Attacks Against The DNS, DNS Monitoring & Countermeasures

Dave Piscitello
VP Security and ICT Coordination
27 June 2016
dave.piscitello@icann.org
Introduction

- VP Security and ICT Coordination, ICANN
- 40 year network and security practitioner
- Roles at ICANN:
  - Technology Advisor
  - Threat responder
  - Investigator
  - Researcher
Agenda

• Overview of the DNS attack landscape
• Attack mitigations and countermeasures
• DNS Monitoring
Attacks Against Name Servers Or Recursors

- “Exploit to fail” Denial of Service (DOS) attack
- “Exploit to own” DOS attack
- Reflection attack
- Amplification attack
- Distributed DOS attack
- Cache Poisoning attack
- Resource Depletion (Exhaustion) attacks
Attacks Involving Stub Resolvers

• Query interception attack
• DNS Response modification
• Configuration poisoning attack
• DNS hostname overflow attack
• DNS as a Covert Exfiltration Channel
• DNS as a Covert Malware Channel
## Summary

1. The DNS is an open system and *open also to abuse*

2. The DNS is a critical Internet database and thus a *target* for attack

3. Any element of the DNS may be *exploited* to facilitate other attacks
Agenda

• Overview of the DNS attack landscape
• Attack mitigations and countermeasures
• DNS Monitoring
Begin With Resource And People Planning

• Inventory assets
• Assess and mitigate risks
  – Identify threats, vulnerabilities and bottlenecks
• Plan
  – Initial Response and Abatement
  – Escalation
• Conduct ongoing intelligence
  – Information to help you identify whether you or your industry are potential target, and why
Resource And Relationship Management

• Know your allies: Maintain points of contact for
  – Mitigation providers
  – Upstream ISPs
  – Hosting providers
  – Vendors and security service technical support
  – CERTs
  – Friendlies, e.g., security community
  – Law enforcement
  – Regulatory authorities (if applicable)
Configuration Management

• Keep software or firmware up to date
  – Operating systems
  – Name server software
  – Security and network systems

• Validate and archive
  – “last known working” configurations
  – zone data
  – Infrastructure topology
Domain Name Registration Protection

- Maintain complete/accurate points of contact
- Monitor Whois record for unauthorized change
- In case of unauthorized transfer, keep records
  - Domain names, proofs of payments, registrar correspondence
  - Demonstrations of use: system/web logs, site archives
  - Legal documents: proofs of incorporation, tax filings, passport, other proofs of identity
  - Any documentation that demonstrates an association between the domain name and you
Be A Good Citizen

Don’t let criminals use your resources to attack others

• Eliminate IP-spoofing (BCP 38)
  – Only allow traffic to exit your networks that uses addresses from blocks you use

• Eliminate open resolvers (BCP 140)
  – Configure your resolvers to only process DNS queries from your networks and hosts

• Add Response Policy Zones to your resolver
  – RPZs are lists of domain names that your name servers should not resolve
Deploy DNS Defenses in Depth

Interpose layers of defense between attackers and your DNS infrastructure.

Mitigation providers and upstream ISPs

attackers

Firewall

DNS proxy, DDoS, or DNS protection Appliance(s)

Name servers, recursors
Add Redundancy To Your DNS: Fail Over

Primary processes 100% of traffic

Secondary processes 0% of traffic

DNS server

Firewall, Switch

DNS server

Secondary processes 100% of traffic

DNS server

Firewall, Switch

DNS server
Add Redundancy To Your DNS: Load Balancing

Primary processes $n\%$ of traffic

When traffic exceeds $n$ secondary is added

Where else can redundancy or diversity be implemented?
Recommended DoS Mitigation Measures

- Anycast routing
- DNS service segregation
- DNS intrusion defenses
- Redundancy and diversity measures
- Over-provisioning?
Anycast Routing For Name Servers

- **Unicast**: one DNS host, one IP address
- **Anycast**: many DNS hosts, one IP address
  - Routing forwards to closest available

Internet user

192.168.11.1

If this DNS server is unreachable, names are resolved using another with same IP
Example: Root Name System

- **Diversity:**
  - Geography
  - Hardware
  - Software
  - Bandwidth
  - Administration

- **Redundancy**
  - Failover
  - Load balancing
  - Anycast IP
DNS Service Segregation

• Design network topology so that critical infrastructure is protected against side attacks
• Run DNS services on separate network segments from other services
• Run authoritatives on separate network segments from recursors
• Separate client networks from services
• Customized defenses for each segment
DNS Security (DNSSEC)

• Protects DNS data against forgery
• Uses public key cryptography to sign authoritative zone data
  – Assures that the data origin is authentic
  – Assures that the data are what the authenticated data originator published
• Trust model also uses public key cryptography
  – Parent zones sign public keys of child zone (root signs TLDs, TLDs sign registered domains...)
Public Key Cryptography in DNSSEC

- Authority signs DNS data with *private* key
  - Authorities must keep private keys secret!
- Authority publishes *public* key for everyone to use
Public Key Cryptography in DNSSEC

• Any recipient of the authority’s DNS data can use the public key to verify that “the data are correct and came from the right place”
How DNSSEC defeats data poisoning attacks

Stub resolver rejects attacker’s DNS data as not validated

Validating recursor rejects attacker’s DNS data as not authentic

Authoritative server

Validating recursive server
Agenda

• Overview of the DNS attack landscape
• Attack mitigations and countermeasures
• DNS Monitoring
Real Time Traffic Analysis & Policy Enforcement

- Certain attacks change host configurations or resolver data
  - DNSchanger malware
  - Cache poisoners
- Track others by examining DNS traffic
- Enforce DNS behavior using access controls or intrusion detection
- Detect or drop – and log
  - DNS malformed traffic
  - “Known malicious” or suspicious DNS traffic patterns
  - Name error responses

Image by dingcarrie
Where to Look

• Host (device) or resolver configuration
• DNS query and response traffic on networks
• Resolver and authority logs
• Event logs
  – Hosts, Security Systems, Network elements
  – Applications (clients or servers)
• Passive DNS replication (sensor networks)
## What To Look For

<table>
<thead>
<tr>
<th>DNS Access Controls</th>
<th>DNS Volumetric Attack Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofed source addresses</td>
<td>Excessive Name errors</td>
</tr>
<tr>
<td>Malformed or suspicious queries</td>
<td>Atypical DNS message sizes</td>
</tr>
<tr>
<td>Malformed or suspicious responses</td>
<td>Atypical use of TCP</td>
</tr>
<tr>
<td>Message length anomalies</td>
<td></td>
</tr>
<tr>
<td>Known bad/suspicious traffic origins</td>
<td></td>
</tr>
<tr>
<td>Known bad/suspicious domains</td>
<td></td>
</tr>
<tr>
<td>Known malicious/covert traffic patterns</td>
<td>Deviations from historical or planned traffic volume</td>
</tr>
<tr>
<td>Network traffic anomaly protection</td>
<td></td>
</tr>
<tr>
<td>Source or connection response rate limiting</td>
<td></td>
</tr>
</tbody>
</table>
How to Look

• Use traffic analyzers, Intrusion Detection Systems, or Internet firewalls to
  – Detect spoofing
  – Enforce egress traffic policy
  – Detect attempts to query unauthorized resolvers
  – Notify if excessive name resolution errors occur

• Examine critical data for “correctness” at DNS zone data and recursor caches

• Use Passive DNS replication to
  – Review what names your users are resolving
  – Populate Resource Policy Zones, domain blocklists
Summary

1. Implement an in-depth defense to mitigate DNS attacks

2. Some mitigations require allies or broad implementation

3. Some of the best mitigations are “soft” (planning or administrative)
## Reading List (Partial)

<table>
<thead>
<tr>
<th>Title</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 10 DNS attacks</td>
<td><a href="http://www.networkworld.com/article/2886283/security0/top-10-dns-attacks-likely-to-infiltrate-your-network.html">http://www.networkworld.com/article/2886283/security0/top-10-dns-attacks-likely-to-infiltrate-your-network.html</a></td>
</tr>
<tr>
<td>Manage your domain portfolio</td>
<td><a href="http://securityskeptic.typepad.com/the-security-skeptic/2014/01/avoid-risks-manage-your-domain-portfolio.html">http://securityskeptic.typepad.com/the-security-skeptic/2014/01/avoid-risks-manage-your-domain-portfolio.html</a></td>
</tr>
<tr>
<td>DNS cache busting</td>
<td><a href="http://blog.cloudmark.com/2014/10/07/a-dns-cache-busting-technique-for-ddos-style-attacks-against-authoritative-name-servers/">http://blog.cloudmark.com/2014/10/07/a-dns-cache-busting-technique-for-ddos-style-attacks-against-authoritative-name-servers/</a></td>
</tr>
<tr>
<td>Protect the world from your network</td>
<td><a href="http://securityskeptic.typepad.com/the-security-skeptic/2013/04/protecting-the-world-from-your-network.html">http://securityskeptic.typepad.com/the-security-skeptic/2013/04/protecting-the-world-from-your-network.html</a></td>
</tr>
<tr>
<td>Protect your DNS servers against DDoS attacks</td>
<td><a href="http://www.gtcomm.net/blog/protecting-your-dns-server-against-ddos-attacks/">http://www.gtcomm.net/blog/protecting-your-dns-server-against-ddos-attacks/</a></td>
</tr>
<tr>
<td>Fast Flux Botnet Detection in Realtime</td>
<td><a href="http://www.iis.sinica.edu.tw/~swc/pub/fast_flux_bot_detection.html">http://www.iis.sinica.edu.tw/~swc/pub/fast_flux_bot_detection.html</a></td>
</tr>
</tbody>
</table>
Questions?

My Contact Info:
dave.piscitello@icann.org
@securityskeptic
www.securityskeptic.com
about.me/davepiscitello

Contact ICANN:
engagement@icann.org
@icann
icann.org
safe.mn/icannsecurityteam