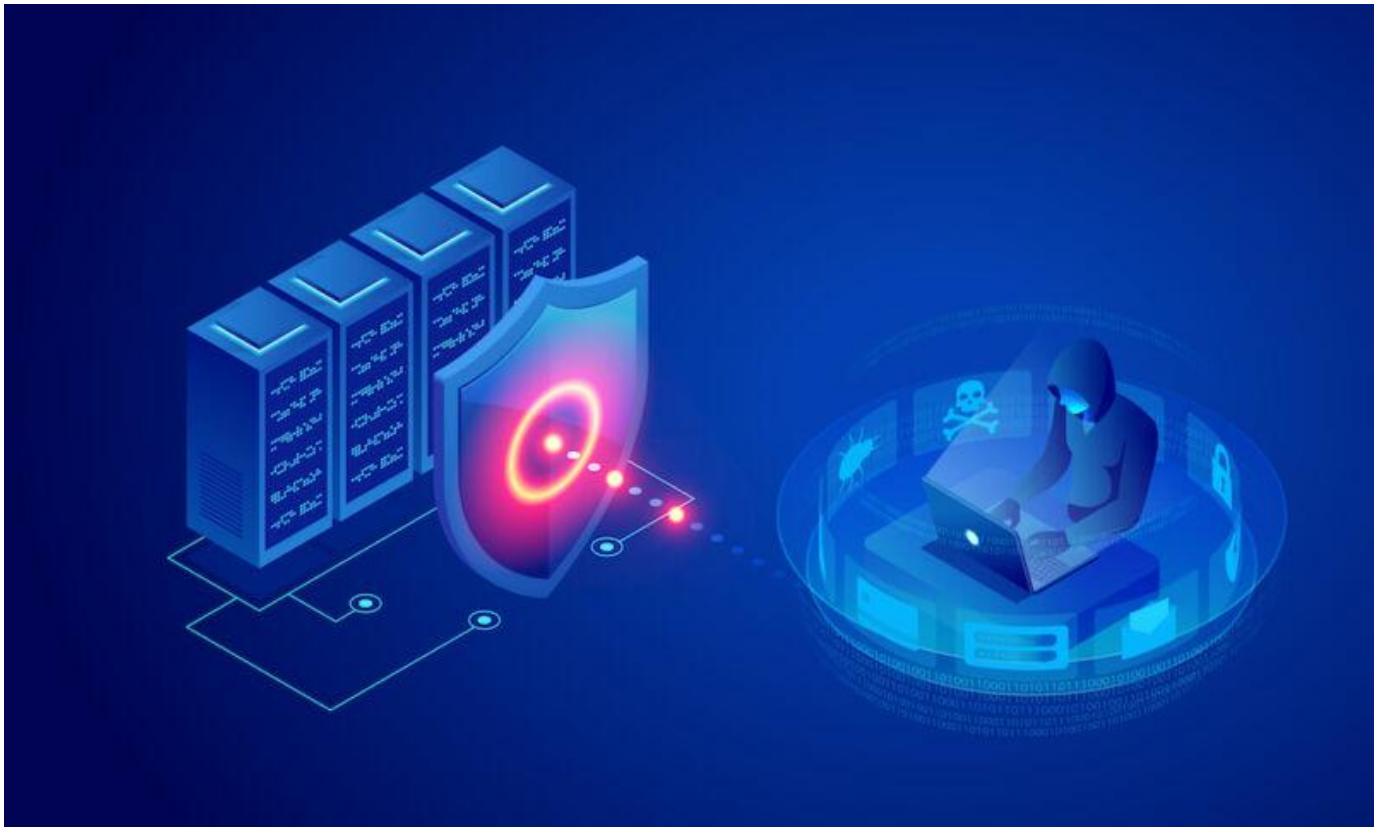
BUILDING A BIGGER DDOS —

New method that amplifies DDoSes by 4 billion-fold. What could go wrong?

New method also stretches out DDoS durations to 14 hours.

DAN GOODIN - 3/8/2022, 6:15 PM



Getty Images

Enlarge

Cybercriminals who use giant floods of data to knock sites offline are leveraging a never-before-seen method that has the potential to increase the damaging effects of those floods by an unprecedented 4 billion times, researchers warned on Tuesday.

Like many other types of distributed denial-of-service attacks, the attacks send a modest amount of junk data to a misconfigured third-party service in a way that causes the service to redirect a much larger response at the intended target. So-called DDoS amplification attacks are popular because they lower the requirements needed to overwhelm their targets. Rather than having to marshal huge amounts of bandwidth and computing power, the DDoSer locates servers on the Internet that will do it for them.

It's all about amplification

FURTHER READING
DDoSers are using a potent new method to deliver attacks of unthinkable size

One of the oldest amplification vectors is misconfigured DNS servers, which increase DDoS volumes by about 54 times. New amplification routes have included the Network Time Protocol servers (about 556x), Plex media servers (about 5x), Microsoft RDP (86x), and the Connectionless Lightweight Directory Access Protocol (at least 50x). Just last week, researchers described a new amplification vector that achieves a factor of at least 65.

Previously, the biggest known amplifier was memcached, which has the potential to increase traffic by an astounding 51,000x.

The newest entrant is the Mitel MiCollab and MiVoice Business Express collaboration systems. Attackers have been using them for the past month to DDoS financial institutions, logistics companies, gaming companies, and organizations in other markets. A fleet of 2,600 servers is exposing an abusable system test facility in the software to the Internet through UDP port 10074, in a break with manufacturer recommendations that the tests be reachable only internally.

FURTHER READING
Microsoft fends off record-breaking 3.47Tbps DDoS attack

The current DDoS records stand at about 3.47 terabits per second for volumetric attacks and roughly 809 million packets per second for exhaustion forms. Volumetric DDoSes work by consuming all available bandwidth either inside the targeted network or service or get between the target and the rest of the Internet. Exhaustion DDoSes, by contrast, over-exert a server.

The new amplification vector provided by the misconfigured Mitel servers has the potential to shatter those records. The vector can do this not only because of the unprecedented 4 billion-fold amplification potential, but also because the Mitel systems can stretch out the attacks for lengths of time not previously possible.

“This particular attack vector differs from most UDP reflection/amplification attack methodologies in that the exposed system test facility can be abused to launch a sustained DDoS attack of up to 14 hours in duration by means of a single spoofed attack initiation packet, resulting in a record-setting packet amplification ratio of 4,294,967,296:1,” researchers from eight organizations wrote in a joint advisory. “A controlled test of this DDoS attack vector yielded more than 400mpps of sustained DDoS attack traffic.”

A single abusable node generating this much amplification at a rate of 80 thousand packets per second can theoretically deliver the 14-hour data flood. Over that time, “counter” packets—which track the number of responses the servers send—would generate roughly 95.5GB of amplified attack traffic destined for the targeted network. Separate “diagnostic output” packets could account for an additional 2.5TB of attack traffic directed toward the target.

A single packet is all it takes

The Mitel MiCollab and MiVoice Business Express services act as a gateway for transferring PBX phone communications to the Internet and vice versa. The products include a driver for TP-240 VoIP processing interface cards. Customers can use a driver feature to stress-test the capacity of their Internet networks. Mitel instructs customers to make the tests available only inside private networks rather than to the Internet as a whole, but about 2,600 servers have flouted that directive.

Mitel on Tuesday released software updates that will automatically ensure the test feature is available inside an internal network.

Page: 1 2 Next →

READER COMMENTS 53

SHARE THIS STORY

DAN GOODIN

Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications. Find him on Mastodon at: https://infosec.exchange/@dangoodin

EMAIL dan.goodin@arstechnica.com

Unsolved Mysteries Of Quantum Leap With Donald P. Bellisario

Today "Quantum Leap" series creator Donald P. Bellisario joins Ars Technica to answer once and for all the lingering questions we have about his enduringly popular show. Was Dr. Sam Beckett really leaping between all those time periods and people or did he simply imagine it all? What do people in the waiting room do while Sam is in their bodies? What happens to Sam's loyal ally Al? 30 years following the series finale, answers to these mysteries and more await.

Unsolved Mysteries Of Quantum Leap With Donald P. Bellisario

Unsolved Mysteries Of Warhammer 40K With Author Dan Abnett

SITREP: F-16 replacement search a signal of F-35 fail?

Sitrep: Boeing 707

More videos

← PREVIOUS STORY

NEXT STORY →

Related Stories

Today on Ars

NEWSLETTER SIGNUP

Join the Ars Orbital Transmission mailing list to get weekly updates delivered to your inbox.

SIGN ME UP →