



Cybercrime Exposures in a new Digital Society

4th ICTET week

ADDIS ABABA - June, 2011

*To show variety of cyber-risks, knowing that once aware of them you
can mitigate impact using tools and re-organized work*



Pascal LOINTIER
President of Clusif
pascal.lointier@clusif.asso.fr

CLUSIF: *Committed to information security*

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

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

Sharing information

Exchanges among officially recognized experts, collective know-how, document database

Develop its positioning

Feedback, increased visibility, Directory of Offering Members

Anticipate trends

The “network”, inform offering members of expectations

Promote IS security



Logo for site web, flyers, commercial ads...

Join...

Working group dynamics

Free documentation Translations (in English, German...)

Public stands taken on issues and consultation responses

Forums for ongoing exchange: MEHARI, threats, CISO

Les groupes actifs en 2011

- Documentation de MEHARI™
- EFIS (Evaluation Financière des Incidents de Sécurité)
- Fiches de sécurité pour la micro-informatique
- Gestion de clés cryptographiques
- Gestion des incidents
- Glossaire
- Guide d'audit de sécurité physique
- PA-DSS
- Panorama de la cybercriminalité
- PCI-DSS
- Principes, mécanismes et bases de connaissances de Méhari
- Sécurité des Applications Web - Suite
- Sécurité des Outils de Communication
- Série 27000
- Virtualisation et Sécurité

Regional initiatives and international joint effort



CLUSI Côte d'Ivoire

Boite Postale 2409 Abidjan 25

Contact : M. KOUAKOU Clauba Jean de la Croix (Président)
 Tel/Fax : (00225) 22 42 42 66
 Secrétariat : contact@clusici.org
 Web : <http://www.clusici.org/>



Club de la Sécurité de l'Information Région Tahiti

Adresse physique : Immeuble SALMON Faa'a Pamatāi - Tahiti - Polynésie Française
 Adresse postale : B.P. 60123 - Hotuarea - 98704 Faa'a - Tahiti - Polynésie Française
 Contact : Matthieu DRUILHE, clusir.tahiti@gmail.com, téléphone : +689 79 82 27
 Site web : <http://www.clusif.asso.fr/clusir-tahiti/>



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

954, avenue Jean Mermoz
 34000 MONTPELLIER
 Contact : Christian FERRAND
 Site web : www.clusir-lr.info



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

S/C INSA
 Département de Génie Electrique et Informatique
 135, Avenue de Rangueil
 31077 TOULOUSE CEDEX 04
 Contact : Laurent PELUD
 Site web : www.clusir-mp.asso.fr



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

16, rue de Pont-à-Mousson
 57000 METZ
 Contact : Thierry RAMARD
 Site web : www.clusir-est.fr



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

500, rue de Paradis
 13008 MARSEILLE
 Contact : Claude LELOUSTRE
 Site web : <http://www.clusif.fr/clusir-paca/>



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

SITIV
 Passage de l'Avenir
 69200 VENISSIEUX
 Contact : Yannick BOUCHET
 Site web : www.clusir-rha.fr



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

1862, avenue Général De Gaulle
 59910 BONDUES
 Contact : Gérard MOLINES
 Site web : <http://www.clusif.fr/clusir-npp/>



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

Technopole Venise Verte
 Rue Euclide
 BP 8421
 79024 NIORT cedex 9
 Contact : Sébastien Gioria
 Site web : <http://www.clusir-poi.fr/>



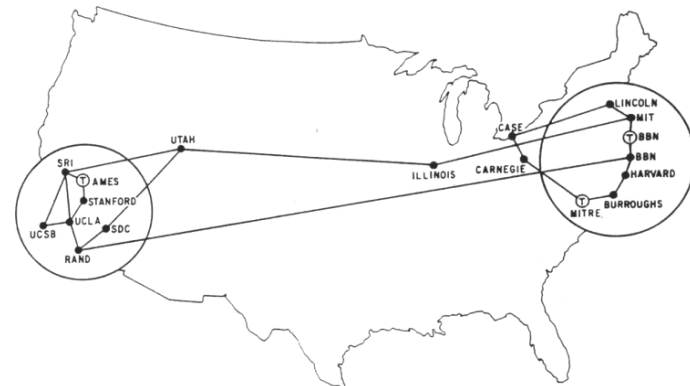
Club de la Sécurité de l'Information Région Aquitaine

s/c Philippe Marty (Vice-Président)
 51 rue Manon Cormier
 33000 Bordeaux
 Contact : Marc Ferrigno

Two legacies... a third new issue

Internet is a cold war solution for military communications

- ✓ Mail authentication
- ✓ Website authentication



MAP 4 September 1971

... nowadays, digital profile and/or avatar

- ☞ An identity which is plural, fragmented, for fun, timeless



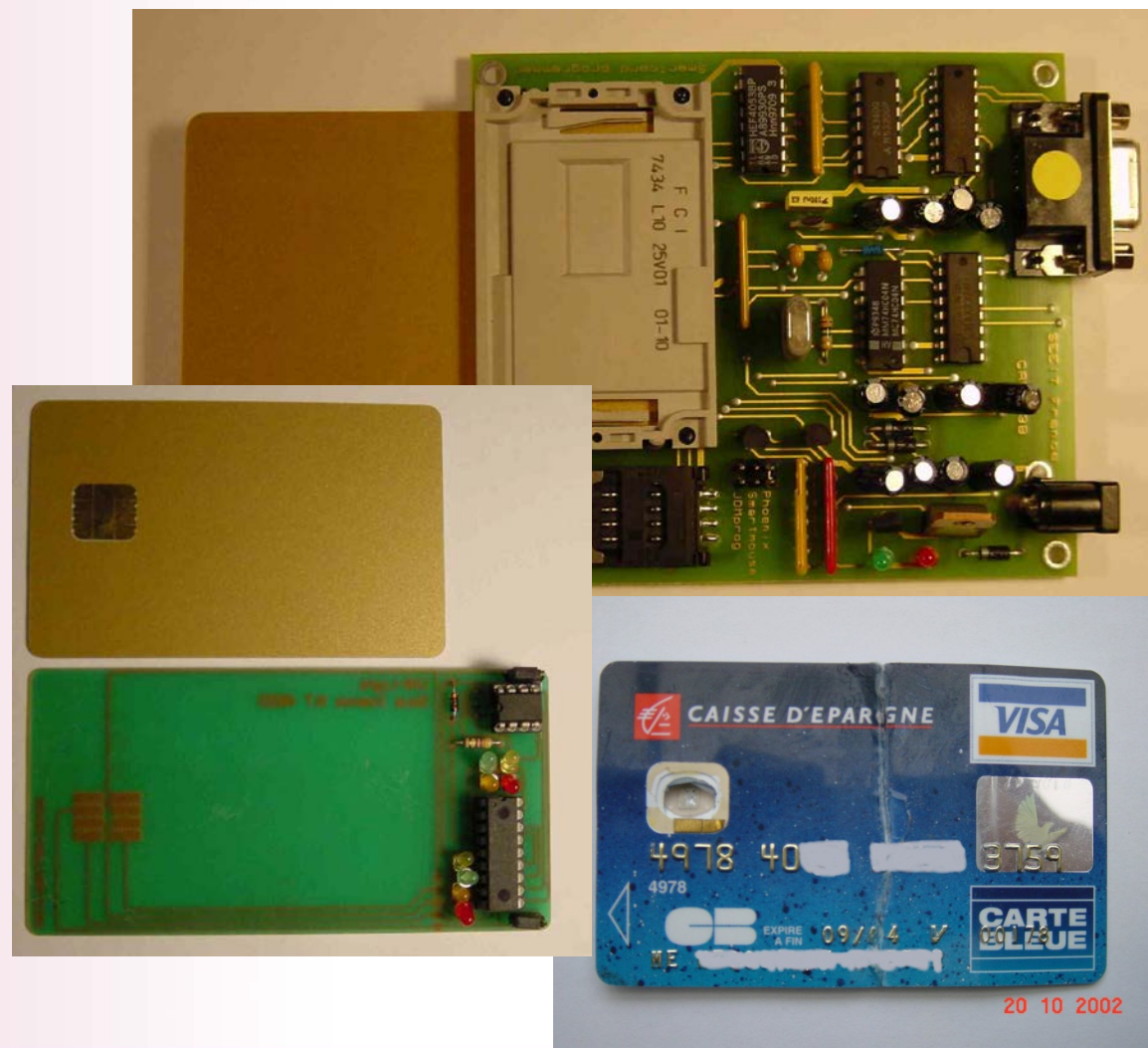
Agenda:

Based on Cybercrime Overviews (including webography)

To put into perspective

- ⊕ **Modus Operandi: professionalized, commercialized, sophisticated**
 - ⊕ From skimming to compromised ATM networks
 - ⊕ Viruses to make profit
 - ⊕ Marketing of malware
- ⊕ **Actors: Cyberterrorism (?), Infowar, Hacktivism**
- ⊕ **Exposures:**
 - ☞ Infrastructures, from SCADA to Data centers globalization
 - ☞ Facility Management over IP
 - ☞ Social Networks, from Usenet to a 5th Power ?

2000 (and cont'd), yescarding



Skimming and criminal organizations



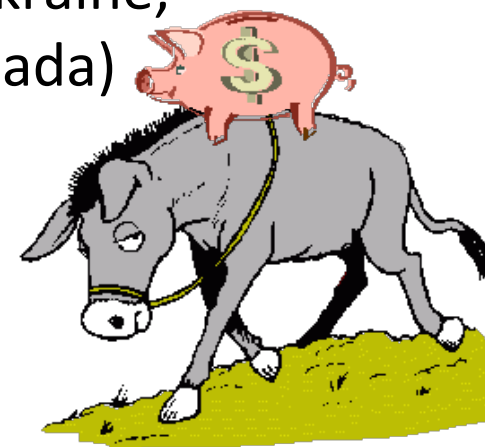
Massive theft of bank card numbers: RBS Worldpay scam

RBS Worldpay: U.S. subsidiary of Royal Bank of Scotland

9 million dollars in fraudulent withdrawals (end 2008):

- With cloned cards
- In a short space of time
- From 2,100 cash machines
- In 280 cities, 8 countries (U.S., Russia, Ukraine, Estonia, Italy, Hong Kong, Japan and Canada)

Highly-organized network of mules



New threats involving ATMs: Cash machines in Eastern Europe compromised

In March 2009, Sophos identifies first malware specifically designed for cash machine

In May 2009, security experts at Trustwave confirm the discovery

This malware was designed for a specific brand
and model of ATM

Inspections were carried out to repair infected machines: Eastern Europe (Russia, Ukraine) mainly affected

Patch developed by the industry

Virus to make profit: Bugbear virus in 2003

W32/BUGBEAR.B@MM

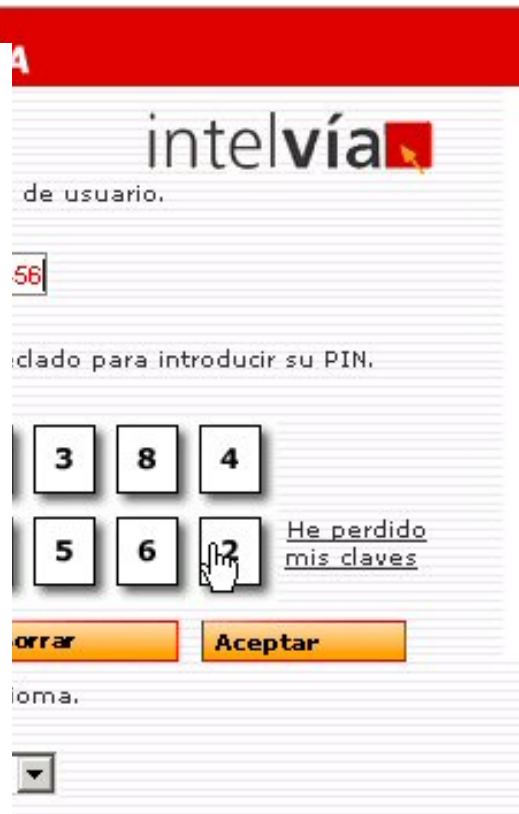
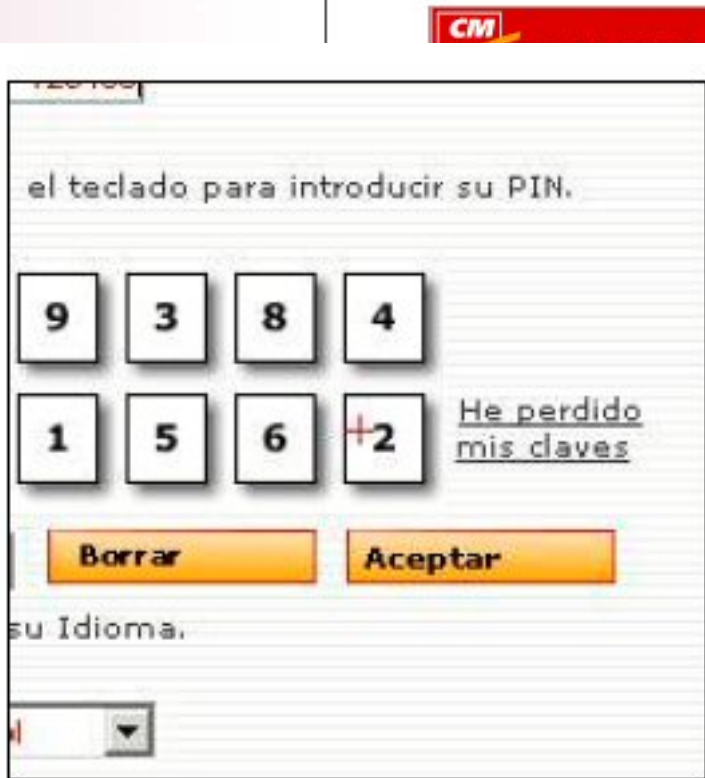
- ✓ The virus contains an EXTENSIVE list of banking domain names (France, Britain, Germany, Australia, Italy, Greece, Denmark, New Zealand, Spain, Brazil, Romania, Poland, Argentina, Switzerland, Finland, Taiwan, Turkey, Iceland, Slovakia, South Korea, United States, South Africa, The Baltic Republics, Austria, Hungary, Norway, the Czech Republic).
- ✓ When the machine boots up, if it belongs to one of the target domains, the registry key responsible for the automatic telephone dialing process is deactivated.
- ✓ The virus looks for passwords in the cache memory and sends them to a pre-defined address chosen at random from a list.
- ✓ Once the task has been completed, the virus restores the registry key.

banquepopulaire.fr
bics.fr
bpic.fr
bpnord.fr
bred.fr
ca-alpesprovence.fr
ca-alsace-vosges.fr
ca-midi.fr
ca-normand.fr ccbonline.com
ccf.fr
cin.fr
covefi.fr
cpr.fr
credit-agricole.fr
credit-du-nord.fr
credityonnais.fr
creditmutuel.fr
-epargne.fr
eurocardmastercard.tm.fr
nxbp.fr
smc.fr
transat.tm.fr

2006, Anserin (Trojan) and Virtual Keyboards

A number of virtual keyboards are already vulnerable.
New versions of Anserin know how to hack into 562 predetermined bank sites.

Cajamurcia - Intelvía - Su Banca en Internet - Microsoft Internet Exp



By doing the same to all strings, we see the trojan monitors the following websites:

- ARGENTINA**
- Banco Hipotecario (www.bancopio.com.ar)
 - Banco de La Pampa (www.blo.com.ar)
 - Banco de la Provincia de Buenos Aires (www.bapra.com.ar)
 - Banco Credicop Coop. Ltda. (www.credicop.com.ar)
 - Banco Ciudad de Buenos Aires (www.bancociudad.com.ar)
 - Banco Nacional del Litoral (www.bnl.com.ar)
 - AEN AMRO Argentina (www.amro.com.ar)
 - Banco Itali del Buen Ayre (www.itali.com.ar)
 - Banco Patagonia (www.bancopatagonia.com.ar)
 - Banco Micro Banco (www.bancomicro.com.ar)
 - BankBoston (www.bankboston.com.ar)
 - Banco FID (www.bancofid.com.ar)
 - Banco Comafi (www.comafi.com.ar)
 - Banco del Chubut (www.bancodelchubut.com.ar)

- BOLIVIA**
- Banco Ganadero (www.bancogad.com.bo)
 - Banco BISA (www.bisa.com)
 - Banco de Crédito de Bolivia (www.bancodcreditobol.com.bo)
 - Banco Santa Cruz (www.bsc.com.bo)
 - Banco Solidario (www.bancosolidario.com.bo)
 - Banco Central de Bolivia (www.bcb.gov.bo)

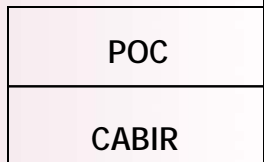
- BRAZIL**
- Caixa Econômica Federal (www.caixa.gov.br)
 - Banriul (www.banriul.com.br)
 - Banco de Estado de Santa Catarina (www.besc.com.br)
 - Santander Banesto (www.santander.com.br)
 - Banco do Brasil (bb.com.br)
 - Banparaná (www.banparana.com.br)
 - e-fim (efim.com.br)
 - Citibank Brasil (www.citibank.com.br/citibank)

- CAPE VERDE**
- Banco de Cabo Verde (www.bcv.cv)

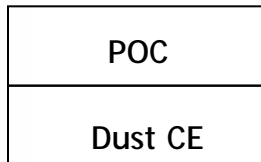
- SPAIN**
- Banca March (www.bancamarch.es)
 - Barceja (www.barceja.es)
 - BIVA (www.bivaf.es)
 - Fibanc (www.fibanc.es)
 - Banco de Valencia (www.banval.es)
 - Banesto (www.banesto.es)
 - Banco Financía Sónitoc (www.banfin.es)
 - Banco Espírito Santo (www.banesp.com)
 - Banco Casters (www.bancocasters.com)
 - Banco Gallego (www.bancogallego.es)
 - Banco Gulpuzcoano (www.bancogulpuzcoano.es)
 - Banco Urquijo (www.bancourquijo.es)
 - Iberdrola (www.iberdrola.es)
 - Banco Popular (www.bancopopular.com)
 - Banesto (www.banesto.es)
 - Bankia (www.bankia.es)
 - Bansecar (www.bansecar.es)
 - Santander Central Hispano (www.santander.com)
 - BBK (www.bbk.es)
 - Caixa Laietana (www.caixa.com)
 - Caja Castilla La Mancha (www.cajalcm.com)
 - Caja de Extremadura (www.cajaextremadura.es)
 - Caja Granada (www.caja-granada.es)
 - Caja Girona (www.cajagir.com)
 - Caja Murcia (www.cajamurcia.es)

2005, Cell phone virus evolution

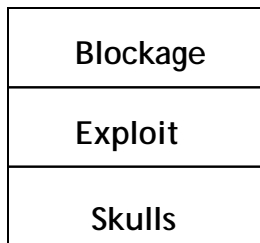
- The first on Symbian
- No payload
- Bluetooth distribution



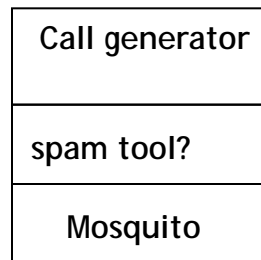
- The first on Win CE
- No payload
- Downloaded via com services



- Action: multiple skull icons
- Action: blocks new updates
- Downloadable in newsgroups
- Targets Symbian series 60

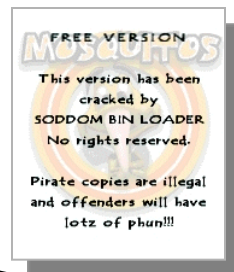
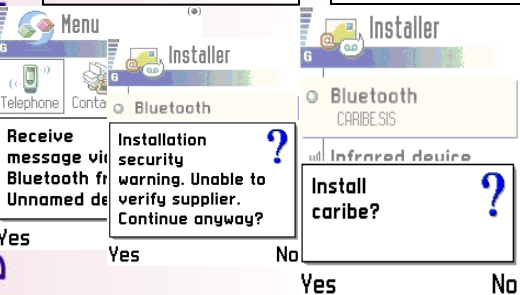


- Action: makes calls at overly expensive rates
- Downloadable in newsgroups
- Targets Symbian series 60



From 30 Dec 2004 to 11 Jan 2005

- Publication of the Cabir Source Code
- Variant D of Skulls, which carries Cabir: infection via file and bluetooth
- Lasco virus/worm. Infection via file and bluetooth
- http://news.zdnet.com/2100-1009_22-5520003.html?tag=defaul
- ...



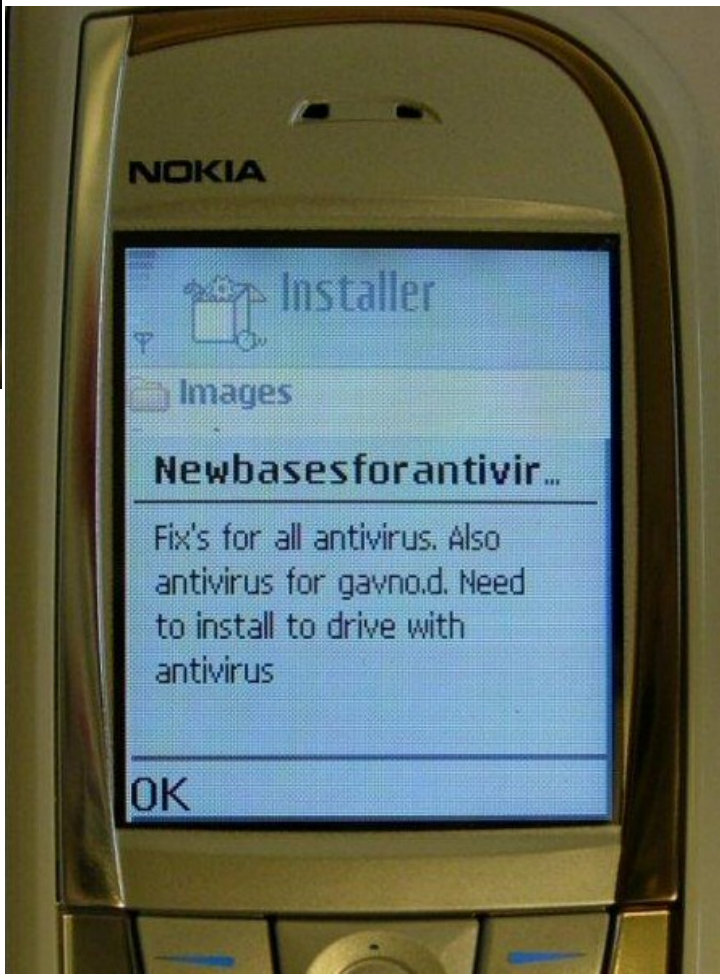
15 June 2004

15 June 2004

Late 2004

Early 2005

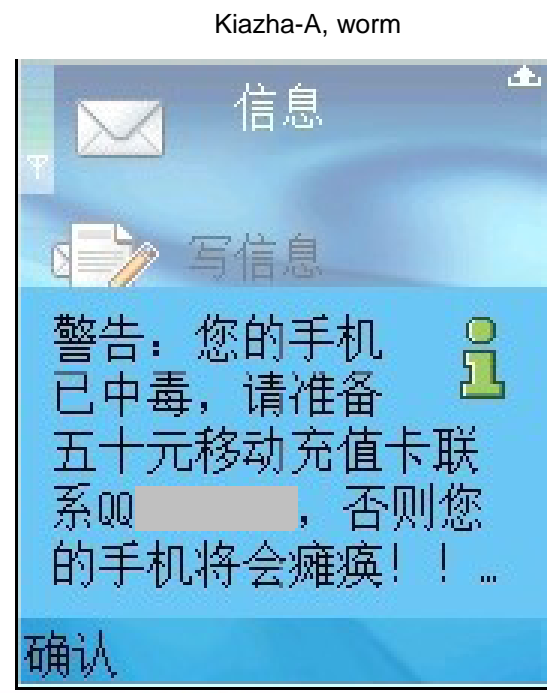
From PoC to real money



05/2007, \$M\$ Trojan :
Viver, high rate calls
(1 to \$10)

01/2008: Kiazha

01/2009: Yxe.A in China,
Indonesia



2003, new hi-tech opportunities for espionage

The hard disks of photocopiers

December 2003 : a Norwegian company specializing in data retrieval published a report which underscored the vulnerability of information stored on copiers and multifunctional machines. The affair began when a dishonest employee retrieved information from a digital copier and passed it on to a competing company. Copiers are increasingly vulnerable. Even so, different solutions are available : removable disks, deletion of data (not overwrite) after photocopying or digitization, use of proprietary algorithms (but not necessarily encryption...) etc.

The importance of Trojan horses

Michaël and Ruth Haephrati

- ✓ Discovered in 2005, the swindle lasted more more than a year.
- ✓ Each target was the subject of an attack through a single Trojan horse created for this reason.
- ✓ The antivirus was ineffective (at the time of the facts) because the program did not circulate on the web.
- ✓ The Trojan horse was sent by e-mail or was integrated into CD containing an imaginary commercial proposal .
- ✓ Once installed, and in exchange for 3000€, the originator provided to his customer an IP address, the user name and a password so that they could access the PC of the victim.

18 Arrested In Israeli Probe Of Computer Espionage

By Glenn Frankel
 Washington Post Foreign Service
 Tuesday, May 31, 2005; Page E01

JERUSALEM, May 30 -- Israel's business sector has been rocked by a major computer espionage scandal that was uncovered when a husband-and-wife book-writing team complained to police that someone had hacked into their computer system and stolen files.

Police said investigators traced the alleged theft to the wife's former son-in-law, a computer programmer, and determined that he had also sold copies of so-called Trojan horse software to private detectives, who used it to spy for corporate clients on competing firms.

Last week, police arrested 16 people in Israel, including senior executives of some of the country's leading high-tech companies and the private investigators they had allegedly employed. At the same time, British authorities, acting on an Israeli request, arrested the former son-in-law and his wife in London and are holding them



Michael Haephrati, 41, and his wife, Ruth Erier-Haephrati, 28, shown in an undated photo, were arrested in London. (Haaretz Daily

Physical Keyloggers Commercially available

BBC NEWS

[UK version](#)
[International version](#)
[About the versions](#)
[Low gr](#)

Last Updated: Thursday, 17 March, 2005, 13:39 GMT

[E-mail this to a friend](#)
[Printable version](#)

UK police foil massive bank theft

Police in London say they have foiled one of the biggest attempted bank thefts in Britain.

The plan was to steal £220m (\$423m) from the London offices of the Japanese bank Sumitomo Mitsui.



Yeron Bolondi was arrested for money laundering and deception

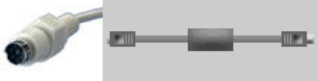
Computer experts are believed to have tried to transfer the money electronically after hacking into the bank's systems.

A man has been arrested by police in Israel after the plot was uncovered by the National Hi-Tech Crime Unit.

Unit members worked closely with Israeli police.


The investigation was started last October after it was discovered that computer hackers had gained access to Sumitomo Mitsui bank's computer system in London.

External KeyGhost Models (PS/2 External Plug-in Cable Type)



External KeyGhost Home Edition (128,000 Keystroke Capacity)	\$89
External KeyGhost Std (500,000+ Keystroke Capacity)	\$99
External KeyGhost Pro (1,000,000+ Keystroke Capacity)	\$149
External KeyGhost Pro SE (2,000,000+ Keystroke Capacity)	\$199

KeyGhost USB Keylogger External Units - (USB Plug-in Cable Type)



NEW! KeyGhost USB Keylogger 128KB - 30cm (short cable) (World's first USB keylogger. Compatible with both Mac and PC systems. 128,000+ Keystroke Capacity)	\$199	<input type="text" value="0"/>
NEW! KeyGhost USB Keylogger 128KB - 120cm (long cable) (World's first USB keylogger. Compatible with both Mac and PC systems. 128,000+ Keystroke Capacity)	\$199	<input type="text" value="0"/>



features

- Quick install



BEFORE



AFTER

Spyphones, GSM jammers...

Find in

Include title and description

Related Searches: [cell spy](#), [cell spy software](#), [spy phone](#), [cell phone spy](#)

Refine search

Categories

- Computers & Networking (11)
 - Software (11)
- Everything Else (8)
 - Information Products (6)
 - Other (2)
- Cell Phones & PDAs (7)
 - Bluetooth Accessories (6)
 - Cell Phones & Smartphones (1)
- Books (6)
 - Other (6)

See all categories

Price

\$ to \$

Condition

New
 Used
 Not specified
[Choose more...](#)

Seller

eBay Top-rated sellers
[Specify sellers...](#)

Preferences

Buying formats

Auction
 Buy It Now
 Include Store inventory
[Choose more...](#)

All items

33 results found for **spy phone software** [Save this search]

View as [Customize view]

- Bluetooth Cell Phone Spy Software
- 2009 Mobil Cell Phone Spy Software Suite
- 2010 EDITION CELL PHONE BLUETOOTH SPY
100% Original Seller - 3 FREE Bonus - 14 Day Money
[Enlarge](#)
- 2010 Spy phone software.All 4 new and older Cell
- 2010 Spy phone software.All 4 new and older Cell
- Bluetooth Cell Phone Spy Software
- SPY PHONE SOFTWARE_MAKES EVERYTHIN
SPY PHONE
- ULTIMATE BLUETOOTH MOBILE PHONE SPY :**
NOW ONLY INSTALLATION INSTRUCTIONS INCLUDED



HI-TECH REMOTE SPY SOFTWARE

REMOTE SPY

HOME FEATURES PURCHASE FAQ SUPPORT ABOUT US

FEATURES

Remote Spy Features

Remote Spy is the latest in high-tech PC surveillance software. It records all Computer and Internet activity on your own PC with our powerful yet simple-to-use Spy Software.

- Window titles
- Passwords used
- Usernames
- Chat Conversations
- Remotely Install!

Spy Software

Remotely Install No Physical Access Needed!
 Install with one Click via email!
 No Physical Member Account!
 Remotely Monitor ANY PC YOU OWN!
 Monitor how your PC is being used while away.

RECORD THE FOLLOWING:

- EMAIL CORRESPONDENCE
- CHAT CONVERSATIONS
- INSTANT MESSAGERS
- OVERALL COMPUTER ACTIVITY
- AND MUCH MORE!!!

RECORD COMPUTER ACTIVITY FROM ANYWHERE!

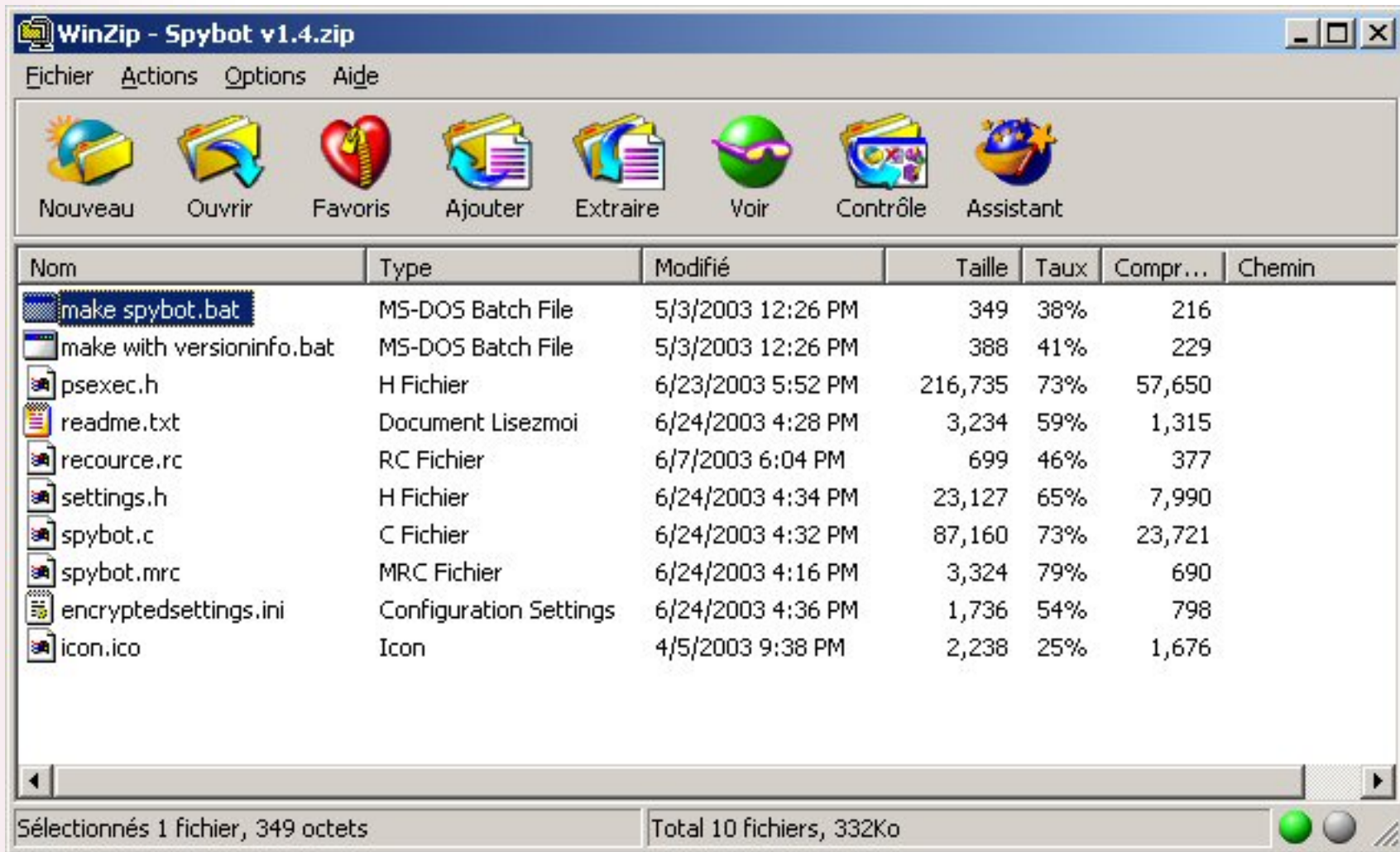
EASY TO SETUP, NO PHYSICAL INSTALLATION NEEDED!

PURCHASE REMOTESPY NOW!

[More Information](#) | [Try The RemoteSpy Demo](#)
[A Secure Order - Get Instant Access!](#)
[See What's New in the latest version](#)

EARN BIG CASH SELLING REMOTESPY
 © 2004-2008 CyberSpy Software, LLC.
 Powerful Remote Spy Software

2004, Robots... available to all.. Need to speak English!



2007, MPack, updated versions

MPack v0.90 stats

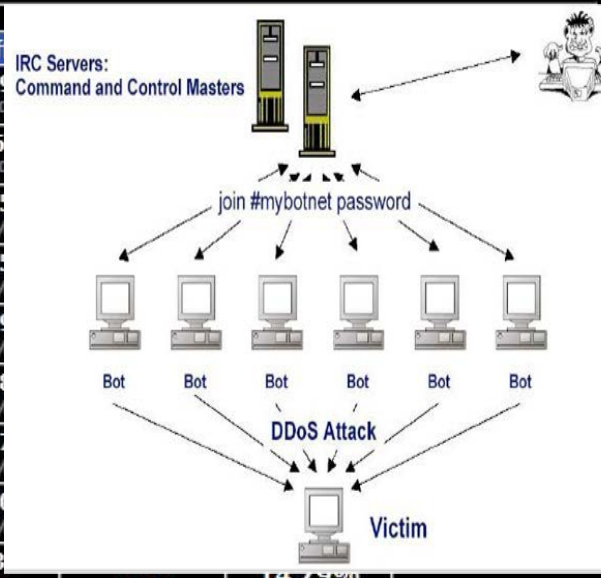
Attacked hosts (total - uniq)	
IE XP ALL	114721 - 96104
QuickTime	2175 - 2048
Win2000	7033 - 6260
Firefox	12885 - 12514
Opera7	1271 - 1264

Traffic (total - uniq)	
Total traff	159073 - 129089
Exploited	44804 - 35574
Loads count	17408 - 15968
Loader's response	38.85% - 44.89%
Efficiency 10.94% - 12.37%	

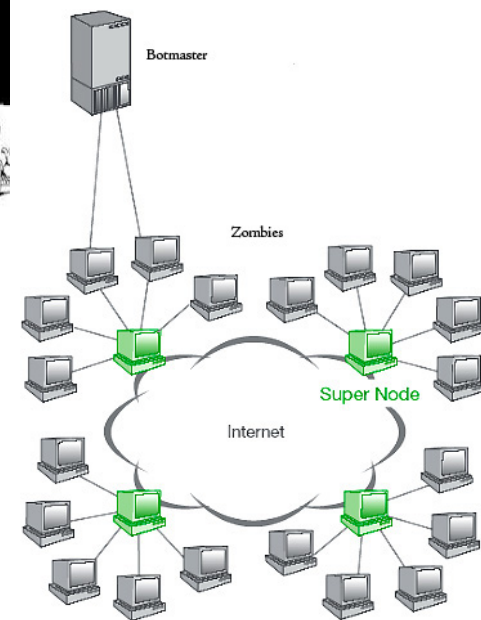
Browser stats (total)	
MSIE	4 0%
Opera	1 0%

Modules state	
Statistic type	MySQL-based
User blocking	ON
Country blocking	OFF

Country	Traffic
RU - Russian federation	11275 - 70.9%
UA - Ukraine	1666 - 10.5%
IT - Italy	704 - 4.4%
GE - Georgia	577 - 3.6%
BY - Belarus	541 - 3.4%
KZ - Kazakstan	309 - 1.9%
US - United states	111 - 0.7%
AZ - Azerbaijan	106 - 0.7%
MD - Moldova republic of	683 - 0.4%



Commercialized tool for distributed Denial of Service attacks (dDoS)



Commercial banners

INSTALLSFORYOU

InstallsForYou means reasonable prices, efficiency, reliability, and high-speed downloads in all countries.

Various packages are available for your business and there is a convenient system of discounts for large orders.

Friendly user support service will help you place your order by informing you of currently available packages and prices.

We have quite a strict 30-day system of originality, so that repeats are not only excluded, but you also get more downloads than you actually ordered.

If for any technical reason your bot/software doesn't work and we have fulfilled our obligations, the order is paid for in customary regime.

DDoS – Service | Устраним конкурентов | качественно | надежно | анонимно |

DDoS – Service | Флуд стационарных и мобильных телефонов

Agenda:

Based on Cybercrime Overviews (including webography)

To put into perspective

- ⊕ Modus Operandi: professionalized, commercialized, sophisticated
 - ⊕ From skimming to compromised ATM networks
 - ⊕ Viruses to make profit
 - ⊕ Marketing of malware
- ⊕ **Actors: Cyberterrorism (?), Infowar, Hacktivism**
- ⊕ Exposures:
 - ☞ Infrastructures, from SCADA to Data centers globalization
 - ☞ Facility Management over IP
 - ☞ Social Networks, from Usenet to a 5th Power ?

2004, Cyber-terrorism - a recurrent term for nearly 10 years

United States- the FBI: “The unlawful use of force against persons or property to intimidate or coerce a government, the civilian population or any segment thereof, in the furtherance of political or social objectives...”

The French Penal Code -Art. 321-1 “the following offenses constitute an act of terrorism when they are intentionally carried out either individually or collectively with the sole aim of causing a serious breach of the peace through intimidation or terror... »

A variety of definitions with specific consequences

Within the same state, depending on the services

Qualifying an act with the term allows for others to be disqualified... or certain police or military actions

A terrorist today may tomorrow be re-labeled a freedom fighter or liberator... or re-qualified as anonymous special forces units



Terrorism - characterizations

Terrorism can differ:

Depending on the area in question: political (separatism, liberation), social (or ethnic), cultural, religious (fundamentalism, apocalyptic)...

Depending on the goal: influence, a claim, repression, conversion, extermination, nihilism...

Empirical criteria

Sudden, unexpected, a surprise

Violence against an 'unarmed' target to terrorize...

The personal involvement of the public (potential victim)

Fear of a repeat attack

Media demands (and the implication that the State can no longer maintain public order).

Internet and ITC – how they are used

1/ A means of linking up (☑ happened already)

Electronic mail, newsgroups Usenet, cell phones, PDA, multimedia data processing and storage

2/ A means of propaganda (websites and newsgroups) (☑ happened already)

Information and support,
media relay (with increasing use of multimedia)

A weapon to discredit

A weapon to incite hatred

Anti-sites, black propaganda.

Internet and ITC – how they are used

3/ A means of financing (☑ already happened)

To raise funds

To exploit IT systems (credit cards, blackmail-extortion), money laundering etc.)

? To engage in phishing

? To access confidential personal data

☞ “Police Arrest Hacker Apparently Linked to Sardinian Anarchist Attacks”,
Corriere della Sierra, 07/01/2005

Internet and ITC – how they are used

4/ Means of direct action. What opportunities?

- ☞ Dependence on digital information
- ☞ Accidental events leading to financial, material and bodily damage
 - 💣 Shutdown of electricity-generating turbines during Y2K tests
 - 💣 Operational safety of general telecom infrastructure or ticket reservation systems
 - 💣 Unavailability of the service authorizing banking transactions
 - 💣 Loss of control of the regulating systems for a section of the gas pipeline network in Russia
 - 💣 Homicide of an individual whose life support system was computer assisted
 - 💣 Death in a recovery ward following a power outage
 - 💣 ...

2007: “Cyberwar” in Estonia or “cyber-riot”?

Internet attacks from late April to mid-May after a monument commemorating Russian soldiers (WWII) was moved.

Street demonstrations

Defacement of Web sites, DoS (denial of service) attacks against Estonian government sites and infrastructures

Government program for the development of new technologies (Estonian Information Society Strategy 2013)

Profusion of neologisms in the press and in blogs: cyberwar, world war web, etc.

Russia is accused...

2007: “Cyberwar” in Estonia or “cyber-riot”?

Mode of operation: Several waves of varying length and intensity

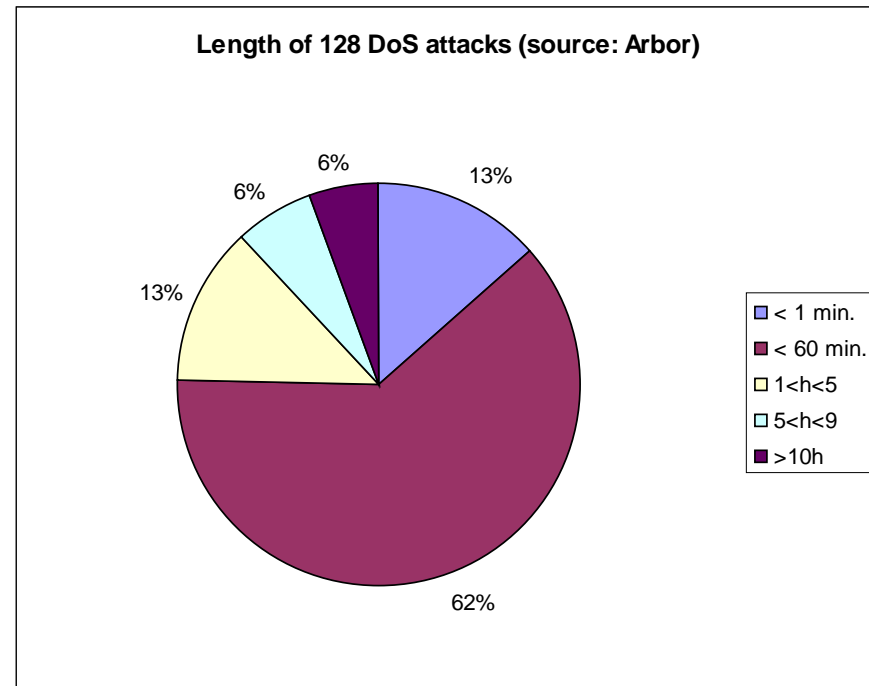
- ☞ As long as 10 heures
- ☞ An initial “emotional” reaction (April 27-29)

“Traditional” DoS attacks (ICMP and TCP-SYN flooding)

More sophisticated use of botnets during the second wave, (-> May 18)

Geographical delocalization (outside Russia)

Cyber-demonstration (violent), yes ; militarized attack (cyberwar)...Nothing established but causes a problem for the State for managing the rapid, “spontaneous” emergence of action groups on the Web, sometimes even linked-synchronized with street demonstrations. The stakes remain the sabotage of infrastructures, national and international opinions of the events....



Some comments

Beyond "hypes"

Electronic Pearl Harbor et Manhattan Cyber Project (# 1995)

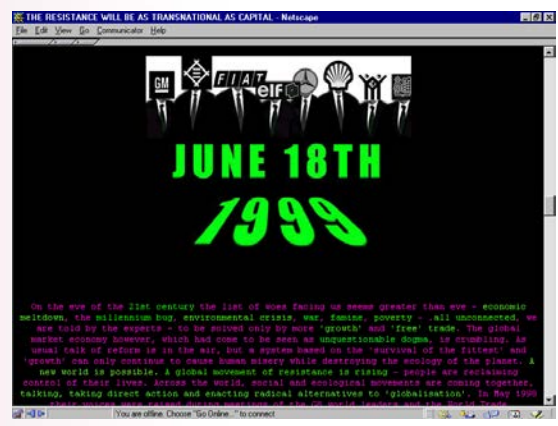
Cyberjihad (NCIS ?, 2006)

Cybergeddon (FBI & DHS, 2009)



... Political violence, hacktivism is using tools more pro-actively

👉 From G8 men to Carbon Market...



Emissions Trading: Attention about phishing email

Dear Madam or Sir,

if you received e-mails containing the request to visit a homepage via a link and to enter your user data of the registry, we ask you to not further take notice of it.

Neither the German Emissions Trading Authority (DEHSt) at the Federal Environment Agency nor the European Commission are sender of these messages. It is a so-called "phishing-attack". The made-up word "phishing" refers to the words "password" and "fishing" and can be translated as "password fishing".

Agenda:

Based on Cybercrime Overviews (including webography)

To put into perspective

- ⊕ Modus Operandi: professionalized, commercialized, sophisticated
 - ⊕ From skimming to compromised ATM networks
 - ⊕ Viruses to make profit
 - ⊕ Marketing of malware
- ⊕ Actors: Cyberterrorism (?), Infowar, Hacktivism
- ⊕ Exposures:
 - ☞ Infrastructures, from SCADA to Data centers globalization
 - ☞ Facility Management over IP
 - ☞ Social Networks, from Usenet to a 5th Power ?

2008, 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

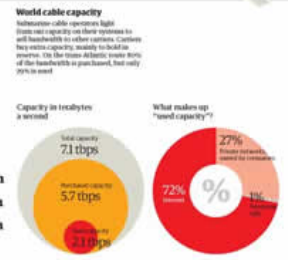
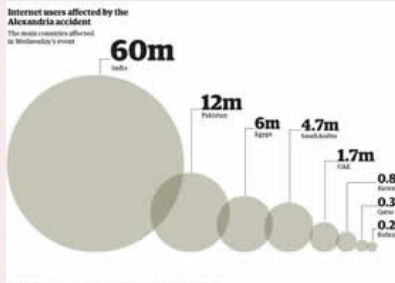
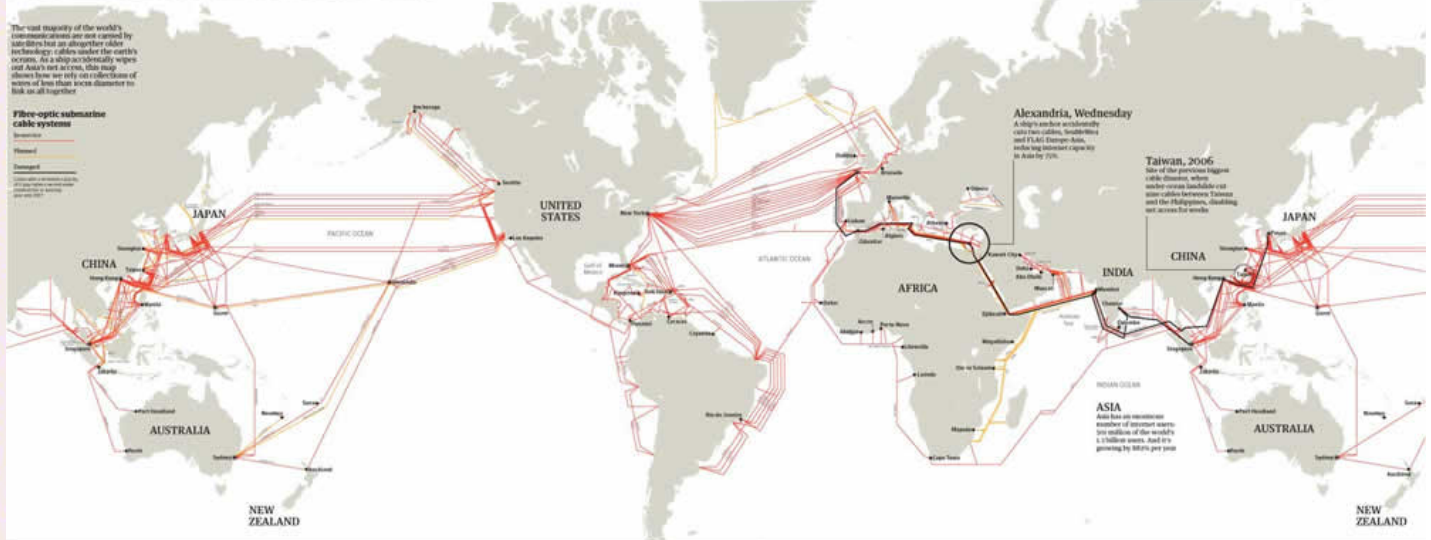
PCCW cuts Pakistan Telecom's access after the error is detected...

Accidental in this case, but potential for fraud

Accidental events

Internet is not virtual...

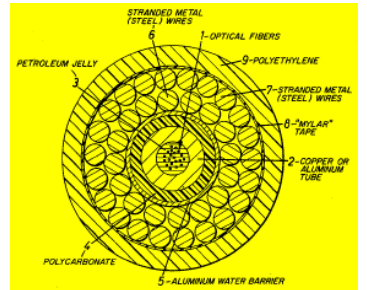
The internet's undersea world



The longest submarine cables

The cables in service from India to Germany to Europe, South Korea connects to different countries with its landing points.

Cable/Line	Length (km)
South Korea	10,000 km
China	10,000 km
USA - Europe	10,000 km
South America	10,000 km



December 22nd, 2008 : 3 cables cut between Sicilia and Tunisia, unknown cause. Voice traffic disruption - Maldives : 100 % , India : 82 % , Qatar : 73 % , Djibouti : 71 % , UAE : 68 % , - Zambia : 62 % , Saoudia : 55 % , etc.

Cloud computing, virtualization: At times, highly...unavailable!

Somewhere out there (cloud ☺) in 2009 – problems for prestigious companies: Air New Zealand, Amazon, (including EC2), Barclay's, eBay (Paypal), Google (Gmail and others), Microsoft, Overblog, Rackspace, RIM, Twitter...

- ☞ Power failures (UPS) and system crashes during reboots
- ☞ Electrical fire, destroyed backup and UPS generators, electrical switches, etc.
- ☞ Bugs in patches
- ☞ Poor router settings between two data centers
- ☞ dDoS attack on DNS resources in a specific data center

Accidental events and malevolent acts (via I.S.)

2003: Slammer worm and **Nuke site** (Ohio)

2003: Nachi worm and Diebold **ATM network**

2003: SoBig virus and **railways signaling** (Florida)

2005: Zotob worm, downtime for 13 facilities for **vehicule assembly line** (USA)

2007: Error of command and accidental contamination (hydroxide de sodium for Ph) for **drinkable water**, dozens of victims, light injuries (Michigan)

Sabotage (via I.S.)

2007: Logic bomb injected by employee into a supervisory system for **water irrigation of a dam** (California)

2007: Taking control and disrupting synchronization of **traffic lights** (California)

2007 (and 2000 in Australia): Logic sabotage via System Administrator of a **water supply system** (California)

2007: Experimental sabotage of an **electric generator** (Idaho-DHS for CNN)

2008: Taking control et **4 wagons derailed**, many injured victims (Poland)

Sabotage (via I.S.)



Poland (Lodz), 4 wagons derailed by a kid

Electric generator destruction « simulation », based on a security hole which has been patched since <http://www.cnn.com/2007/US/09/26/power.at.risk/index.html>



IP Migration

After telephones, other types of general infrastructure are migrating to IP networks:

Full migration (including transport or terminal equipment) or partial (supervision, ordering, reporting...)

Surveillance and access (doors, badge readers, cameras, motion sensors, fire/moisture detectors...)

Air conditioning, heating, furnishings (blinds)

Energy (inverters, generators...)

SCADA systems (coordination, industrial processes...)

DCPs & RTUs with Alarms & Warning Systems

[SatLink2 Transmitter/Logger](#)



- 4 Analog Input, 10 SDI-12 Sensor Interfaces
- Pocket PC & Internet Communications
- Display, Enclosure, XLite & many more options

[More »](#)

[SatLink2 - 40 Watts For Buoy Applications](#)



- Ideal for Buoy Applications
- Pocket PC Communications
- 4 Analog & 10 SDI-12 Interfaces

[More »](#)

[Xlite Datalogger 9210-XXXX Compact Version Of Xpert](#)



- 486 @ 66 MHz processor, 32 bit
- Expandable
- Scaleable
- 4 MB Standard Log **Expandable to over 1 Gigabyte**

[More »](#)

[Xpert Datalogger/Controller, 8080-XXXX](#)



- Windows CE Operating System, a 486 Processor, C++ Programming & an **INCREDIBLE NUMBER OF INPUTS**
- Digital I/Os - Unlimited
- Analog Inputs - Unlimited
- 4 MB Standard Log **Expandable to over 1 Gigabyte**

2009, SWATTING for Money

Hammond (Indiana, USA), 2009 July : beginning of trial for young hackers who were selling online video access (partyvanpranks.com) to swat action. At first, they took remote control of video surveillance



Google Search: camera linksys inurl:main.cgi

Another webcam, Linksys style.

- * inurl:"ViewerFrame?Mode=
- * intitle:Axis 2400 video server
- * intitle:"Live View / - AXIS" | inurl:view/view.shtml^
- * inurl:ViewerFrame?Mode=
- * inurl:ViewerFrame?Mode=Refresh
- * inurl:axis-cgi/jpg
- * ...

Downtown Fairburn AX
COMI

ZOOM Wide Tele

Mon Sep 14 07:40:09 2009

Select preset position:
- None -

FOCUS

IRIS

PAN Left Right

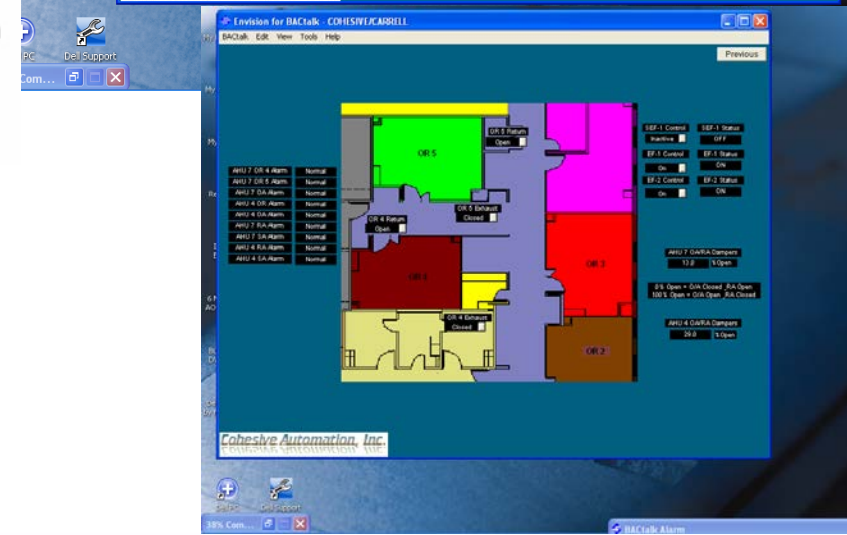
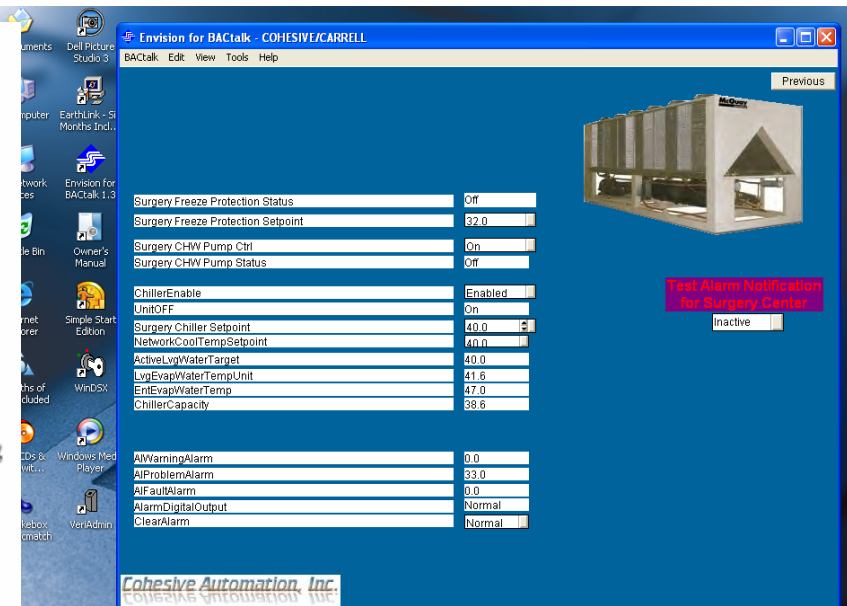
TILT
Up
 Down

2009, Hacking HVAC in Hospital

FACTS IN SUPPORT OF AFFIDAVIT

6. On 6/24/2009, The Dallas Division of the FBI was contacted by Special Agent Charles Provine of the FBI in the Jackson Division of the FBI regarding a computer intrusion of a Heating Ventilation and Air Condition (HVAC) computer system at a Dallas, TX hospital, the Carrell Clinic located at 9301 North Central Expressway, Dallas, Texas. This was believed to present a risk to health and safety as the Hospital was a facility that kept patients around the clock who could be adversely affected by the cooling if it were turned off during Texas summer weather conditions and the hospital also maintained drugs which could be adversely affected by the lack of proper cooling if the intruder were to disturb the HVAC system. SA Provine stated that he was in contact with Lieutenant (LT) Lannie Hilbolt, Texas Attorney General's office and CW-1, a network

Page 4 of 18



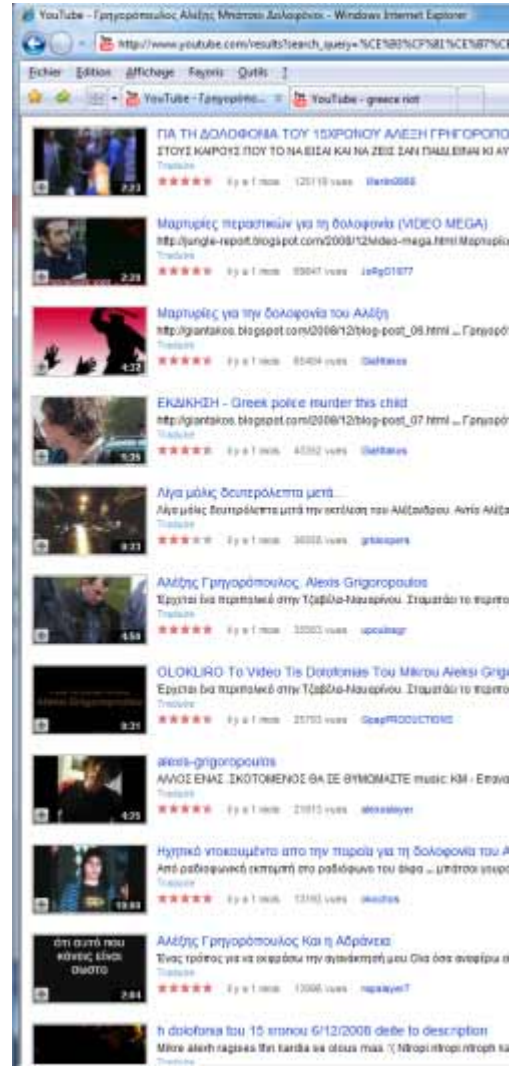
2008, Social networking– Social risks – Greece

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.



2008 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,

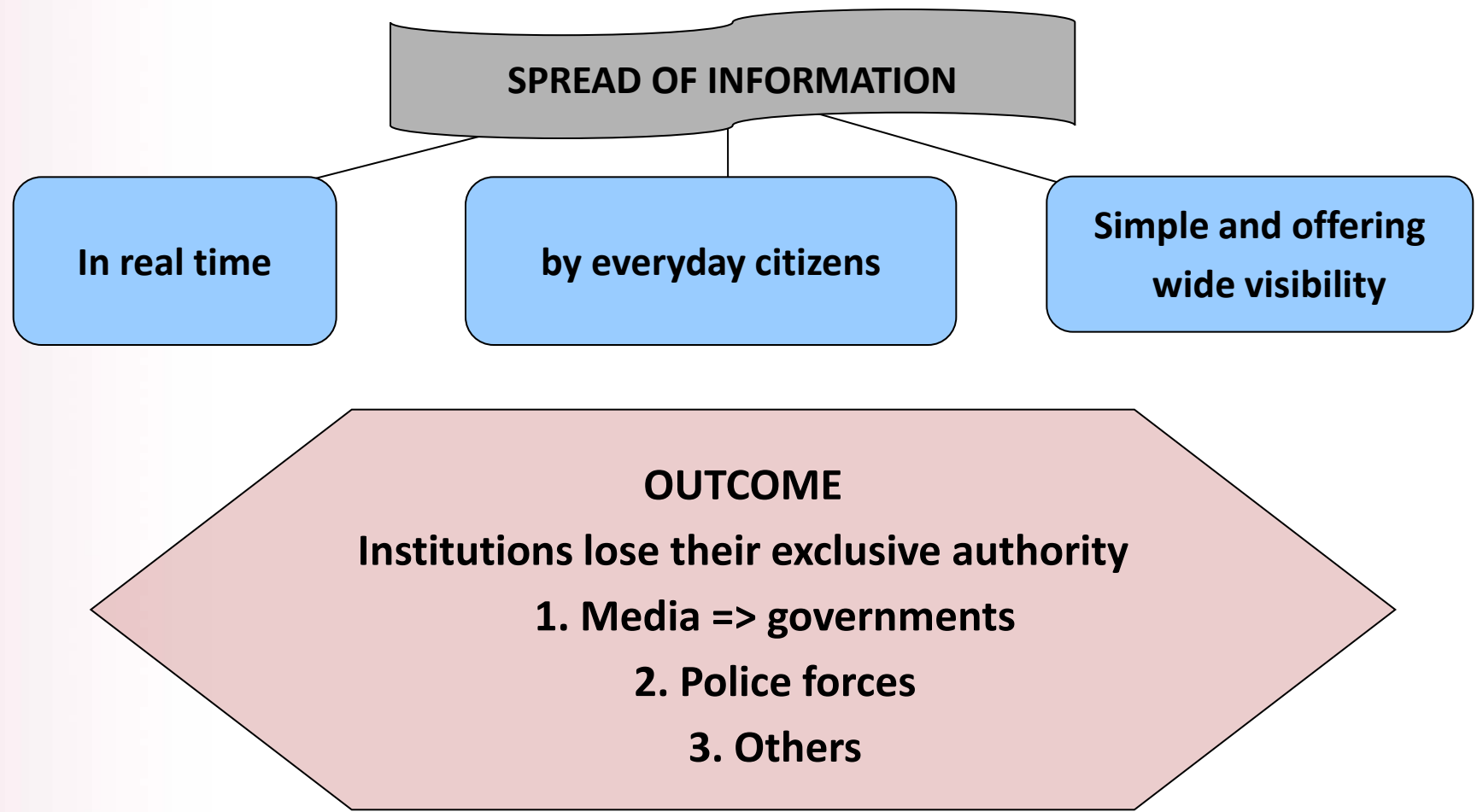
Stalking,

Bullying

Risk of non-removability



Web 2.0 – the 5th power?



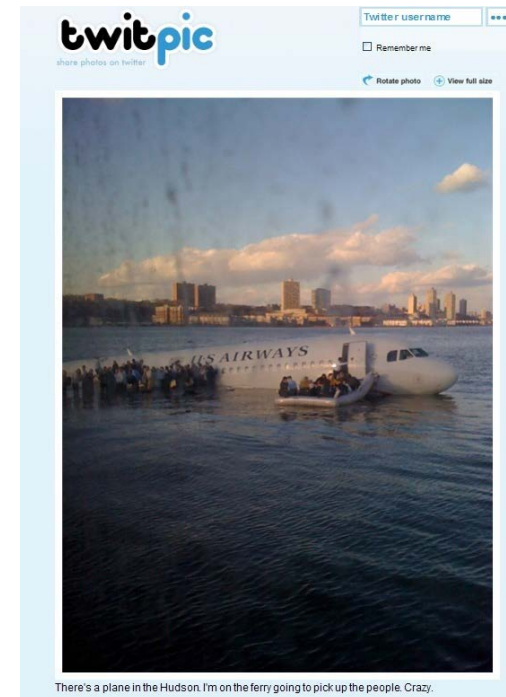
1. Competing with the media

January 2009

Perfect water landing of a US Airways aircraft in the Hudson River in New York

Minutes after the accident, Janis Krums posts her now famous tweet:

"There is a plane on the Hudson. I am on the ferry to pick up the people. Crazy."



2. Competing with police forces

Anti-pedophile activities
Perverted Justice
Wikisposure



December 2009
Live manhunt on Google Wave



China:
“Human flesh search engines”

CHINA, Monday 19 January 2009

Internet vigilantes in China defend virtual lynching

Pascale Nivelles - Beijing

They're known as “renrou sou suo”, “human flesh search engines”. They hunt down misery and injustice, even if it means subjecting their targets to public prosecution

2010 Updates...

Stuxnet targeting industrial O.S.

Botnets

Commercially based unsecurity of smartphones

Wikileaks, Anonymous, compulsory info disclosure b/o
Employees



Cybercrime Overview 2009

Paris
January 13, 2010

www.clusif.asso.fr

free downloads




- **CONFERENCES** 25 documents
("FORENSICS 2010 : Synthèse et recommandation de l'IRCGN", "FORENSICS 2010 : Perquisitions, saisies, etc. : quelques principes (Rôle de l'avocat)", "FORENSICS 2010 : Témoignage du FSSI du Ministère de la Santé", "FORENSICS 2010 : Cadre légal de la perquisition et télé-perquisition (OCLCTIC)", "PCI-DSS 2011 : Synthèse de la conférence", "PCI-DSS 2011 : Introduction", "FORENSICS 2010 : Introduction", "CIL 2010 : Les recommandations du CIL AREVA", ...)
- **CONFERENCES - INTERVENTIONS EXTERNES** 15 documents
("MEHARI 2010 : Une méthode de gestion de risques conforme à la norme ISO 27005", "Conformité : quel apport pour la sécurité, la continuité d'activité", "Smartphones : les paradoxes d'une mise en sécurité", "Cyberdéfense et guerre de l'information", "La malveillance téléphonique - Synthèse d'un groupe de travail du CLUSIF", "Gérer ses risques avec la méthode MEHARI conforme à ISO 27005", "Approche militaire des actions informatiques", "Communication et Sécurité", ...)
- **CYBER-CRIMINALITE** 21 documents
("Panorama de la Cyber-criminalité - Année 2010", "Cybercrime Overview - 2009", "Panorama de la Cyber-criminalité - Année 2009", "Cybercrime Overview - 2008", "Panorama de la Cyber-criminalité - Année 2008", "Cybercrime Overview - 2007", "Panorama de la Cyber-criminalité - Année 2007", "Cybercrime Overview - 2006", ...)
- **DOSSIERS TECHNIQUES** 29 documents
("Gestion des incidents de sécurité du système d'information", "BREVE INFO CLUSIF - PCIDSS v2.0 : quels changements ?", "Moyens de Communication Voix : Présentation et Enjeux de Sécurité", "Web application security: managing web application security risks", "PCI DSS : une présentation", "Sécurité des applications Web", "Synthèse : Chiffrement des données locales des moyens nomades", "Bots et Botnets", ...)
- **FICHES MICRO-INFORMATIQUE** 9 documents
("PHYS06 : Local technique", "PHYS05 : Equipements électriques", "PHYS04 : Câblage réseau local", "LOGI02 : Chiffrement", "LOGI01 : Contrôle d'accès (Poste de travail)", "ADMI04 : Audit et contrôle", "ADMI03 : Surveillance", "ADMI02 : Journalisation", ...)
- **GESTION DES RISQUES** 4 documents
("L'infogérance", "Risk Management - Concepts and Methods", "Gestion des risques: concepts et méthodes", "RM

Productions

- Documents en ligne
- Vidéos
- Télécharger MEHARI™
- Sinistralité
- Glossaire des menaces

Services

- Cybervictim ?
- Forum MEHARI.info
- Formation MEHARI
- Prestataires
- NOUVEAU ! Formations SSI**
- Master SSI
- Forum Stages
- CLUSIR (régions)
- CLUSI (international)
- Liens

-  [RSS/docs CLUSIF](#)
-  [RSS/actus CLUSIF](#)
-  [RSS/actus CLUSIR](#)

