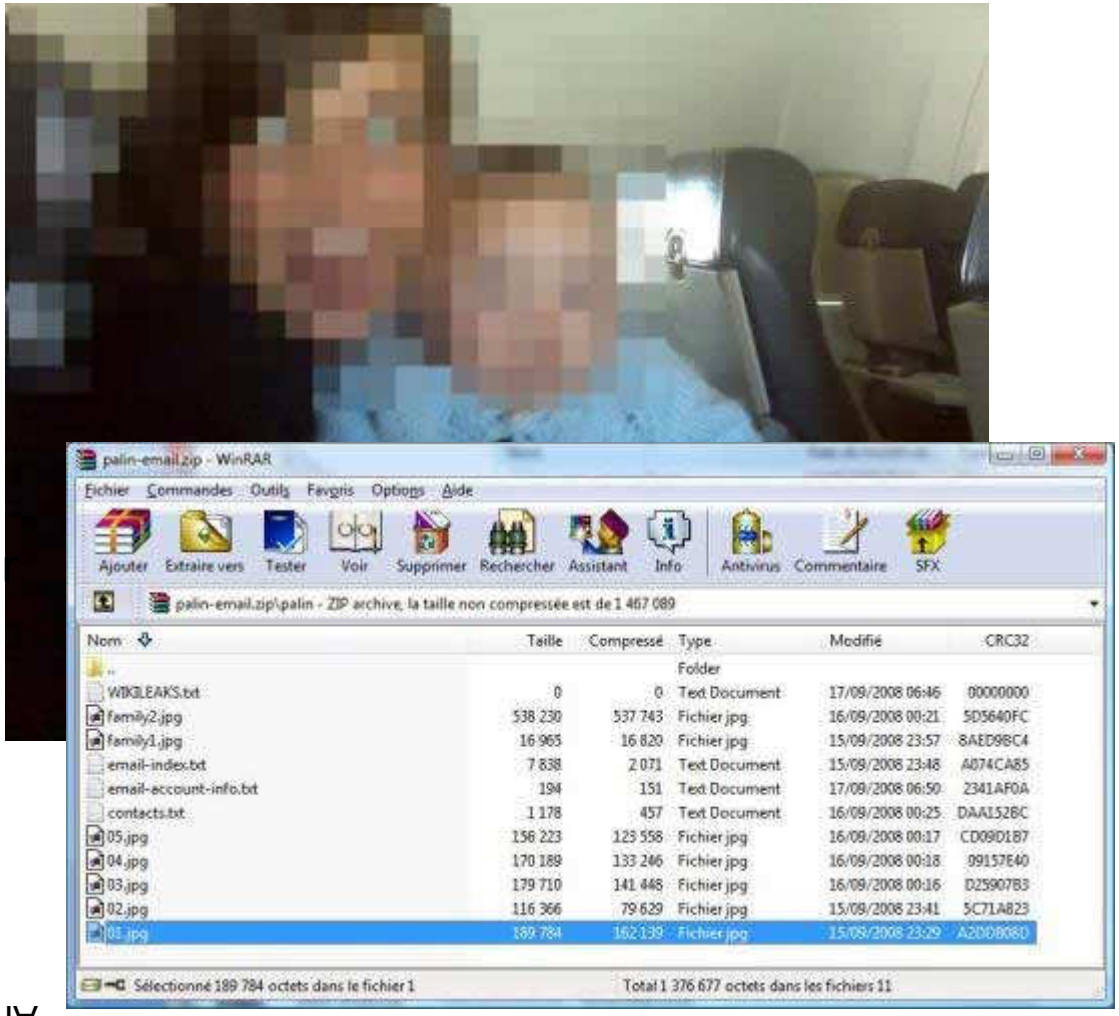


Social networking – Personal risks

Publication of potentially sensitive information

The answers to security questions for password retrieval can sometimes be found in social networking profiles.

Sarah Palin's Yahoo account security question (Septembe 2008) was "where did you meet your husband?"



Answer: Wasilla High school

Social networking – Personal *and* business risks

Love, doubt, uncertainty, betrayal

An employee is monogamous. Their relationship with the workplace is, in part, based on emotion. The employer on the other hand is polygamous, and maintains a more 'fact'-based relationship with the employee…

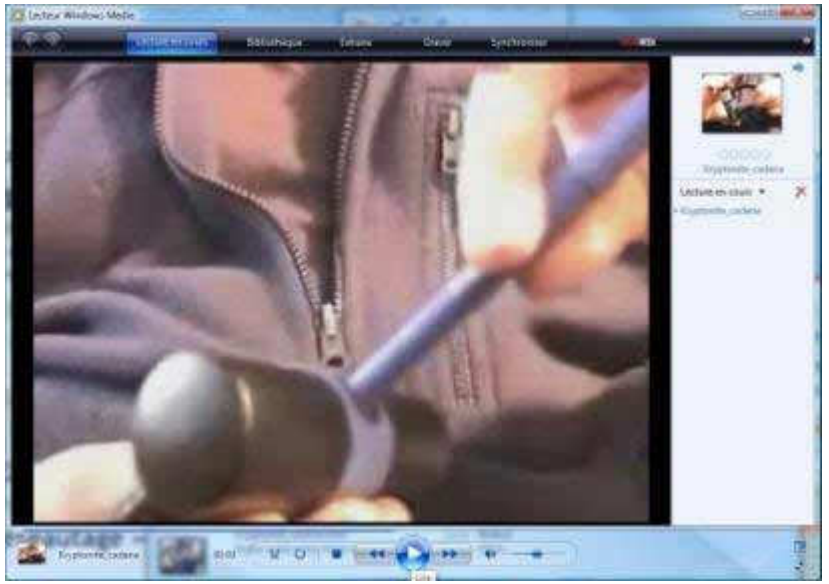
March 2008: In Cholet, a Michelin employee is fired for posting insulting messages about his employer on the Internet. In the letter of dismissal, Michelin refers to an 'obligation of loyalty' to the company.

Social networking – Business risks

Defamation

The retransmission of a television report with a different title, multiplying the number of viewers worldwide.

http://www.dailymotion.com/video/x3awn1_pfizer-contamine-des-enfants-africa



A video showing how a simple bic pen can be used to open Kryptonite bicycle locks. The story takes on epic proportions.

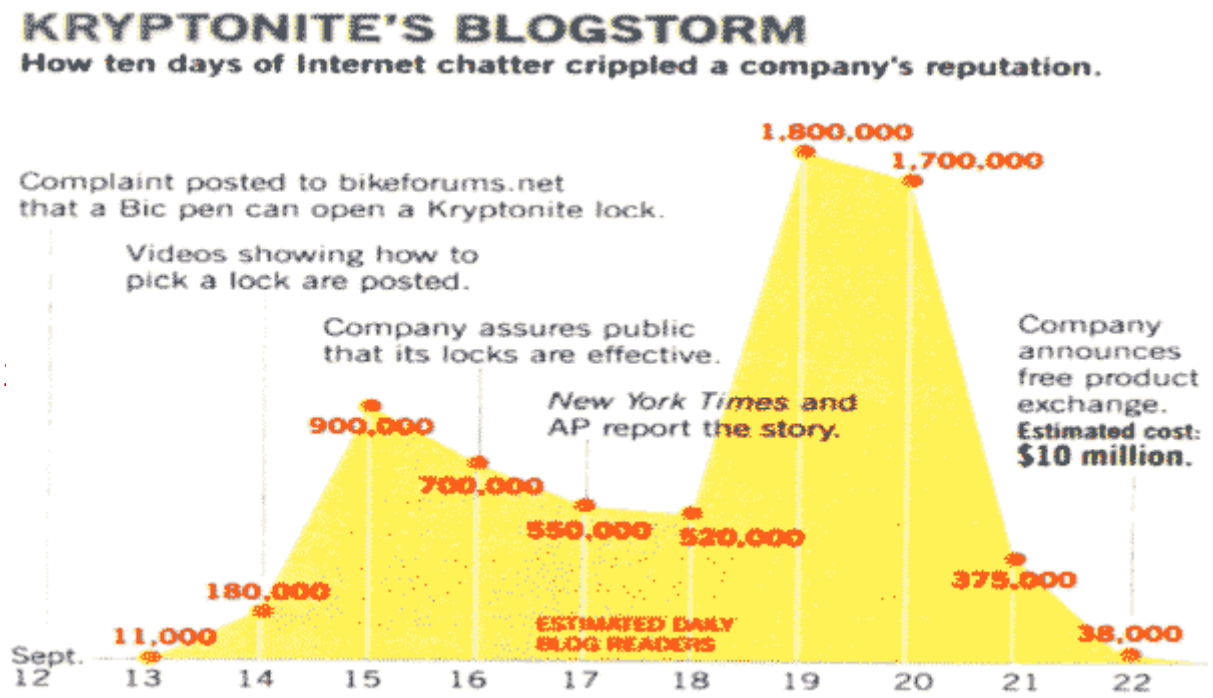
Source: http://www.rezonance.ch/fs-search/download/SKOCH_Rezonance_Reputation_160108-2s.pdf?version_id=1971752

Social networking – Business risks

Defamation

Amazon CEO Jeff Bezos: "If you make customers unhappy in the physical world, they might each tell 6 friends. If you make customers unhappy on the Internet, they can each tell 6,000 friends."

Time it takes to:
Create a blog => 2 minutes
Index a blog => 5 minutes
Make a video using a cell phone => 1 minutes
Put the video on YouTube => 15 minutes



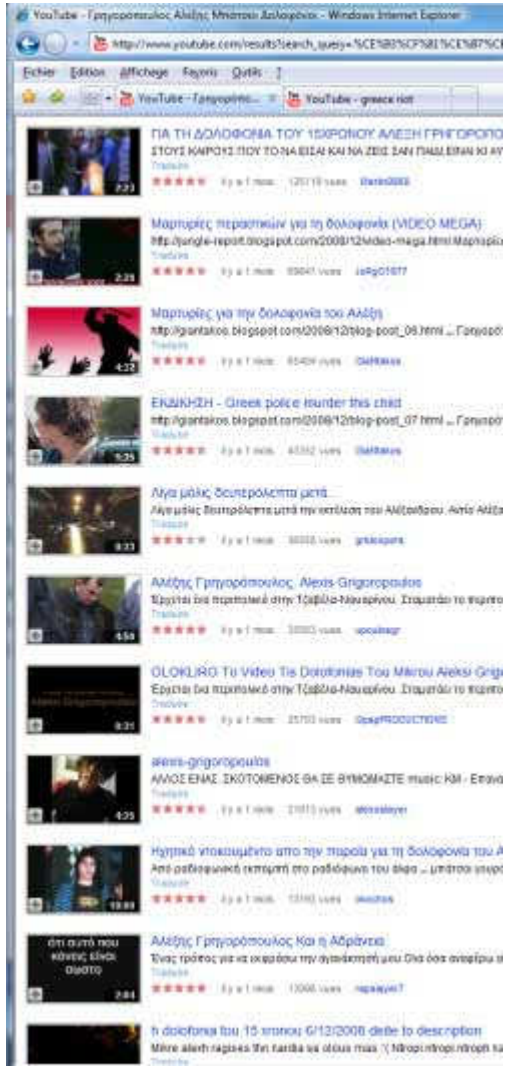
Source: http://www.rezonance.ch/fs-search/download/SKOCH_Rezonance_Reputation_160108-2s.pdf?version_id=1971752

Social networking– Social risks

From inciting violence to 'webolution'

After violence erupted in French suburbs in November 2005, bloggers were questioned over "the use of Internet to incite intentional and dangerous damage".

Similar events recently occurred in Greece (December 2008), but here, Internet appears to have served as an information tool for broadcasting amateur videos criticizing the Greek government's official announcements.



Social networking – Social risks

Agendas, propaganda and creating legends

September 2008

- As Sahab, a production company with close ties to Al Qaeda, has been publishing messages across the web for a long time.

December 2008

- On Facebook, hundreds of people sign up to groups which glorify the mafia bosses of the Cosa Nostra

Groupe : **FANS DI TOTO' RIINA...UN UOMO INCOMPRESO!**

Taille : 327 membres

Type : Intérêts communs - Histoire

December 2008

- YouTube and Twitter are at the heart of the Israeli-Palestinian conflict

Social networking – Social risks

Misinformation, activism, aiding terrorism

Certain Wikipedia entries contain fabricated / inaccurate theories and misinformation:

- Church of Scientology
- Diebold voting machines
- 9 / 11 attacks

http://www.fas.org/irp/eprint/mobile.pdf

Terrorist organizations have their own social networking sites

Activist groups use social networking to share beliefs and ideas

Social networking – Social risks

Twitter

Twitter is a social networking and microblogging tool that lets users tell their network "what they're doing". Updates can be sent online, or via instant messaging or a mobile device.

Example Afghanistan Tweets

"I'm in Bagram waiting for a flight to Camp Salerno by Kwost in the volatile east of Afghanistan near the Paki. border. Hot days/cold nights."

"Hi from Bagram air field; 20 minutes from now I'll hopefully board a flight to the Pakistan border."

"Flying to Bagram, Afghanistan in 12 hours. The journey is about to begin!"

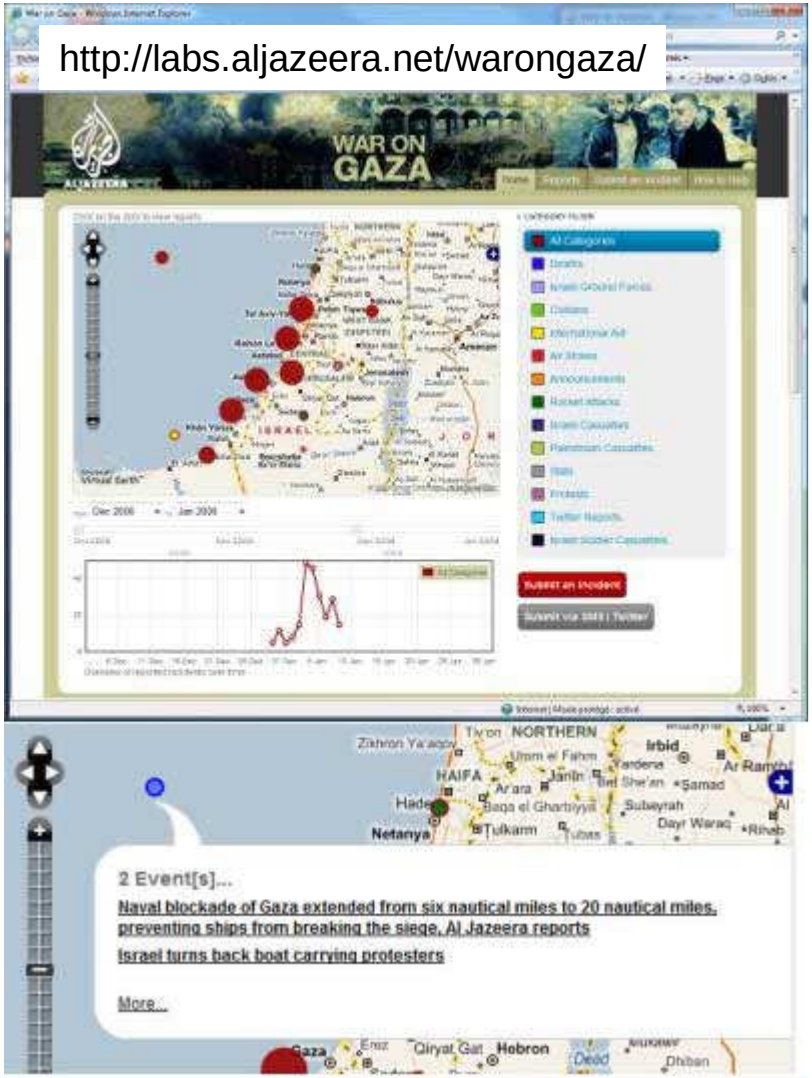
Example Fort Huachuca Tweets

"Email I just got: "We are changing all of the PMs tasks at Ft. Huachuca. I hope this does not add a lot of extra work on your end." HA!"

"...is at Ft. Huachuca. It was great seeing him last night passing through Tucson International."

Updates, called *tweets*, are short (140 characters long) so users can update quickly and spontaneously.

Note: Like Facebook and Myspace, Twitter accounts can also be hacked. Recent victims include Britney Spears and Barack Obama



Social networking – Social risks

Accidental publication of sensitive information

Twitter could prove to be very useful to terrorist activists. Warblogs, a potential source of information leaks, worry army commanders. If revealing a classified image is problematic, so is showing one out of context or that has been altered.

FOR OFFICIAL USE ONLY

Scenario 1:
Terrorist operative "A" uses Twitter with (or without) using a cell phone camera/video function to send back messages, and to receive messages, from the rest of his cell. Operative "A" also has a Google Maps Twitter Mash Up of where he is under a code word for other members of his cell (if they need more in-depth directions) posted on the WWW that can be viewed from their mobiles. Other members of his cell receive near real time updates (similar to the movement updates that were sent by activists at the RNC) on how, where, and the number of troops that are moving in order to conduct an ambush.

Scenario 2:
Terrorist operative "A" has a mobile phone for Tweet messaging and for taking images. Operative "A" also has a separate mobile phone that is actually an explosive device and/or a suicide vest for remote detonation. Terrorist operative "B" has the detonator and a mobile to view "A's" Tweets and images. This may allow "B" to select the precise moment of remote detonation based on near real time movement and imagery that is being sent by "A."

Scenario 3:
Cyber Terrorist operative "A" finds U.S. Army Smith's Twitter account. Operative "A" joins Smith's Tweets and begins to elicit information from Smith. This information is then used for a targeting package (targeting in this sense could be for identity theft, hacking, and/or physical.) This scenario is not new and has already been discussed for other social networking sites, such as My Space and/or Face Book.

Longbow en vallée d'Uzbin

Du 27 décembre matin au 28 décembre 2008 soir, l'état-major multinational du Régional Command –Capital (RC-C) de Kaboul, commandé par le général français Michel Stollsteiner a dirigé une opération mettant en œuvre une grande partie des troupes du bataillon français (BATFRA) et un bataillon de l'armée nationale afghane avec l'appui de la FIAS dans la vallée d'Uzbin au nord-est du district de Surobi.

Mise en place du dispositif

Point de situation

Cette opération était la sixième menée depuis le 6 Août dans cette vallée qui n'est pas encore entièrement sécurisée. Remontant plus au nord, c'est la première fois que les forces afghanes allaient à la rencontre des populations des villages de Hoseyn Kheyl et de Kabratu et qu'elles pouvaient y mener des actions civilo- militaires au profit des villageois.

Le dispositif est déployé

Comme lors des opérations précédentes, il s'agissait d'entretenir la confiance des responsables locaux et de la population envers les forces de

Social Networking – New evidence of threats

Conclusion

In the near to mid-term future, virtual worlds and social networking sites will increasingly merge. The frontier between work and play will become increasingly blurry. Dangers will be heightened.

Most networking schemes rely on a profit-based economic model. Aside from the risk of misuse, could stored personal data be used to commercial ends?

Finland, November 11 2007: using the pseudonym Sturmgeist89, the murderer posted a series of videos on YouTube

Finland, September 23 2008: using the pseudonym Wumpscut86, the murderer posted a series of videos on YouTube

Social networking – New evidence of threats

Conclusion – Aspects to monitor

Ordinary threats are very compatible with social networking sites:

- Networking sites are targets for viruses, spams, phishing, identity theft and security flaws.

An individual's 'private sphere' is shrinking day by day:

- Users reveal detailed information about their private (and professional) lives, sometimes without realizing it.
- Others can express their opinions about a user or publish photos without his or her permission.
- Once this information is spread, it cannot be removed.

Social networking – New evidence of threats

Conclusion – Aspects to monitor

Businesses are also targets:

- By using unofficial communication methods, employees can – intentionally or not – damage their company's brand/image by spreading inappropriate, sensitive or confidential information.
- Rumour and misinformation campaigns, mounted as games, for personal gain or revenge, can quickly lead to significant financial loss.

And society in general:

- Propaganda and misinformation can also be socially harmful.
- Isolated extremists, rabble rousing groups and even terrorists can recruit members, express their views, and access sensitive information that can be used to disrupt public order.

Webography

« Qu'est-ce que le Web 2.0 ? »: http://www.neteco.com/128670-web-tribune-thierry-gagnaire.html

Qu'est ce que les réseaux sociaux: http://www.ed-productions.com/leszed/index.php?qu-est-ce-que-les-reseaux-sociaux

Fréquentation des réseaux sociaux: http://web-2-geek.blogspot.com/2008/07/frequentation-des-reseaux-sociaux.html

Le Web 2.0 favoriserait la fuite d'informations: http://www.lemondeinformatique.fr/actualites/imprimer-le-web-20-favoriserait-la-fuite-d-informations-22459.html

Ever put your CV on a job site?: http://www.avertlabs.com/research/blog/index.php/2008/07/14/ever-put-your-cv-on-a-job-site/

Facebook's Virus Reappears, But Facebook's Vaccine Works As Advertised: http://www.alleyinsider.com/2008/8/facebook-s-virus-reappears-but-facebook-s-vaccine-works-as-advertised

Antisocial Networks: Turning a Social Network into a Botnet: http://www.ics.forth.gr/~elathan/publications/facebot.isc08.pdf

Un salarié de Michelin licencié pour s'être épanché sur le net: http://www.lefigaro.fr/actualite-france/2008/12/13/01016-20081213ARTFIG00580-un-salarie-de-michelin-licencie-pour-s-etre-epanche-sur-le-net-.php

Jail for Facebook spoof Moroccan: http://news.bbc.co.uk/2/hi/africa/7258950.stm

La justice se penche sur le cas du hacker de Sarah Palin: http://www.silicon.fr/fr/news/2008/10/09/la_justice_se_penche_sur_le_cas_du_hacker_de_sarah_palin

Israël attaque Gaza sur YouTube: http://www.infos-du-net.com/actualite/15032-israel-gaza-YouTube.html

Sur Facebook, les mafiosi sont sympas: http://www.lemonde.fr/europe/article/2009/01/07/sur-facebook-les-mafiosi-sont-sympas_1138748_3214.html

AlQaida-Like Mobile Discussions & Potential Creative Uses: http://www.fas.org/irp/eprint/mobile.pdf

A DigiActive Introduction to Facebook Activism: http://www.digiactive.org/wp-content/uploads/digiactive_facebook_activism.pdf

Les comptes Twitter de Britney Spears et d'Obama ont été piratés: http://www.neteco.com/249664-comptes-twitter-britney-spears-obama-pirates.html

Le FBI prévient de la venue prochaine du "Cyber Armageddon": http://www.silicon.fr/fr/news/2009/01/07/le_fbi_previent_de_la_venue_prochaine_du__cyber_armageddon_

Les blogs militaires: http://www.c2sd.sga.defense.gouv.fr/IMG/pdf/thematique9charte.pdf

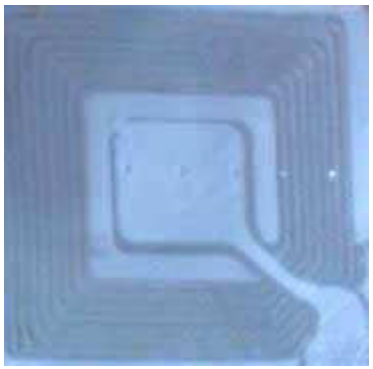
Overview 2008

- Web 2.0 and social networking: further evidence of threats…
- **Hardware security and network trust**
  Spreading problem of chip hacking
  Internet routing: errors, fraud, opportunities…
- Organized crime in the digital world
- Media hype and unexploited security flaws: how real are the threats?
- From internal sabotage to attacks on infrastructure security

Presentation outline

When electronics teams up with IT…

- the MiFare RFID chip hack
- E-passports
- Cold boot Attacks



Network trust

- BGP, YouTube and Internet routing
- MD5 and false certificates

Have threats to information security evolved?

Information security threats have evolved to encompass both the logical and physical

A new movement emerged several years ago:

Smart card attacks

- Side channels, DPA/SPA

PayTV, fake decoders, hacked chips…

Jailbreaking (iPhone v1 and v2)

Video game consoles and modding

- Hacking game consoles; mod chips and flash cards: DS, Xbox, PS2

DEFCON lock-picking

- *"All your locks are belong to us"*

The use of these techniques is now steered towards more 'serious' ends.

2008 hardware presentation…

25C3, Berlin, December 2008

- Over 15 of around 100 presentations focused on hardware
  - ☞ RFID, NFC, DECT, GSM, JTAG, WII, Zigbee

CanSecWest 2008 (March)

- RFID, Mobitex network, Cold boot attacks

BlackHat Europe 2008 (March)

- Reverse engineering hardware, GSM hacking, side channels, physical security

RFID?

Strong growth in 2008

RFID = *Radio Frequency Identification*

Usually passive tags (memory + antenna)

- Power supplied by a reader

Problem: what type of security?

- Cryptography required to ensure privacy and prevent tag cloning
- Significant hardware constraints, costs

NXP: Mifare Classic RFID chip

Statement published by the CCC (Chaos Computer Club, Germany) on 1/1/2008: Encryption scheme of the chip has been cracked

Mifare: an NXP product, mainly used in contactless smart card applications (RFID technology)

- Public transportation systems (London, Perth, Amsterdam…)

In the Netherlands, two ticket systems in use:

- The 'ultra light' single-use card: simple memory + contactless system, no protection
- The 'classic' card, for monthly passes: same system, but protected by a secret cryptographic algorithm (CRYPTO1)

Ultralight card

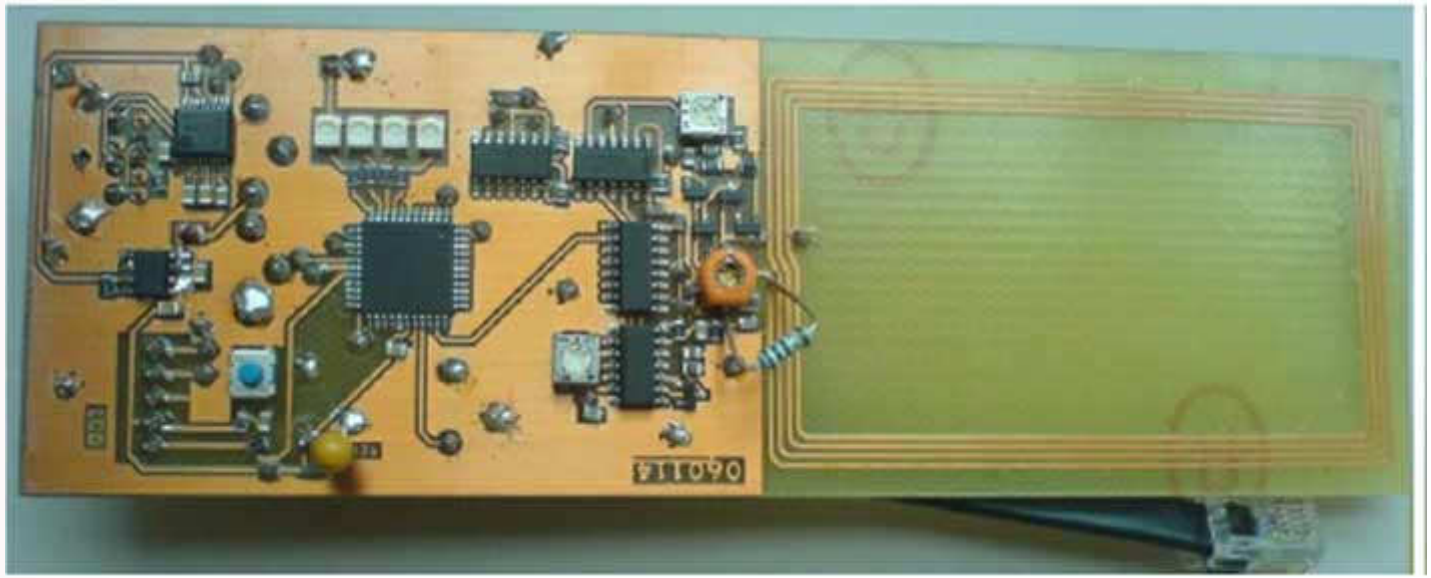
Ticket cloning possible

University of Amsterdam, Pieter Siekerman and Maurits van der Schee

Proof of concept (Ing. R. Verdult)

Emulating and cloning of RFID tag

Resetting of ghost back to initial state before use (endless trips possible)

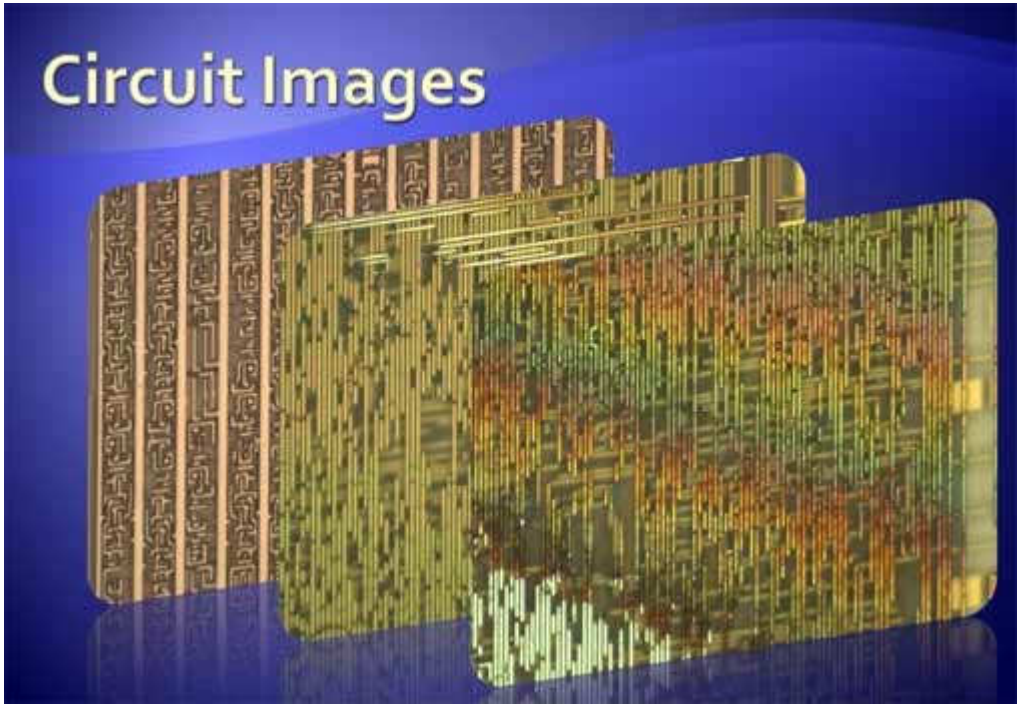


Ghost device Source: Proof of concept, cloning the OV-Chip card, Ing. R. Verdult

Classic Card (Mifare Classic)

Analysis of NXP chip hardware!

It shouldn't be a problem (*Security by Obscurity*???)



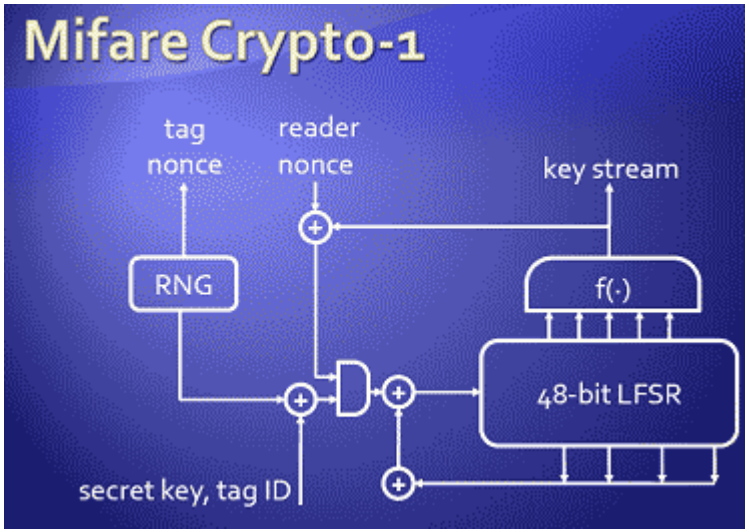
Mifare internals - Source: CCC 2007 – Mifare Security

Mifare Classic card analysis (Reverse Engineering)

Mifare Classic: cryptography

But the proprietary Crypto-1 algorithm, and its 48-bit secret key, are weak

Easy to automatically read the chip's memory ports



Mifare Crypto-1 - Logical view of secret algorithm – (Reverse engineering – Electronic Low level analysis) – Source: CCC 2007 – Mifare Security

Mifare classic

Cracking the chip: obtaining secret key

- Weak pseudo-random generator (16 bits, LFSR-based, derived from time read)
- Monitoring of the pseudo-random generator

Use of FPGA for computing

- $100 of material for one week of (non-optimized) computing

-> RFID cloning possible

"Producing a fraudulent card remains complex and risky, and manipulating the card is of limited value," added the spokesperson. "It needs a qualified computer specialist to set up, and risks detection by our staff or police."

Semiconductor company NXP, which manufactures the Mifare Classic chips, claimed that publication of the details had gone against the principles of responsible disclosure.

"NXP Semiconductors regrets that the Radboud University Nijmegen has revealed details of the protocol and the algorithm of Mifare Classic, as well as some practical attacks on Mifare Classic infrastructures," said an NXP spokesperson. "A broad publication of detailed information to carry out attacks with limited means is, at this moment in time, contradictory to the scientific goal of prevention and the responsible disclosure of sensitive information."

The MBTA and RFID…

Massachusetts Bay Transportation Authority

Defcon 16, "Anatomy of a Subway Hack"

Widespread media attention in August after judge orders halt to presentation

Hacking-centred approach, including physical, logical and hardware security

Analysis of Charlie Tickets

Pre-paid, rechargeable ticket

Magnetic strip

(ticket amount + checksum)

Analysis of Charlie Cards

Mifare classic

Obtaining key, cloning…

Security by Obscurity…

Security by obscurity is generally a bad idea

- Kerckhoffs' Principle (1883…)

Principle ok (??) for security of material?

- Warning: may no longer be valid in 2008

Industry needs to evolve on this point, as sometimes held to be valid

- Scored during common criteria evaluations

E-passport?

Do you recognize this person?

Passersby reported seeing him at Amsterdam's Schiphol airport in late September 2008…

E-Passports and security

Massive wave of new generation passports

- ☞ Biometrics – E-Passport

Uses a RFID-type chip containing:

- Name, date of birth, passport number
- Biometric information (photo, fingerprints)
- (Optional) anti-cloning cryptosystems
- Signature (data integrity)

Standards set out by the ICAO (*International Civil Aviation Organization)*

Publication of numerous attacks since 2005

- Remote country recognition (Example of error message on Belgian passport in April 2008)

Cloning problem…

British e-passport problem: several reading and cloning proof of concepts in 2006, 2007 and 2008

Digital certificates are not being properly read

Demonstration by Adam Laurie to the British press (06/07)

Modification: PoC in August and October 2008

Problem checking certificates -> data integrity

Cloning: Active authentication is not used (or not used enough) by majority of countries

Solution: E-Clown for Nokia 6131 NFC / 6212 NFC

E-Passports: the problem

Data is signed with a digital certificate

The certificate belongs to the country issuing the passport

These certificates should be shared between countries to ensure the authenticity of the signatures (creation of a public key directory (PKD)

In October 2008, only 10 out of 50 countries had accepted to share certificates

Of these, only 5 have actually shared them…

Cold boot (1/3)

Purpose: To access normally confidential data stored in computer RAM

- First proof of concept: February 2008
- Pwnie award (BH2008 USA) in the most innovative research category!

Actual threat:

- Access to private keys
- Access to cryptographic keys (on hard drive for example)

Requirements: For the attack, a PC that is on, in sleep mode, or has been recently switched off

Principle: PC memory is read by rebooting the machine on a controlled OS

- Rebooted to a CD, USB flash drive
- Memory is extracted and read on another system
- Cooling the memory chips using a can of compressed air extends the time during which data may be preserved (several minutes)

Cold boot (2/3)

Cold booting explained:

- These attacks work well
- Accessing the data held in RAM (which is normally protected from retrieval by the OS…)
- The research team has developed well-functioning algorithms to search for secret keys
- The success of an attack depends on what type of memory is involved

Threat: PC in sleep mode, theft at airport...

Use of an upside down spray canister to freeze memory chips and prolong accessibility of data

Source: http://citp.princeton.edu/memory/media/

Cold boot (3/3)

Simple protection

- Turn off your PC (rather than leaving it in sleep mode)

Not another example of failed disk encryption!

Research carried out to counter these attacks

- Clearing of memory if PC is shutdown or put into sleep mode
- Sensor systems to detect abnormal cooling of a PC
- Storage of keys in low memory address (overwritten when rebooted)
- Key expansion and hash function
- Holding keys in MMX processor registers

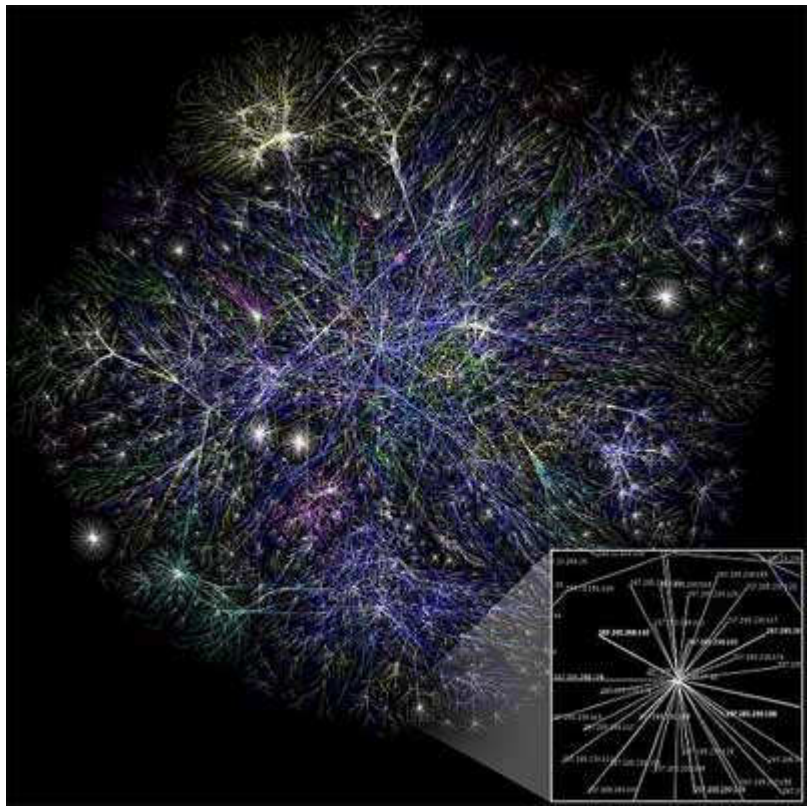
Does the Internet inspire trust?

The Internet model is based on trust

- DNS servers organized in a hierarchy
- Border gateway protocol (BGP)
- Registration and use of domain names…

Self-managing system

- Autonomous Systems (AS)
- Internet governance
- Net neutrality
- International context…



Internet mapping – Source: wikipedia.org

Internet routing (finding your way around)

Internet = network of networks

Exchange of routing information (BGP, Inter-Autonomous System Routing)

Trust model: routes and known routes are announced

Everything works well, except…

CLUSIF

PTA

Corrigendum- Most Urgent

GOVERNMENT OF PAKISTAN
PAKISTAN TELECOMMUNICATION AUTHORITY
ZONAL OFFICE PESHAWAR
Plot-11, Sector A-3, Phase-V, Hayatabad, Peshawar.
Ph: 091-9217279- 5829177 Fax: 091-9217254
www.pta.gov.pk

NWFP-33-16 (BW)/06/PTA February ,2008

Subject: **Blocking of Offensive Website**

Reference: This office letter of even number dated 22.02.2008.

I am directed to request all ISPs to immediately block access to the following website

URL: http://www.youtube.com/watch?v=o3s8jtvvg00

IPs: 208.65.153.238, 208.65.153.253, 208.65.153.251

Compliance report should reach this office through return fax or at email peshawar@pta.gov.pk today please.

Deputy Director
(Enforcement)

To:
1. M/s Comsats, Peshawar.
2. M/s GOL Internet Services, Peshawar.
3. M/s Cyber Internet, Peshawar.
4. M/s Cybersoft Technologies, Islamabad.
5. M/s Paknet, Limited, Islamabad
6. M/s Dancom, Peshawar.
7. M/s Supernet, Peshawar.

Official document of the Pakistani government requesting that access to YouTube be blocked within the country

BGP and YouTube

Pakistan Telecom incident and YouTube null route

- February 24 2008: Error causes access to YouTube to be cut off worldwide
- More specific null route spread on Internet

PCCW cuts Pakistan Telecom's access after the error is detected…

Accidental in this case, but potential for fraud

BGP and re-routing

DEFCON / Pilosov & Kapela incident

Presentation at DEFCON gathering in August 2008

More specific BGP announcement for Defcon's network

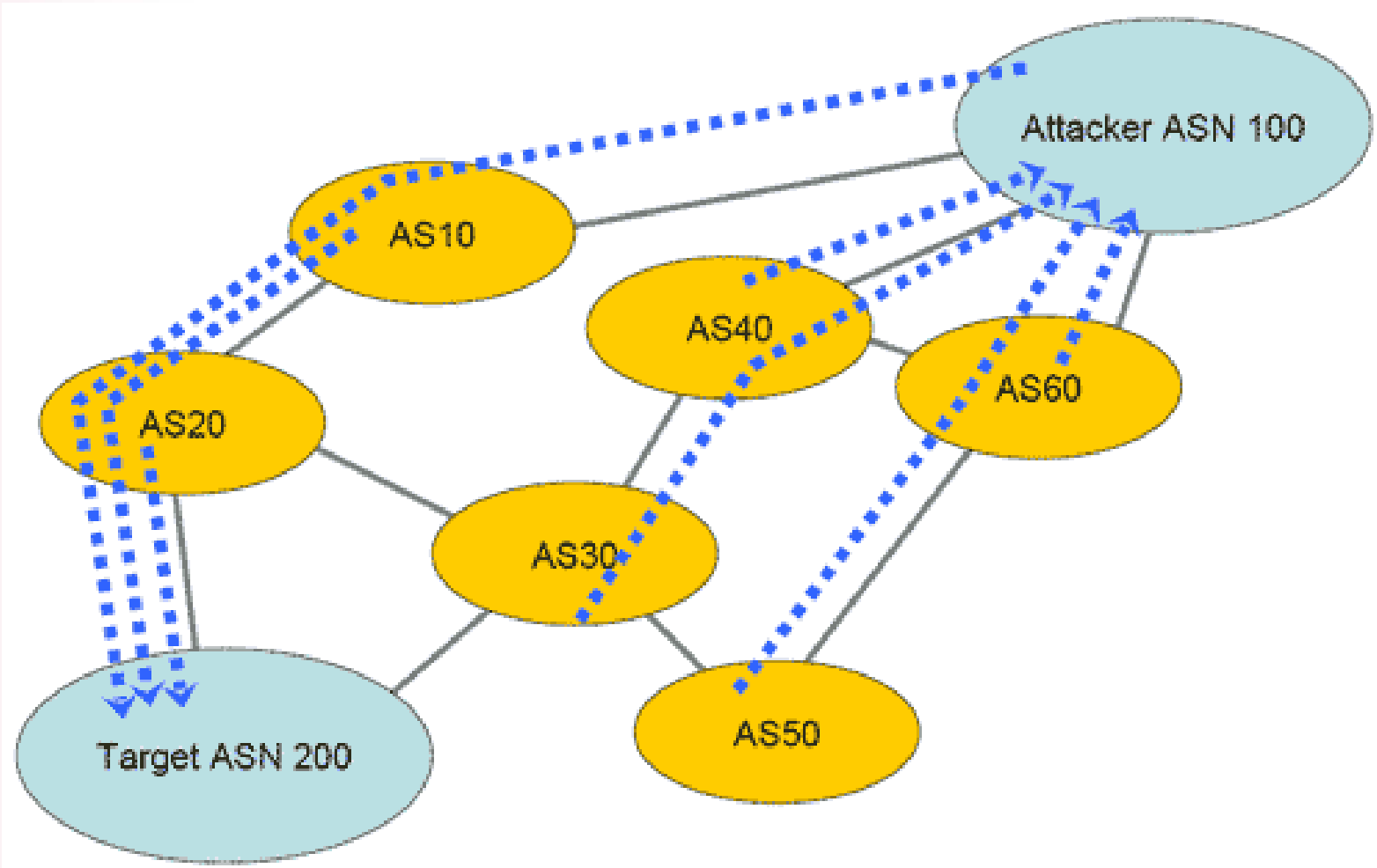
Transparent, static re-routing

and masking

→ « MITM » inward trafic !

This is not a failure – it's how the BGP model functions

BGP and MITM



The 100 network reroutes traffic to the 200 network by announcing a specific BGP route path.
The 100 network redirects traffic via a static route to the 200 network, making the attack very stealthy

PKI, certificates and MD5…

Proof of concept demonstration at 25C3 (Berlin, December 2008)

"MD5 considered harmful today: Creating a rogue CA certificate"

How?

- Creation of a rogue Certificate Authority certificate trusted by common web servers
- Fake certificate appears to be signed by a trusted root CA

Affected CAs

Certain conditions required:

Based on MD5 'collisions'

- CAs that use SHA-1 appear (for now) to be OK

- CSR must be predicted
- Certificate serial number
- Validity period…
- Presentation at CCC focused on Rapid SSL's fast issuance of certificates

- Use of significant computer power to create the MD5 collision
- Cluster of 200 PlayStation 3s used over period of a few days…

SSL and the consequences…

Very advanced man-in-the-middle attacks possible…

Certificate is valid! Attack therefore transparent

SSL and certificate model used by commercial websites is not designed to provide 'strong authentication'

Most attacks occur at the client end

Internet has not collapsed this time…

Consequences…

MD5 made slightly more vulnerable…

SHA-1 should replace MD5 immediately

NIST competition to develop a new cryptographic hash algorithm: SHA-3

- 51 competitors are currently being selected… (some have already been eliminated)
- Goal: publication of SHA-3 standard by 2012

Webography (1/2)

Mifare

Security Failures in Secure Devices, Christopher Tarnovsky
http://www.blackhat.com/presentations/bh-dc-08/Tarnovsky/Presentation/bh-dc-08-tarnovsky.pdf
Side Channel Analysis and Embedded Systems – Impact and Countermesures, Job de Haas
http://www.blackhat.com/presentations/bh-dc-08/DeHaas/Presentation/bh-dc-08-dehaas.pdf
Mifare – Little security, Despite obscurity
http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html
Smart Cards in Public Transportation: the Mifare Classic Case
http://www.laquso.com/VVSS2008/presentations/0-Jacobs.pdf
Principe de Kerckhoffs
http://fr.wikipedia.org/wiki/Principe_de_Kerckhoffs

MBTA

Anatomy of a Suway Hack, Defcon 16
http://www.defcon.org/html/defcon-16/dc-16-speakers.html#Anderson

Cold Boot Attacks

Let we remember: Cold Boot Attacks on Encryption Keys
http://citp.princeton.edu/memory/
Wikipedia : Cold Boot Attack
http://en.wikipedia.org/wiki/Cold_boot_attack
Braving the Cold: New Methods for Preventing Cold Boot Attacks on Encryption Keys
http://www.blackhat.com/presentations/bh-usa-08/McGregor/BH_US_08_McGregor_Cold_Boot_Attacks.pdf

Webography (2/2)

E-passport

THC Clones Biometric ePassport - Elvis Presley Passport
http://www.darknet.org.uk/2008/10/thc-epassports-thc-clones-biometric-epassport-elvis-presley-passport/
ePassports reloaded
https://www.blackhat.com/presentations/bh-usa-08/van_Beek/bh_us_08_van_Beek_ePassports_Reloaded_Slides.pdf
EPassport emulator
http://freeworld.thc.org/thc-epassport/
eClown (clonage de ePassport sur téléphone Nokia NFC)
http://www.dexlab.nl/

MD5

MD5 considered harmful
http://www.win.tue.nl/hashclash/rogue-ca/
25C3 « Creating a rogue CA Certificate
http://events.ccc.de/congress/2008/Fahrplan/events/3023.en.html
The SHA-3 zoo
http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo

BGP and YouYube / BGP rerouting

Pakistan hijacks YouTube
http://www.renesys.com/blog/2008/02/pakistan-hijacks-YouTube-1.shtml
Stealing The Internet - A Routed, Wide-area, Man in the Middle Attack
https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf

CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Overview 2008

- Web 2.0 and social networking: further evidence of threats…
- Hardware security and network trust
  Spreading problem of chip hacking
  Internet routing: errors, fraud, opportunities…
- **Organized crime in the digital world**
- Media hype and unexploited security flaws: how real are the threats?
- From internal sabotage to attacks on infrastructure security

Presentation outline

- Numerous types of counterfeiting
- Shady hosts – an important feature of criminal Internet activities
- Fictitious lottery announcements: a common spam scam in 2008
- Creativity of criminal groups to make money: new types of SMS viruses, selling botnets…
- Concealment 'by accident'

Counterfeiting

Medicines

Cigarettes

Music and videos

Running shoes, stereo equipment…

Counterfeit anti-virus software

Counterfeit hardware

Example of counterfeit prescription drugs in 2008

REUTERS

LATEST NEWS RETAIL SALES DIVE AS HOLIDAY SPENDING SLUMPS

Top News
Reuters top ten news stories delivered to your inbox each day.
Subscribe

See how you can accelerate application deployment time with our storage solutions to help your company go further, faster.
> Watch Our Webcast

You are here: Home > News > Article

Rogue Internet Pharmacies on the Run: LegitScript Shuts Down 500 No-Prescription-Required...

Tue Nov 18, 2008 1:00am EST

Email | Print | Share | Reprints | Single Page [-] Text [+]

Rogue Internet Pharmacies on the Run: LegitScript Shuts Down 500 No-Prescription-Required Online Pharmacies

Websites fueling prescription drug abuse, selling non-FDA approved drugs taken offline

ARLINGTON, Va., Nov. 18 /PRNewswire/ -- LegitScript, an online pharmacy certification program, announced today that it has succeeded in getting nearly 500 "rogue" Internet pharmacy websites shut down.

The sites had been selling prescription drugs or steroids without requiring a prescription, a practice that is illegal and considered unsafe by medical authorities. In most cases, the drugs were sold from outside of the United States.

"The Internet is a safer place today because these illicit prescription drug websites have been terminated," said John Horton, LegitScript's President.

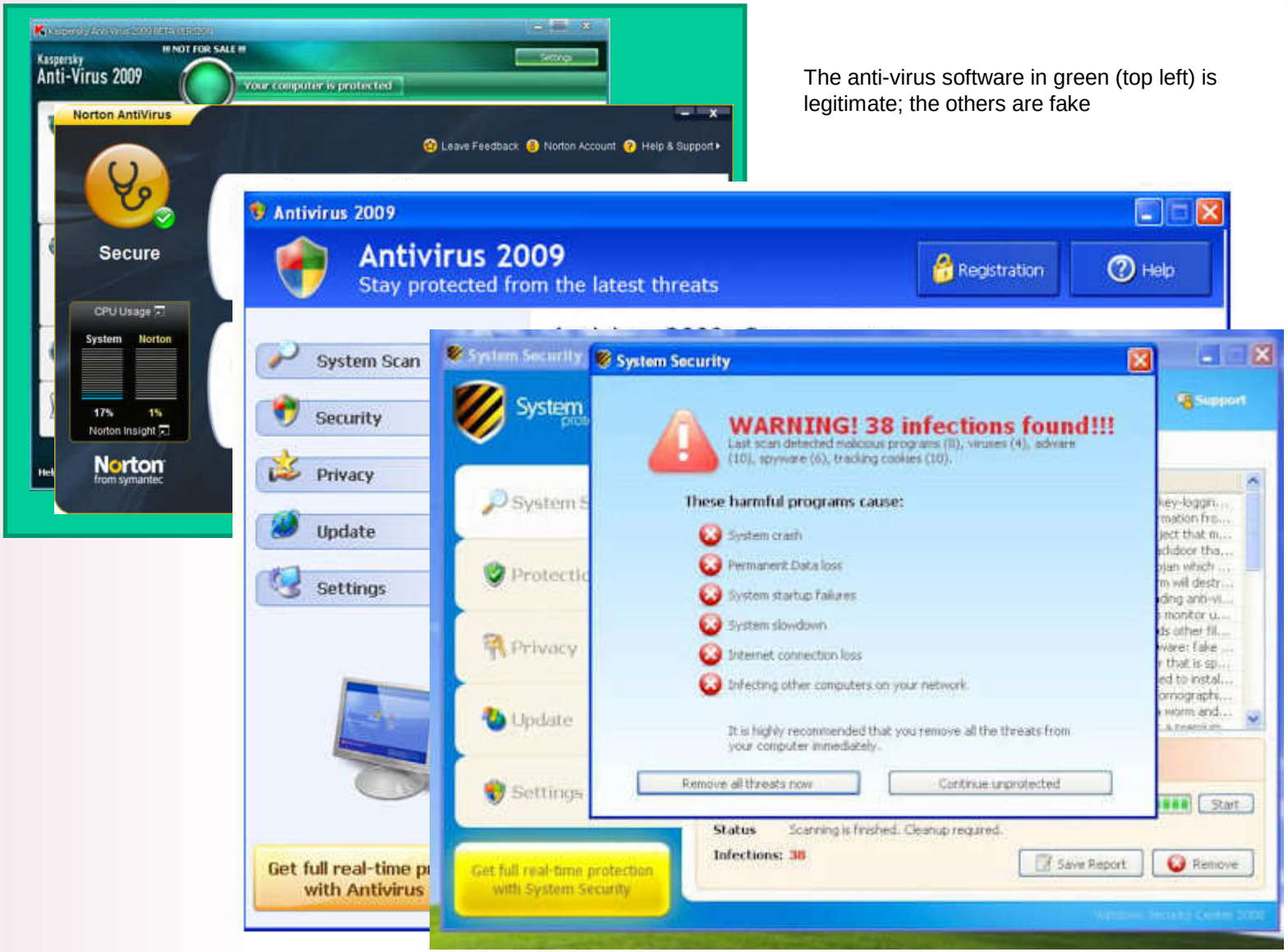
Among the domain name registrars to take the lead in shuttering the rogue Internet pharmacies was Directi.

Horton praised the domain name registrars that terminated the rogue Internet pharmacies. "Directi, in particular, has been a leader in fighting rogue Internet pharmacies, and has steadily demonstrated its commitment to Internet safety by refusing to sponsor websites engaged in spam, malware, the illicit

CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Counterfeit anti-virus software



The anti-virus software in green (top left) is legitimate; the others are fake

Counterfeit anti-virus software

30 signatures recorded in 09/2007 compared to 2100 one year later.

All possible techniques used to get the product out there, including referencing on Google.

Thousands of users cheated out of 40 €. The credit cards used to pay are in fact debited several times.

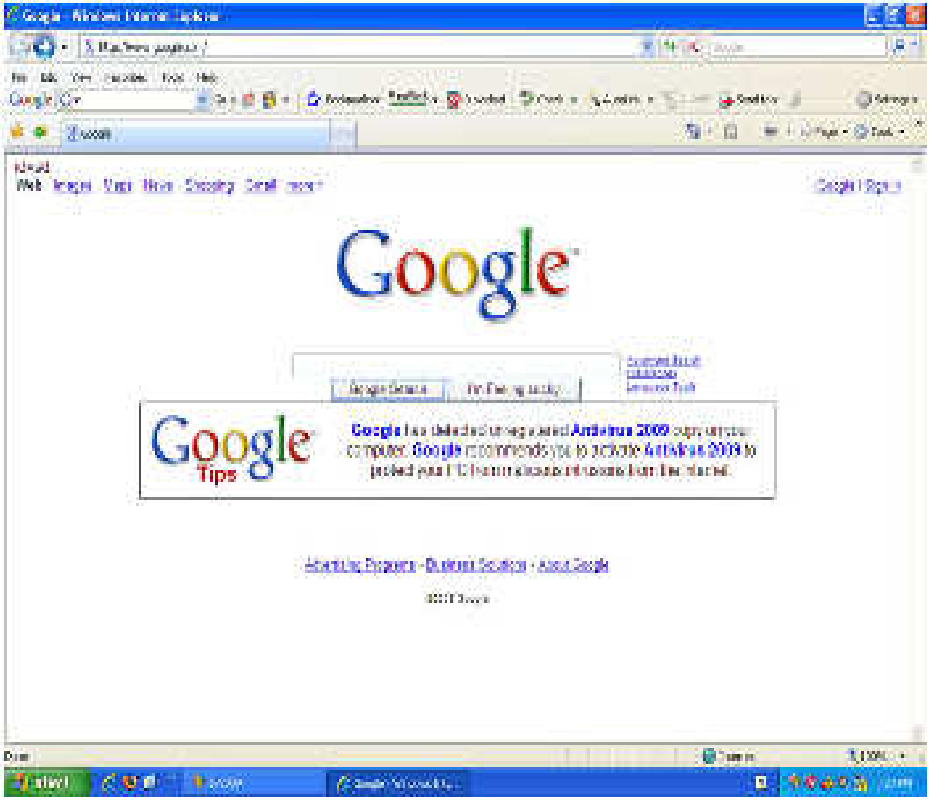
Microsoft is suing certain 'dealers' of these fake programs.

Warning: do not hit enter…

Screen showing a fake version
of a legitimate Windows error message

Counterfeit anti-virus software – how it works

- Provides links and 'redirectors' to counterfeit product sites by 'tricking' web search engines
- Encourages visitors to click on warning or flashing messages (free! free!)
- User installs software, which immediately detects a 'problem' that can only be removed by purchasing a full licence
- Even Google's home page can be altered…



'Google tips' shown on the search engine's home page, encouraging the user to purchase the fake anti-virus software

Counterfeit anti-virus software – how it works

The user pays 40 euros. His or her problems have just begun…

The program continues to annoy the user, whose bank account is debited several times

Recurring links to dishonest hosts are found (discussed further on)

Counterfeit network hardware

Example of counterfeit CISCO hardware

- Large-scale production of CISCO hardware in China
- Sold by dealers known to purchasers
- Even large U.S. clients – why not European as well?
- Feb. 2008: 'Cisco Raider': $76m worth of hardware in over 400 seizures
- Concerns are being voiced not only as to the quality but the integrity of this hardware

Dishonest hosts

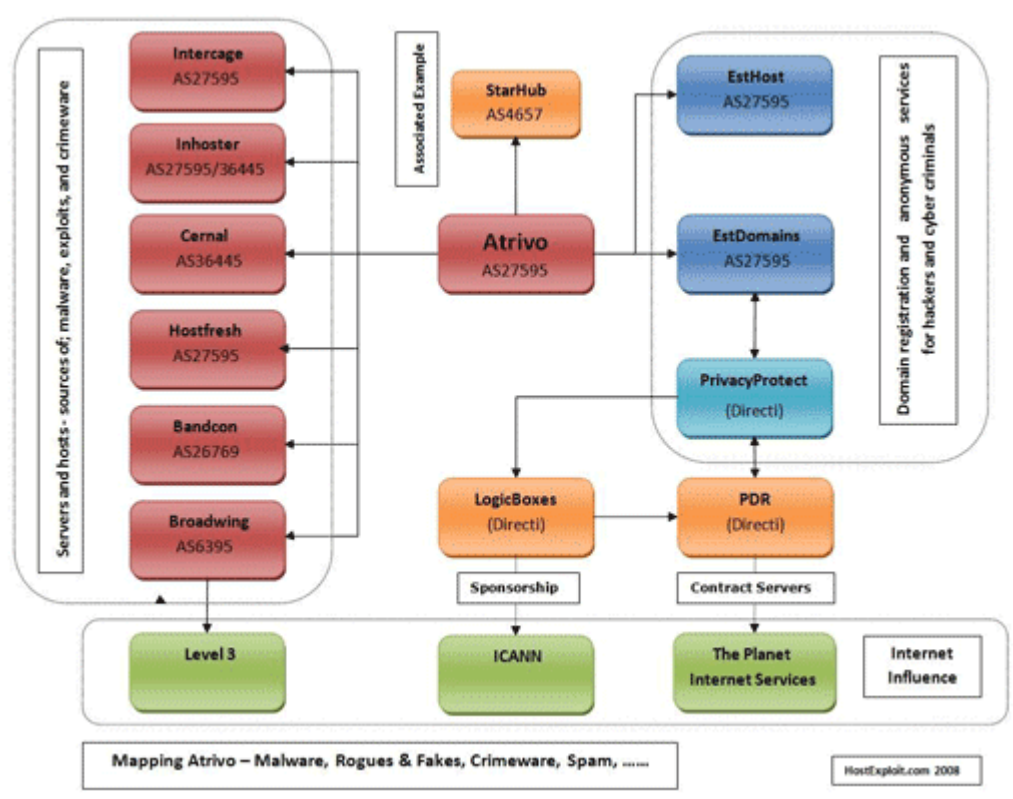
Previously considered a way of safeguarding free expression

Used to host illegal activities, send spam, control botnets

After the Russian Business Network was put to sleep in 2007, dishonest hosts still made their mark in 2008

A new way to fight them involves mobilizing certain actors on the Net…

Atrivo



Known for years as a host for a wide variety of illicit activities

Linked to several other entities to reinforce the system

Forced to 'shut down' in September 2008, but activities continue on the Internet

(Jart Armin)

McColo

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 th
wrinkle that I haven't seen before.

After my machine got infected, it wen
send SPAM?" test that Bots do - ie, the
the test domain is also hosted by McC

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

Above you see Srizbi sending a blank r
208.72.168.85. A quick 'dig' of bestyo
explaination is that Srizbi wanted to s
to a domain that was controlled by the
there's no need for it to try and possib

After it does the SPAM test, you can s
headers to take away identifyable info

POST /r/A1412B-12F1E6-A55215 HTTI
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.

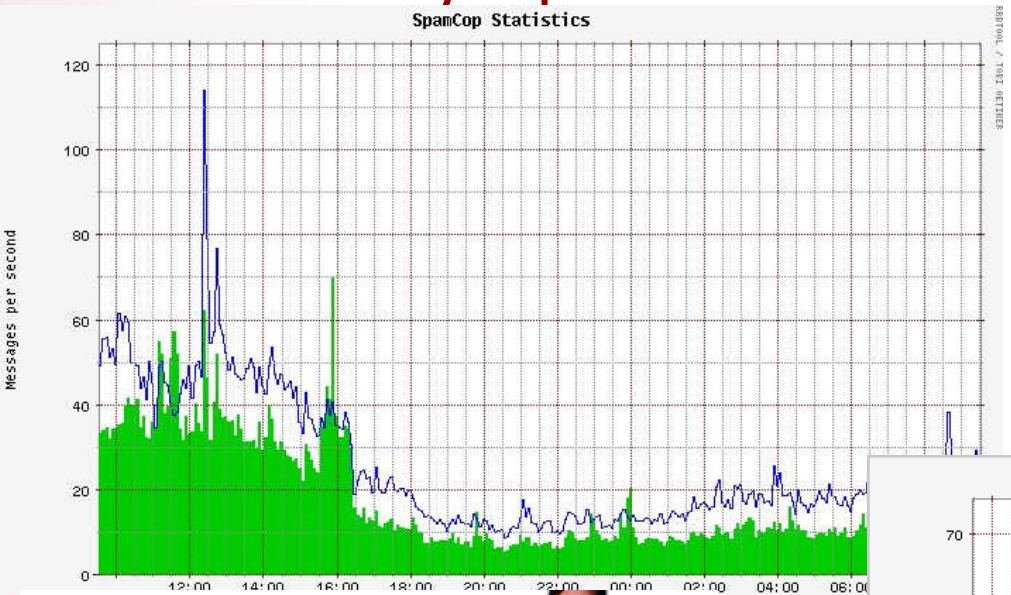
Strange mailing address for a host!

Articles about McColo

CLUSIF

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

McColo – Only a part of the solution



SECURITY FIX

Brian Krebs on Computer Security

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

Retail Fraud Rates Plummeted the Night McColo Went Offline

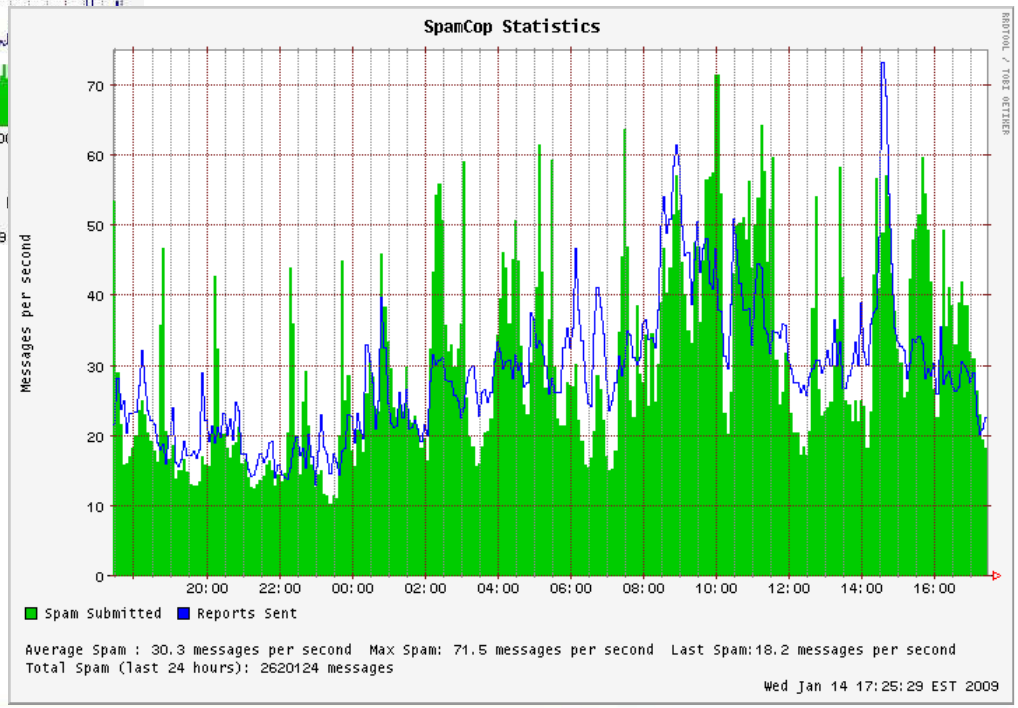
One month after the shutdown of hosting provider McColo Corp., spam volumes are nearly back to the levels seen prior to the company's take down by its upstream Internet providers. But according to one noted fraud expert, spam wasn't the only thing that may have been routed through the Silicon Valley based host: New evidence found that retail fraud dropped significantly on the same day.

It is unclear whether the decrease in retail fraud is related to the McColo situation, but in speaking with **Ori Eisen**, founder of 41st Parameter, he said close to a quarter of a million dollars worth of fraudulent charges that

Top left: Spamcop statistics the day of the takedown

Bottom left: Article on the effects of the takedown on credit card fraud

Below: Recent Spamcop statistics



McColo – Was it the right solution?

Was an investigation underway? Should there have been one? Yes, probably, to collect evidence on site – although this hosting service provider's existence seems ephemeral.

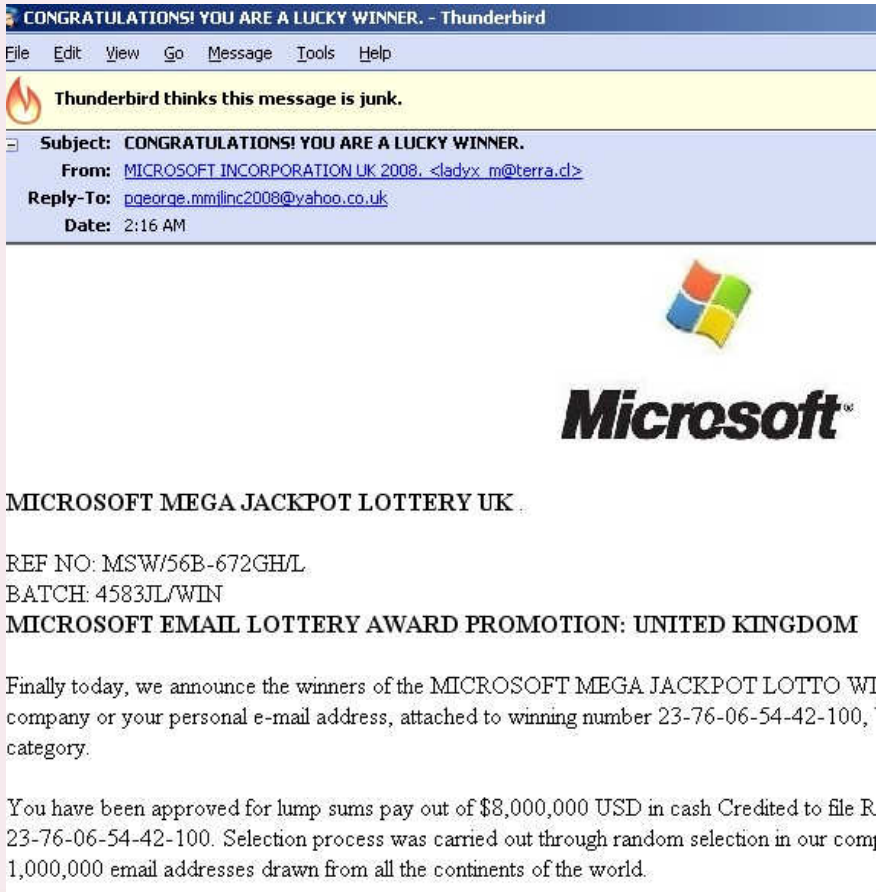
Short-term effects → a sustained and massive campaign by Internet professionals against these practices is necessary – goes against Net neutrality principles. What to do next?

Coordinated police, judicial and professional action seems necessary

Fake lottery scams (2007 in review)

Still a problem:

http://www.consumerfraudreporting.org/lotteryscamnames.php



CONGRATULATIONS! YOU ARE A LUCKY WINNER. - Thunderbird

File Edit View Go Message Tools Help

Thunderbird thinks this message is junk.

Subject: CONGRATULATIONS! YOU ARE A LUCKY WINNER.
From: MICROSOFT INCORPORATION UK 2008. <ladyx_m@terra.cl>
Reply-To: pgeorge.mmjlinc2008@yahoo.co.uk
Date: 2:16 AM

Microsoft

MICROSOFT MEGA JACKPOT LOTTERY UK .

REF NO: MSW/56B-672GH/L
BATCH: 4583JL/WIN
MICROSOFT EMAIL LOTTERY AWARD PROMOTION: UNITED KINGDOM

Finally today, we announce the winners of the MICROSOFT MEGA JACKPOT LOTTO WI company or your personal e-mail address, attached to winning number 23-76-06-54-42-100, category.

You have been approved for lump sums pay out of $8,000,000 USD in cash Credited to file R 23-76-06-54-42-100. Selection process was carried out through random selection in our com 1,000,000 email addresses drawn from all the continents of the world.

Examples of fake lottery spam

CERTIFICAT GAGNANT
TOMBOLA
COCA-COLA

Ceci est pour certifier que la somme de cent Mille Euros (100.000) appartenant à la COCA-COLA COMPAGNIE constitue une donation a [redacted] lauréate de la TOMBOLA internationale COCA-COLA COMPAGNIE exécutée en AFRIQUE et en EUROPE portant le numéro du code d'identification 7PUY2006 / BT 12052006720.

LE CONTEXTE IMPLIQUE

(1)QUE LES DITS FONDS NE PROVIENNENT PAS DU FAIT DE LA VENTE DE DROGUES DURES C'EST-A-DIRE COCAINE, HEROINE, OPIUM OU D'AUTRES DROGUES (MEDICAMENTS) LIEES.

(2)LES FONDS MENTIONNES CI-DESSUS NE SONT ISSUS D'UN BLANCHISSEMENT D'ARGENT OU PEUVENT ETRE COMME ISSUS D'UN SABOTAGE ECONOMIQUE

(3)COMME MENTIONNE CES FONDS NE SONT PAS D'ORIGINE ET SANS CONSEQUENCES !

Par conséquent, moi MAITRE KOUASSI WILLIAMS principal du Cabinet Williams à Abidjan reconnait Mme ISABELLE MOURIER comme bénéficiaire avantageux de ces fonds de Cent Mille Euros (100.000) et déclarons par le présent certificat que les informations mentionnées ci-dessus sont correctes et ceci dans le respect des règles et des lois en vigueur.

Le cabinet de MAITRE KOUASSI WILLIAMS se tient responsable de l'exactitude des informations ci-dessus mentionnées.

Cette attestation est signée sous la supervision de MAITRE KOUASSI WILLIAMS pour le Ministère de la Justice.

COCA-COLA COMPAGNIE
ISABELLE MOURIER

prends la vie côté Coca-Cola

Fake lottery scams

Winners must pay to receive their money, of course ☺

Industry players are beginning to mobilize

To report fake lotteries (and other scams) (in French): https://www.internet-signalement.gouv.fr/

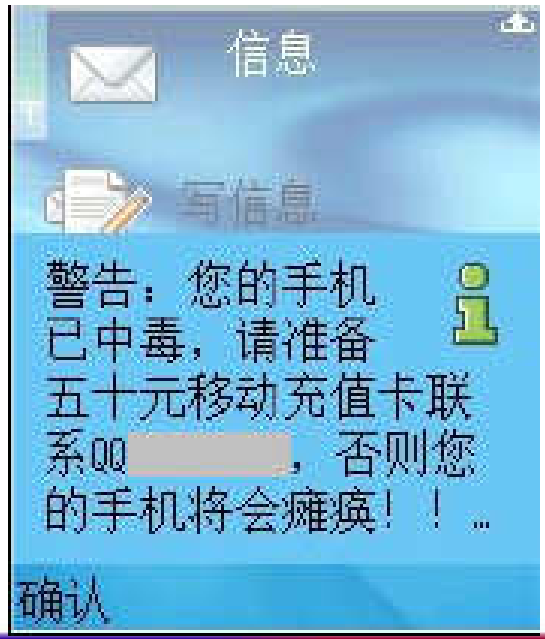
Ransomware: Chinese worm targets GSM phones

Imagine turning on your phone to find the following message: prepare a recharge card of 10 euros, or I will be paralysed.

This is what happened to Chinese subscribers. The Kiazha.A worm is spread via MMS or

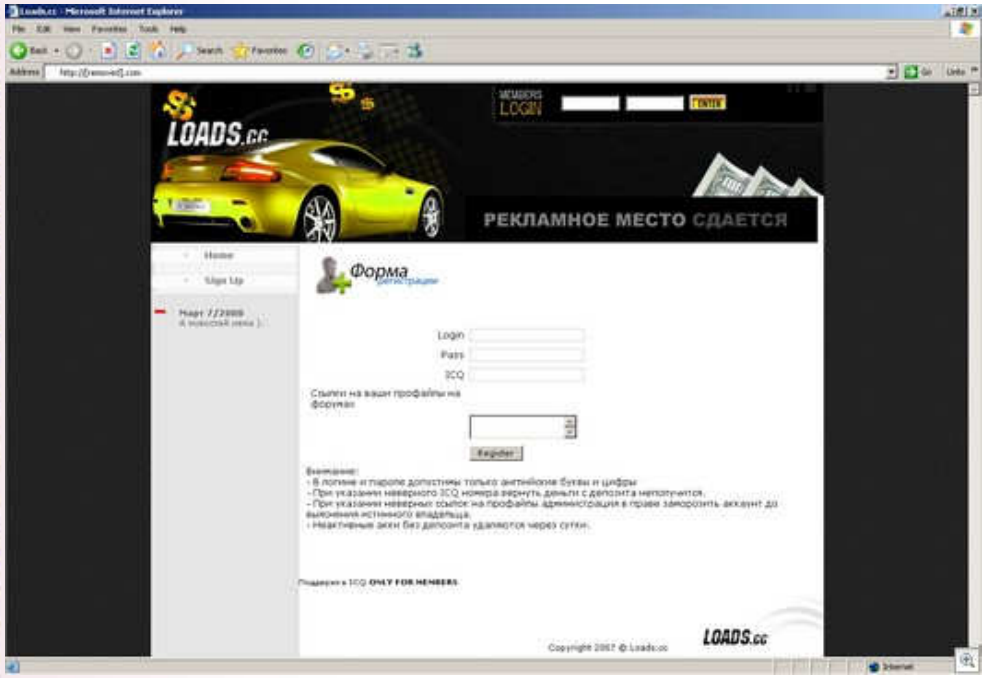
BlueTooth and uses a game network that communicates via SMS.

Profit, profit and more profit…



Screenshot of the Kiazha.A worm

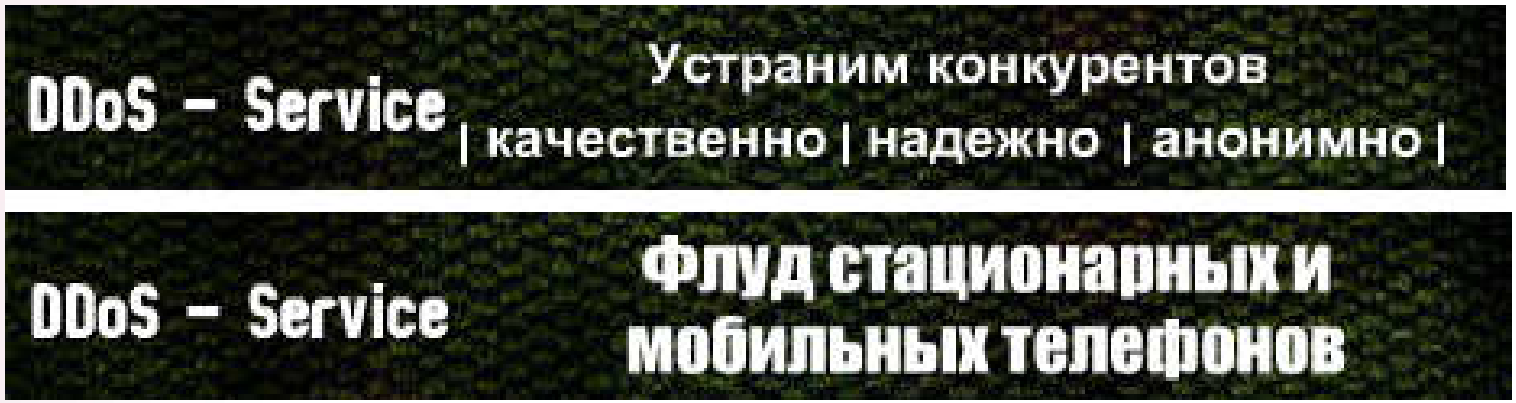
Online sale of criminal services



Loads.cc homepage in January 2008

One group, selling the services of its botnet (Loads.cc) was the target of DNS attacks… by competitors.

Online sale of criminal services



Banner ads for DDoS attack 'rental'

"Will eliminate competition: high-quality, reliable, anonymous."
"Flooding of stationary and mobile phones."
"Pleasant prices: 24-hours start at $80. Regular clients receive significant discounts."
"Complete paralysis of your competitor/foe."

Concealment – by 'accident'

piratage

Nouveau coup de filet des gendarmes dans le milieu « warez »

Une quinzaine de personnes, suspectées d'intrusions sur des serveurs d'entreprises à des fins de piratage, ont été interpellées.

Philippe Crouzillacq, 01net., le 21/11/2008 à 18h20

partager sur Viadeo | écrire à l'auteur | imprimer l'article | envoyer par mail | forum > 50 avis

L'enquête ouverte en septembre 2006 par la brigade de gendarmerie de Paris-Exelmans a abouti mardi matin à l'interpellation dans toute la France d'une quinzaine de personnes, d'une moyenne d'âge de 30 ans.

Elles sont suspectées *« d'intrusion dans des systèmes automatisés de données »* , c'est-à-dire de s'être introduites dans des serveurs d'entreprises à des fins de diffusion sauvage et illégale de contenus culturels.

No PC is immune (especially in the case of botnets), and 'warez' are the 'coolest' type of content…

Concealment – by 'accident'

Different techniques:

While the term 'Pubstro ' may sound amusing, it refers to a computer taken over by someone else for the purpose of illegal content distribution.

In the case of a botnet, the person's machine simply relays information (phishing, spam, child pornography…)

Occurs following a technical error from a host (misdirected DNS query)

Problems caused by 'accidental' concealment

Cluttered resources, loss of data and valuable time, security of other data weakened…

Pubstros attract police attention

Image problems

Unfortunately, there are likely dozens of new victims.

Webography (1/2)

CISCO

http://www.abovetopsecret.com/forum/thread350381/pg1

http://www.informationweek.com/news/personal_tech/showArticle.jhtml?articleID=206901053

Fake anti-viruses

http://garwarner.blogspot.com/2008/12/more-than-1-million-ways-to-infect-your.html

http://www.heise-online.co.uk/security/Rogue-anti-virus-products--/features/112231

http://www.heise-online.co.uk/news/Washington-and-Microsoft-sue-fake-anti-spyware-vendors--/111644

ATRIVO

http://hostexploit.com/downloads/Atrivo%20white%20paper%20090308ad.pdf

Webography (2/2)

McColo

http://hostexploit.com/downloads/Hostexploit%20Cyber%20Crime%20USA%20v%202.0%201108.pdf

Lottery scams

http://www.microsoft.com/france/securite/lottery/default.mspx

https://www.internet-signalement.gouv.fr/

GSM viruses

http://www.avertlabs.com/research/blog/index.php/2008/03/04/crimeware-goes-mobile/

Counterfeiting (pubstros)

http://www.01net.com/editorial/396899/nouveau-coup-de-filet-des-gendarmes-dans-le-milieu-warez-/

http://www.01net.com/editorial/382842/arrestation-de-trois-gros-pourvoyeurs-de-films-pirates/

Overview 2008

- Web 2.0 and social networking: further evidence of threats…
- Hardware security and network trust
  Spreading problem of chip hacking
  Internet routing: errors, fraud, opportunities…
- Organized crime in the digital world
- **Media hype and unexploited security flaws: how real are the threats?**
- From internal sabotage to attacks on infrastructure security

Presentation outline

- Media hype
- Information security and the media
- DNS flaw
- TCP flaw
- Examples of hype

… Nevertheless, real flaws did occur in 2008!

Media hype

Definition

- Pejorative term referring to disproportionately concentrated media coverage of a certain topic
- A similar term is "media circus" = an event considered as being overmediatized in light of its actual importance
- These terms are critical of media manipulation that is used:
  - ☞ to distract public attention from other facts/events
  - ☞ for commercial gain
- Internet = amplifier

Information security and the media

A welcome combination

Period in which ignorance (or worse, misinformation) dominated

Over the last 7 years or so:

- ☞ Real demand for information from the public
- ☞ Growing media interest in ISS
- ☞ Journalists are increasingly better informed, specialized and have a critical approach
- ☞ High-quality media content and formats

Information security and the media

A welcome combination

Why?

- Computer fraud is no longer an epiphenomenon: mafia...
- Massive, spectacular attacks with serious effects on the economy have occurred in the past
- Complex attacks are appearing which affect the general public

Information security and the media

A welcome combination

The fight against obscurantism and clichés

Excellent prevention and information tool for the general public

- Also an excellent prevention and information tool for business IT users
- Good practices, pragmatism – shows companies that security doesn't just involve gadgets and anti-virus software
- Primary tool against attacks that exploit unsuspecting users

Information security and the media

Blunders, sensationalism, media hype?

- DNS flaw
- TCP flaw
- Examples of buzz

DNS flaw

DNS spoofing: making a DNS entry point to a different IP address

Real flaw – problem related to how DNS works

Attacker responds before the valid DNS server

Affects web navigation, sending of external e-mails, VPN connections, etc.

These attacks require several underlying conditions to work

Announced in June without any explanation, details published by mistake in July, Black Hat Security Conference in August

Patching the DNS flaw is important for DNS admins

DNS flaw

- Game between conference organizers and those who uncover vulnerabilities
  - Self-promotion for Dan Kaminsky
  - Promotion of the Black Hat Conference
  - Headline-grabbing articles for months

TCP flaw

- Sockstress denial of service attacks on all TCP/IP stacks, including Windows
- Announcement in September: Internet is dead
- Explanation expected at T2 Conference in Helsinki, but none was given
- So big it's growing everywhere
- Still waiting for information and yet people don't stop talking about it
- Big publicity for a little-known information security conference

TCP flaw

Profiteers

Fake SNMP flaw

- Has always existed

```
Hello Folks,

We have become aware of a distributed refraction denial of service
vulnerability in SNMP. A discription of the issue is below and a proof of
concept code is at the bottom of this message. We would appreciate your help
in determining the validity and effectiveness of this issue. Any feedback you
may have would be very helpful.

According the party that has reported this issue:

"79 byte request gets a 56680 byte return. Thats an amplification of 717 times
based on my computer. Other computers may give slightly more or less.

The core problem with UDP is its simple to spoof depending on network
configuration.  This is true with most ISP's. Another factor is that UDP rfc
limits replys by 1514 bytes. Which means that it must fragment the reply.
Adding to the effectiveness since the ethernet and udp headers must be
repeated each time."


This information is not yet public, please do not publicly disclose this
information.

We are tracking this matter as VU#453707, please include this unique tracking
number in the subject line of any further email messages we exchange on this
topic
.  Please let us know if you have any questions, comments, feedback, etc.

Thanks.
Chris Taschner
------------------------------
CERT Vulnerability Analyst
+1 412-268-7090
http://www.cert.org
```

Examples of hype

- Black Monday for computer viruses
  - Announced by many anti-virus software publishers
    - ☞ Differing dates
    - ☞ Absolutely nothing happened
- MD5 hack on P2P networks
  - Blackhat Europe
  - Nothing new, fake numbers, but useful for fake CAs
- Elcomsoft
  - Frequent announcements of brute-force attacks on various algorithms – cracking WPA
  - Released software with GPU support for MD5 hashes, although it performs 2 to 3 times slower than others

Real flaws

There have been real flaws however in 2008

- Not always well understood
- Not reported as they should be by the press
- Examples
  - Mifare classic for physical security
  - PKI, certificates and MD5: (trust issues)
  - Certain evaluations by Microsoft
  - Opinions about client-side problems

Real flaws

Microsoft example: MS08-067

- Remote execution – all systems up to Windows 2003 Service Pack 2
- Potential for anonymous and effective exploit
- Word got out on specialized sites
- But not on general interest sites (as with previous patches)
- Treated in the same way as previous Microsoft flaws by the press
- No explanation of its impacts across systems
- Several successful worm exploits as a result of this vulnerability

Real flaws

- Client-side flaws
  - Flash, Internet Explorer, etc.
  - Make client-side attacks very easy, by simply visiting a website
  - Rarely reported in the press
  - Potentially devastating effects of client-side attacks
    - ☞ Goes beyond infections from downloading and running malicious .exe files

Webography

DNS flaw / Kaminsky

- http://www.wired.com/techbiz/people/magazine/16-12/ff_kaminsky?currentPage=1
- http://www.hsc-news.com/archives/2008/000346.html

TCP flaw / T2 Conference

- http://www.ossir.org/windows/supports/2008/2008-11-04/OSSIR-20081104-v0.1.pdf
- http://www.t2.fi/conference/

Examples of hype

- MD5 hack: http://sid.rstack.org/blog/index.php/282-casser-du-md5-avec-classe-ou-pas
- Benchmark MD5: http://3.14.by/en/read/md5_benchmark
- Black Monday: http://seclists.org/isn/2008/Nov/0063.html

Overview 2008

- Web 2.0 and social networking: further evidence of threats…
- Hardware security and network trust
  Spreading problem of chip hacking
  Internet routing: errors, fraud, opportunities…
- Organized crime in the digital world
- Media hype and unexploited security flaws: how real are the threats?
- **From internal sabotage to attacks on infrastructure security**

Case study: sabotage by network administrator

San Francisco (July): The city's network administrator is fired for insubordination. Before leaving, he locks up the new network containing nearly 60 % of all local government data and creates a new administrator password for himself alone.

The ex-employee is arrested. He first gives false information, then refuses to reveal the real password!

The mayor contacts experts in Silicon Valley and at Cisco. The data remains inaccessible for weeks…

Case study: sabotage by network administrator

New Jersey (November): a pension fund decides to fire a dozen people…including the network administrator. After parting with the company, the ex-employee sends a series of e-mails – initially to voice his discontent with the lay-off agreement, then to announce that he has installed several *backdoors* and will alert the media after his attack.

Aside from police action, the company had to overhaul its internal and remote access protocol, install log analysis tools, limit user access rights and privileges, and call in a response team after the incident.

Case study: payment terminal fraud

New England (March): Hannaford, a grocery store chain, discovers a credit card data breach.

Around 4.2 million numbers were hacked (card number, expiry date, but not the cardholder name). The information obtained was then sent overseas. The breach began in December. 300 servers were affected, in stores in Florida (106), New England (165) and in franchises (24).

Case study: payment terminal fraud

Consequences:

1,800 proven cases of fraud over the course of March

Re-issuing fees for approx. 100,000 cards

$5 million class action suit led by a law firm

Millions of dollars invested in security: encryption of data in transit, 24-hour monitoring system

Hannaford compliant with the PCI standard… which was quickly modified to account for the operating mode!

Case study: data theft and ransom demand

- Illustrates the dramatic growth and volume of personal data theft
- Data can be accidentally leaked, but reports show that this accidentally leaked data can also be used to fraudulent ends (ransom requests), or be obtained via intrusion with threats of exposing it (the sale in Hamburg, for example, of 21 million card numbers for €12 million.)
- St. Louis, November: Express Scripts, a company which manages medical prescription information, is blackmailed via e-mail. The writer of the e-mail threatens to release 75 patient files. Information on millions of patients is stored in the database. (# 50)
- The ransom amount is not disclosed to the public

Case study: data theft and ransom demand

Consequences:

Creation of a crisis website to inform patients and manage complaints

Identity restoration services offered by consultant/security firm, commitment to pay for any monetary losses

Use of an investigation firm

$1 million reward offered to help catch the blackmail artists!

Infrastructure: cutting of undersea cables

Mediterranean sea, Egyptian coast (February): two undersea Internet cables are *accidentally* cut. India is affected, and data must be re-routed via cables in Asia-Pacific. Two ships are inspected.

In the following weeks, a 'wave' of other cuts are played up by the media, including unexplainable cuts in the Middle East and United Arab Emirates.

22 December: 3 cables are cut between Sicily and Tunisia – the cause is unknown. State of telephone traffic: Maldives : 100 % down, India: 82 % down, Qatar: 73 % down, Djibouti: 71 % down, United Arab Emirates: 68 % down, Zambia: 62 % down, Saudi Arabia: 55 % down, etc.

Infrastructure : cutting of undersea cables

Because incidents occurred in such a short space of time, conspiracy theories emerge... Other sources believe the events are statistically normal.

One objective fact is the damage – in certain cases severe, but of short duration – to telecommunications.

This also demonstrates the risk of sabotage and the feasability of this type of attack.

Infrastructure: *malware* in hospitals

London (November): 3 hospitals in London disconnect their IT network for at least two days after an accidental virus outbreak caused by the Mytob worm (the first strain of which appeared in 2005). The worm is believed to have entered the system via NHSmail, a system used by one million staff members. The worm installs a backdoor that allows unauthorized remote access (spyware).

Over 5,000 PCs were exposed…

Consequences:

Arriving ambulances were diverted.

Officials say patients suffered no bodily harm.

Infrastructure: *malware* in hospitals

St. Cloud (U.S.) (March): computer programmer found guilty of placing a logic bomb in a computer-based training program for hospital staff. No damage, except the cost of restoring the program.

Walter Reed (U.S.) (June): a file containing personal (but not medical) data on 1,000 patients is leaked via a P2P application. The file is discovered by a data mining company doing research for a client.

Infrastructure: derailing a streetcar

Lodz (Poland) (January): a 14 year-old derails four streetcar vehicles after taking control of the command and control system. His actions caused several incidents (derailments, emergency stops) by changing signals at the last minute. 12 people were slightly injured in another 'accident'.

The operating mode required studying the system at length to understand how it worked. The teen then built an infrared remote control.

Infrastructure: derailing a streetcar

The 'makeshift' material used (Source: telegraph.co.uk)

Webography

http://www.theregister.co.uk/2008/07/16/sf_sysadmin/

http://www.computerworld.com/action/article.do?command=printArticleBasic&taxonomyName=Security&articleId=9119792&taxonomyId=17

http://www.itworld.com/legal/57799/sysadmin-under-house-arrest-blackmailing-finance-company

http://www.theregister.co.uk/2008/03/18/hannaford_data_breach/

http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=109&STORY=/www/story/03-19-2008/0004777355&EDATE=

http://www.foxnews.com/printer_friendly_wires/2008Apr22/0,4675,HannafordSecurityBreach,00.html

http://www.theregister.co.uk/2008/11/13/express_scripts_extortion/

http://www.arabianbusiness.com/510132-internet-problems-continue-with-fourth-cable-break?ln=en

http://www.arabianbusiness.com/510232-flag-plays-down-net-blackout-conspiracy-theories?ln=en

http://www.pcinpact.com/actu/news/48031-rupture-cable-ralentit-web-asiatique.htm

http://www.networkworld.com/news/2008/111908-british-hospitals-hit-with-malware.html?fsrc=rss-security

http://www.startribune.com/local/16839951.html

http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=211201106

http://www.theregister.co.uk/2008/01/11/tram_hack/

To conclude, we would have also liked to look at:

Georgia: Hacktivism or offensive information battle?

Warblogs and mobblogs: manipulation, misinformation

Eco-terrorism and the Internet