DDoS Mitigation Playbook

DDoS Scope: ccTLD DNS infrastructure

TLD-OPS Workshop

Version 1.0 - April 25, 2018

Workshop Overview

The goal of the workshop was to explore how TLD-OPS members can collaborate to develop a DDoS Mitigation Playbook. The focus was on DDoS targeted at the unicast and anycast Authoritative DNS infrastructure, operated by the ccTLD and their DNS provider partners.

Motivation

This workshop was in response to the TLD-OPS DDoS Mitigation workshop held at ICANN58 in Copenhagen on March 12, 2017. Since DDoS attacks may have a severe impact on the target (and potentially collateral damage for others), the TLD-OPS Standing Committee believes it is important to mobilize the collective experience of the TLD-OPS community to develop and document a framework to better prepare the ccTLDs in responding to DDoS attacks.

The workshop facilitated this dialog through sharing of experiences, discussion, and generation of ideas.

TLD-OPS DDoS Mitigation Workshop #2- ICANN61, 2017-10-29, General Observations

We had a smaller group for this workshop: 22 people. This allowed for good dynamics & collaboration. We gathered in front of a single flipchart, went through previous workshop results, and expanded each topic to focus on elements that would be part of the guidebook, for each lifecycle stage. The results that were captured in flip charts are interpreted in this document.

The life cycles for 'effective' DDoS mitigation are:

- Identify
- Protect
- Detect
- Respond
- Recover

The scope of this document is not to develop a complex security framework for DDoS mitigation. The goal is to highlight the important components in each life cycle for a ccTLD to be effective in mitigating a DDoS attack (if and when implemented).

It was mentioned in the workshop that it's always a good idea to implement best practice such as IT (ITIL) Service Operations and Information Security Management (cybersecurity).

IDENTIFY:

The objective of IDENTIFY is to document and understand your ccTLD DNS infrastructure before an attack occurs -- to know who to call, who to rely on, who to notify (and the escalation path for issue resolution). Ensure you have a solid relationship with your ISPs, vendors, the government, the press, the registrants and the internet users of your ccTLD. This is the work that needs to be performed on an ongoing basis before an attack occurs.

CONTACTS	
Your ccTLD Management Team	Title, name, phone number, home phone number, home email (Chair - Board of Directors)
IANA Emergency Number	+1 (310) 306-6308 (to be updated)
Anycast Vendors	SOC/NOC email and phone numbers, contact numbers
Transit ISP Upstream	SOC/NOC email and phone numbers, contact numbers
In Country ISP	SOC/NOC email and phone numbers
CERT	SOC/NOC email and phone numbers Contact name, phone number, email
Major Resolver Operators (Recursive)	IP addresses Operator, email and phone numbers
TLD-OPS Contact List	Access to TLD-OPS contact list
Press	Contact name, phone number, email
Regulator	Contact name, phone number, email
Software Vendors	Contact name, phone number, email
Forensics consultant	Contact name, phone number, email
Registrants	Method to reach registrants effectively
Other relevant contacts	

Clearly documenting your ccTLD DNS infrastructure:

It is very important to clearly document your ccTLD DNS infrastructure, which name servers you have in operation, their physical location, the network connections, the transit providers, IXP connections, Anycast providers, the capacity of each transit and IXP link.

This is the asset that you need to protect.

ccTLD Name Server, IPv4 and IPv6 addresses.

- Example…
- ;; AUTHORITY SECTION:
- dk. 172800 IN NS a.nic.dk.
- dk. 172800 IN NS b.nic.dk.
- …
- ;; ADDITIONAL SECTION:

- `a.nic.dk.  172800  IN  A  212.88.78.122`
- `b.nic.dk.  172800  IN  A  193.163.102.222`
- `b.nic.dk.  172800  IN  AAAA  2a01:630:0:80::53`
- …

Accurate DNS, Network and Server topology:

Document the network, server and software architecture for your ccTLD DNS infrastructure, and update this on a regular basis.

<Insert network diagrams here>

- Provide links to network and topology diagrams

Hidden Master IP addresses

Hidden Master	
IP Address	Access list details (in case you need to add a new provider)
How to add	Quick steps to add a new name servers…

DNSSEC Signing Infrastructure

Add details of your DNSSEC Infrastructure and Key storage/protection here.

Important Recursive Name Servers using your ccTLD (example would be large ISP recursive name servers in your country service a large population)

Recursive	
ISP Name	IP Addresses
How to whitelist	Quick steps to whitelist some recursive?

Keeping your information up to date:

Access to important Information	
Password Safe	Location (to login in routers and servers)
Equipment Inventory	Location (what's the IP address, name)
Communication plan	Location (how do we reach out, communicate)
Roles and responsibilities	Location (who does what when)
DR, BCP plans	Location

Risk management process:

Identify risks and the associated impact and likelihood if they were to occur, and map this on the business impact analysis for the ccTLD resolving service(s). Create a process to regularly review and update this document.

Change management process:

It is critical that this information stays current; implement processes to keep this information up to date. Create a quarterly process to review and update this document.

PROTECT:

The goal of PROTECT is to develop and implement the appropriate safeguards to ensure delivery of your ccTLD authoritative DNS services, and to enable the ability to contain or limit the impact of a DDoS attack.

Specifically against DDoS attacks, the outcome of PROTECT is to develop and implement best security practices such as access controls, protective technologies, diversity and DNS architecture. This section focuses on identifying best security practices (processes) for technology, people, and partners.

Technology:

Implement safeguards to ensure secure and stable operations.

Access lists:

- ACL where appropriate, only allow traffic to destination port 53 (TCP/UDP)
- ACL for out of band management

Anycast:

- Implement global anycast DNS topology to increase delivery resiliency
- Deploy local anycast nodes to increase delivery resiliency (DNS Nodes without global transit), preferably by:
    - Extending your global anycast DNS with local anycast nodes that serve a specific 'important' resolver community (major in country ISP, government, regional networks)
    - Adding local anycast nodes at key IXPs

Other safeguards:

- DNS server software diversity (Bind, NSD, Knot, etc…)
- Remotely triggered black hole (RTBH) filtering
- DDoS mitigation hardware
- Implement RRL (a must)
- Protection of management interface (separate physical port/cable, transit, VPN tunnel, …)
- Sufficient system resources (from a capacity view)
- Sufficient network connectivity and diversification in the selection of service provider (ISP, IXP, etc.)

People/Process:

Train IT team

- Security Awareness Trainings
- Annual exercise <- share script on TLD-OPS & DDoS attack simulation
- Configuration hardening (best practice, …) and PEN testing
- How to use external DNS monitoring tools (i.e. DNSMON, DNS-OARC, BGPMon or similar?)
- No manual changes, use config and change management process

Work with ISP (transit providers) in advance

- Find out how they can help to mitigate future DDOS events
- Make sure they understand the importance of your ccTLD

Partners:

Work with partners where DDoS mitigation services can be of use:

- Add 3rd party permanent anycast providers
- Secure emergency 3rd party anycast providers
- Investigate DDoS Scrubbing services

DETECT:

The goal of DETECT is to develop and implement the appropriate activities to identify -- in a timely manner -- the occurrence of a DDoS attack, and to determine the scope and breadth of the DDoS attacks. The better the detection mechanism is, the more effective the mitigation techniques can be.

The outcomes for DETECT are internal and external DNS monitoring and detection processes.

Monitoring:

Internal Monitoring

- SNMP monitoring traffic (router, servers, links)
- Threshold alarms notification (sms, email) resilience
- Understand normal operation for each node.
- DNS Analysis tools
- PCAP Capture (provides a full picture when incident occurs, but traffic volumes can create an internal DoS when under DDoS attack, see note below)

External Monitoring

- External RIPE Atlas DNSMON (DNS query response time, query loss and trends)
- ISP transit link statistics (real usage of outbound traffic to your DNS node)
- ICANN SLA Monitoring (ICANN Monitoring System API (MoSAPI)) (still in early adoption for ccTLDs)
- Netlabs 360 - https://ddosmon.net/

Scalable tools (functional under DDoS mode)

- PCAP, some tools may break under DDoS or negative affect operations
    - Procedure to disable temporarily data collection in adverse conditions
    - Real-time remote log shipping to make sure no data loss occurs

Identifying the type of attack:

Understand the attack

- Type of attack
- List of classic attacks, profile, and tools and mitigation
- Origin (where is it coming from?)
- Which nodes (what's impacted)
- What is the real impact to internet users?

RESPOND:

The goal of RESPOND is to develop and implement the appropriate activities to take action regarding a detected DDoS attack. The respond function supports the ability to mitigate the impact of a potential DDoS event.

The outcome of RESPOND includes response planning, communications, analysis, and mitigation.

Response Plans:

DON'T PANIC! The community will most likely detect the occurrence of a DDoS on your ccTLD at the same time you do, and the community will want to help you mitigate the attack.

- Communicate
- Continue Analysis
- Solve the problem
- Focus on the core of the problem
- Document {what you change, and observations}

Communication Plan:

Communication is key in mitigating the attack.

Communication Mechanisms	
Local CERT	Contact local CERT even if the attack is not fully identified
TLD-OPS	Send email to tld-ops@dns-oarc.net Ask for help with further attack identification
Conference Bridge	Ask TLD-OPS/ICANN to open a conference bridge to collaborate on mitigation
Outreach	Ask/authorize TLD-OPS members to reach out on alternate mailing list/groups to assist in attack mitigation
other	

RECOVER:

The goal of RECOVER is to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a DDoS attack. The recover function supports timely recovery to normal operations to reduce the impact from a DDoS attack.

The outcomes of RECOVER include recovery planning, improvements, lessons learned, and communications.

Recovery:

- Roll back from temporary measures
- Restore DNS infrastructure to original state
- Document permanent changes
- Compile notes

Lessons Learned:

- Hold post-mortem meeting with relevant (internal) stakeholders
- Document:
    - What worked
    - What didn't
    - Identify improvements

Improvements:

- Identify
- Evaluate
- Share
- Implement improvements

Communications:

- Communicate to partners, customers, employees, registrants