CESNET

(D)DoS attacks targeted the www services operated in The Czech Republic

Andrea Kropáčová

andrea@cesnet.cz, CESNET a. l. e.

andrea@csirt.cz, CZ.NIC a. l. e.

CSIRT.CZ
powered by CZ.NIC

CESNET a. l. e.

- http://www.cesnet.cz/
- Established in 1996 by all Czech universities and CAS
- Members
  - 25 Czech universities
  - Academy of Sciences of The Czech Republic
  - Police Academy of The Czech Republic
- Main goals
  - operation and development of the Czech NREN
  - research and development of advanced network technologies and applications
  - broadening of the public knowledge about the advanced networking topics

CZ.NIC a. l. e.

- CZ.NIC, a. l. e.
- Founded by leading ISP in 1998
- 109 members (membership is open)
- Noncommercial, neutral
- ~70+ employees
- Key activity – operation of the domain .cz
- MoU with MoIT and NSA
- Other activities
    - research and development in area of security
    - **operating of CSIRT.CZ** (National CSIRT of Czech Republic)
    - education, trainings ...

(D)DoS attacks

- Between 4th and 7th March 2013
  - two waves every day – 9-11am, 2-4pm
- Target: www servers operated in the Czech Republic
  - very visible ==> very popular and attractive for media :-)
- Good order of targets
  - Monday 4th March – most visited news' media www servers
  - Tuesday 5th March – the most widely used search engine (seznam.cz)
  - Wednesday 6th March – bank websites
  - Thursday 7th March – 2 mobile operators

(D)DoS attacks – technical aspects

- Source: RETN through NIX.CZ
- (D)DoS
- Methods: SYN-Flood, IP-Spoofing, reflection („bouncing“)
- For ISP „weak“
  - low volume (up to 1Gbps)
  - packet rate ~ 1 – 1.5 ps (detectable)
- For end-networks or services strong enough
  - traffic concentrated to the one point
  - FW died, LB died ..., syn-cookies was not applied

(D)DoS attacks – defence

- Used solution
  - Filtration, scrubbers
  - Controlled shutdown of service (waiting for the end of attack :-)
  - Moving service to another address space (short TTL in DNS)
  - Traffic restriction just for networks in Czech Republic

- ISP and end-networks and services administrators
  - They knew what to do
  - They communicated and co-operated well
  - If it was possible they shared relevant information

CERT/CSIRT in Czech Republic

- **CESNET–CERTS** (established 2004)
  - Operated by CESNET, http://csirt.cesnet.cz/
- **CZ.NIC–CSIRT** (established 2008)
  - Operated by CZ.NIC, http://www.nic.cz/csirt
- **CSIRT–MU** (established 2008)
  - Operated by Masaryk university in Brno, http://www.muni.cz/csirt
- **ACTIVE24–CSIRT** (established 2012)
  - Operated by Active24 (important domain registry)
- **CSIRT.CZ**, National CSIRT of the Czech Republic (established 2008)
  - Operated by CZ.NIC, http://www.csirt.cz/
- ***Governmental CERT***
  - *National Security Authority, http://www.nbu.cz/*

(D)DoS attacks & CERTs

- All CERT/CSIRT teams were involved
  - information, data and contact sharing
- CSIRT.CZ
  - communication and coordination center
- Hunting attacking machines
  - looking for malware (CSIRT-MU, CESNET-CERTS)
- Communication with RETN
  - CSIRT.CZ, Active24-CSIRT
- VC meeting on Wed 6th March
  - CSIRT.CZ, CESNET, CSIRT-MU, NIX, GTS, Ceska sporitelna
- CZ.NIC-CSIRT created a „DDoS generator”
  - verification of volume of the attack

(D)DoS attacks – lesson learned

- Great exercise!
- Community is able to cooperate
  - and share info, know-how and data!
- Facebook could be helpful :-)
  - Seznam.cz informed users via Facebook profile
- Honeypots should be secured and monitored also ;-)
  - reflection („bouncing“) mechanism
- Legislation as a block for cooperation
  - some subjects had data and wanted to share them, but they couldn't as we have Electronic Communication Act
- Media apocalypse
  - We dedicated 1 (Mon), 2 (Tue, Wed), 4 (Thu) persons for PR --> was not enough, catastrophic scenarios were published

(D)DoS attacks – “benefits”

- Discussion about security and anti-ddos methods started
  - at ISP level and end-network level
    - ingress filtering
    - anti-ddos methods
    - principles of defense, tools, “security as a service”
  - at national/governmental level
    - several meetings, workshops, presentations
    - NSA established „expert working group“
  - at NIX.CZ level
    - about policy
    - closer cooperation in case of severe problem

(D)DoS attacks – “benefits”

- ISP and administrators are more willing to **cooperate** and **share** data and knowledge
- Network and services admins pay more attention to
  - **security**
    - ask for special workshops
    - want to recommend basic security tools and methods
    - want to test their infrastructure
  - **results (warnings) produced by security tools**
    - willing to share them
    - want to analyze them
    - want to correlate them

(D)DoS attacks – conclusion

- Impacts – primarily in media :-)
- Damages
  - Human resources, work, salary, advertising ... YES
  - Reputation...? ... NO
- There is still trust to system
  - No leakage of users data or sensitive data
  - No money stolen
- Areas for improvement were identified
  - Technical
  - Organizational
  - Cooperation

(D)DoS attacks – conclusion

Great exercise!

Thanks to ENISA for CE2010, CA2011, CE2012!

Thank you for your attention!

CESNET, a. l. e.

Andrea Kropáčová / andrea@cesnet.cz