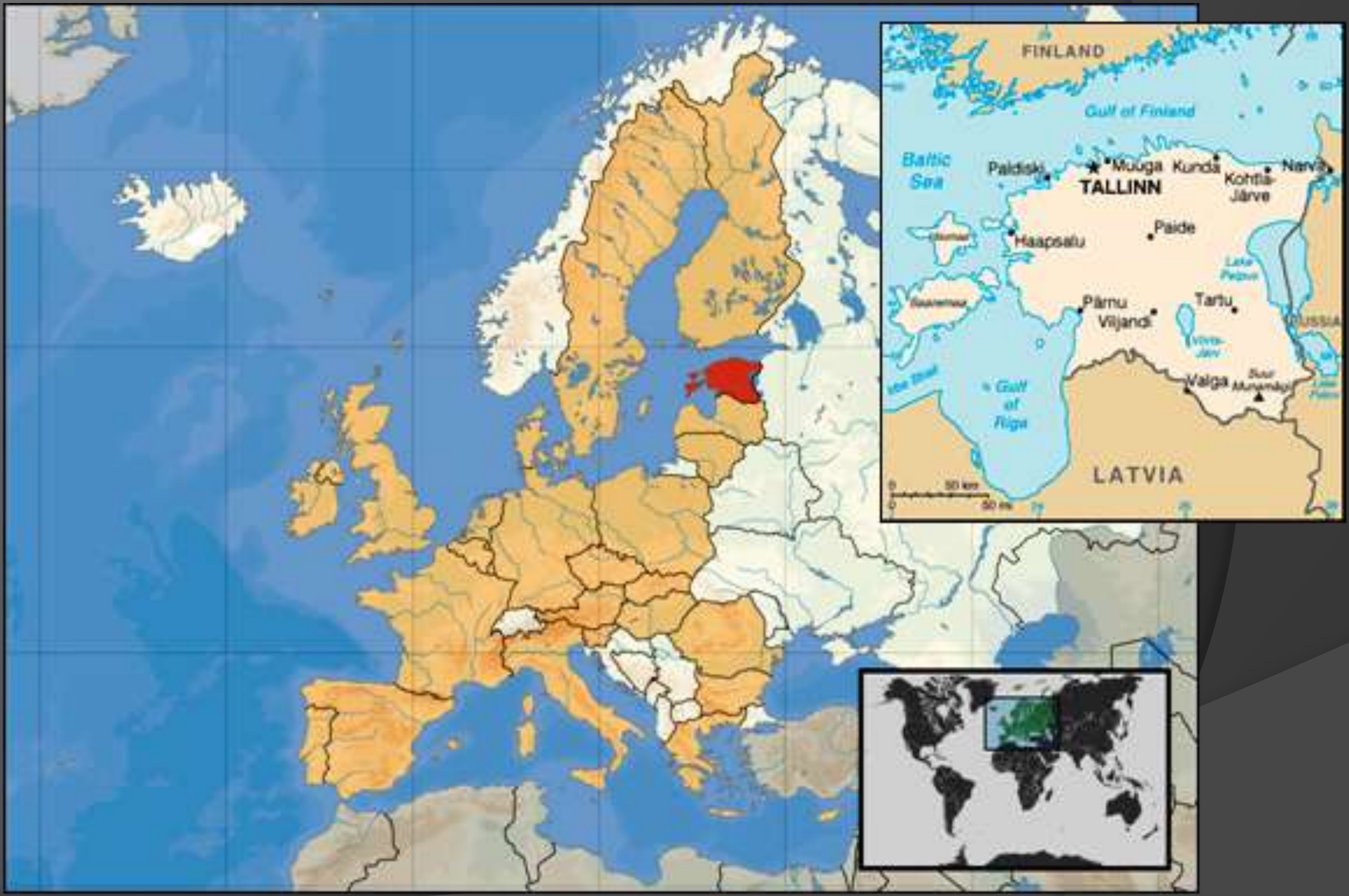
ESTONIA CYBER ATTACKS 2007



Estonia

- Officially known as Republic of Estonia.
- Located at Baltic Region of Northern Europe.
- Territory covers 45,227 km^2.
- Capital is Tallinn.
- Democratic parliamentary republic.
- Population of only 1.46 million.
- Official language is Estonian.
- Estonian Declaration of Independence in Pärnu on 23 February and in Tallinn on 24 February 1918.
- Prime Minister is Andrus Ansip.

Infrastructure and e-infrastructure

- X-Road (started on 2001) is a data exchange layer use by the Government organization in Estonia to interconnect each other.
- More than 355 government agencies had joined together in the virtual world.
- All the citizens have a ID-Card that allow the citizen to connect with the Government organizations and bank.
- The most "wired" and advanced country in Europe in the terms of e-Government of Estonia.
- The first country in the world to use Internet voting in local elections (2005).

Infrastructure and e-infrastructure

- List of major commercial ISP’s:
  - Atlas Data Communications (Estonian Telephone Company Data Services).
  - Data Telecom (EUnet).
  - DELFI Online.
  - EsData Ltd.
  - Infonet Ltd.
  - Mainor Anet.
  - TELE2 - Levicom Broadband.
  - Uninet Data Communications.

X-Road

- Was launched on 2001.
- It’s a virtual world that’s connects more than 355 government agencies and their server.
- Platform-independent.
- Enables secure data transfer between digital state databases and enables secure data transfer between individuals and state institutions.
- Data and requests that being send to the agencies will pass through the security server then to SOAP servers.

X-Road

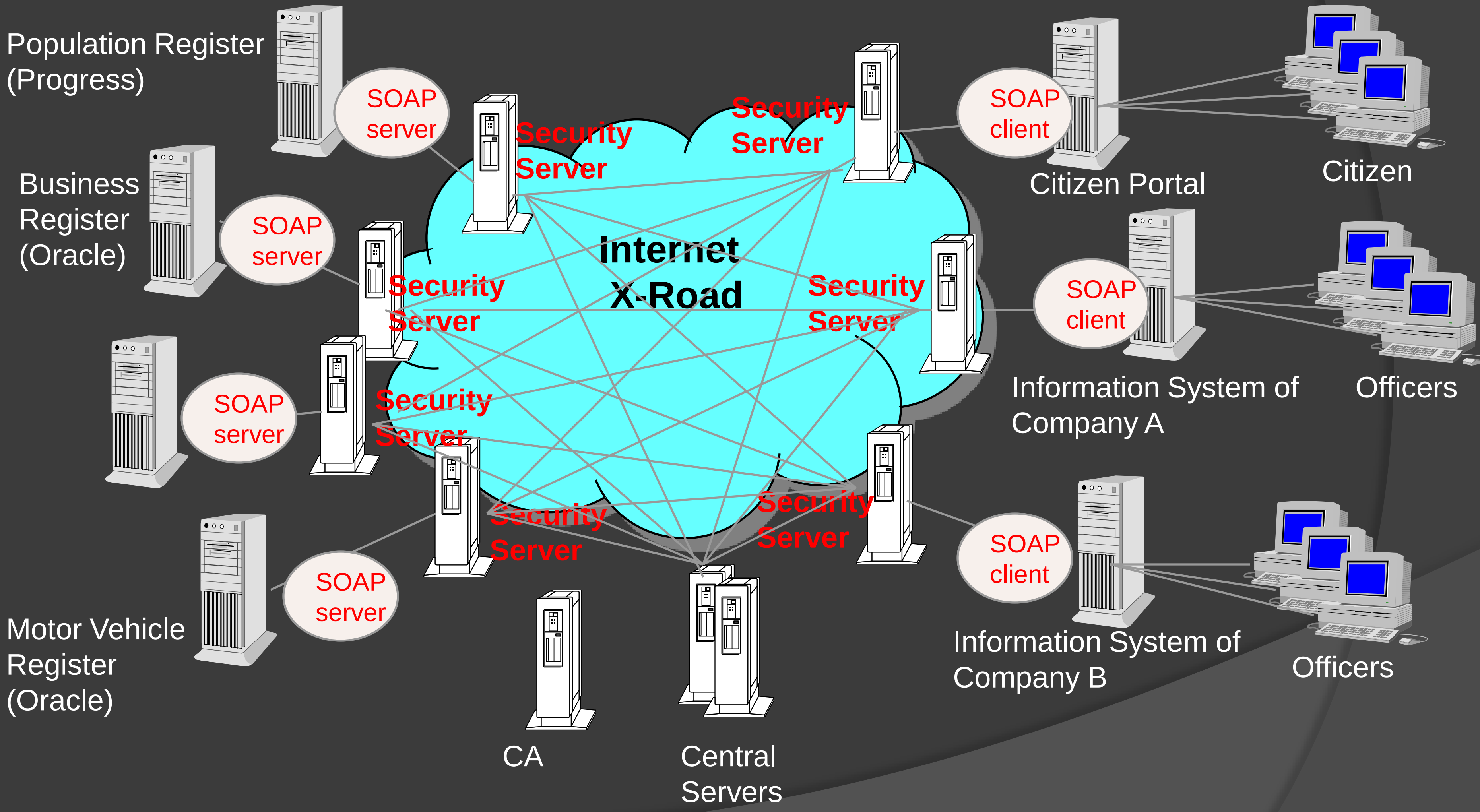
- Security servers are physically separate computers, which have specialized software installed.

- Security servers encrypt and decrypt data, keep logs, and deny permission to unauthorized users.

- Traffic between Security Servers is encrypted with PKI. Security Servers have to be certified by X-Road CA (Certification Authority).

- SOAP –(Simple Object Access Protocol) is a protocol for exchanging XML-based messages over computer network, normally using HTTP.

X-Road


Population Register
(Progress)
SOAP server
Business Register (Oracle)
SOAP server
SOAP server
Motor Vehicle Register (Oracle)
SOAP server
Security Server
Security Server
Security Server
Security Server
Security Server
Security Server
Security Server
Security Server
Internet
X-Road
SOAP client
Citizen Portal
Citizen
SOAP client
Information System of Company A
Officers
SOAP client
Information System of Company B
Officers
CA
Central Servers

Estonia cyber attacks 2007

- Known as the Estonian Cyberwar.
- Started on April 27, 2007 and this attacks last about 3 weeks.
- Series of attacks targeting government portals, parliament portal, banks, ministries, newspapers and broadcasters of Estonia.
- Estonians claimed this attacks as a political attack or revenge from Russians.

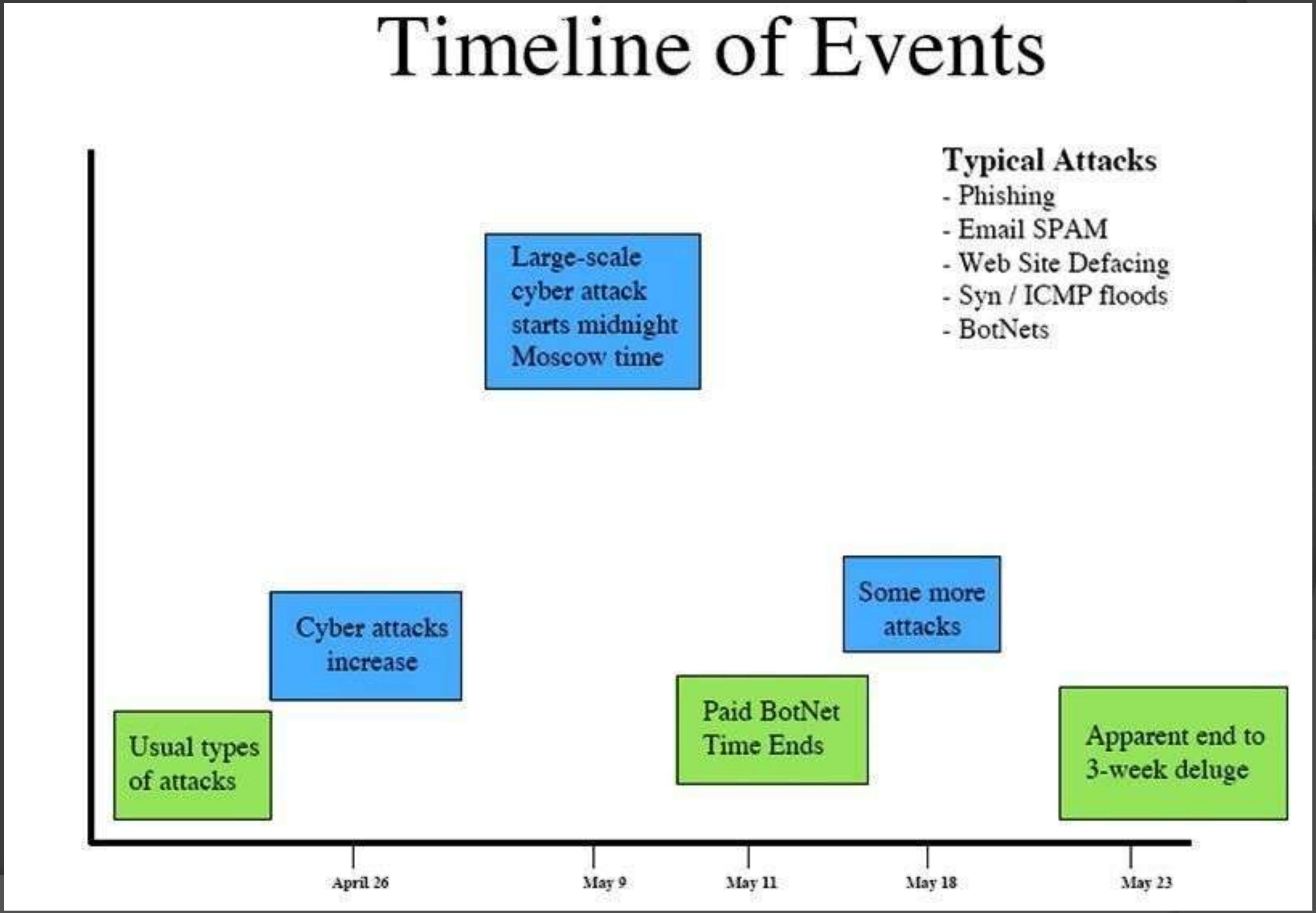
Why cyber attacks 2007 happened ?

- On 27 April 2007, the Estonian government moved a controversial Soviet-era World War II memorial from a square in the capital city of Tallinn to a more secluded location.

- Protests erupted in Estonia and Russia, where Estonia's Moscow embassy was blockaded.

- The Russian government protested vociferously and issued threats.

How the attack took place ?



Timeline of Events

Typical Attacks
- Phishing
- Email SPAM
- Web Site Defacing
- Syn / ICMP floods
- BotNets

Usual types of attacks

Cyber attacks increase

Large-scale cyber attack starts midnight Moscow time

Paid BotNet Time Ends

Some more attacks

Apparent end to 3-week deluge

How the attack took place ?

- Weeks of cyber attacks followed, targeting government and banks, ministries, newspapers and broadcasters Web sites of Estonia.
- Some attacks took the form of distributed denial of service (DDoS) attacks (using ping floods to expensive rentals of botnets).
- 128 unique DDOS attacks (115 ICMP floods, 4 TCP SYN floods and 9 generic traffic floods).
- Used hundreds or thousands of "zombie" computers and pelted Estonian Web sites with thousands of requests a second, boosting traffic far beyond normal levels.
- Attacker commanding other computers to bombard a web site with requests for data, causing the site to stop working.

How the attack took place ? Cont..

- Some web site been shut down by the attacker for some time.
- Spamming of bigger news portals commentaries and defacements including that of the Estonian Reform Party website also occurred.
- Access to the banks, government agencies website become unavailable such as Estonian national Web sites, including those of government ministries and the prime minister's Reform Party.
- A flood of junk messages was thrown at the e-mail server of the Parliament, shutting it down.

How the attack took place ? Cont..

- First wave of attacks (DDoS):

  - 27 April 2007, Konstantin Goloskov a commissioner from Republic of Moldova pro-Kremlin organized DDoS attacks to Estonia’s ISP and governmental websites.

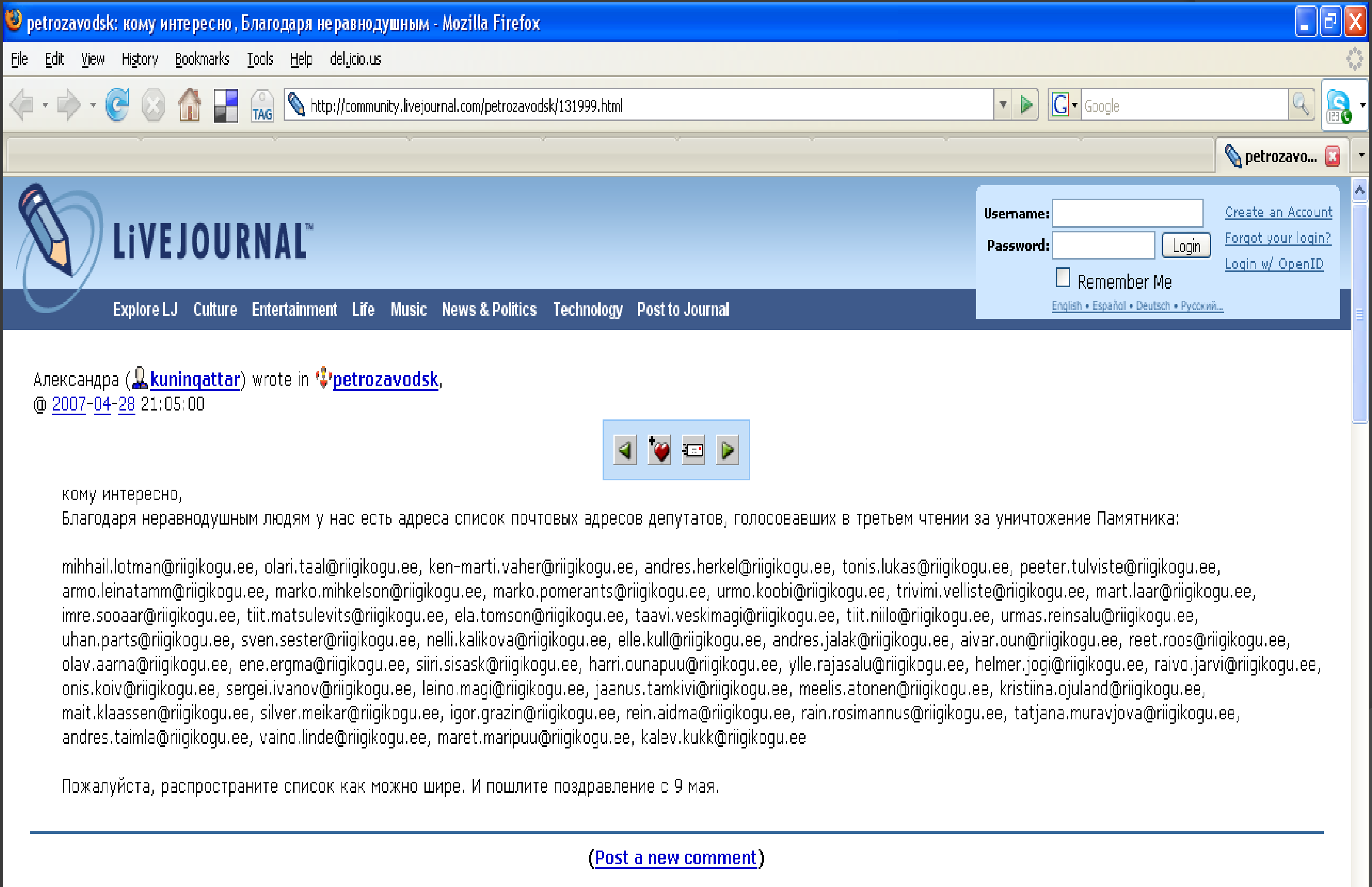
  - Commands of ICMP attacks posted to various boards, blogs and chats on Russian Internet.

  - These commands converted into a batch file and uploaded to a web address below:

    “http://fipip.ru/raznoe/pingi.bat”

How the attack took place ? Cont..

- Second wave of attacks:
  - 30 April 2007, Livejournal users have posted a list of email address of Estonia’s parliament deputies.
  - These posts were urging users to share the list of emails and cause multiple letters to the Estonia’s deputies with “congratulations of the Victory Day”.
  - This action resulted millions of letters being sent and led to mail servers mainframes failure for 2 days.


petrozavodsk: кому интересно, Благодаря неравнодушным - Mozilla Firefox
File Edit View History Bookmarks Tools Help del.icio.us
http://community.livejournal.com/petrozavodsk/131999.html
Google
petrozavo...
LiVEJOURNAL™
Explore LJ Culture Entertainment Life Music News & Politics Technology Post to Journal
Username:
Password:
Login
Create an Account
Forgot your login?
Login w/ OpenID
□ Remember Me
English • Español • Deutsch • Русский...

Александра (kuningattar) wrote in petrozavodsk,
@ 2007-04-28 21:05:00

кому интересно,
Благодаря неравнодушным людям у нас есть адреса список почтовых адресов депутатов, голосовавших в третьем чтении за уничтожение Памятника:

mihhail.lotman@riigikogu.ee, olari.taal@riigikogu.ee, ken-marti.vaher@riigikogu.ee, andres.herkel@riigikogu.ee, tonis.lukas@riigikogu.ee, peeter.tulviste@riigikogu.ee, armo.leinatamm@riigikogu.ee, marko.mihkelson@riigikogu.ee, marko.pomerants@riigikogu.ee, urmo.koobi@riigikogu.ee, trivimi.velliste@riigikogu.ee, mart.laar@riigikogu.ee, imre.sooaar@riigikogu.ee, tiit.matsulevits@riigikogu.ee, ela.tomson@riigikogu.ee, taavi.veskimagi@riigikogu.ee, tiit.niilo@riigikogu.ee, urmas.reinsalu@riigikogu.ee, uhan.parts@riigikogu.ee, sven.sester@riigikogu.ee, nelli.kalikova@riigikogu.ee, elle.kull@riigikogu.ee, andres.jalak@riigikogu.ee, aivar.oun@riigikogu.ee, reet.roos@riigikogu.ee, olav.aarna@riigikogu.ee, ene.ergma@riigikogu.ee, siiri.sisask@riigikogu.ee, harri.ounapuu@riigikogu.ee, ylle.rajasalu@riigikogu.ee, helmer.jogi@riigikogu.ee, raivo.jarvi@riigikogu.ee, onis.koiv@riigikogu.ee, sergei.ivanov@riigikogu.ee, leino.magi@riigikogu.ee, jaanus.tamkivi@riigikogu.ee, meelis.atonen@riigikogu.ee, kristiina.ojuland@riigikogu.ee, mait.klaassen@riigikogu.ee, silver.meikar@riigikogu.ee, igor.grazin@riigikogu.ee, rein.aidma@riigikogu.ee, rain.rosimannus@riigikogu.ee, tatjana.muravjova@riigikogu.ee, andres.taimla@riigikogu.ee, vaino.linde@riigikogu.ee, maret.maripuu@riigikogu.ee, kalev.kukk@riigikogu.ee

Пожалуйста, распространите список как можно шире. И пошлите поздравление с 9 мая.

(Post a new comment)

A post containing email address of Estonia’s parliament deputies

How the attack took place ? Cont..

- Third wave of attacks:

  - 3 – 9 May 2007, Estonia’s websites been attacked with various tools such as SQL injections (known vulnerabilities in Apache, PHP).

  - Script kiddies were stoked into fervour by President Vladimir Putin’s speech.

How the attack took place ? Cont..

- The attack heavily affected infrastructures of all network:
  - Routers damaged.
  - Routing tables changed.
  - DNS servers overloaded.
  - Email servers mainframes failure, and etc.

How the attack took place ? Cont..

- Inoperability of the following state and commercial bodies:
  - The Estonian presidency and its parliament.
  - Almost all of the country’s government ministries.
  - Political parties.
  - Three news organizations.
  - Two biggest banks and communication’s firms.
  - Governmental ISP.
  - Telecom companies.

How the attack took place ? Cont..

- Continues attack caused processing and buffer of the system.

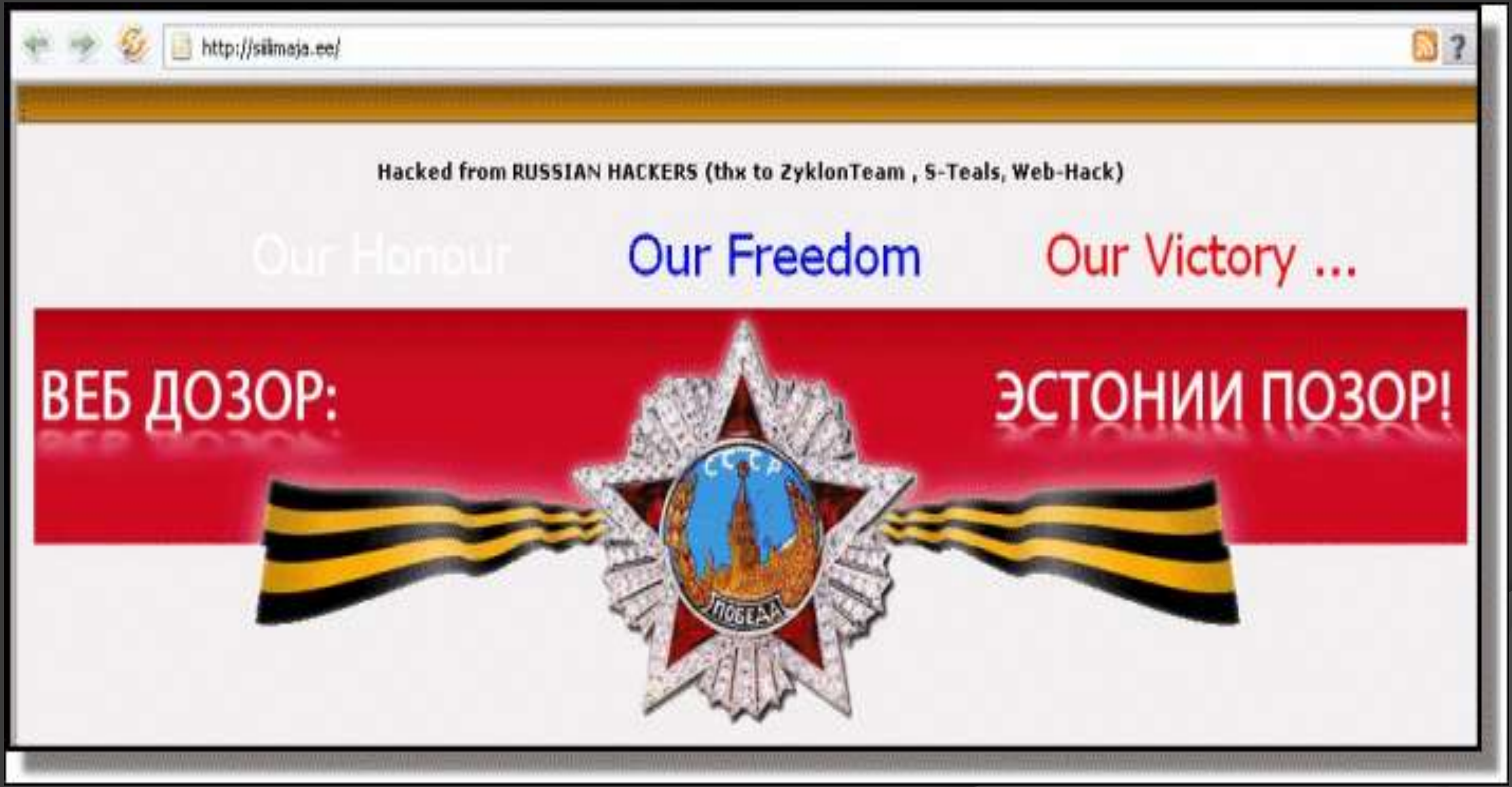
- The received packets/messages processed by network device/services, even processing unnecessary packets/messages.
  - This can be recover if the packets/messages is for limited time. The effect will be minor.
  - The continuous of answering the packets/messages, the device processing more than the system can maintain.
  - It will effect the performance, response time or complete loss of connection.

How the attack took place ? Cont..

- The network device has a limited buffer that predefined, which stored temporary data for processing or sending.
  - The attacker test the maximum buffer can be supported by a device before stop for further processing. This methods is used during early stage of attacking by sending a large amount of data packets.
  - Large groups of network consists of millions of bot/zombie effected by botnet, create network router load and send it to the target of high rate of very small packets.
  - This work load being continuously processed by the devices and may become failure of unable of perform.
  - Other request or message of normal user unable to be processed.
  - The buffer overflow be occur of devices have request of higher priority to be filled into the buffer.
  - Network devices need to attend the high priority request from others.
  - Processing endless request cause DDoS.

How the attack took place ? Cont..

- Some web sites been Defaced.



Hacked from RUSSIAN HACKERS (thx to ZyklonTeam , S-Teals, Web-Hack)

Our Honour Our Freedom Our Victory ...

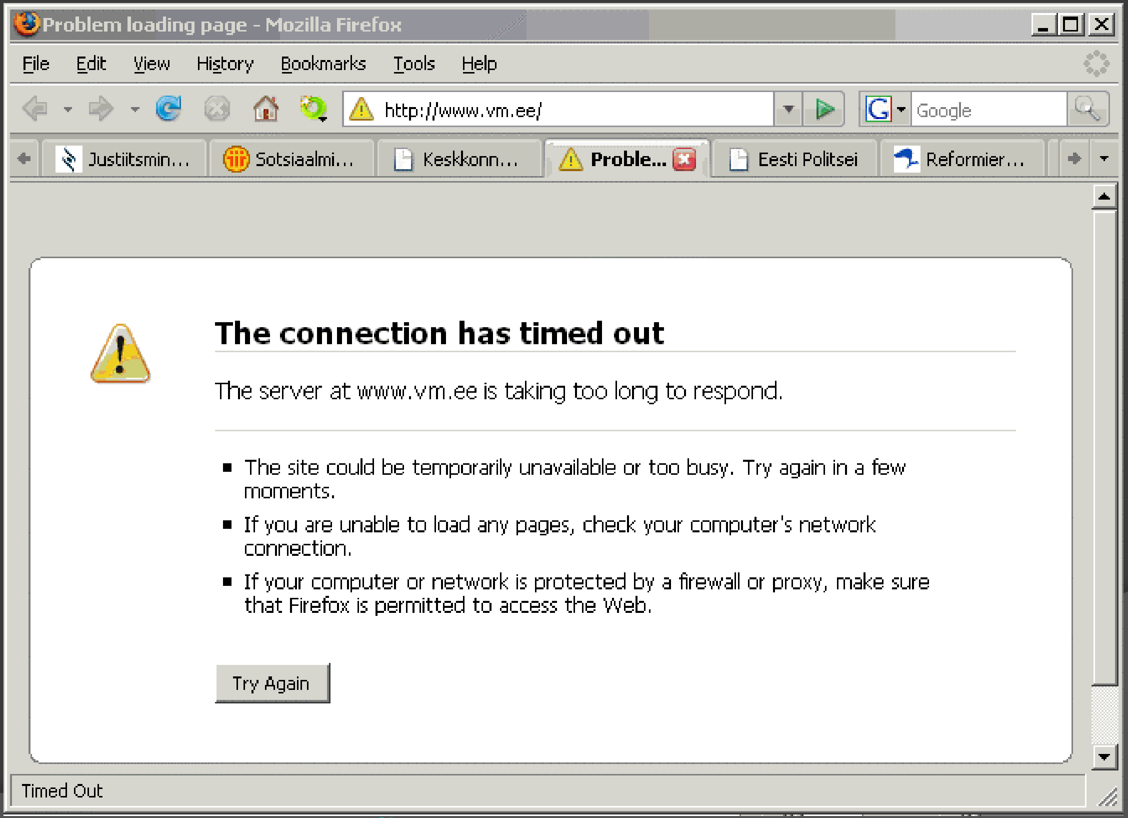
ВЕБ ДОЗОР: ЭСТОНИИ ПОЗОР!

Examples of Estonia website that was deface by Russian crackers.

How the attack took place ? Cont..

- Hackers broke into the Web site of the Reform Party, posting a fake letter of apology from the prime minister, Andrus Ansip, for ordering the removal of the highly symbolic statue.

- Attackers can clog not only the country’s servers, but also its routers and switches, the specialized devices that direct traffic on the network.



The connection has timed out

The server at www.vm.ee is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

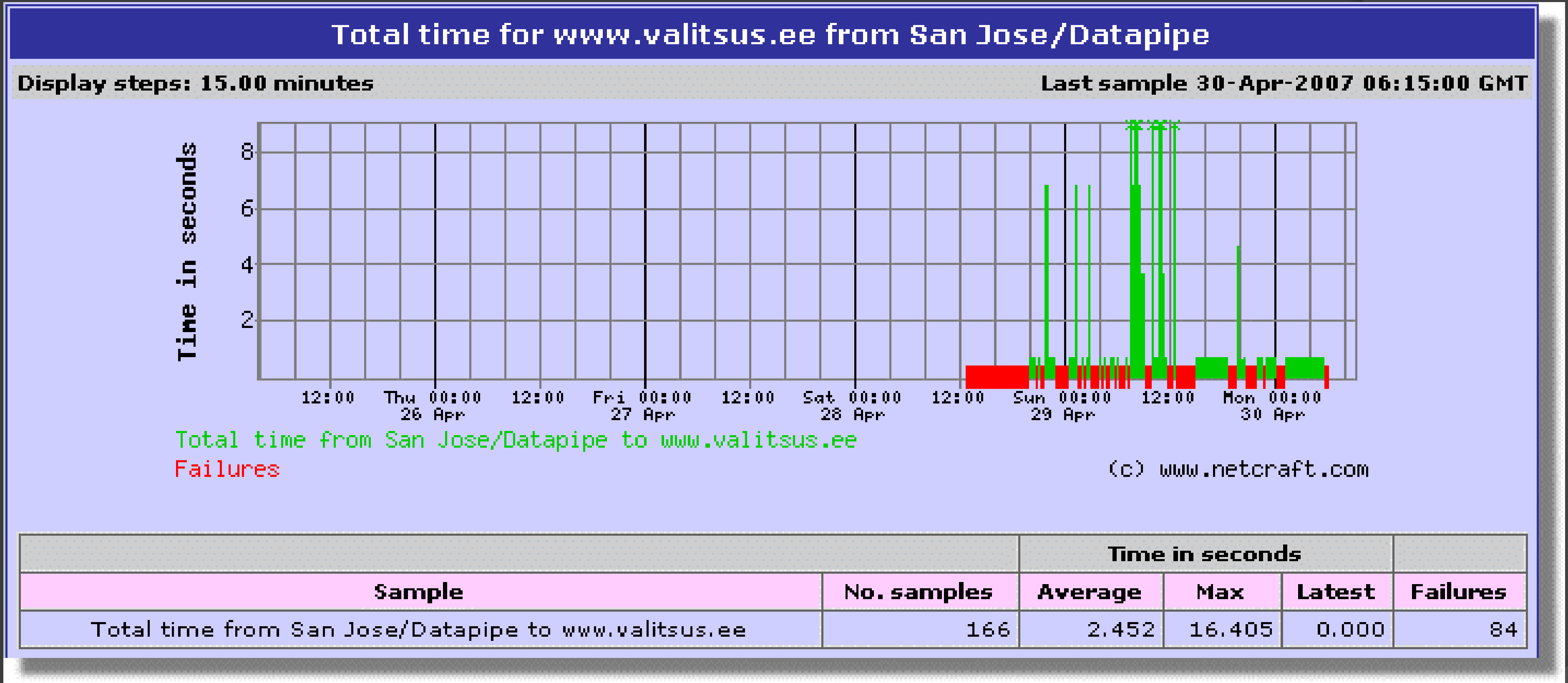
www.valitsus.ee unavailable for sometime.

How the attack took place ? Cont..

The sites that were attacked on Saturday, April 28th at 15:00 GMT, included:

- www.mkm.ee (Ministry of Economic Affairs and Communications): unreachable
- www.peaminister.ee (Website of the prime minister): unreachable
- www.riigikogu.ee (Estonian Parliament): unreachable
- www.sisemin.gov.ee (Ministry of Internal Affairs): unreachable
- www.valitsus.ee (Estonian Government): unreachable
- www.vm.ee (Ministry of Foreign Affairs): unreachable

How the attack took place ? Cont..



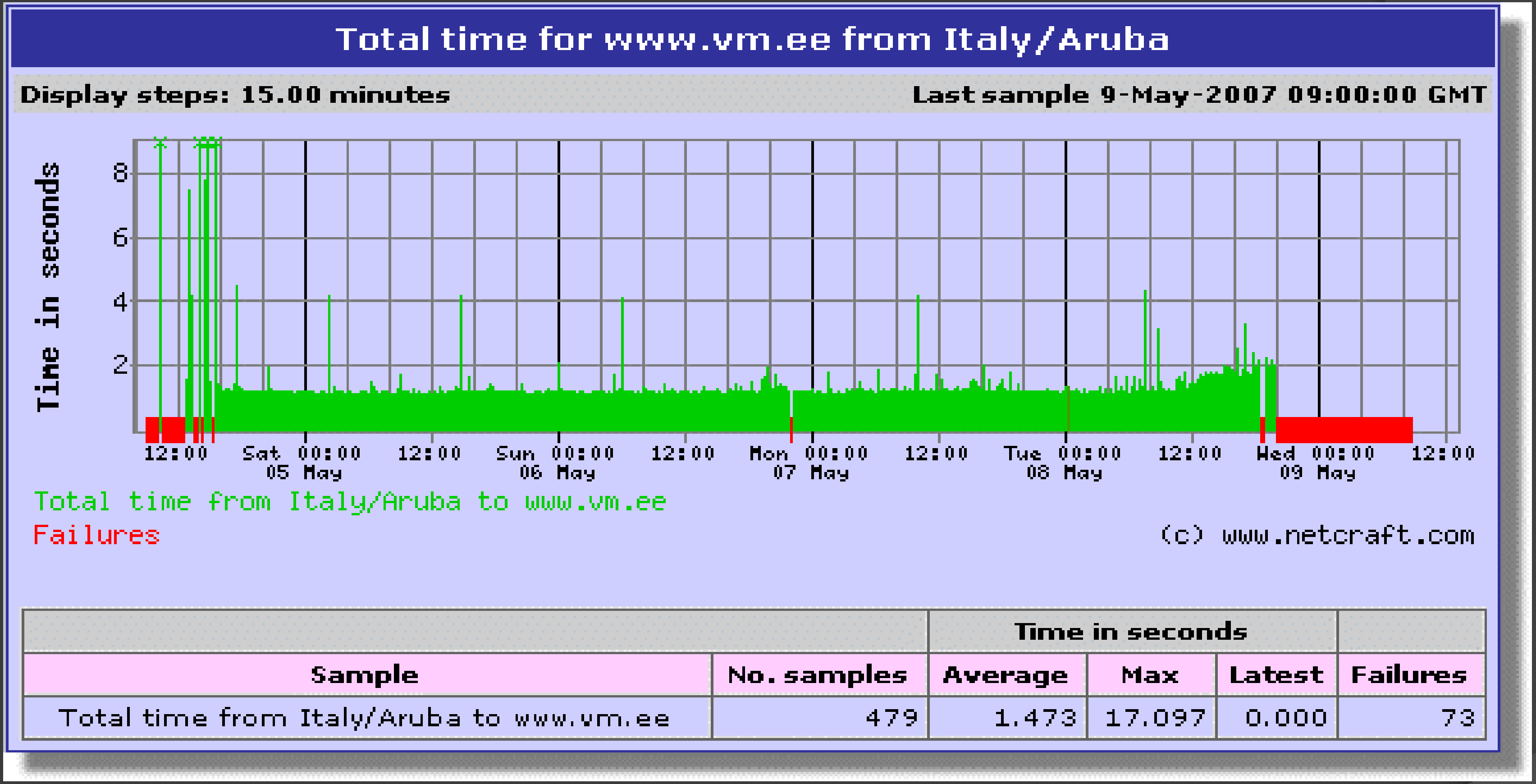
Total time for www.valitsus.ee from San Jose/Datapipe

Display steps: 15.00 minutes Last sample 30-Apr-2007 06:15:00 GMT

		Time in seconds			
Sample	No. samples	Average	Max	Latest	Failures
Total time from San Jose/Datapipe to www.valitsus.ee	166	2.452	16.405	0.000	84

- www.valitsus.ee has been analysis by the Netcraft.
- The web site was under attacked on 29 April to 30 April.
- The red color on the diagram shows the website failure and been attacked.
- The green color on the diagram shows the websites can be access but require long time to access.

How the attack took place ? Cont..



Total time for www.vm.ee from Italy/Aruba

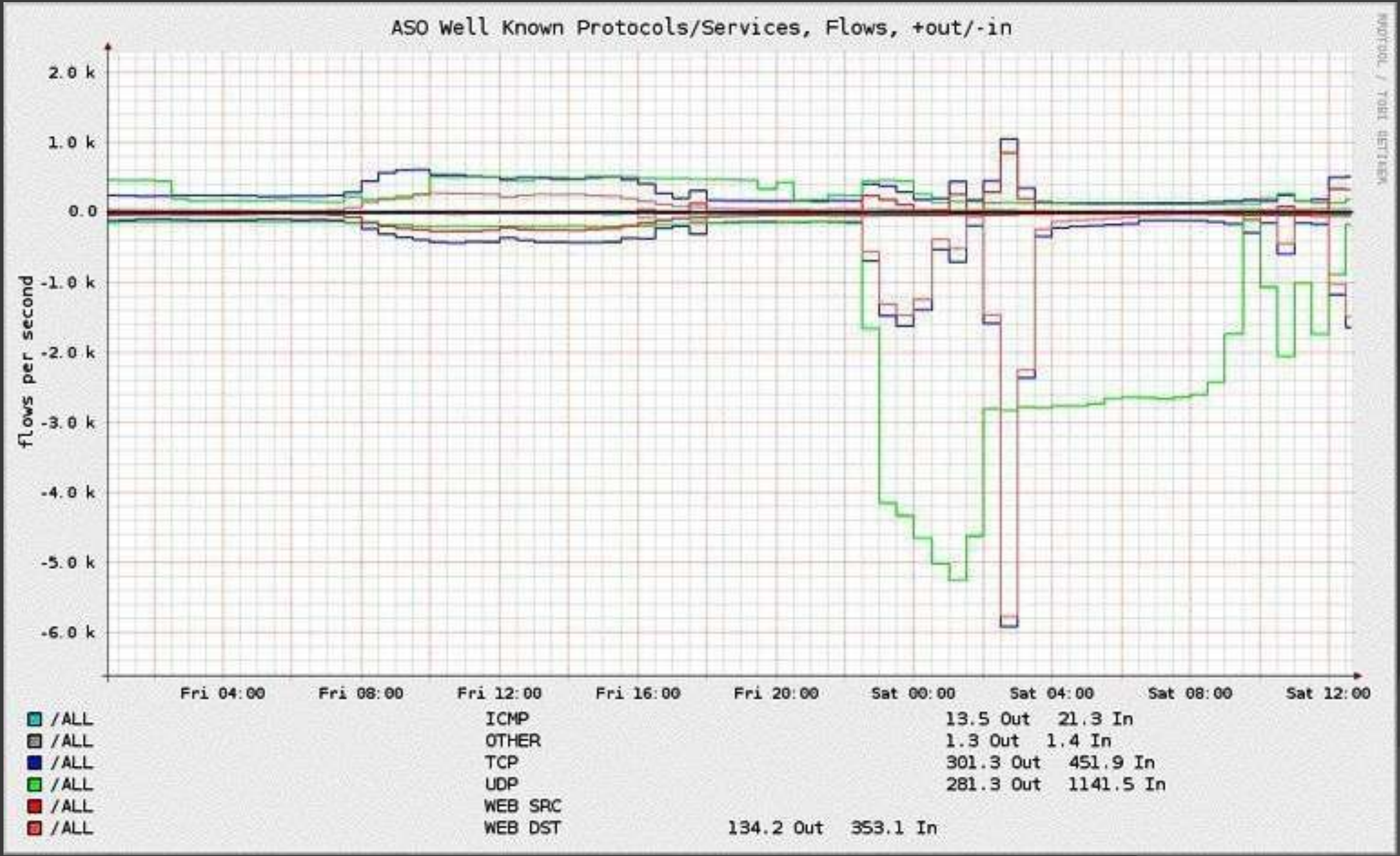
Display steps: 15.00 minutes

Last sample 9-May-2007 09:00:00 GMT

		Time in seconds			
Sample	No. samples	Average	Max	Latest	Failures
Total time from Italy/Aruba to www.vm.ee	479	1.473	17.097	0.000	73

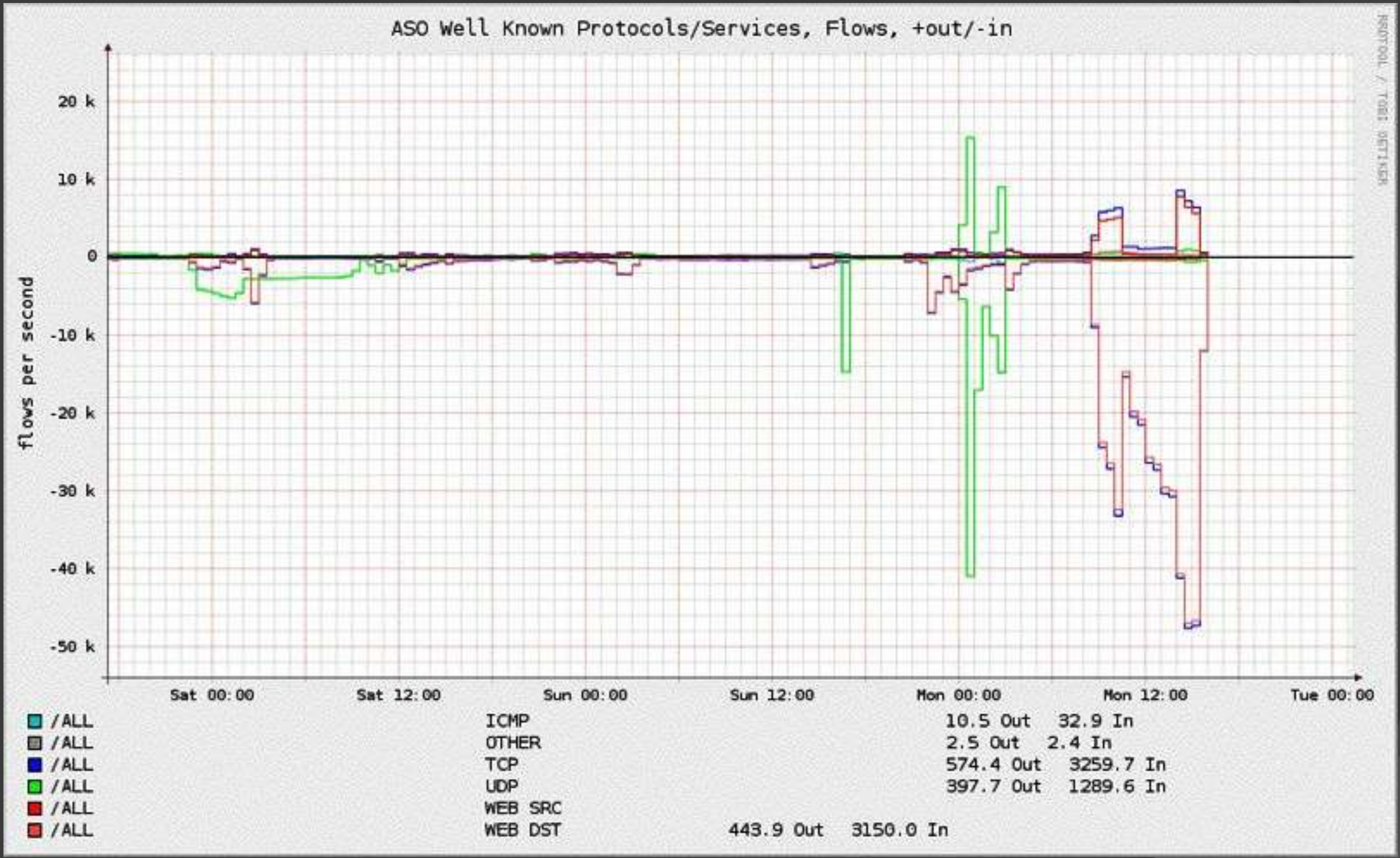
- Massive attack on the 9 May 2007, large of botnet attack against multiple Estonian targets DDoS.
- The red color on the diagram shows the website can’t been access.
- The green color on the diagram shows the website traffic clear well accessibility.

How the attack took place ? Cont..



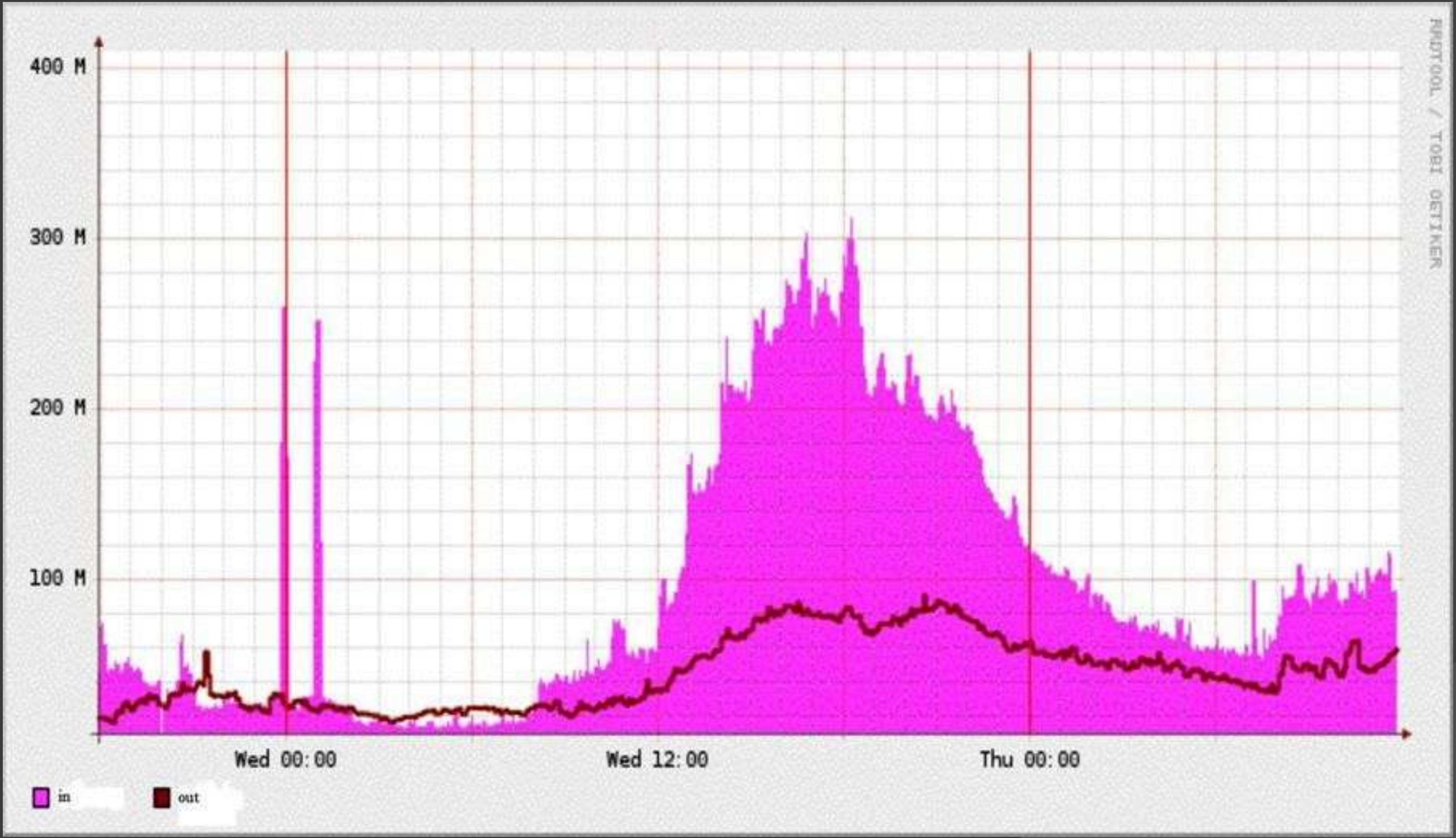
- Attack on the 27th April 2007.
- The incoming traffic (-ve scale) more than outgoing (+ve scale).

How the attack took place ? Cont..



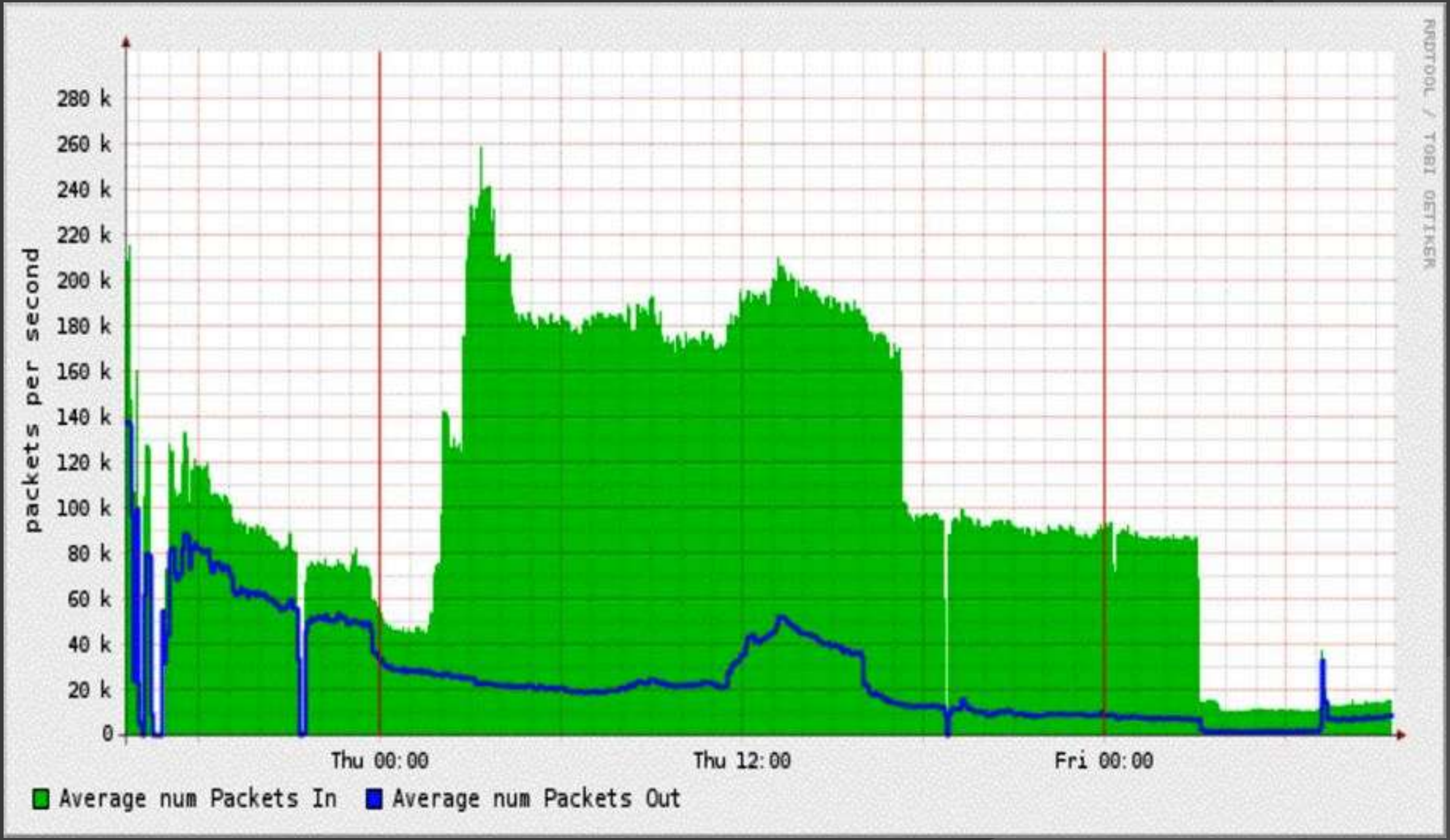
- Attack on the 28th – 30th April 2007.
- The incoming traffic (-ve scale) more than outgoing (+ve scale).

How the attack took place ? Cont..



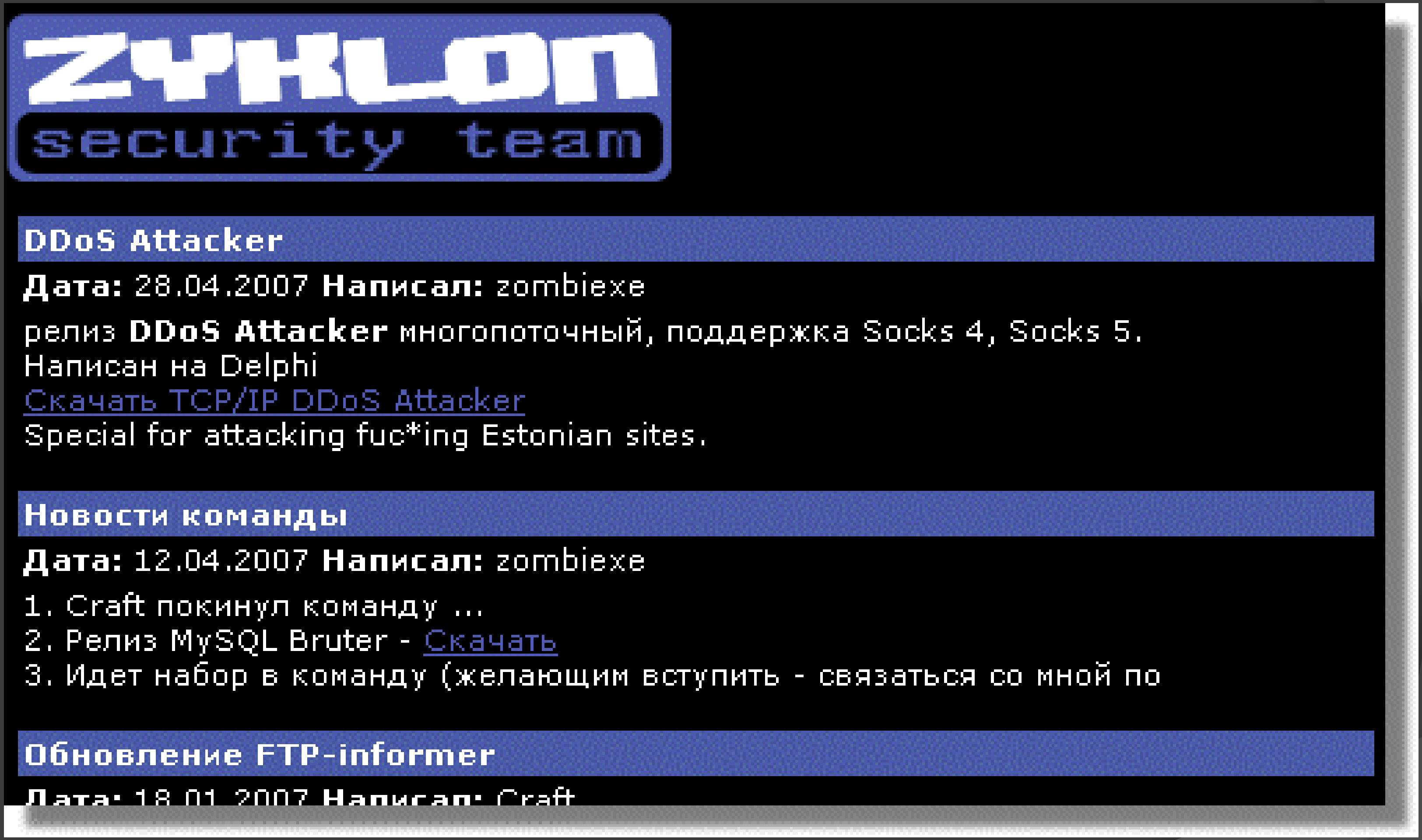
Traffic in bps on 2nd May 2007

How the attack took place ? Cont..



Traffic on 11th May 2007

How the attack took place ? Cont..



ZYKLON security team

DDoS Attacker

Дата: 28.04.2007 **Написал:** zombiexe

релиз **DDoS Attacker** многопоточный, поддержка Socks 4, Socks 5.
Написан на Delphi
Скачать TCP/IP DDoS Attacker
Special for attacking fuc*ing Estonian sites.

Новости команды

Дата: 12.04.2007 **Написал:** zombiexe

1. Craft покинул команду ...
2. Релиз MySQL Bruter - Скачать
3. Идет набор в команду (желающим вступить - связаться со мной по

Обновление FTP-informer

Дата: 18.01.2007 **Написал:** Craft

- Russian hacker site, offering Denial of Service(DoS) tools on internet.

How Estonia overcome the attack ?

- Estonia's Computer Emergency Response Team (CERT) acted as a coordinating unit, concentrating its efforts on protecting the most vital resources.
- Closing down the sites under attacked to foreign internet addresses and keep the sites only accessible to domestic users.
- Cutting 99% of bogus traffic which was originated outside Estonia.
- Implemented an online "diversion" strategy that made attackers hack sites that had already been destroyed.
- Implemented advanced filters to the traffic, then Cisco Guard was installed to lower malicious traffic.

How Estonia overcome the attack ?

- Identification and further blockade of bots from root DNS servers.
- CERT persuaded ISPs around the world to blacklist attacking computers which overwhelm Estonia’s bandwidth.
- Germany, Slovakia, Latvia, Lithuania, Italy and Spain supported and funded CERT the hub in the Estonian capital Tallinn to protect the security.
- Block all .ru domain.
- The president gave up his own website and let them continue to attack it so that they would not be able to destroying more critical things.

How Estonia overcome the attack ? Cont.

- The Estonian CERT analyze server logs and data to find out who is behind the attacks.
- NATO assisted Estonia in combating the cyber attacks and has voted to work with member governments to improve cyber security.
- NATO's new cyber-warfare center will be based in Tallinn.
- Estonia called in July 2008 for an international convention on combating computer-based attacks.

How did they trace the IP of the attacker ?

- The only problem with launching the DDoS and Zombie attack is that you need to send out the virus first, that leaves a signal of your IP.

- Once it is downloaded to your zombielike computer which needs to receive instructions, so the creator of the virus will send out the target and they start attacking the website by using up lots of data, in fact too much that it even crashes it.

- But to send out the command you will need to send out a signal which also contains your IP which has been spoofed.

- CIA and the MI6 tech boffs will have to find the IP of the attacker that went to spoof the IP for years.

Reference

- http://www.dcestonian.com/estonews/articles/07/cyber1217.htm
- http://www.nato.int/
- http://computer.howstuffworks.com/die-hard-hacker1.htm
- http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia#cite_note-epl-7
- http://www.valitsus.ee/
- http://www.ria.ee/xroad/presentation/
- http://blog.wired.com/27bstroke6/2007/08/cyber-war-and-e.html
- http://news.cnet.com/Cyberattack-in-Estonia-what-it-really-means/2008-7349_3-6186751.html
- http://www.f-secure.com/export/sites/fs_global_site/2007/1/WrapUp_H1_2007.pdf
- X-Road_regulations.pdf
- xtee_mess.ppt
- X_road_overview.doc

The End