March (D)DOS attacks in Czech Republic

Jaromir Talir • jaromir.talir@nic.cz • 28.05.2013

CZ DOMAIN REGISTRY

Agenda

- Targets
- Types of attacks
- Cooperation during attacks
- Reactions
- Countermeasures
- Conclusions

Targets

- Systematic selection of most popular targets
  - Monday 4.3. – Most popular news servers
  - Tuesday 5.3. – Biggest portal seznam.cz
  - Wednesday 6.3 – Most popular banks
  - Thursday 7.3 – Two major mobile operators
- Timing was usually 9-11am & 14-16pm
- Websites and other services unaccessible
  - E-commerce, Public transport SMS tickets

Types of attacks

- SYN Flood
  - SYN packets with DST address of target and many spoofed SRC addresses
- TCP reflection attack
  - SYN packets with DST addresses of routers and SRC address of target
- Strength was not big: 1-1.5 Mpps (<1 Gbps)
  - Impact on badly configured firewalls, load balancers etc..

Cooperation during attacks

- CZ.NIC operates national CSIRT team
  - Incident reporting
  - Coordination infrastructure
- Activity during attacks
  - Information exchange (conference call)
  - Data analysis
  - Media communication

Cooperation during attacks

- Good cooperation of targets with their ISPs
  - Technical support
  - Assistance with mitigation
- Soon became evident that all traffic comes from RETN network (via peerings in NIX.CZ)
  - People trying to find help in RETN failed
  - Later RETN provided information that it was customer network and that there are no data to help in investigation

Reactions

- Big media impact
  - Title pages in newspapers (“who will be the next?”)
  - TV news headlines
- Legal activities
  - Police announced investigation
  - Timing of attacks correlated with finalization of controversial anti-cybercrime law

Countermeasures

- Infrastructure upgrades and reconfiguration
  - Enabling SYN cookies
- NIX.CZ initiatives
  - Remotely triggered black hole filtering platform
  - Parallel “secure” VLAN for cooperating partners
    - Must implement BCP 38
    - Must be easily contactable
    - In case of attack, victim can leave “unsecure” VLAN and still is reachable

Conclusion

- Attacker will hardly be identified
  - Could be anybody (rather single source DOS than DDOS)
  - Somebody with deep insight into Czech market
- Most of operators cooperated well
- CSIRT team experiences proved to be useful

Thank You

Jaromir Talir • jaromir.talir@nic.cz

CZ DOMAIN REGISTRY