Phone calls disrupted by ongoing DDoS cyber attack on VOIP.ms

Threat actors asking $4.2 million from VoIP.ms to stop DDoS attack.

AX SHARMA – SEP 22, 2021 8:03 A.M. |

Credit: Icons8 Team

Quebec-based provider of telephony services VoIP.ms is facing an aggressive Distributed Denial of Service (DDoS) cyber attack, causing a disruption in phone calls and services. The incident began around September 16 and has put a strain on the VoIP provider's systems, websites, and operations.

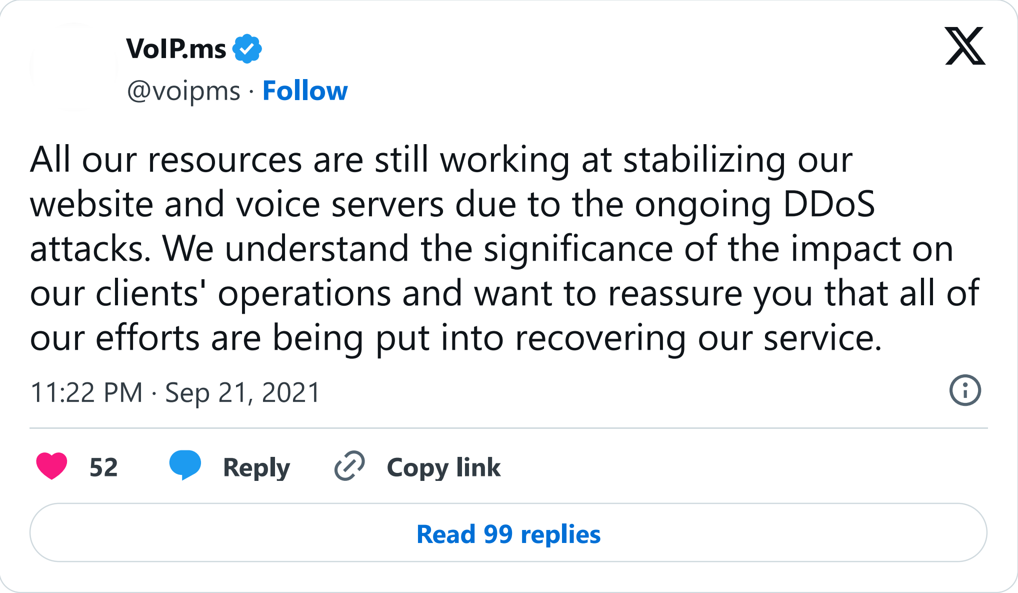
VoIP.ms serves over 80,000 customers across 125 countries, many of whom are now facing issues with voice calls.

Voice calls and services disrupted by DDoS attack

Last week, Canadian voice-over-IP service provider VoIP.ms announced that it became aware of an issue that was preventing customers from accessing its website and was working toward a solution. Fast-forward to today: the issue is ongoing and has been attributed to a persistent DDoS attack.

DDoS is a form of cyber attack in which multiple computers, or "bots," are simultaneously engaged by an attacker to make a large number of requests to an Internet server beyond the server's capacity. As such, an Internet server, when facing a sophisticated DDoS attack, may offer degraded performance to customers, or crash altogether. VoIP is a set of technologies that make telephone calls possible via Internet-connected servers, which, like any Internet service, makes them vulnerable to DDoS attacks.

As of today, VoIP.ms is still battling the cyber attack:

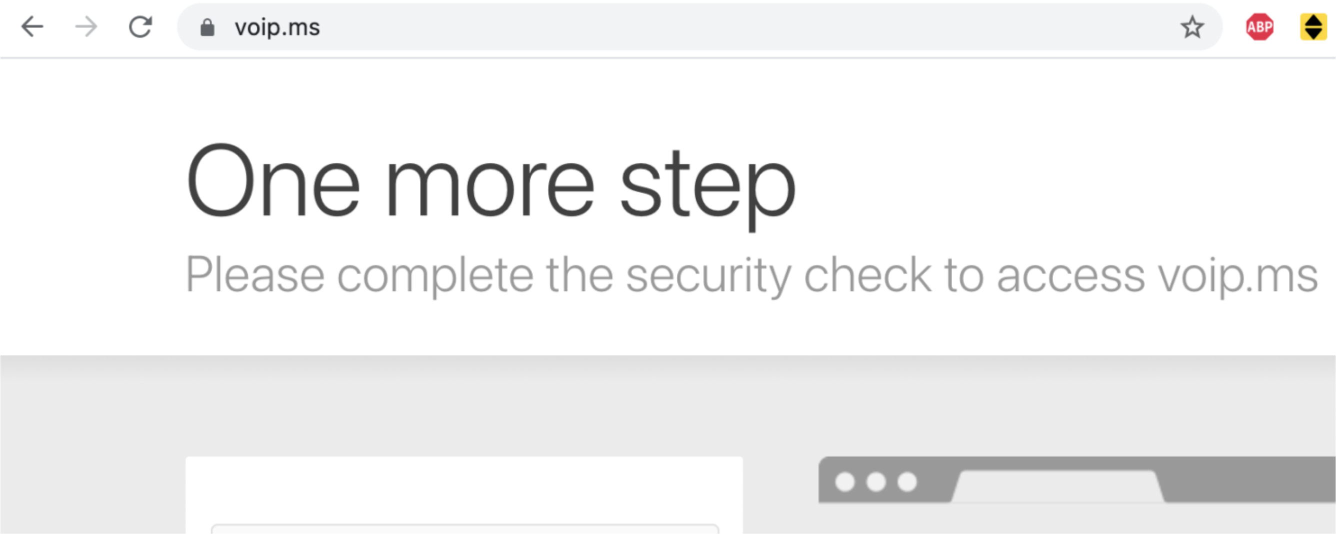


VoIP.ms
@voipms · Follow

All our resources are still working at stabilizing our website and voice servers due to the ongoing DDoS attacks. We understand the significance of the impact on our clients' operations and want to reassure you that all of our efforts are being put into recovering our service.

11:22 PM · Sep 21, 2021

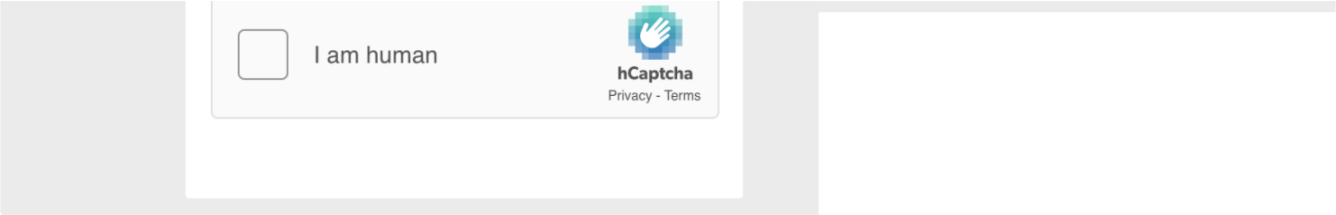
As seen by Ars, the VoIP.ms website is now requiring visitors to solve captchas before letting them in. Prior to this, the website was throwing HTTP 500 (service unavailable) errors on occasion.



One more step

Please complete the security check to access voip.ms

VoIP.ms website asks for captcha. Credit: Ax Sharma



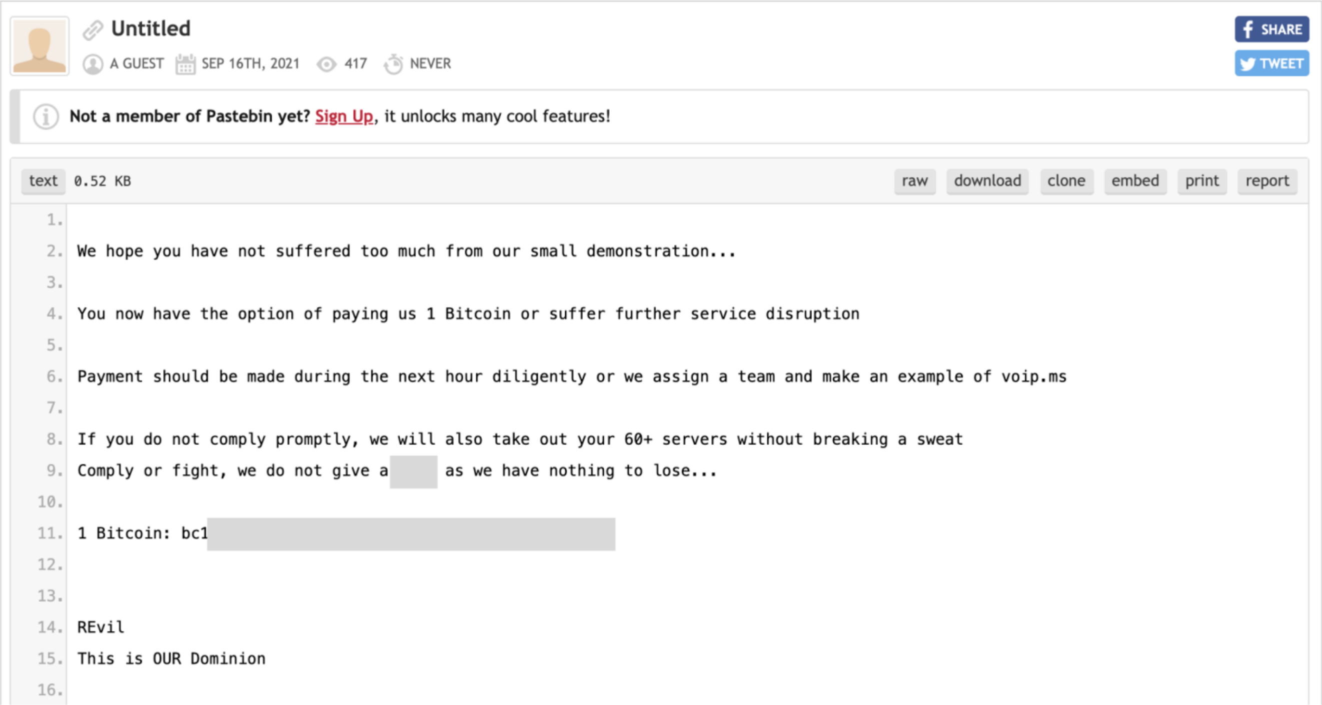
Once in, the website states: "a Distributed Denial of Service (DDoS) attack continues to be targeted at our Websites and POP servers. Our team is deploying continuous efforts to stop this however the service is being intermittently affected."

Threat actors demand over $4.2 million in extortion attack

Tweets exchanged between VoIP.ms and the threat actors provide interesting insights. The threat actors behind the DDoS attack go by the name "REvil," but it cannot be authoritatively established if they represent the same REvil ransomware gang that is known to have previously attacked prominent companies, including the world's largest meat processor, JBS.

Further, based on the multiple demands made by the threat actor to VoIP.ms for bitcoins, this incident has been labeled an extortion attack.

"This is possibly a cyber extortion campaign. They bring down services via DDoS and then demand money. Don't know if the DDoS attack and the ransom demand are from the same idiots," noted Twitter user *PremoWeb*, pointing to a Pastebin note that has now been removed. The removed note retrieved by Ars shows the attackers' initial ask was for 1 Bitcoin, or a little over US$42,000:



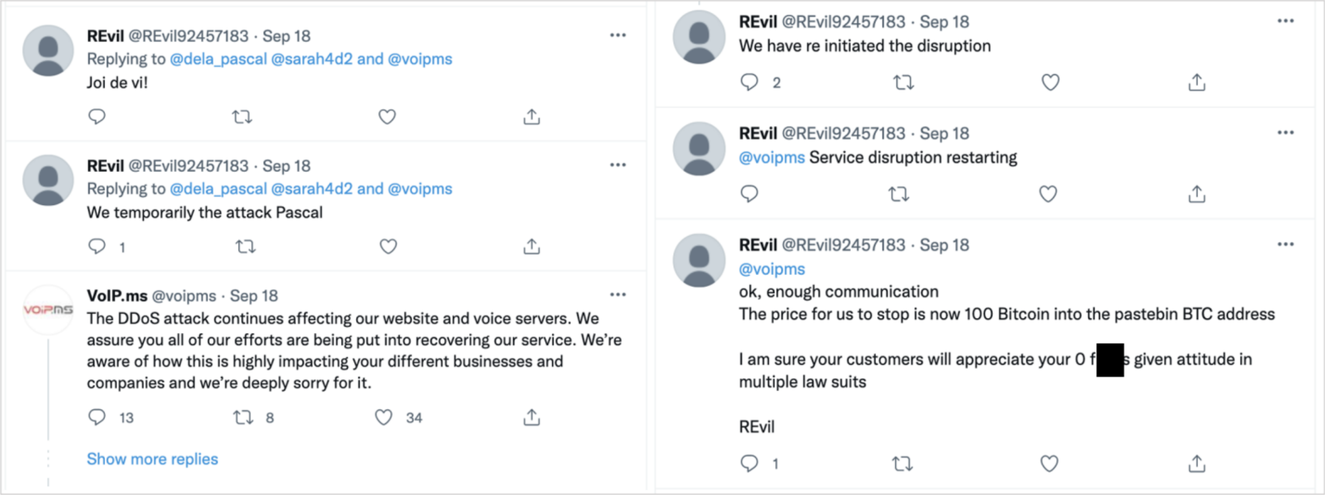
Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

```

We hope you have not suffered too much from our small demonstration...

You now have the option of paying us 1 Bitcoin or suffer further service disruption

Payment should be made during the next hour diligently or we assign a team and make an example of voip.ms

If you do not comply promptly, we will also take out your 60+ servers without breaking a sweat
Comply or fight, we do not give a [redacted] as we have nothing to lose...

1 Bitcoin: bc1[redacted]


REvil
This is OUR Dominion

```

Now-removed Pastebin note retrieved by Ars. Credit: Ax Sharma

But, two days later, the demand was upped to 100 Bitcoins, or over US$4.2 million:

"Ok, enough communication... The price for us to stop is now 100 Bitcoin into the pastebin BTC address. I am sure your customers will appreciate your 0 [expletive] given attitude in multiple law suits," read the tweet signed "REvil."



REvil @REvil92457183 · Sep 18
Replying to @dela_pascal @sarah4d2 and @voipms
Joi de vi!

REvil @REvil92457183 · Sep 18
Replying to @dela_pascal @sarah4d2 and @voipms
We temporarily the attack Pascal

VoIP.ms @voipms · Sep 18
The DDoS attack continues affecting our website and voice servers. We assure you all of our efforts are being put into recovering our service. We're aware of how this is highly impacting your different businesses and companies and we're deeply sorry for it.

REvil @REvil92457183 · Sep 18
We have re initiated the disruption

REvil @REvil92457183 · Sep 18
@voipms Service disruption restarting

REvil @REvil92457183 · Sep 18
@voipms
ok, enough communication
The price for us to stop is now 100 Bitcoin into the pastebin BTC address

I am sure your customers will appreciate your 0 f[redacted]s given attitude in multiple law suits

REvil

Attackers increased demand from 1 BTC to 100 BTC.

Earlier this month, UK-based telecom VoIP Unlimited was slapped with a similar DDoS attack, suspected to originate from "REvil." However, threat actors behind these attacks are likely different from the REvil ransomware operator.

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

VoIP.ms customers can monitor the company's Twitter feed for updates on the situation.

AX SHARMA

Ax Sharma is a security researcher, engineer, and reporter.