Common DNS threats and counter measures

Thomas Kuiper, TWNOG, December 2019

About Gandi.net

- **2.5 million domain names managed**
- **800+ extensions supported: .TW, .SG, .COM, .NEW, ...**
- **Offices in France, Luxembourg, Taiwan, United States**
- **Almost 20 years old**
- **Service in Chinese, French, English, Japanese**
- **Corporate Brand protection service**
- **Thousands of resellers**
- **Full Domain API’s**

Type of threats to the DNS system

We classify the type of attack towards the DNS in three types

Denial of Service.

Data Corruption.

Information Exposure.

Type of threats to the DNS system

Denial of Service. Data Corruption. Information Exposure.

Physical Infrastructure	Buildings, power supplies, network connections
Network Infrastructure	Servers and related systems where queries are sent and received
Management Infrastructure	Processes for creation, modification, deletion of DNS content
Administrative Infrastructure	Support agreements, fault escalation procedures, staffing
Technical Infrastructure	

Type of threats to the DNS system

Denial of Service. Data Corruption. Information Exposure.

Authority Impersonation	Impersonation of the authority, corruption of data at the source
Cache Corruption	Corruption of the data on the authoritative server
Application to Cache Corruption	Corruption of the data within a DNS cache
System Corruption	Corruption of the data in transit
Protocol Corruption	(between authority and database, between authoritative server and a DNS resolver, between a resolver and the requesting application)

Type of threats to the DNS system

Denial of Service. Data Corruption. Information Exposure.

Domain Front Running	Using WHOIS to discover which domains are available, commonly typo-squated and therefore registered
Cache Snooping	Unauthorized party has access to the DNS cache
Zone Walking	NSEC RR’s can be used to enumerate contents of a zone
NXDOMAIN redirection	ISP intercepting NXDOMAIN, resulting in redirection to third party sites and untrusted sites to deliver ads or malware
Compromised account	Login credentials are stolen, account is misused

Type of threats to the DNS system

Denial of Service.	Data Corruption.	Information Exposure.
Physical Infrastructure	Authority Impersonation	Domain Front Running
Network Infrastructure	Cache Corruption	Cache Snooping
Management Infrastructure	Application to Cache Corruption	Zone Walking
Administrative Infrastructure	System Corruption	NXDOMAIN redirection
Technical Infrastructure	Protocol Corruption	Compromised account

Mitigations using Hardening and Distribution

Denial of Service. Data Corruption. Information Exposure.

Physical Infrastructure	Physically protect systems from attack or accident
Network Infrastructure	Replicate facilities, systems, and services in multiple physical locations and using independent infrastructures
Management Infrastructure	
Administrative Infrastructure	Use multiple independent implementations for services
Technical Infrastructure	Use “Anycast” routing for DNS to reduce the risk that a denial of service (accidental or malicious) will completely disable the DNS

Mitigations using Vigilance and staying updated

Denial of Service. Data Corruption. Information Exposure.

Authority Impersonation	Increase vigilance to ensure corruptions are detected
Cache Corruption	Use DNSSEC to protect data in transit and in storage, reducing the risk of cache poisoning and man-in-the-middle attacks
Application to Cache Corruption	
System Corruption	Ensure all systems have security patches applied, are up-to-date and are configured using best practices
Protocol Corruption	Secure the transit path of DNS messages as much possible • Restrict domain name zone transfers to authorized parties • Use NSEC3 in DNSSEC to prevent Zone Walking

Mitigations by using Access limitations and Legal frameworks

Denial of Service. Data Corruption. Information Exposure.

Domain Front Running	ICANN can enforce registries and registrars (and their resellers) to abide restrictions prohibiting such behavior.
Cache Snooping	Access to caches must be limited to trusted clients.
Zone Walking	NSEC3 can be used to mitigate the risks
NXDOMAIN redirection	Ensure ISP's, hotspot providers understand the ramifications of advertisings displayed and forwarding DNS queries to ensure privacy is not compromised
Compromised account	Use Two-Factor authentication, strong passwords, and a registrar adhering to the latest security standards

There are also threats from the DNS…

DNS Amplification Attacks

As DNS responses are usually much bigger than the request there's the possible to use amplification for an attack through spoofing. Attackers are difficult to be traced back.

Fast Flux

"Fast flux" is an evasion technique that cyber-criminals use to evade identification and to frustrate law enforcement and anticrime efforts aimed at locating and shutting down web sites used for illegal purposes.

DNS as a covert channel

DNS requests and responses can be used as a channel for covert communications. DNS have been used as the mechanism for communications between botnet command and control servers that make up the botnet.

Mitigation of threats from the DNS…

DNS Amplification Attacks	Firewalls, access controls, rate limiting
Fast Flux	Early detection by registrars, Honeynet project
DNS as a covert channel	Monitoring for unusual patterns

Using Gandi.net to strengthen your domains against threats

- As Gandi customer, you can enable Two-Factor Authentication on account. Gandi supports both U2F and WebAuthn compliant software devices (YubiKey, Microsoft Windows Hello, Android 7 and later, Apple iOS13 and later) at no extra charge.
- You can create teams with multiple access levels to your domains of your organization(s) at no extra charge.
- Build your own tools using our API at no extra charge.
- Use DNSSEC with your domain name at no extra charge.
- Our Corporate customers can use Registry Lock and other measures

Using Gandi.net to strengthen your domains against threats

- Gandi's DNS is included with every domain name, located in multiple locations worldwide and using Anycast.
- We monitor our DNS infrastructure 24 hours/day, 7 days per week.
- Our datacenter infrastructure has multilevel access security

Use our Corporate Domain service to fully protect your brand, used by 500+ top brands in the world such as Gartner, Rolex, KKBOX,..

gandicorporate.com

gandi.net

no bullshit™