HC3: Sector Alert

April 07, 2023 TLP:CLEAR Report: 202304071200

Alert for DNS NXDOMAIN Attacks

Executive Summary

Through a trusted third party, information was shared with HC3 regarding a distributed denial-of-service (DDoS) attack, which has been tracked since November 2022. These attacks are flooding targeted networks and servers with a fake Domain Name Server (DNS) request for non-existent domains (NXDOMAINs).

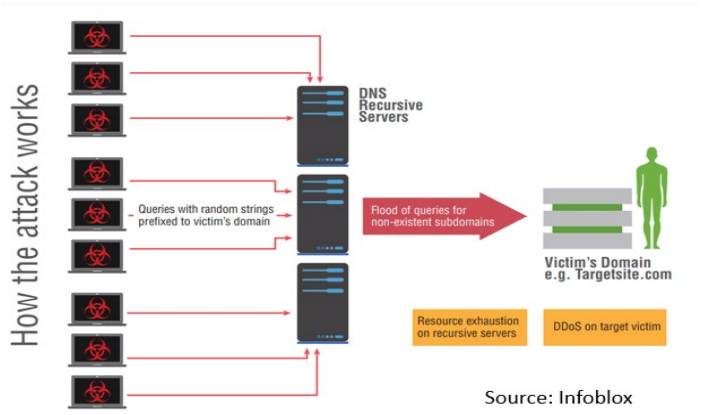
Report

A DNS NXDOMAIN flood DDoS attack is one of the various denial-of-service attacks that will target the DNS. The threat actor wants to overload the DNS server with a large volume of requests, which can be either non-existent or invalid. In this type of DDoS, the DNS server will spend time trying to locate something that does not exist instead of processing the legitimate user request. As the volume of invalid requests increases, the authoritative server will begin slow down, preventing legitimate requests from getting a response. Additionally, legitimate clients trying to access the website will increase the load even further. In most cases, the DNS proxy server and the DNS authoritative server will use all their time handling those bad requests. When successful, the outcome of these attacks can result in higher utilization of resources on the server, and the cache will be filled up with NXDOMAIN replies. This can ultimately slow or completely prevent an authorized user from gaining access to a website or services. Like other DDoS attacks, these are also carried out by large botnets, which can consist of thousands of compromised devices located worldwide, making detecting and blocking this type of DNS attack difficult. As a result, NXDOMAIN DDoS attacks could negatively impact network providers, website owners, and end-users or customers.

Network Providers: If network providers cannot control or mitigate the attack, it may lead to their customers being unable to access their websites and services.

Website Owners: Website or other service providers are typically the intended victim of NXDOMAIN attacks and are affected by having their service inaccessible to legitimate customers.

Users & Customers: End users are also affected because they cannot access the products or services offered by the website that is under attack.



During normal operations, receiving small amounts of NXDOMAIN responses is considered normal. They can result from several things, such as users mistyping web addresses or dead hyperlinks that reference servers which no longer exist. In most cases, these requests are typically redirected to authoritative nameservers, which are the DNS servers used to host the records of public services, so that users and clients across the Internet can locate them.

Tactics, Techniques, and Procedures (TTPs)

The current identified TTPs for this campaign consist of:

- A large amount of DNS queries for non-existent hostnames under legitimate domains
- The traffic consists of UDP packets encapsulated in IPv4 and IPv6
- The DNS servers respond with an NXDOMAIN error
- The source IPs are widely distributed
- The source IPs could be spoofed

Mitigations and Recommended Actions

HC3 encourages organizations to remain cautious when blocking IPs, because this could result in legitimate users being prevented from accessing public services. According to NETSCOUT, there are several mitigations available for DNS NXDOMAIN Flood DDoS Attacks:

- Blackhole routing/filtering suspected domains and servers
- Implement DNS Response Rate Limiting
- Block requests from the client's IP address for a configurable period of time
- Be sure that cache refresh takes place, ensuring continuous service
- Lower the timeout for recursive name lookup to free up resources in the DNS resolver
- Increase the time-to-live (TTL) on existing records
- Apply rate limiting on traffic to overwhelmed servers

References

What is NXDOMAIN or DNS NXDOMAIN Flood DDoS Attack?
What is a DNS NXDOMAIN Flood DDoS Attack? | NETSCOUT

NXDOMAIN Attacks
https://www.whatsmydns.net/dns-security/dns-attacks/nxdomain-attacks

NXDOMAIN Attack Methods and Mitigation
https://www.infoblox.com/wp-content/uploads/2016/04/infoblox-solution-note-nxdomain-attack-methods-and-mitigation.pdf

What is a DNS flood: NXDOMAIN Flood?
https://www.f5.com/glossary/dns-flood-nxdomain-flood#:~:text=The%20DNS%20NXDOMAIN%20flood%20attack,for%20invalid%20or%20nonexistent%20records.

What is an NXDOMAIN Attack?
https://threat.media/definition/what-is-an-nxdomain-attack/
NXDOMAIN Attack
https://www.linkedin.com/pulse/nxdomain-attack-nicholas-doropoulos?trk=articles_directory

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback