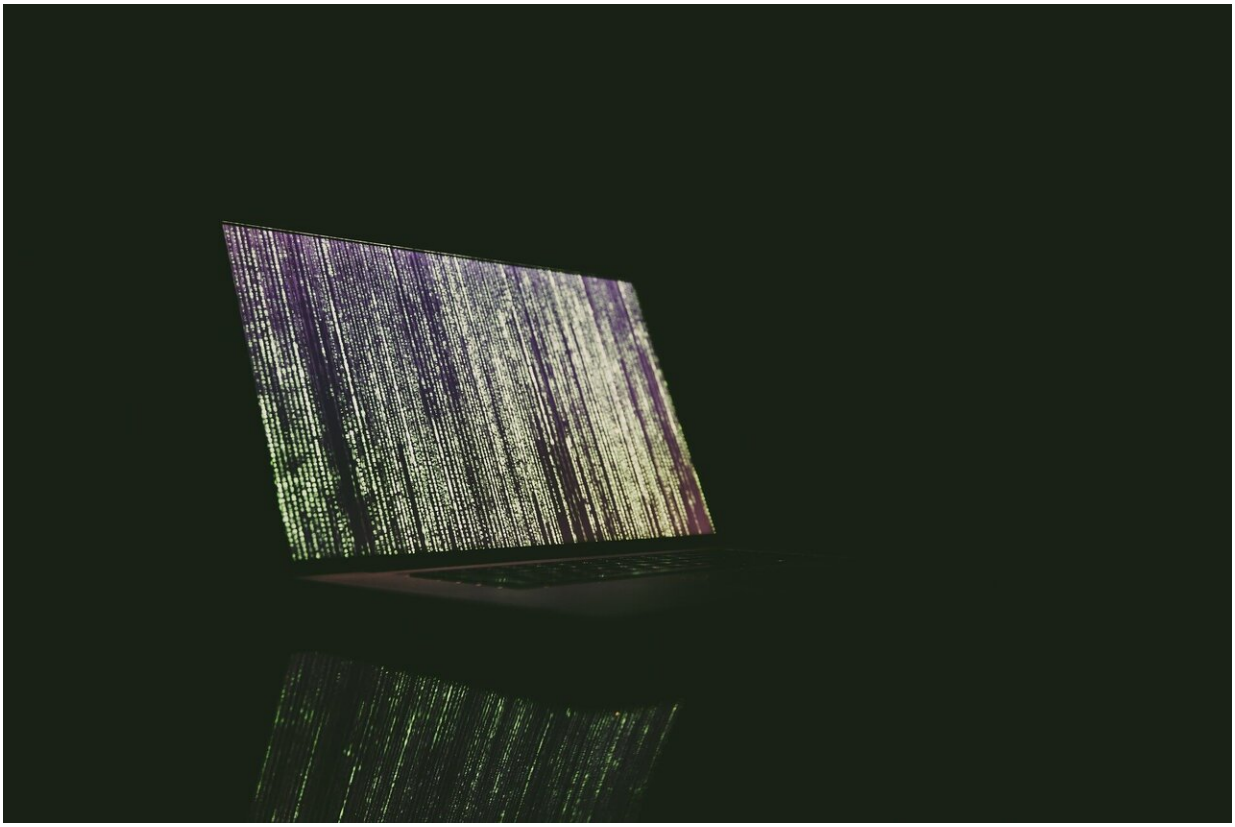
Akamai speaks out on uptick of DDoS attacks

September 20 2019, by Nancy Cohen



Credit: CC0 Public Domain

Internet security's big bully: Distributed Denial of Service (DDoS) which messes up normal traffic of a targeted server or network with a flood of HTTP requests, malformed packets. Crash, bam boom. Missions

accomplished. Users cannot get back in.

Akamai's Jonathan Respeto blogged some ugly findings on Wednesday. A team at Akamai had been checking out a new DDoS vector that leverages a UDP Amplification technique known as WS-Discovery (WSD). The situation now is such that "multiple threat actors" are leveraging this DDoS method to ramp up attacks.

For those who are less familiar with discovery lingo, UDP stands for User Datagram Protocol. *TechTarget* tells readers it is an alternative communications protocol to Transmission Control Protocol used for establishing low-latency and loss-tolerating connections between applications on the internet.

On Wednesday, Respeto blogged that "Since UDP is a stateless protocol, requests to the WSD service can be spoofed."

WSD stands for Web Services Dynamic Discovery. Catalin Cimpanu in *ZDNet* described WSD as "a multicast protocol that can be used on local networks to 'discover' other nearby devices that communicate via a particular protocol or interface."

OK, then here is the ugly role WSD is playing in this case, as Akamai's Respeto discovered.

He provided a history of how it came about and the trouble now:

WSD was shipped as a default feature set and service starting with Windows Vista. It has been included in HP printers since 2008. As for devices that the Acamai team discovered on the Internet to be incorrectly exposing and responding to WSD, "most consist of CCTV cameras and DVR [digital video recorder] systems, a trend that isn't surprising at this point."

Anthony Spadafora in *TechRadar* said that the attackers' technique in abusing the WSD protocol was "used by a wide array of network devices to automatically connect to one another. The WSD protocol allows devices to send user datagram protocol (UDP) packets over port 3702 to describe the capabilities and requirements of a device."

What first put Akamai on the wrecking-ball trail? Respeto said that "one of our customers came under fire. The attack, which targeted the gaming industry, weighed in at 35/Gbps at peak bandwidth." More research by the team was done on WSD protocol implementations:

Respeto said "the SIRT was able to achieve amplification rates of up to 15,300% of the original byte size. This places WSD in 4th place on the DDoS attacks leaderboard for highest reflected amplification factor."

From the service provider company DDoS-GUARD:

"Certain commands to UDP protocols elicit responses that are much larger than the initial request. Previously, attackers were limited by the linear number of packets directly sent to the target to carry out a DoS attack; now a single packet can generate between 10 and 100 times the original bandwidth. This is called an amplification of the attack."

Something called the Bandwidth Amplification Factor can measure the potential effect of an amplification attack, and is "calculated as the number of UDP payload bytes that an amplifier sends to answer a query, compared to the number of UDP payload bytes of the query."

There's scant excuse to say 'so what' here. Spadafora said the amplification "makes WSD one of the most powerful techniques in a hacker's arsenal for amplifying DDoS attacks which can be crippling to businesses and consumers."

One cause for concern this time around hinged on the very pool of available devices.

Spadafora: "...the new technique being employed by hackers is still cause for concern due to the pool of available devices which Akamai estimates is over 802k." Lily Hay Newman in *Wired*: "Akamai estimates that as many as 800,000 devices exposed on the internet can receive WS-Discovery commands. Which means that by sending 'probes, a kind of roll-call request, you can generate and direct a firehose of data at targets."

What's in it for the hackers? What are they getting out of this? Robert Hackett on Thursday in *Fortune* took a stab at answers. He said knocking targets offline in "distributed denial of service" attacks was "sometimes just for kicks and giggles, other times until a victim pays ransom."

Mitigation?

Respeto said that "Just placing blocks on the UDP source port 3702 will prevent the traffic from hitting your servers. But that is only half of the issue, as the traffic is still congesting bandwidth on your router. This is where your DDoS mitigation provider would come in and add the needed ACL to block the attack traffic."

ACL stands for Access Control Lists. ACLs are the packet filters of a network, said *iTT Systems*. "They can restrict, permit, or deny traffic which is essential for security. An ACL allows you to control the flow of packets for a single or group of IP address or different for protocols, such as TCP, UDP, ICMP, etc."

Some of Respeto's conclusions:

(1) "WSD is a major risk on the Internet that can push some serious

bandwidth using CCTV and DVRs.". Manufacturers can limit the scope of the UDP protocol on port 3702 to the multicast IP space.

(2) "Organizations should be ready to route traffic to their DDoS mitigation provider if they're hit with this large attack. Due to its large amplification factors, we expect that attackers will waste little time in leveraging WSD for use as a reflection vector."

What's next?

Hackett saw "security-minded groups" as likely to look to persuade those in possession of vulnerable devices—whether businesses or consumers—to update them. For the technically minded, he added, "that means blocking communications to port 3702." They may also recommend applying firewalls or removing devices from the public Internet. "Ultimately, if the problem gets out of hand, Internet Service Providers could be drawn in, blocking suspicious traffic."

More information: blogs.akamai.com/sitr/2019/09/ …-hitting-35gbps.html