.tr DDoS Attack

December 2015

Attila Özgit
.tr ccTLD Manager
Dec, 2015 .tr DDoS Attack

A Summary of a 3 weeks long experience ...
Before DDoS

- Infrequent Small scale DoS and DDoS Attacks
  - Few times every year
  - 5-30 mins. each
  - Mostly to our registry services
    - www.nic.tr

- 6 NS at 5 different locations
  - All open source
    - Linux, Bind, NSD
  - Average Bandwidth: 1.5 Mbps per server
  - 1.250 QPS per server
Communication Infrastructure

- 3 major ISPs serving TR Internet
  - Each connected to Tier-1 at various locations
    - No topology info on our side
  - Abstraction: 3 major pipes to TR
- 4 NSs downstream of ISP-A
- 1 NS downstream of ISP-B
- 1 NS @Europe
Anatomy of the DDoS

[Diagram showing the anatomy of a DDoS attack, with an attacker sending spoofed UDP packets to a botnet, which then sends queries to open authoritative DNS servers that are not rate-limited. The queries are amplified by 10th to 150th in nic.tr DNS servers.]
DDoS Attack

- Started at 14 December 2015 10:20
  - Went on nearly for 3 weeks
  - Towards the end, changed its target to Finance and Government sectors
- Basically a "DNS (UDP) Amplification Attack"
  - Botnets sending spoofed query packets to
    - Open DNS resolvers
    - Authoritative DNS servers (no rate limiting)
  - Amplified by 10-150 times by victims
  - %25 of victims are from TR IPs
  - Targets 6 NS Servers
  - Secondary target was our registry services (Web)
During the Attack ...

- Mainly between 09:00-17:00
  - Working hours! (1\textsuperscript{st} shift)
  - 185,000 QPS per server
- Reduced rate and different nature of attack during 2\textsuperscript{nd} and 3\textsuperscript{rd} shift
- All NSs were almost always up
  - Reachability and delay problems due to overloaded pipes
- Volume
  - One ISP reported 220 Gbps attack bandwidth
  - No synchronized picture of attack history
- Might be one of the largest DDoS attack observed at the time
Basic Defense Mechanisms

- Make the surface to be attacked wider
  - Increasing the # of NSs
- Analyze traffic
  - Figure out drop rules to be used
- Adaptively react by reconfiguring mitigation services and devices
  - Attackers were highly adaptive to our defence
Observations

- Major attack classes
  - UDP flooding
  - Spoofed packets
    - Source Port 53, Destination Port 53
    - ...
    - Almost all known attack patterns

- Other attacks
  - Application attacks
    - TCP based

- No Ingress/Egress filtering in subnets
- 8% of registered NSs in our registry DB are “Open Resolvers”
Observations and Lessons

- **Importance of quick RZM mechanisms**
  - Updates were not quick enough
    - DOC Checks *(Not Anymore)*

- **Effective communication mechanisms**
  - Within the registry tech team
    - Use of Near Real Time technologies (Chat, etc.)
  - Between Registry and Upstream Operator
    - Tech team correspondance
  - Critical communication should be in written form
    - Rules to be coded
  - All critical communication should be tolerant to DNS failures

Dec 2015 DDoS Attack on .TR
Observations and Lessons

- Effective (and concurrent) communication with
  - IANA/ICANN
  - Other ccTLDs
  - Other organizations within the country
    - National CERT
  - Press (Media)
  - Upstream operators
After the Attack

- Infrequent, relatively light, 5-10 minutes DDoS Attacks are still coming in

- Administrative measures
  - List of critical domain names (Gov, Banks, etc.) expanded
    - $100 \rightarrow 600 \rightarrow 1,000+$

- Temporarily
  - Zone Updates are done 3 times per day
  - Manual inspection of zone updates
Current DNS infrastructure

- 8 ns for tr.
  - 2 of 8 are ANYCAST (DynDNS)
- 12 ns for second level (com.tr, gov.tr etc...)
  - 3 of 12 are ANYCAST (DynDNS, PCH)
- With ANYCAST 100+ DNS servers
- Isolated zone creation
  - Locked critical names
  - Automated security checks
  - Security checks by humans
- Multiple hidden master servers
Thank You