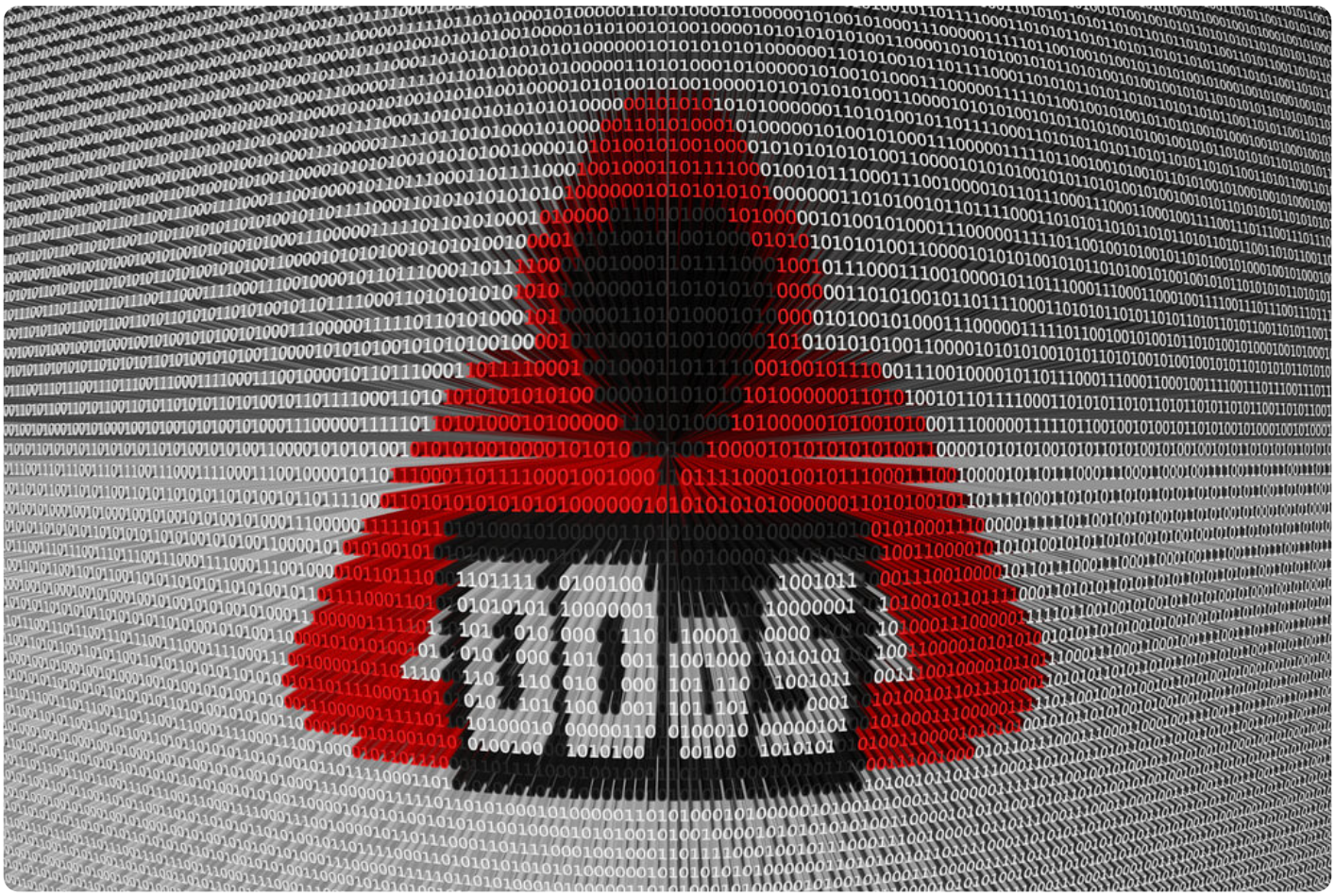
DNS Flood Attack: What It Is and How to Avoid It with DNS Lookup Online Tools

Posted on January 27, 2020



These days, even large-scale operations suffer from Domain Name System (DNS) flood attacks despite using advanced solutions and subscriptions to the best anti-denial-of-service (DoS) protection services. Attackers always seem to come up with a way to launch distributed DoS (DDoS) attacks of unmatched sizes to take their victims' sites offline. To date, the worst DDoS attack seen was 1.7 TBps strong. Resulting losses are difficult to ignore, as these range between $120,000 and $2 million.

DNS flood attacks typically employ traffic from various spoofed IP locations. They also mimic legitimate requests, and thus are tricky to diagnose. With large packets involved, incidents can quickly drain resources and take the victim's platforms offline for hours. DNS floods are classified as layer 7 attacks as they affect application availability within a network.

Spoofing is easier to accomplish with this type of threat as it abuses the User Datagram Protocol (UDP). In a Transmission Control Protocol/Internet Protocol (TCP/IP) setup, a three-way handshake takes place to establish a valid connection between local hosts and servers. UDP only triggers a two-way "verification" process for name resolution, which makes it easier for threat actors to forge packet formats.

Mitigation services or so-called "data scrubbing centers" are often called in to fix DNS flood-related breaches. Most onsite security solutions used by businesses are rendered insufficient. It's also rare for companies to have a network capacity that can handle inflated packet sizes. While scalable bandwidths are available, not all businesses have access to them.

Differences Between a DNS Flood and an Amplification Attack

To further understand what constitutes a DNS flood, it helps to distinguish it from an amplification attack. While their objectives are more or less the same, their subjects and techniques differ.

What sets flood attacks apart from amplification attacks is that the former target the resolver of a

DNS provider with multiple sources of traffic. In simpler terms, a hacker uses several botnets to direct UDP packets to a single destination until it can no longer serve legitimate user requests.

An amplification attack, on the other hand, sends multiple spoofed queries to various open resolvers, often in low volumes. They, of course, add up and elicit large responses from the unsecured servers, which return the requests to a forged address (that of the victim). Note that high-bandwidth devices are also involved in some amplification attacks.

In recent years, we have seen the rise of a more sophisticated form of DNS flood attack — DDoS attacks. An infamous example of this threat involved the use of the Mirai botnet — an army of bots composed of billions of insufficiently secured Internet of Things (IoT) devices, such as routers, closed-circuit TV (CCTV) cameras, and smart TVs. The botnet targeted the servers of DNS provider Dyn with a 1.2 TBps-strong DDoS attack.

DNS Lookup Online Tools Help Prevent DNS Flood Attacks

DNS lookup online technologies provide security professionals with comprehensive information on botnet operators. They can use DNS Lookup API, or Reverse IP/DNS API depending on the cases, to track an adversary's host infrastructure. The abovementioned tool lets users obtain up to 50 resource record types on a specific domain from its exhaustive database.

Here's how infosec professionals can use **DNS lookup online** tools to enrich their threat intelligence:

- DNS Lookup API helps cyber investigators put an end to highly damaging attacks. Cyberforensics professionals can use DNS Lookup API in combination with other WHOIS lookup tools to gain a more detailed look at the servers the offenders use to launch their malicious campaigns. They can then cross-check the API results to verify the accuracy of other intel such as internal network logs to see if any of the domains accessing systems need to be blocked.

- Penetration testers can rely on **DNS lookup online** tools to search for exposed DNS records on a client's network infrastructure. It aids in conducting passive reconnaissance, enabling pen testers to map out potential attack surfaces by using indexed DNS information.

- Companies can protect themselves from email bombing and phishing campaigns by using DNS Lookup API as well. They can extract domains connected to emails received via their data loss prevention (DLP) software and then use the API to check if their DNS records are configured correctly.

- **DNS lookup online** tools allow security engineers to determine network traffic anomalies. Although spoofed IP addresses are involved in DNS flood attacks, old trends are still likely to emerge if the attackers used shared resources (i.e., IP addresses involved in previous attacks). A reverse IP/DNS API can also be integrated into intrusion detection systems (IDSs) to help users identify and block malicious IP addresses that are sending their networks high-volume packets in instances, perhaps, of distributed denial-of-service (DDoS) attacks.

Organizations can shield themselves from DNS flood attacks by regularly inspecting their network for vulnerabilities and investing time in domain research and monitoring. **DNS lookup online** tools like DNS Lookup API, or Reverse IP/DNS API can augment their threat intelligence and enhance their security solution capabilities.