Radware Cybersecurity Advisory

Escalating Trends in DNS Flood Attacks

June 7, 2023

The Domain Name System (DNS) is a fundamental pillar of our digital economy. Denial-of-service attacks targeting DNS can severely impact businesses and cause damage to revenue, customer trust, and business reputation. Our latest analysis indicates a growing trend in the ratio of DNS Flood attacks over the last three quarters. Notably, the frequency of these attacks in the first month of Q2 2023 was four times higher than the corresponding month in Q2 2022. This escalating situation peaked in April when we observed the largest DNS Flood attack in the past two years, registering a rate of 1.29 million DNS queries per second.

Despite the increasing frequency and complexity, it is important to note that DNS Floods are application-level attacks, designed to overwhelm the server without necessarily saturating the internet connection. Our analysis confirms that in the last two years, all observed DNS Floods maintained a traffic rate considerably below 1Gbps, underlining their strategic focus on disrupting service rather than consuming bandwidth.

As such, these findings indicate the urgent need for heightened vigilance and fortification of DNS defenses to counteract this escalating threat landscape.

Insights

- There has been a significant escalation in the proportion of DNS Flood attacks in the recent three quarters.
- The frequency of DNS Flood attacks in the first month of Q2 2023 was quadruple that of the same month in Q2 2022.
- In April 2023, we recorded the most significant DNS Flood over the past two years, with a peak attack rate reaching 1.29 million DNS queries per second.
- In 2023, two-thirds of the observed DNS Floods targeted DNS type A records.
- The second most leveraged query type was the DNS AAAA record query, which contributed to 8% of the attacks, followed by the DNS MX record query, which made up 4%.
- One in every six DNS Floods in 2023 incorporated a mix of different query types within a single attack.
- DNS Floods are application-layer attacks, with the primary goal of overloading the server rather than saturating the internet connection. Over the past two years, all DNS Floods have kept their traffic rate significantly below 1Gbps.

No DNS, No Business

The digital era has catalyzed rapid growth in online commercial activities, making e-commerce and online platforms a vital component of the global economy. However, this technological advancement is not without its vulnerabilities. A crucial and ubiquitous part of this digital ecosystem is the DNS, which acts as the internet's phonebook, translating human-readable domain names into IP addresses. When a DNS service is subjected to a cyberattack, such as denial-of-service (DoS) or distributed denial-of-service (DDoS), the disruption caused can be catastrophic for businesses.

Radware Cybersecurity Advisory

Escalating Trends in DNS Flood Attacks

June 7, 2023

Denial-of-service attacks are malicious attempts to overwhelm a network, service, or server with excessive traffic or requests, causing them to slow down significantly or, worse, crash. The fundamental aim of these attacks is to disrupt the targeted system's regular functioning, denying legitimate users access to the services or information they seek.

DNS is a particularly popular target for these attacks because of its vital role in internet traffic routing. When a DNS server falls victim to a DoS attack, users cannot access the websites, services or APIs associated with that server because their browsers and applications can't resolve the IP addresses corresponding to those domain names. As a result, the user experience is significantly degraded or entirely disrupted, resulting in lost revenue, damaged reputation, and a decline in customer trust.

The impact of a DNS-based DoS attack can be colossal, particularly for e-commerce businesses. It's not simply a matter of lost sales during the outage period. Consider that in 2022, Amazon AWS (cloud) generated over $80 billion in revenue, an average of over $152,000 per minute. The potential loss from even a brief outage is staggering. Furthermore, these disruptions damage the business's reputation, undermine consumer confidence and lead to potential long-term loss of customers. Additionally, businesses may face legal ramifications if unable to meet Service Level Agreements (SLAs) due to such disruptions.

DIFFERENT TYPES OF DNS DENIAL-OF-SERVICE ATTACKS

DNS denial-of-service attacks can come in various forms, each with unique techniques and impacts. Here are the most common attack types:

- **DNS Amplification Attack**: This is a type of network-level, reflection-based, volumetric DDoS attack where the attacker crafts a DNS query packet with a forged source IP address (the victim's). It sends it to a legitimate, open, DNS resolver, which subsequently replies to the victim with a large amount of data. The goal is to overwhelm the victim's network with traffic.
- **DNS Flood Attack**: A DNS Flood is a type of application-layer DDoS attack that seeks to overload a DNS server with a high volume of requests until it becomes unresponsive. The requests appear legitimate, making it difficult to filter out malicious traffic.
- **DNS NXDOMAIN Attack**: In this type of DNS Flood attack the attacker sends a high volume of requests for non-existent or invalid domains, resulting in DNS recursion and NXDOMAIN (nonexistent domain) responses. The server must work hard to try and resolve these spurious requests, thus consuming valuable resources instead of processing legitimate requests. When a DNS server is under NXDOMAIN attack, the cache of the DNS server will be flooded with NXDOMAIN results, forcing the server to resolve legitimate requests repeatedly instead of fetching the answer from its cache.
- **Phantom Domain Attack**: This attack involves the attacker setting up one or more phantom domains that do not respond to DNS queries and sending requests to the victim's DNS server to resolve the

phantom domains. The victim's DNS server gets overwhelmed when it tries to resolve the phantom domains through non-responsive servers. This causes the recursive server to spend valuable resources waiting for responses that will never come.

- **Pseudo Random Subdomain (PRSD) Attack**: Also known as water torture attacks, this attack is similar to the DNS NXDOMAIN attack. The attacker sends a massive number of requests for non-existent subdomains of a valid and existing domain through different recursive resolvers. This causes the authoritative server to consume resources trying to resolve these nonexistent subdomains, eventually leading to a denial of service.

In each case, the attacker's objective is to disrupt the DNS service and make the websites and online services that rely on it inaccessible. These attacks exploit different aspects of the DNS protocol, making them challenging to defend against and highlighting the importance of implementing robust DNS security measures.

DNS Flood Trends

A quantitative analysis of the most common types of DNS Floods detected and mitigated by our Cloud DDoS Protection Service points to an increasing trend in the occurrence and intensity of such DDoS attacks.

GROWING TREND

DDoS attacks consist of one or more attack vectors. By determining the proportion of attacks utilizing a DNS Flood attack vector in relation to the overall count of attacks, we can gauge the progression of DNS Floods over time, irrespective of the total activity or the number of customers protected by our services.

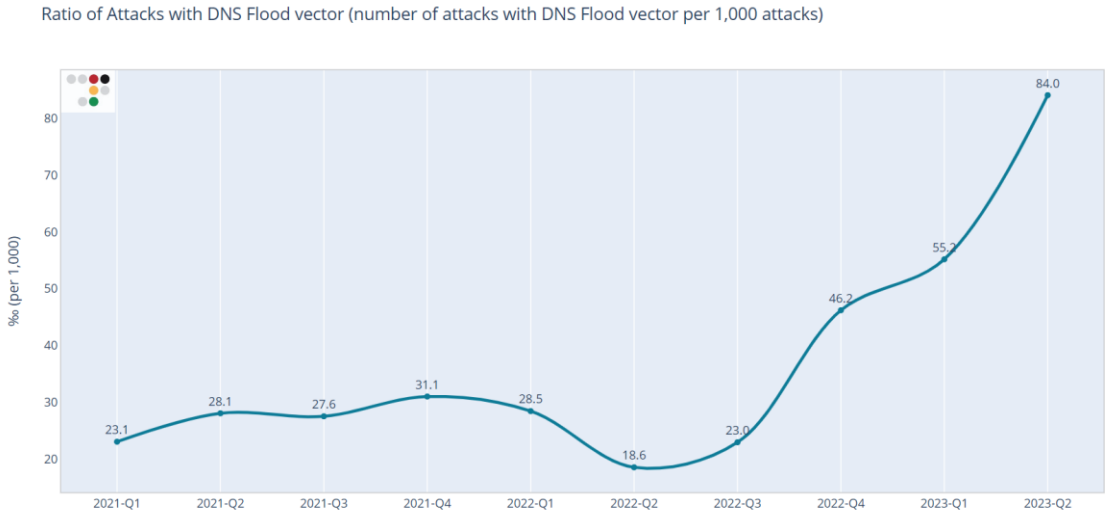

Figure 1: DNS Flood Attack Ratio Evolution over Time

Throughout 2021 and the first half of 2022, fewer than 32 out of every 1,000 attacks incorporated a DNS Flood vector. However, from Q3 of 2022, we noted a marked increase in the proportion of attacks featuring a DNS Flood vector. The ratio experienced a twofold surge from Q3 to Q4 of last year, rising to 84 attacks per 1,000 in April of 2023 with each involving a DNS Flood component. This dramatic increase first emerged in Q4 of last year, and by the initial month of Q2 2023, it had quadrupled compared to the same period in 2022.

The area chart depicted in Figure 2 traces the development of the count of DNS Flood attacks according to each query type. A description of the key DNS record types can be found in Table 1 at the end of this document. The total number of DNS Floods mitigated each month corroborates the escalating trend discerned in the previous DNS Flood attack ratio. From September 2022 onwards, the monthly volume of DNS Floods has consistently surpassed the figures recorded in the preceding months.

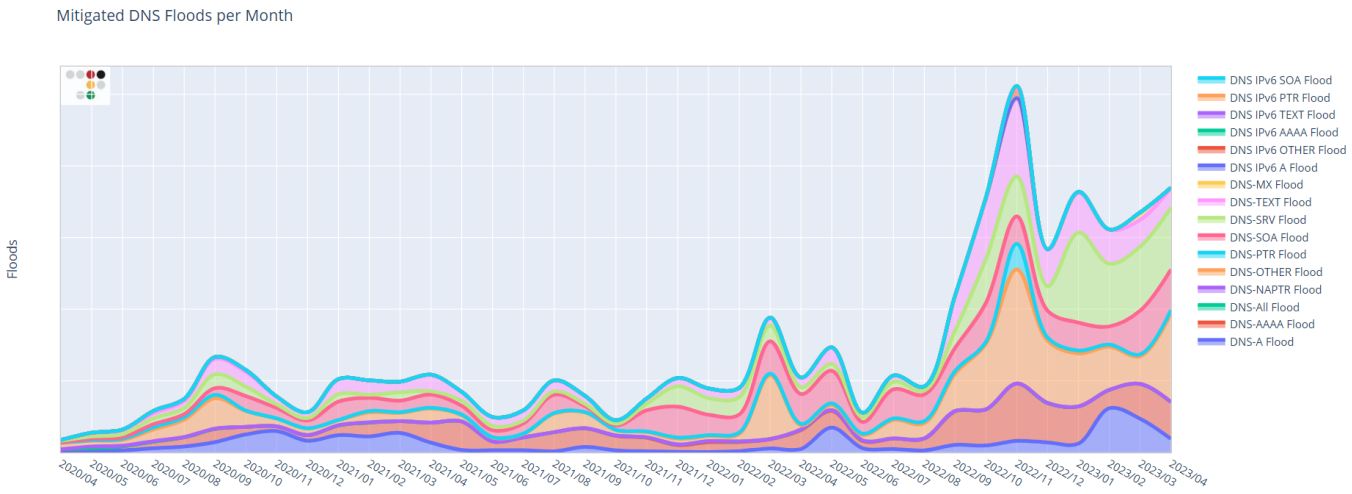

Figure 2: Number of DNS Floods per Month

FLOODS HITTING HARDER

DNS Floods are application-layer assaults with the objective of compromising the server's capability to manage valid DNS requests. The pace of these requests determines the total effect on the server. The blue trajectory in Figure 3's chart illustrates the highest DNS query rate detected each quarter, denoted in queries per second (QPS). Aside from a notable DNS Flood attack in Q1 of 2021, which peaked at 1.59 million QPS, the DNS Floods since Q4 of last year have been significantly larger in scale compared to prior quarters. The largest DNS Flood in the past two years was observed in April 2023, registering an attack rate of 1.29 million DNS queries per second.

The red trajectory in Figure 3's chart demonstrates the peak traffic of the most significant DNS Flood each quarter. The traffic rate shows a consistent pattern aligning with the maximum query rate. It is important to

understand that application-level attacks focus on overloading the server, which does not necessarily equate to a traffic volume high enough to saturate the server's internet connection. The red line effectively emphasizes this point, considering that the most substantial DNS Flood recorded a traffic volume of less than 1.3Gbps, and all DNS Floods monitored over the past two years remained notably under the 1Gbps threshold.

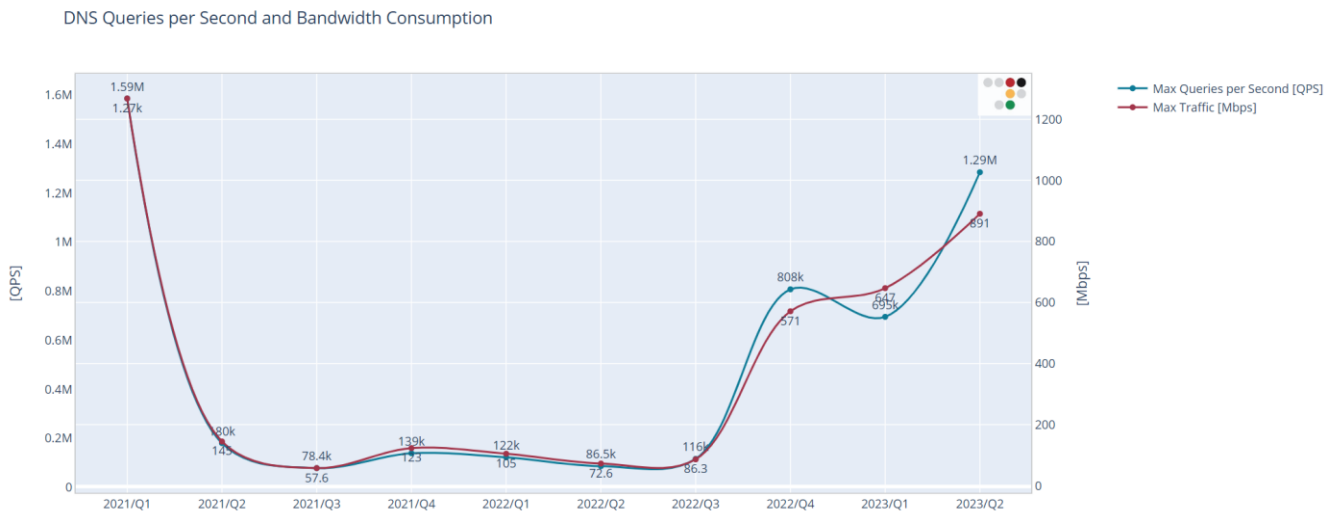

Figure 3: Queries per Second and Bandwidth Consumption by DNS Floods

DNS FLOOD TYPES

The most prevalent DNS query leveraged in DNS Floods in 2023 was the regular hostname to IPv4 query, accounting for almost 65% of the attacks. The second most used query was the hostname to IPv6 query, deployed in close to 8% of all DNS Floods in 2023. Over 15% of the DNS Floods consisted of a mixture of various types of queries, termed as DNS-ALL Flood in the chart in Figure 4. MX queries took the third spot in terms of their usage in DNS Floods.

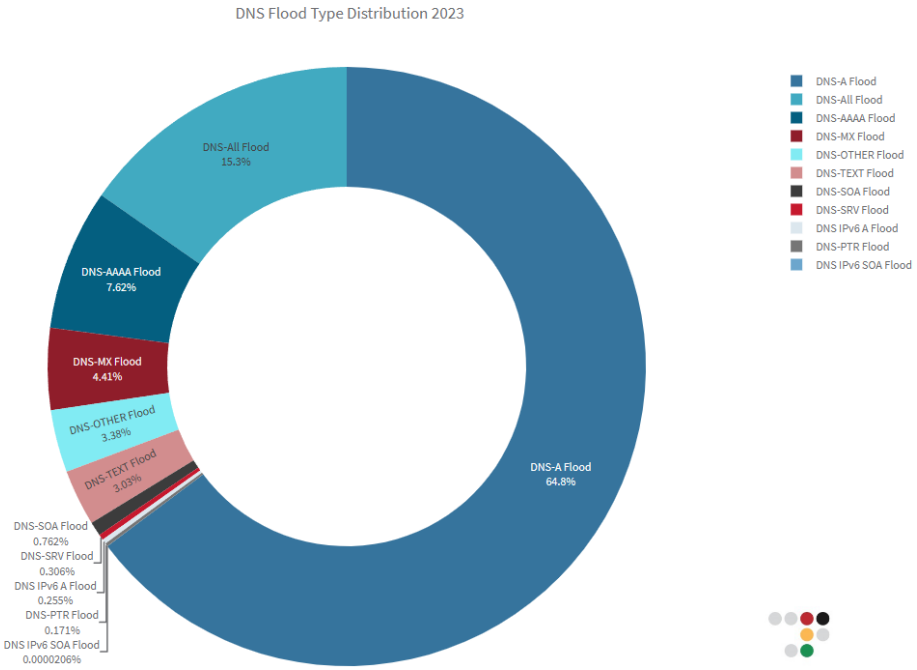

Figure 4: DNS Flood Type Distribution in 2023

Conclusion

In conclusion, DNS is a fundamental pillar of the digital economy, and DoS attacks targeting DNS can severely impact businesses. As the adage goes, "No DNS, no business." In other words, the potential damage to revenue, customer trust, and business reputation from a DNS outage due to a DoS attack can be enormous. Therefore, to ensure business continuity and robust cybersecurity, businesses must prioritize protecting their DNS infrastructure, monitoring threats, and employing necessary countermeasures, including redundancy planning and leveraging cloud-based solutions. In the cyber landscape, vigilance and preparation are the keys to survival and prosperity.

Table 1: Common DNS Record Types

A	The address mapping record, also known as a DNS host record, stores a hostname and its corresponding IPv4 address.
AAAA	The IP Version 6 address record stores a hostname and its corresponding IPv6 address.
CNAME	The canonical name record is used to alias a hostname to another hostname. When a DNS client requests a record that contains a CNAME, which points to another hostname, the DNS resolution process is repeated with the new hostname.
MX	The mail exchanger record specifies an SMTP email server for the domain.
NS	The name server record specifies that a DNS Zone, such as "example.com," is delegated to a specific authoritative name server and provides the address of that name server.
PTR	The reverse-lookup pointer record provides the IP address of a hostname (reverse DNS lookup).
SRV	The service location record is like the MX record, but for other services.
TXT	The text record can contain arbitrary information and typically carries machine-readable data such as opportunistic encryption, sender policy framework (SPF), DKIM, DMARC, etc.
SOA	The Start of Authority record appears at the beginning of a DNS zone file and indicates the authoritative name server for the current DNS zone, contact details of the domain administrator, domain file version number, and information on how frequently DNS information for this zone should be refreshed.
NAPTR	The Naming Authority Pointer records map domain names to URIs (uniform resource identifiers) and other resources. NAPTR records are commonly used for applications in internet telephony.

EFFECTIVE DDOS PROTECTION ESSENTIALS

Hybrid DDoS Protection – Use on-premise and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high-volume attacks and protects from pipe saturation

Behavioral-Based Detection - Quickly and accurately identify and block anomalies while allowing legitimate traffic through

Real-Time Signature Creation - Promptly protect against unknown threats and zero-day attacks

A Cyber-Security Emergency Response Plan - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Intelligence on Active Threat Actors – High fidelity, correlated and analyzed data for preemptive protection against currently active known attackers

For further **network and application protection** measures, Radware urges companies to inspect and patch their network to defend against risks and threats.

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top-10 coverage against defacements, injections, etc.

Low false positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the widest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options - on-premises, out-of-path, virtual or cloud-based

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.