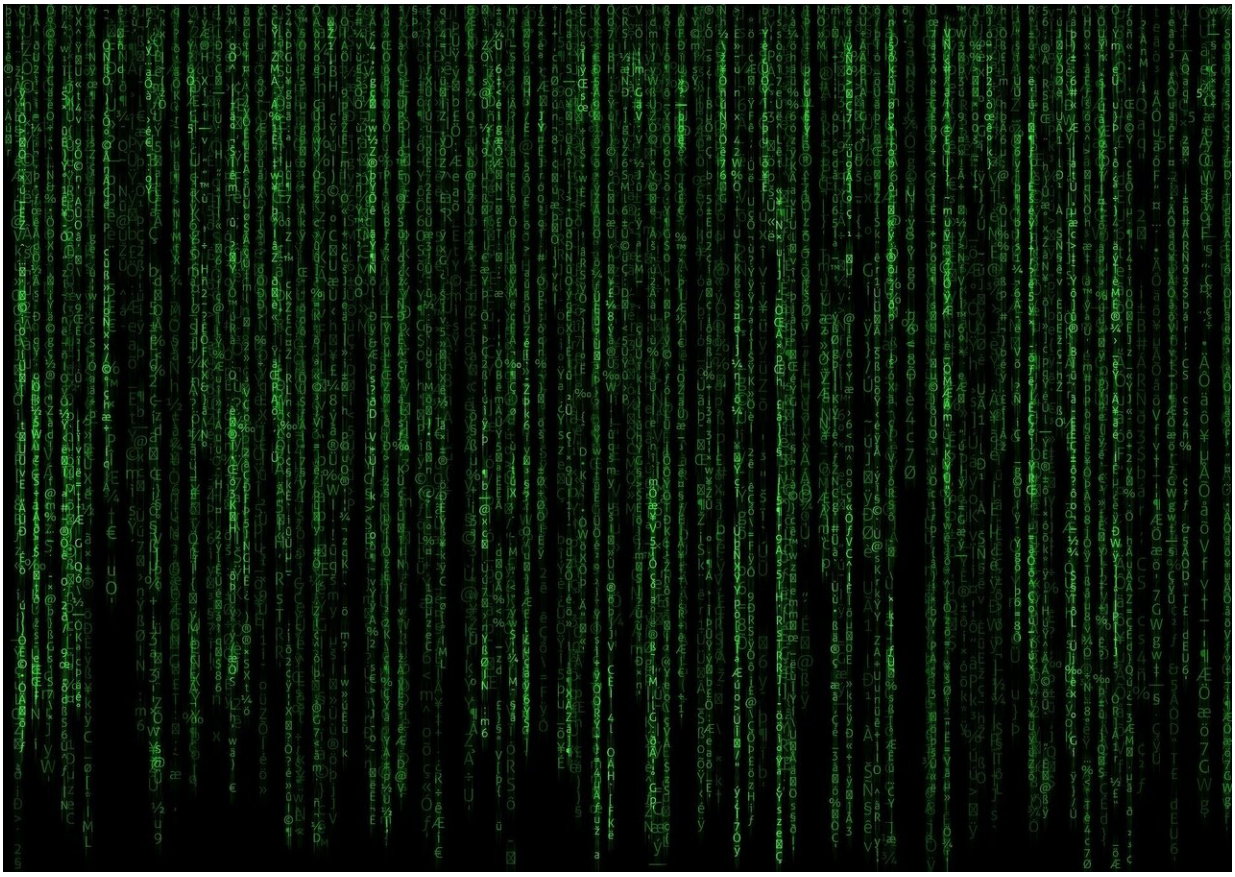
DNS cache poisoning ready for a comeback

November 11 2020, by Holly Ober



Credit: Pixabay/CC0 Public Domain

Agroup led by UC Riverside computer security researchers unveiled discovery of a series of critical security flaws that could lead to a revival of DNS cache poisoning attacks this week at the 2020 ACM SIGSAC Conference on Computer and Communications Security. The attack

succeeds by derandomizing the source port and works on all layers of caches in the DNS infrastructure, such as forwarders and resolvers.

The researchers found that 34% of the open resolvers on the internet are vulnerable, a figure that includes 85% of the most popular DNS services, including Google's 8.8.8.8 and CloudFlare's 1.1.1.1. As part of their research, the group received permission to attempt harmless test attacks against select popular DNS servers, and succeeded in all of them.

The Domain Name System, or DNS, links domain names with their corresponding Internet Protocol, or IP, addresses. For example, when you open a browser and type "ucr.edu" into the address bar, you are asking for an IP address—a set of numbers computers use to communicate with one another. The DNS directs requests for the name "ucr.edu" to the IP address of the UC Riverside web server, and the user sees the UC Riverside website.

DNS cache poisoning is a type of attack that injects a malicious IP address for a targeted domain name into DNS caches. Instead of directing the victim to the desired website or service, the corrupted DNS record sends them to one that looks just like the real one but is controlled by the attackers. The owner of the malicious IP address is able to capture information the victim enters, including usernames, passwords, and other sensitive information.

DNS cache poisoning attacks were once popular but are easily thwarted by randomizing the number of the port sending the request, known as the source port, or randomizing the numbers of other locations involved in communications within and between networks. Since browsers began incorporating randomization-based defenses, DNS cache poisoning has become more difficult and fallen in popularity.

The new attack derandomizes the source port, the most common

defense, and affects all layers of DNS caching.

Zhiyun Qian, an associate professor of computer science and engineering at UC Riverside's Marlan and Rosemary Bourns College of Engineering; and doctoral students Keyu Man and Zhongjie Wang collaborated with several colleagues at Tsinghua University to carry out the research in the DNS system.

Qian's group used a device that can spoof IP addresses and a computer able to trigger a request out of a DNS forwarder or resolver. Forwarders and resolvers are part of the DNS system that help figure out where to send requests. In the case of a forwarder attack, this can happen when the attacker is located in a local area network managed by a wireless router. For example, an attacker can join a public wireless network in a coffee shop, a shopping mall, or an airport. In a resolver attack, this can include any network where the attacker is an insider or owns a compromised machine. Last but not least, any public resolvers on the internet, such as servers provided by Google and Cloudflare, are also targets.

Next, the researchers leveraged a novel network side channel to carry out the attack. More specifically, they used a channel affiliated with, but outside of, the main channels used in the domain name requests to figure out the source port number by developing a method to hold the channel open long enough to run 1,000 guesses per second until they hit the right one. With the source port derandomized, the group was able to insert a malicious IP address and successfully pull off a DNS cache poisoning attack.

They then conducted numerous additional real-world experiments under realistic server configuration and network conditions that showed their basic method could be easily adapted to work throughout the DNS system. In fact, they have already demonstrated the attack against

popular public DNS servers—with authorization, of course.

To counter this critical vulnerability, the researchers recommend additional randomness and cryptographic solutions.

More information: Keyu Man et al. DNS Cache Poisoning Attack Reloaded, *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (2020). DOI: 10.1145/3372297.3417280

Provided by University of California - Riverside