VoIP.ms phone services disrupted by DDoS extortion attack

By **Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)**

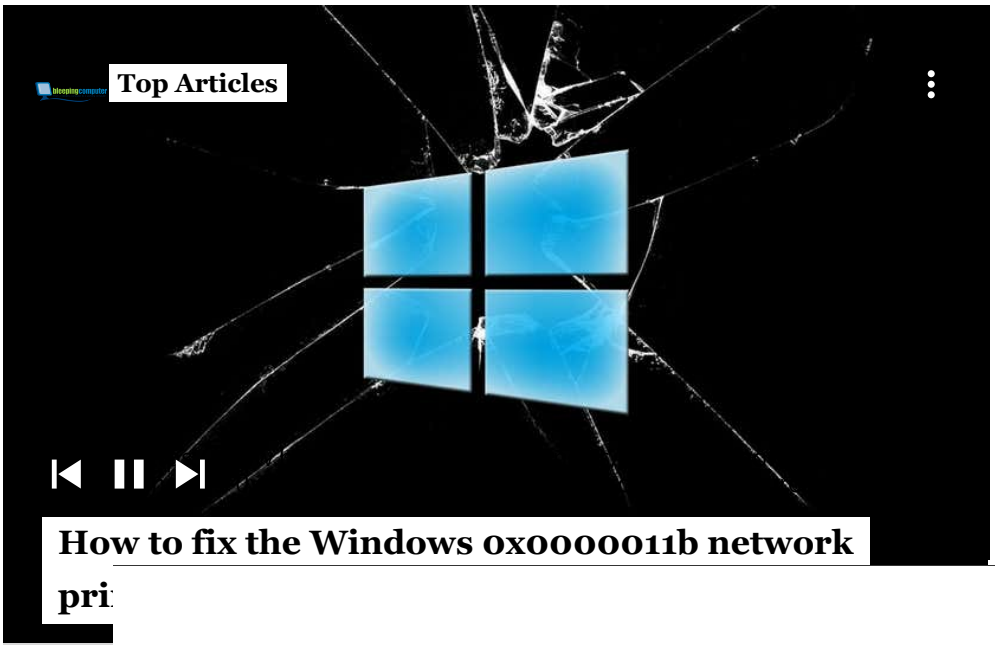
September 20, 2021 11:39 AM **0**

Threat actors are targeting voice-over-Internet provider VoIP.ms with a DDoS attack and extorting the company to stop the assault that's severely disrupting the company's operation.

VoIP.ms is an Internet phone service company that provides affordable voice-over-IP service to businesses around the world.

Phone services disrupted as site goes down

On September 16th, 2021, VoIP.ms became the victim of a distributed denial-of-service attack targeting their infrastructure, including DNS name servers.



(https://twitter.com/voipms/status/1438537573358505984)

As customers configured their VoIP equipment to connect to the company's domain name, the DDoS attack disrupted telephony services, preventing them from receiving or making phone calls.

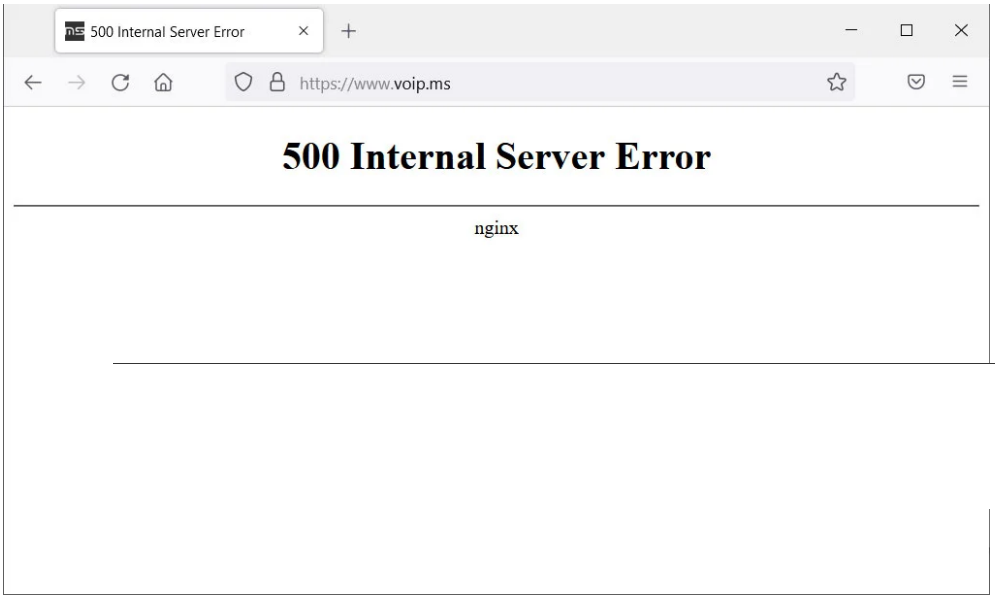
As DNS was no longer working, the company advised customers to modify their HOSTS file to point the domain at their IP address to bypass DNS resolution.

However, this just led the threat actors to perform DDoS attacks directly at that IP address as well.

To mitigate the attacks, VoIP.ms moved their website and DNS servers to Cloudflare, and while they reported some success, the company's site and VoIP infrastructure still have issues due to the continued denial-of-service attack.

"A Distributed Denial of Service (DDoS) attack continues to be targeted at our Websites and POP servers. Our team is deploying continuous efforts to stop this however the service is being intermittently affected. We apologize for all the inconveniences," says an announcement posted to the VoIP.ms website.

At the time of this writing, the site is bouncing back and forth between being accessible and displaying a 500 Internal Server Error, as shown below.



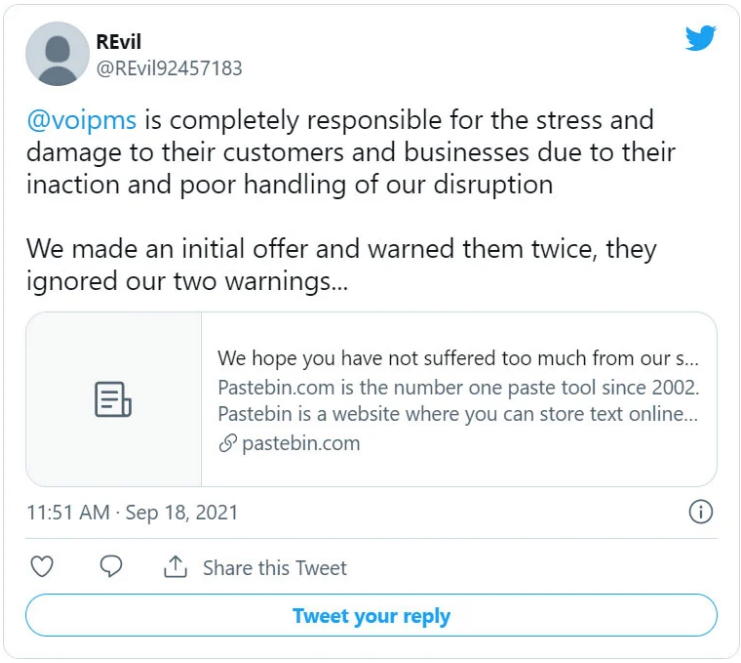
VoIP.ms site

Today, customers continue to experience issues with their telephone service, including loss of service, dropped calls, poor performance, and the inability to forward lines.

Threat actors demand ransom

On September 18th, a threat actor using the name 'REvil' claimed responsibility for the attack and posted a link to a ransom note posted to Pastebin.

This ransom note has since been removed from Pastebin, but BleepingComputer was told it asked for one bitcoin, or approximately $45,000, to stop the DDoS attacks.



REvil is f
(https://
1-000-pl
to attack
(https://www.bleepingcomputer.com/news/security/revil-ransomware-is-back-in-full-attack-mode-and-leaking-data/) after their disappearance on July 13th (https://www.bleepingcomputer.com/news/security/revil-ransomware-gangs-web-sites-mysteriously-shut-down/).

REvil is not known for DDoS attacks or publicly demanding ransoms, in a manner done in the VoIP.ms attack. This attack's method of extortion makes us believe that the threat actors are simply impersonating the ransomware operation to intimidate VoIP.ms further.

Soon after their original tweet, the threat actors raised their extortion demand to 100 bitcoins, or approximately $4.3 million.

The customers' responses to the attack against VoIP.ms have been mixed.

Some feel that VoIP.ms should pay the ransom to restore services before they themselves do not lose customers. At the same time, other VoIP.ms customers are vowing to stick with them and telling the company not to give in to the ransom demand.

BleepingComputer has contacted VoIP.ms with questions regarding the attack but has not received a reply.

Related Articles:

Admin of DDoS service behind 200,000 attacks faces 35yrs in prison (https://www.bleepingcomputer.com/news/security/admin-of-ddos-service-behind-200-000-attacks-faces-35yrs-in-prison/)

Yandex is battling the largest DDoS in Russian Internet history (https://www.bleepingcomputer.com/news/security/yandex-is-battling-the-largest-ddos-in-russian-internet-history/)

MikroTil
(https://
on-secur

New Mēris botnet breaks DDoS record with 21.8 million RPS attack (https://www.bleepingcomputer.com/news/security/new-m-ris-botnet-breaks-ddos-record-with-218-million-rps-attack/)

FTC warns of extortionists targeting LGBTQ+ community on dating apps (https://www.bleepingcomputer.com/news/security/ftc-warns-of-extortionists-targeting-lgbtq-plus-community-on-dating-apps/)

CYBERATTACK (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/CYBERATTACK/)

DDOS (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/DDOS/)

DISTRIBUTED DENIAL-OF-SERVICE (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/DISTRIBUTED-DENIAL-OF-SERVICE/)

EXTORTION (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/EXTORTION/)

VOIP (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/VOIP/)