Estonian cybercrime legislation and case-law. Responses to the 2007 cyberattacks

Markko Künnapu

Ministry of Justice

ESTONIA

Some basic facts

- 56% of all families use internet
- 52% have broadband connection (2 Mbit)

- 98% bank transactions electronically
- 91% income tax declarations electronically

- 1164 free WiFi access points

- 2001 X-Road
- 2002 ID card (currently 1,054,595 active ID cards
- 2003 e-government
- 2003 e-tax board
- 2005 e-voting (local governments)
- 2007 e-voting (Parliament)

- 2007 mobile ID
- 2007 e-police
- 2008 e-health
- 2009 e-voting (European Parliament)

Cybercrime legislation

- Council of Europe Convention on Cybercrime
- Council Framework Decision on attacks against information systems 2005/222/JHA

Statistics

PC	2003	2004	2005	2006	2007	2008
§ 206	3	6	2	7	7	9
§ 207		2	4		5	1
§ 208			3	1	2	2
§ 213	19	36	46	72	128	367
§ 216[1]						
§ 217	10	16	16	17	12	22

Cyberattacks

Why to choose cyberattack?

- can be committed from a long geographical distance
- possibility to remain anonymous
- transborder nature makes it hard to track and investigate
- easy and does not require much resources and skills
- cheap compared to possible profits or damages (financial, critical infrastructure)

Some highlights

Estonia (2007)

Radio Free Europe (2008)

Lithuania (2008)

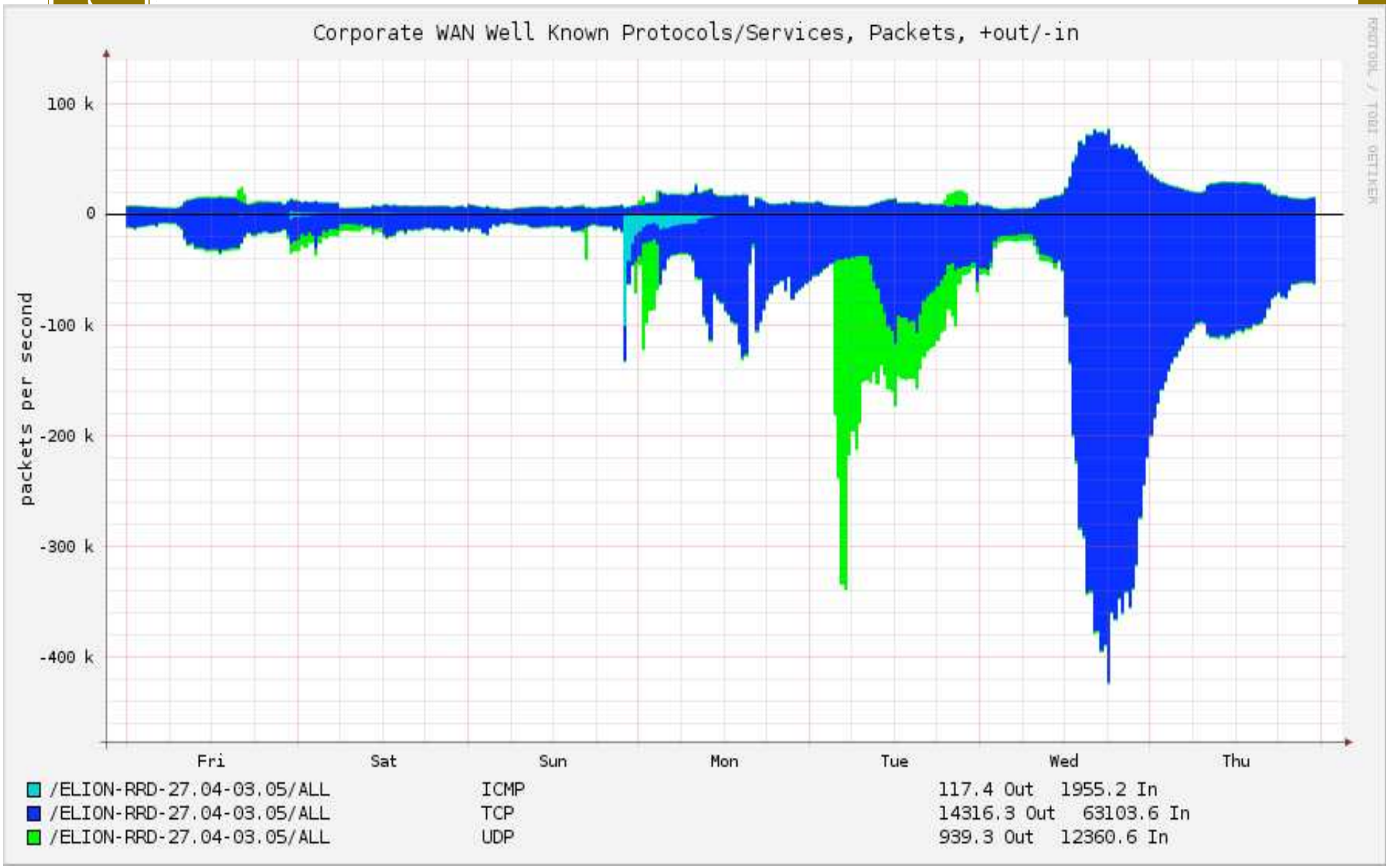
Burma (2008)

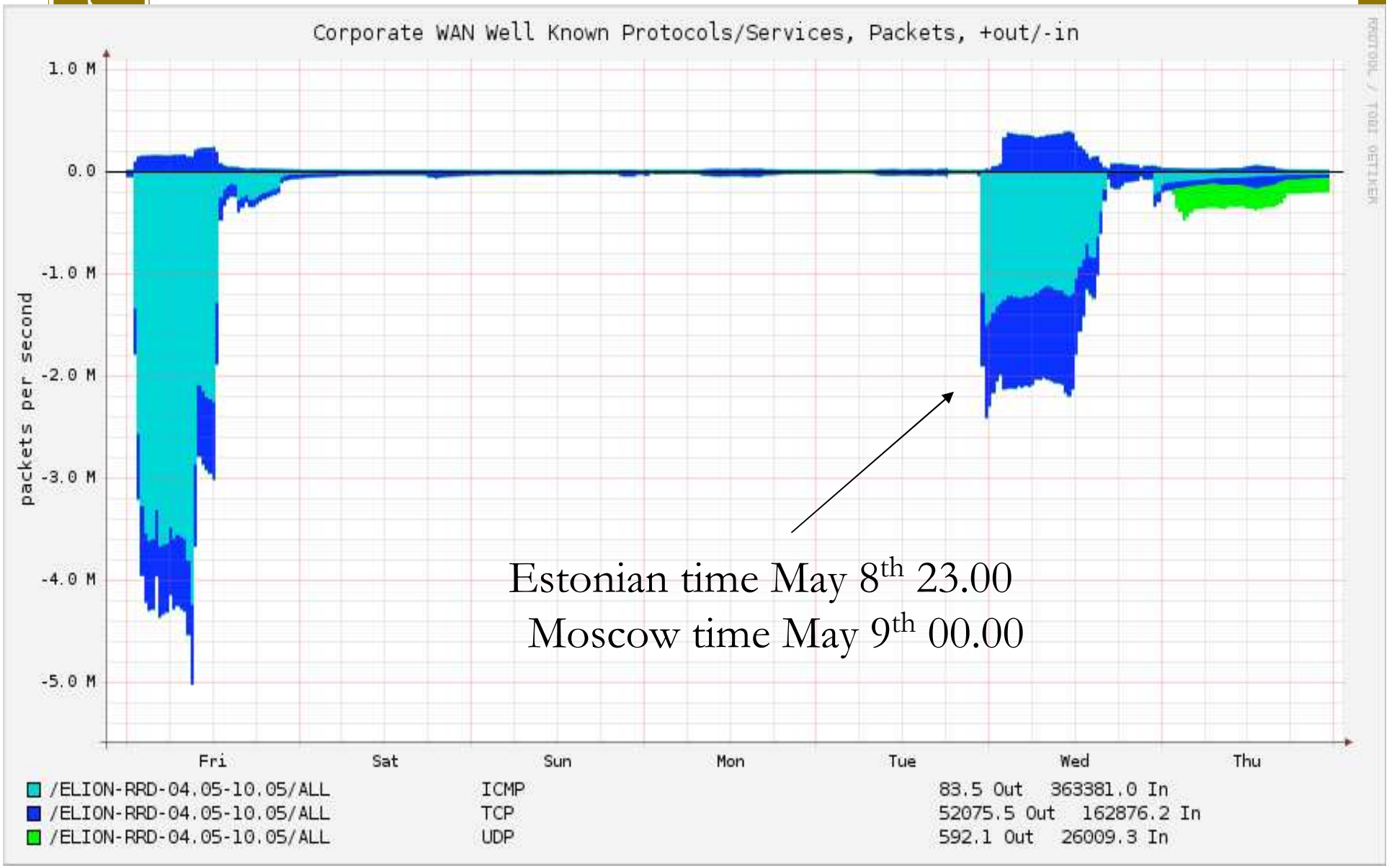
Georgia (2008)

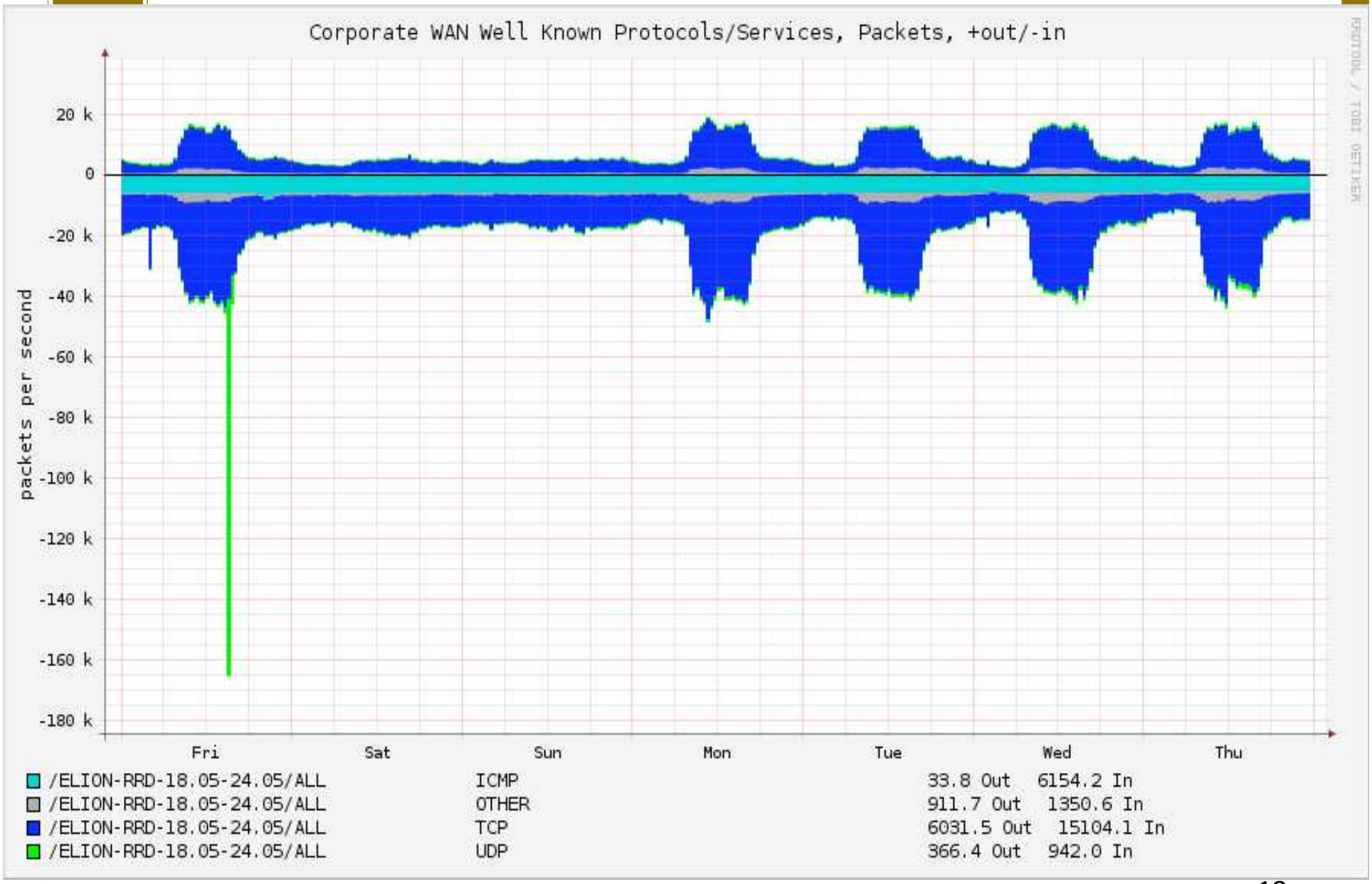
South Korea & USA (2009)

Cyberattacks agains Estonia

- in April and May 2007 large-scale politically motivated attacks against Estonian information systems
- at first riots, violence and looting at the streets during April 26-27
- April 27th – May 18th cyberattacks
- 4 waves of cyberattacks


Corporate WAN Well Known Protocols/Services, Packets, +out/-in
100 k
0
-100 k
-200 k
-300 k
-400 k
packets per second
Fri
Sat
Sun
Mon
Tue
Wed
Thu
/ELION-RRD-27.04-03.05/ALL ICMP 117.4 Out 1955.2 In
/ELION-RRD-27.04-03.05/ALL TCP 14316.3 Out 63103.6 In
/ELION-RRD-27.04-03.05/ALL UDP 939.3 Out 12360.6 In


Corporate WAN Well Known Protocols/Services, Packets, +out/-in
1.0 M
0.0
-1.0 M
-2.0 M
-3.0 M
-4.0 M
-5.0 M
packets per second
Fri
Sat
Sun
Mon
Tue
Wed
Thu
Estonian time May 8th 23.00
Moscow time May 9th 00.00
/ELION-RRD-04.05-10.05/ALL ICMP 83.5 Out 363381.0 In
/ELION-RRD-04.05-10.05/ALL TCP 52075.5 Out 162876.2 In
/ELION-RRD-04.05-10.05/ALL UDP 592.1 Out 26009.3 In


Corporate WAN Well Known Protocols/Services, Packets, +out/-in
packets per second
20 k
0
-20 k
-40 k
-60 k
-80 k
-100 k
-120 k
-140 k
-160 k
-180 k
Fri
Sat
Sun
Mon
Tue
Wed
Thu
/ELION-RRD-18.05-24.05/ALL ICMP 33.8 Out 6154.2 In
/ELION-RRD-18.05-24.05/ALL OTHER 911.7 Out 1350.6 In
/ELION-RRD-18.05-24.05/ALL TCP 6031.5 Out 15104.1 In
/ELION-RRD-18.05-24.05/ALL UDP 366.4 Out 942.0 In

Cyberattacks

- hacking
- defacement
- spam
- DDoS incl. botnets
- incitement to hatred and violence at internet websites and chatrooms
- providing guidelines how to attack, incl list of Estonian servers

Target websites and servers

- The President
- Government
- Ministries
- Police
- Banks
- Online media
- Prime Minister’s Party

Recovery

- close cooperation between national CERT-s, blocking and filtering traffic
- close cooperation between public and private sector – exchange of information, logfiles etc
- international experts

Results

- IP addresses were from all over the world
- attacker botnets were in Europe and USA
- criminal investigations were initiated
- only 1 convicted person

- international co-operation was problematic
- co-operation between CERT-s
- co-operation in criminal matters between law enforcement authorities
- legal assistance and extradition was refused

Legislation analysis

- Penal Code
- Electronic Communications Act
- Information Society Services Act
- Data Protection Act
- Public Information Act
- soft law, recommendations, standards

Shortcomings in law

- PC treated information systems equally
- punishments for cybercrimes were too low
- surveillance action was not possible for all cybercrimes

- existing regulation was not clear enough – computer sabotage ?
- substantial loss as compulsory element
- politically motivated DDoS – a new quality ?

- mutual legal assistence vs social contacts
- requesting information – procedure is time consuming
- problems concerning requests, denial of assistance
- data protection rules

Amendments to PC

- clearer regulation concerning cybercrimes
- computer virus, malware and spyware
- increasing punishments
- critical infrastructure
- cyberterrorism

§ 207. Hindering of operation of computer system

(1) Unlawful interference or hindrance of the operation of a computer system by way of entry, transmission, deletion, damaging, alteration or blocking of data is punishable by a pecuniary punishment or up to 3 years' imprisonment.

(2) **The same act, if significant damage is thereby caused, or the operation of a computer system of a vital sector (critical infrastructure) or the provision of public services is thereby hindered is punishable by a pecuniary punishment or up to 5 years' imprisonment**

(3) An act provided for in subsection (1) or (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment.

§ 217. Unlawful use of computer system

(1) Unlawful access to a computer system by way of removal or circumvention of a code, password or other protective measure is punishable by a pecuniary punishment or up to 3 years' imprisonment.

(2) The same act, if:

1) it causes significant damage, or

2) is committed by using a computer system containing a state secret, classified foreign information or information prescribed for official use only, or

3) a computer system of a vital sector (critical infrastructure) has been accessed, is punishable by a pecuniary punishment or up to 5 years' imprisonment.

(3) An act provided for in subsection (1) or (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment.

Cybercrime as a terrorist crime

§ 237. Acts of terrorism

(1) Commission of a criminal offence against international security, against the person or against the environment, or a criminal offence dangerous to the public posing a threat to life or health, or the manufacture, distribution or use of prohibited weapons, the illegal seizure, damaging or destruction of property to a significant extent **or interference in computer data or hindering of operation of computer system** as well as threatening with such acts, if committed with the purpose to force the state or an international organisation to perform an act or omission, or to seriously interfere with or destroy the political, constitutional, economic or social structure of the state, or to seriously interfere with or destroy the operation of an international organisation, or to seriously terrorise the population is punishable by five to twenty years' imprisonment, or life imprisonment.

(2) The same act, if committed by a legal person, is punishable by compulsory dissolution.

(3) For the criminal offence provided in this section, the court shall impose extended confiscation of assets or property acquired by the criminal offence pursuant to the provisions of § 83-2 of this Code.

Prevention

- coherent policy
  : data
  protection
  computer system security
  criminal
  legislation
- co-operation between private sector, CERT, law enforcement

- Cybersecurity Strategy 2008 – 2013
- Critical Infrastructure Protection
- Critical Information Infrastructure Protection

Examples from case-law

Lauri Nõmme # 1

- high school student, 2nd place in informatics competition, used to programme, hacker
- attacked CV database, started a code that attempted to download all the contents
- tried to delete the database
- computer related fraud, computer sabotage

- was acquitted

- attack was performed from a computer that other persons had also access to
- several users, computer files were not password-protected
- password for computer system was written on the desk
- motive, mental element could not be proved

Lauri Nõmme # 2

- illegal access to computer system
- previosly obtained user names and passwords
- copied personal data
- copied, altered and deleted data
- gained access as root, blocked legitimate users
- used home computer
- plea bargaining - convicted

VN

- illegal access to server that hosted several websites
- copied all data and deleted the contents of the server afterwards
- demanded 500 USD from owner for returning data, received about 120 USD

Janno K

- DoS attack against local government's mail server – e-mails in every 2 seconds
- sending at least 1039 e-mails (most of them with attachments) were proved
- expertise and witness testimonies
- Illegal access - acquittal
- Prosecutors Office qualified sending e-mails as distributing computer virus ???
- final decision was made by Supreme Court
- what where the problems?

Eugene A, Jevgeni M

- sent infected e-mails and installed spyware using software vulneralbility
- victim TS was in Lithuania
- spyware sent online banking user name and passwords to ftp-server
- transferring money from TS bank account to GF bank account in Estonia and to EA e-money account (total 1100 EUR)
- fine + confiscation of computer systems

Ilya K, Dmitri T and others

- computer related fraud, money laundering
- distributed a Trojan horse code that was disguised as new software update
- publicised advertisement in Europe, hired “financial managers”
- used online banking user names and passwords to get access to victim's bank accounts
- transferred money to “managers”

- bank transactions and Western Union
- countries involved: Austria, Denmark, France, Greece, Italy
- financial damage caused 200 000 EUR
- from one person 90 000 EUR
- money went via Austria – Latvia – China – Russia – Ukraine – Estonia
- criminal's living standards were high, police suspected higher amount of criminal profits

Dmitri G

- during riots and cyberattacks in April, May 2007 (25.04.-04.05.2007)
- system interference
- ping -n 5000 -l 1000 xxx.xx
- webserver of the Prime Minister's Party
- used his home computer
- acted with other persons whose identity could not be proved

Thank you!

Markko Künnapu
markko.kynnapu@just.ee
Tel. +372 6208 205
Fax +372 6208 109