Powerhost's ESXi Servers Encrypted with New SEXi Ransomware

By Madalina Popovici

Published: 2024-04-05 · Archived: 2026-04-02 11:57:14 UTC

IxMetro Powerhost, a Chilean data center and hosting provider, has become the latest target of a cyberattack by a newly identified ransomware group dubbed SEXi.

This malicious group successfully encrypted the company's VMware ESXi servers, which host virtual private servers for their clients, as well as the backups, putting a significant portion of hosted websites and services out of commission.

How is PowerHost responding to the attack?

Following the attack, PowerHost, which operates across the USA, South America, and Europe, has been striving to mitigate the impact on its customers.

Despite efforts to restore the compromised data from backups, the company faces challenges due to the encryption of these backups as well.

In an effort to address customer concerns, PowerHost has extended an offer to impacted VPS customers, proposing to set up new VPS systems for those who still possess their website content, enabling them to resume online operations.

The ransom demand and negotiations

Negotiations with the perpetrators revealed a ransom demand of two bitcoins per victim, totaling an astronomical sum of $140 million.

PowerHost's CEO, Ricardo Rubem, shared insights into the negotiations and the advice received from security agencies, emphasizing the high risk and low success rate of giving in to ransom demands.

> From the very beginning of the issue, we have been in contact and collaborating with various security agencies in various countries to determine if they were aware of this ransomware.
>
> All the information we've gathered indicates that these are new variants with a very high level of damage. Personally, I negotiated with the hijacker, who demanded an exorbitant amount of bitcoins per customer: 2 BTC for each, which added up to around 140 million.
>
> However, even if we could muster the required amount, would it really help us? The unanimous recommendation of all law enforcement agencies is not to negotiate, as in more than 90% of cases, criminals simply disappear after payment.
>
> PowerHost CEO Ricardo Rubem (source)

SEXi ransomware

PowerHost was attacked by a new type of ransomware, according to CronUp cybersecurity expert Germán Fernández.

This ransomware encrypts files and leaves behind a ransom note titled SEXi.txt.

So far, this ransomware has only attacked VMware ESXi servers. Its name, “SEXi,” is a clever play on the word “ESXi.”

What do the experts say?

Germán Fernández discovered that the ransomware encrypted virtual machine files and marked them with a unique SEXi extension, as evidenced by the content of the ransom notes.

These notes instruct victims to download the Session messaging app for communication and include a specific contact address for negotiations.

Ransomware note (source)

BleepingComputer has some insights from SANS instructor Will Thomas about new ransomware variants named SOCOTRA, FORMOSA, and LIMPOPO, active since February 2024.

These variants, which add unique extensions like .LIMPOPO to files, don’t seem to relate directly to their namesakes. But interestingly, these campaigns, including the SEXi ransomware, **share a common Session contact ID in their ransom notes**, suggesting a uniform approach to victim communication.

The LIMPOPO variant, in particular, is believed to be developed from the leaked Babuk ransomware source code, known for targeting ESXi servers.

Currently, there’s no sign of Windows-targeted encryptors in these campaigns, nor clear evidence of double extortion tactics being used, though the situation could change as these are new operations.

Additional Resources

How to Mitigate Ransomware
How to Prevent Ransomware

If you liked this piece, follow us on **LinkedIn**, **Twitter**, **Facebook**, and **YouTube** for more cybersecurity news and topics.

Neutralize ransomware before it can hit.

Heimdal™ Ransomware Encryption Protection

Specifically engineered to counter the number one security risk to any business – ransomware.

- Blocks any unauthorized encryption attempts;
- Detects ransomware regardless of signature;
- Universal compatibility with any cybersecurity solution;
- Full audit trail with stunning graphics;

Madalina, a seasoned digital content creator at Heimdal®, blends her passion for cybersecurity with an 8-year background in PR & CSR consultancy. Skilled in making complex cyber topics accessible, she bridges the gap between cyber experts and the wider audience with finesse.

Source: https://heimdalsecurity.com/blog/powerhosts-esxi-servers-encrypted-with-new-sexi-ransomware/