The evolving DNS threat landscape

DNS was not designed for security

The Domain Name System (DNS) was designed in the 1980s when Internet access was restricted to government agencies, scientists, and the military. The system's early architects were concerned about reliability and functionality, not security. As a result, DNS servers have always been vulnerable to a broad spectrum of attacks, including spoofing, amplification, and denial-of-service.

And these attacks are becoming more common. According to IDC's 2021 Global DNS Threat Report, 87% of organizations suffered a DNS attack in the past year — an increase of eight percentage points from the year prior. Many of these attacks had serious consequences. 76% of DNS attacks caused application downtime, the report found — and the average attack took over five and a half hours to mitigate.

A number of factors explain this increase in attacks — and organizations need a plan to address all of them.

Recent years have caused two changes to the existing DNS landscape: newly discovered DNS vulnerabilities, and changing Internet browsing habits stemming from the Covid-19 pandemic. To respond to these new threats — and defend against existing ones — organizations need to

To respond to these new threats — and defend against existing ones — organizations need to give DNS security higher priority in general and implement a multilayered approach that extends beyond DNSSEC.

New cyber threats exploit and abuse DNS

In 2021, 44% of organizations identified DNS-based attacks as one of their top security challenges. A quick look back over the past year makes the reasons clear.

For starters, several new DNS-related vulnerabilities have recently been discovered, including:

- **“Forgot Password” cache poisoning attacks.** ‘Forgot password’ links are common in web applications, but a vulnerability discovered in July 2021 made them vulnerable to DNS cache poisoning attacks. Security researchers discovered that, by performing a cache poisoning attack on 146 vulnerable web applications, they could redirect password reset emails to attacker-controlled servers. This enabled them to click on the link and reset the user’s password, providing legitimate access to their account.

- **Data exposure in managed DNS.** Research presented at Black Hat USA 2021 demonstrated that bugs in certain managed DNS services could expose corporate DNS traffic containing sensitive information. By registering a domain on Amazon’s Route53 DNS service or Google Cloud DNS that had the same name as the DNS name server, the attacker could force all DNS traffic to be sent to their server. This exposed sensitive information and could enable DNS spoofing attacks.

- **tsuNAME DDoS attacks against DNS servers.** tsuNAME is a flaw in DNS resolver software that enable DDoS attacks against DNS servers. Domains with “cyclic dependencies'' can exist, where domain A delegates to domain B and vice versa. Vulnerable DNS resolvers will start looping when presented with domains causing cyclic dependencies. In one case, just two misconfigured domains created a 50% traffic increase for .nz’s authoritative DNS servers in 2020.

Additionally, the surge in remote work has inspired further DNS attacks. Since the beginning of the Covid-19 pandemic, several attack varieties have targeted home routers with DNS hijacking. In DNS hijacking, the attacker causes the DNS record for a legitimate domain to point to a site under their control. In these recent attacks, the compromised site claimed to offer Covid-19 information, but actually installed malware on the user’s device.

With many employees working full or part-time from home, a compromised device represents a significant network security risk. Overall, a report by the Global Cyber Alliance found that roughly a third of data breaches worldwide stem from DNS security gaps.

Existing DNS threats persist as well

These novel DNS attack vectors join a long list of established threats. Some of the most common attacks involving DNS infrastructure include:

- **DNS Denial-of-Service attacks:** which take down DNS services, making the sites that they serve unreachable. These attacks could waste server resources by requesting non-existent domains (NXDOMAINs) or random subdomains or could perform a Distributed DoS (DDoS) attack against a DNS server.

- **DNS spoofing:** similar to DNS hijacking but target DNS resolvers, which cache commonly or recently requested DNS records. A DNS spoofing or cache poisoning attack introduces false DNS records into a resolver's cache, causing requests for those domains to be routed to an attacker-controlled website.

- **DNS DDoS amplification:** which takes advantage of services that communicate over UDP and have responses that are much larger than the corresponding request. These factors allow an attacker to send requests to the service and have their much larger responses sent to the target. A DNS amplification attack floods the target with DNS responses, consuming bandwidth and overwhelming target servers.

- **DNS Tunneling:** exploits DNS traffic's permissions to pass through corporate firewalls. These attacks use DNS traffic to carry data between malware and the attacker-controlled data server.

The impact of DNS attacks

The significant variety within the DNS attack landscape means attack consequences vary as well. Regardless of the circumstance, said consequences are often severe.

DNS DDoS attacks — such as those exploiting the aforementioned tsuNAME flaw — can result in poor performance or outright downtime for entire web applications. DNS is a crucial first step in a website's ability to load quickly, and such attacks use server resources that could otherwise be used to handle legitimate requests. In 2020, 42% of organizations that suffered a DNS attack reported that their website had been compromised in some way.

Even attacks not designed to take down DNS services, such as DNS DDoS amplification or DNS tunneling, can create heavy volumes of traffic to DNS servers. This poor performance has multiple secondary consequences, including lower conversion rates, lower organic search rankings, and more.

Spoofing, hijacking, and cache poisoning attacks can also hurt website conversions by directing prospective customers away from the legitimate website. In addition, having one's site be seen as poorly secured can hurt an organization's brand reputation in the long run.

DNS attacks can also have severe consequences for an organization's network security. The aforementioned vulnerabilities in certain managed DNS providers resulted in private traffic being exposed to attackers — a critical data security issue. And DNS tunneling attacks that install and control malware on a network can have any number of consequences, including data loss and ransom demands.

Overall, the average cost per DNS attack in 2020 was over $900,000.

Mitigating the threat of DNS attacks

A number of steps can help organizations mitigate DNS attacks. At the very top of the list: implement DNS security solutions of some kind. IDC's report found that 42% of organizations have not deployed dedicated DNS security solutions.

Protecting against these attacks requires DNS security solutions. However, these solutions must be carefully designed and implemented to ensure that they do not negatively impact the performance of legitimate DNS requests.

Some DNS attack mitigation options include:

- **DNSSEC:** DNSSEC is a security protocol that signs responses from DNS servers. This helps to protect against DNS hijacking and spoofing by authenticating the data returned to the client.
- **Redundant infrastructure:** DoS attacks against DNS infrastructure commonly work by sending the target DNS server more traffic than it can handle. By overprovisioning servers and using anycast routing, traffic can be load-balanced between multiple servers. This ensures availability if one server is overloaded or goes down.
- **DNS firewall:** A DNS firewall sits between a domain's authoritative nameserver and users' recursive resolvers. The firewall can rate limit requests to protect against DDoS attacks or filter traffic to block malicious or suspicious requests.
- **Encrypted DNS:** By default, DNS is an unencrypted and unauthenticated protocol. DNS over HTTPS (DoH) and DNS over TLS (DoT) provide encryption and authentication.

Securing DNS with Cloudflare

Securing DNS with Cloudflare

Cloudflare helps millions of customers mitigate across the full DNS threat spectrum. Cloudflare managed DNS offers one-click DNSSEC to protect against DNS spoofing and hijacking attacks. It is built on Cloudflare's 100 Tbps of total network capacity — many times larger than the largest-ever DNS DDoS attack and blocks DDoS attacks in addition to other attack varieties.

The Cloudflare network is powered by threat intelligence from millions of websites, APIs, and networks, staying ahead of the latest vulnerabilities automatically.

And these protections come with no performance tradeoffs. Cloudflare operates the world's fastest authoritative DNS, with an 11 ms average lookup time. You can even maintain your existing DNS infrastructure while using Cloudflare DNS as a secondary DNS or in a hidden primary setup.

This article is part of a series on the latest trends and topics impacting today's technology decision-makers.

Key takeaways

After reading this article you will be able to understand:

- The importance of DNS security
- The recent DNS vulnerabilities and their consequences
- How to identify common DNS attacks
- How to improve DNS security

RELATED RESOURCES

- Whitepaper: Improving DNS security, performance, and reliability
- What is DNS?
- Cloudflare DNS

Dive deeper into this topic

Dive deeper into this topic

Learn more about DNS security challenges, and how to address them without risking performance challenges in the Improving DNS security, performance, and reliability whitepaper.

Get the paper

Receive a monthly recap of the most popular Internet insights!

Subscribe to Trending Stories

Sales

Enterprise Sales

Become a Partner

Contact Sales:
+55 (11) 3230 4523

Getting Started

Community

Developers

Support

Company

Company

Privacy Policy Terms of Use Report Security Issues Cookie Preferences Trademark