



Cybercrime : a basis for cyberwar ?



"Cyberthreats – Cyberwar – Cyberdefence :
Pearl Harbor or a Death of thousand cuts ?"



Brussels, 19 November 2012

© Luc Beirens - Federal Computer Crime Unit - Direction economical and financial crime

Presentation

- **@LucBeirens**
Chief Commissioner
Head of the Federal Computer Crime Unit
Belgian Federal Judicial Police
Direction Economical and financial crime

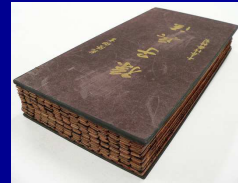


Chairman of the EU Cybercrime task force
representing the organization of heads of
national hightech crime units of the EU



War ?

- Vom Krieg - Carl **Von Clausewitz** 19th C
 - War is the continuation of *Politik* by other means => **Imposing your will to opponent**
- Antoine-Henri **Jomini** => **Occupy his territory**
- Art of War - **Sun Tzu** (500 BC)
 - Find weak points
 - Be **first** to occupy terrain
 - Use **deception** & keep **secrecy**
 - Use spies



Cybercrime threats © Belgian Federal Computer Crime Unit

Goal of my presentation

- General trends in our society
- Analysis of "ordinary" cybercrime
 - Tools and techniques / infrastructure
- Can these be the "other means" ?
- Do they allow to engage in war according Sun Tzu's art of war ?



Cybercrime threats © Belgian Federal Computer Crime Unit

General trends today

- Evolution towards **e-society**
 - replace persons by e-applications
 - Interconnecting all systems (admin, industrial, control)
 - Mobile systems – Cloud
 - Social networks => new
- **IP** is **common platform** offered by **many ISPs** integrating telephony / data / VPN & all new apps =opportunities / Achilles tendon / scattered traces
- **Poor security** in **legacy** applications and protocols (userid+pw)=> identity fraud is easy
- **Enduser** is not yet educated to act properly



First conclusions ?

- Society is thus very **heavily depending** on ICT
- ICT = **important vulnerability** of modern society
- **End user** = weakest link => biggest danger
- Need to
 - Guarantee continuity of ICT functioning
 - Availability and integrity of data
- Data is more and more **in the cloud**
 - Accessible from all over the world
 - **Outside jurisdiction** of your country



Cybercrime today



© Luc Beirens - Belgian Federal Computer Crime Unit

What do criminals want ?

- *Become **rich / powerfull** rapidly, easily, very big ROI in an illegal way if needed*
- ***Destabilize (e-)society** by causing troubles*



Cybercrime against citizens

- Creation of **false internet profiles**
- **Hacking** / abuse of internet accounts
- **Payment card** fraud (credit/debit/fuel)
 - Shouldersurfing / skimming / hacking DB
- **eBanking** fraud
- **Extortion** with data / pictures / videos



© Luc Beirens - Belgian Federal Computer Crime Unit


Cybercrime against organizations

- **Defacement** of websites
- **Hacking** of internet servers & **extortion**
- Divulging of **confidential/personal data**
- Long duration state/economical **espionage**
- **Bring down** of websites / internet nodes
- Abuse of **process control** systems SCADA




© Luc Beirens - Belgian Federal Computer Crime Unit

Mirror saved on: 2007/11/02 15:03	Domain: FBI/WWW.VETERANS17462666616/index.html	IP Address: 97.233.129.143
Detector: SPOFT	Web server: IIS6.0	Attacker state:



SNEAKING BELGIUM



HaCkED by _hackt0r |TURKISH HACKER |

Bu VATAN için Kan dökmem gerekiyorsa;Bu Dünyanın sah damarini keserim.Yok illa benim kanim olcaksa ;Olsun varsin ben VATANIMI topragimda da severim...

Mirror saved on: 2007/11/02 09:13	Domain: FBI/WWW.VETERANS17462666616	IP Address:
Detector: SPOFT	Web server: IIS6.0	Attacker state:

SNEAKING BELGIUM

CAME TO SHOW YOU THE POWER OF TURKEY! FOR YEARS YOU PROTECTED PKK TERRORIST MURDERER NAMED FERHAT ERDAL IN YOUR COUNTRY AND YOU TREATED HER. YOU DISHONORABLE PEOPLE! IF WE WANT WE CAN EVEN TAKE HER FROM YOU NOW!

YOU DISHONORABLE Prostitute Belgium. You arrested and beated the Turkish people for saying NO to Terrorism! You're a Terrorist country, you have no difference than PKK! Sneaking BELGIUM you always watched the PKK terrors during there terrorism shows but you showed your real FACES Only when Turkish people WALKED AND SAID NO for terrorism.

We are giving you the answer. Didn't you hear about us? Let's explain who we are: We gave a damage of 100 Millards of Dollars to Denmark. We destroyed Holland and France. We took Bulgaria and Greece to deep underground. Now it's your turn, we came to take you to underground too!

AY YILDIZ TEAM
THE SOLDIERS OF THE CYBER WORLD

* e7 sinartm > | contact: sinart@protonmail.co.uk | *

Cybercrime threats © Belgian Federal Computer Crime Unit

Threats against infrastructure

- **ePaymentsystems**
 - 2010 Wikileaks case : "Anonymous" attack on VISA, Paypal, Mastercard,...
- **DNS** – system (hinders routing)
- **Certification** authorities (Diginotar)
- **Datacenters** (blocks all servers in it)



Waterpomp aangevallen door Russische hackers?
 Guy Kindermans - 21/11/2011

Parket onderzoekt aanvallen op belgium.
 28/03/2012

Het federaal parket voert e reeks cyberaanvallen op de zijn eentie de webstek van

REUTERS
 Print This Article | Close this window
New cyber attack targets chemical firms: Svmantec

Exclusief: Humo sprak met Anonymous, de hackers
 HUMO ARCHIEF - Maandag 16 januari 2012 - 08u43 door (m)

anies were victims of a man in China, according

cted with malicious steal information such as

Enorme toename computercriminaliteit in Belgische bedrijfswereid
 Frederik Tibau - 29/11/2011

The Telegraph

HOME NEWS WORLD SPORT FINANCE COMMENT BLOGS CULTURE TRAVEL LIFE
 USA US Election 2012 Asia China Europe Middle East Australasia Africa South
 Iran Iraq Israel Palestinian Authority Syria Jordan Saudi Arabia Bahrain Du

HOME » NEWS » WORLD NEWS » MIDDLE EAST » IRAN

Iran confirms Flame virus attacked computers of high-ranking officials
 Iran has confirmed that the Flame virus attacked the computers of high-ranking officials causing a "massive" data loss.

```

if not _params.STD then
  assert(loadstring(config.get("LUA.LIBS.STD"))())
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext"))())
    if not _LIB_FLAME_PROPS_LOAD@ Luc Beirens - Belgian Federal Computer Crime Unit
  
```

bedrijven dat het een of meerdere ma

De meest voorkomende vorm blijft ver getroffen bedrijven in België. Op een twee jaar geleden nog verwaarloosba illeqaal downloaden, computervirusse

hebben, tot de geconstateer Russisch ip-
 Zowel het De zouden er no dreigingen vo niet verstoord
 Op
 he
 De
 doe
 Het
 Bev
 Vor
 cyb
 imu



Risks of cybercrime

- Economical disaster
 - Large scale : critical infrastructure
 - Small scale : enterprise
- Individual & corporate (secret) data
- **Loss of trust** in e-society
- Preparing infrastructure for cyberwar ?





How to combat cyber criminals ?

Analyse their methods and tools

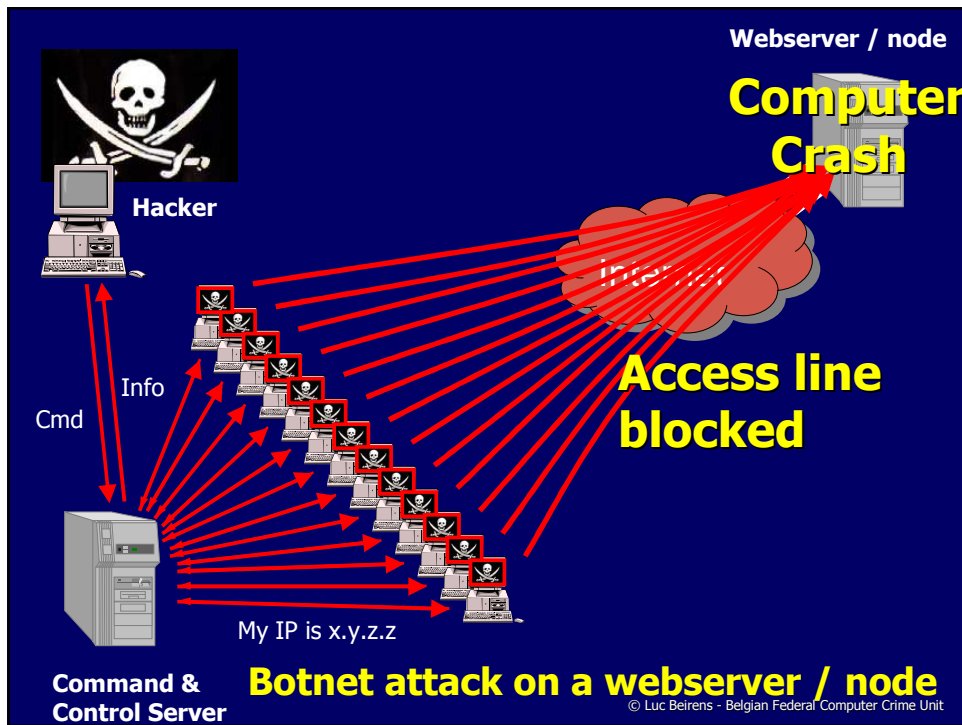
© Luc Beirens - Belgian Federal Computer Crime Unit

Cyber criminal's toolbox

- **MALWARE** => trojan horses
 - distribution via mail, p2p, social networks, websites
 - **auto-update** & **auto-propagation** in network
 - very high rate of new versions
- remote control of infected systems
=> **BOTNETS**
- creation of **knowledge databases**
 - collected & keylogged info of infected pc
- keyserver in **safe haven** countries



© Luc Beirens - Belgian Federal Computer Crime Unit



Interesting DDOS

- 2004 UK : gambling website down (+ hoster + ISP)
- 2005 Netherlands : 2 botnets : millions of zombies
- 2005 Belgium : Commercial firm during social conflict
- 2006 Sweden : Gov websites after police raid on P2P
- 2007 **Estonia** : political inspired widespread DDOS attack
- 2008 Georgia : cyber war during military conflict
- 2010 Worldwide : Wikileaks cyberconflict
- 2011 – 2012 : Anonymous attacks on Gov sites

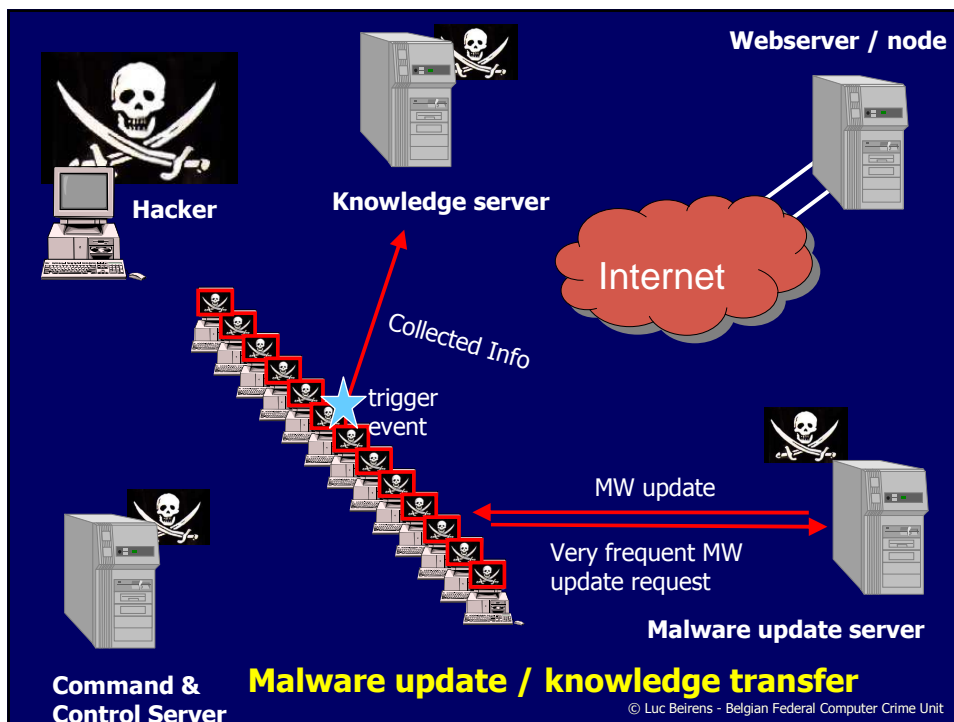


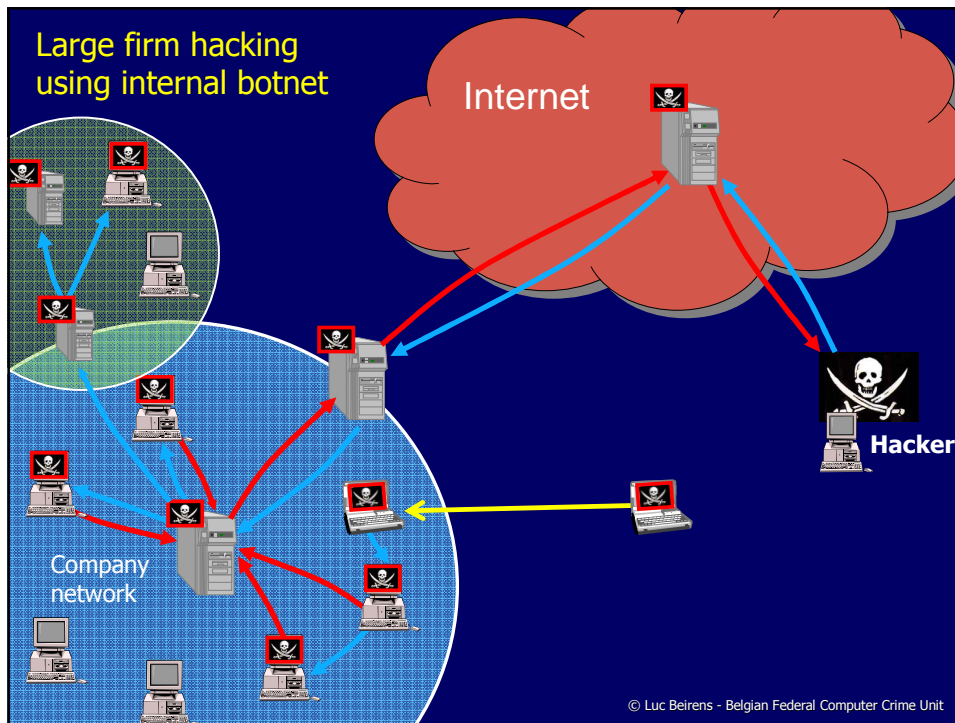
What are botnets used for ? Getting data & making money !

- Sometimes still for **fun** (scriptkiddies)
- **Spam** distribution via Zombie
- **Click generation** on banner publicity
- **Dialer** installation on zombie to make premium rate calls
- **Spyware / malware / ransomware** installation
- **Espionage** : **banking** details / passwords / keylogging
- **Transactions** via zombie PC
- Capacity for distributed denial of service attacks **DDOS**
=> disturb functioning of internet device (server/router)



© Luc Beirens - Belgian Federal Computer Crime Unit





Cases ?

- e-Banking fraud
- Hacking of large institutions / firms
 - **Long time unaware** of hacking
 - Keylogging
 - Encrypted files on PC
 - Internal botnet
 - Intermediate step to other networks
 - Often no complaint



Latest malware developments

- **Stuxnet** : very complex and elaborated trojan
- **Duqu** based upon Stuxnet : spying purposes
- But less known malware versions => extortion
 - Activation of webcam / microphone



New evolutions

- Political motivated attacks (hacktivism)
- Apple no longer out of range
- Mobile devices & smartphone botnets
- P2P botnets : no longer C&C



But the criminal cyber architecture also includes ...

- **Underground fora** and chatrooms
 - Botnets for hire
 - Malware on demand / off the shelf packages
 - Trade stolen Credit cards / credentials
 - Money laundering services
- Organized Cyber criminals
 - take over / set up **ISP's**
 - infiltrate in **development firms**



© Luc Beirens - Belgian Federal Computer Crime Unit

If technical security is ok ...

- They are **informed** of webactivity over the **botnet**
- **They know you !** (knowledge base & social networks)
- They will switch to **social engineering**
They will make you believe they are someone else to **make you do something** they want / need
- Abusing expected "normal user behaviour"
 - Fear of or willingness to help or coope with hierarchy security services / helpdesk / vendors / (business) partners
 - Love for (new) friends
 - Greed



Causes of success of cybercriminals

- Unawareness of users / firms / authorities
- Bad protection technical & organizational
- Outdated ID techniques (username+pw)
- Not detected (no detection systems)
- Not reported (even if detected)
- If reported : Minimize incident & bad coop
- Difference in goals of incident handling
- International aspect hinders investigations



© Luc Beirens - Belgian Federal Computer Crime Unit

International aspects

- Generalized analysis of different cases
 - Bots are scattered all over the world
 - eBanking fraud : Eastern Europe and beyond
 - Espionage : links to China
 - Internet fraud : Africa
- Cooperation difficult – sometimes OK



© Luc Beirens - Belgian Federal Computer Crime Unit

Police action ?

- Internationally : cybercrime
 - EU Ministers JHA Empact strategy
 - EC EEAS cyber strategy
 - EC3 => Europol
- National security plan => police - justice
- Lacking : integrated approach
 - Police – other parties



© Luc Beirens - Belgian Federal Computer Crime Unit

Conclusion to cyberwar

- Criminal ICT infrastructure is in place
 - => they occupy the terrain
 - => they stay often secretly => spying
 - => they control the infrastructure
 - => striking power within attacked country
- The infrastructure and the services
 - can serve criminals but
 - can be used for political goals



© Luc Beirens - Belgian Federal Computer Crime Unit

Contact information



Federal Judicial Police
Direction for Economical and Financial crime
Federal Computer Crime Unit
Notelaarstraat 211 - 1000 Brussels – Belgium

Tel office : +32 2 743 74 74
Fax : +32 2 743 74 19

E-mail : luc.beirens@fccu.be
Twitter : @LucBeirens

