# Researchers thwart DDoS technique that threatened large-scale cyberattack

May 29 2020

Credit: CC0 Public Domain

In October 2016, a cyberattack temporarily took down Amazon, Reddit, Spotify and Slack for users along the U.S.'s East Coast. Mirai, a botnet of hacked security cameras and internet routers, aimed a flood of junk

traffic at the servers of Dyn, a company that provides the global directory (or phonebook) for the web known as the Domain Name System or DNS.

Now researchers at Tel Aviv University and the Interdisciplinary Center (IDC) of Herzliya say that a weakness in the DNS could have brought about an attack of a much larger scale.

In their new study, which will be presented at the USENIX Security Conference in August 2020, the research group, co-led by Prof. Yehuda Afek of TAU's Blavatnik School of Computer Science, and Prof. Anat Bremler-Barr, vice dean of IDC's Efi Arazi School of Computer Science, together with TAU doctoral student Lior Shafir, provides new details of a technique that could have allowed a relatively small number of computers to carry out DDoS (distributed denial of service) attacks on a massive scale, overwhelming targets with false requests for information until they were thrown offline.

As early as February, the researchers alerted a broad collection of companies responsible for the internet's infrastructure to their findings. The researchers say those firms, including Google, Microsoft, Cloudflare, Amazon, Dyn (now owned by Oracle), Verisign, and Quad9, have all updated their software to address the problem, as have several makers of the DNS software those companies use.

Through joint research projects, Prof. Afek and Prof. Bremler-Barr have already stopped hundreds of thousands of DDoS cyberattacks over the last two decades, starting with the design of the first DDoS attacks scrubber server at Riverhead Networks, a company they co-founded with Dr. Dan Touitou in 2001.

"The DNS is the essential internet directory," explains Prof. Bremler-Barr. "In fact, without the DNS, the internet cannot function. As part of

a study of various aspects of the DNS, we discovered to our surprise a very serious breach that could attack the DNS and disable large portions of the network."

The new DDoS technique, which the researchers dubbed NXNSAttack (Non-Existent Name Server Attack) takes advantage of vulnerabilities in common DNS software. DNS converts the domain names you click or type into the address bar of your browser into IP addresses. But the NXNSAttack can cause an unwitting DNS server to perform hundreds of thousands of requests in response to just one hacker's request.

"The attack in 2016 used over 1 million IoT devices, whereas here, we see the same impact with only a few hundred," says Prof. Afek. "We are talking about a major amplification, a major cyberattack that could disable critical parts of the internet."

The way it works is that when a client machine tries to reach a certain resource on the internet, it issues a request with the name of the resource to a resolver type DNS server, which is in charge of translating the requested name into an IP address. In order to find the required IP address, the resolver goes into an exchange of messages with several DNS servers of another type, called "authoritative." The authoritative servers redirect the resolver from one to the other, essentially telling it to "go and ask that one" until the resolver reaches an authoritative server that knows the final answer—the requested IP address.

"To mount the NXNSattack," continues Prof. Afek, "an attacker either acquires for a negligible price or simply penetrates an authoritative server, which would redirect the resolver to send an enormous number of requests to the authoritative servers. This happens while the resolver is trying to answer the particular request that the attacker has crafted.

"The attacker sends such a request multiple times over a long period of

time, which generates a tsunami of requests between the DNS servers, which are subsequently overwhelmed and unable to respond to the legitimate requests of actual legitimate users."

Mr. Shafir explains further: "A hacker that discovered this vulnerability would have used it to generate an attack targeting either a resolver or an authoritative DNS server in particular locations in the DNS system. In either case, the attack server would be incapacitated and its services blocked, unable to function due to the overwhelming number of requests it got. It would prevent legitimate users from reaching the resources on the internet they sought."

The research for the study formed part of Mr. Shafir's Ph.D. work; he built a set up with an authoritative server, on which he simulated an attack on the servers, generating a tsunami of requests between the servers, incapacitating them as a result.

"Our discovery has prevented major potential damage to web services used by millions of users worldwide," concludes Prof. Yehuda Afek. "The 2016 cyberattack, which is considered the greatest in history, knocked down much of the internet in the U.S. But an attack like the one we now prevented could have been more than 800 times more powerful."

**More information:** Link to the study: cyber-security-group.cs.tau.ac.il/

Provided by Tel Aviv University

threatened-large-scale.html