Ransomware Desires VMware Hypervisors in Ongoing Campaign

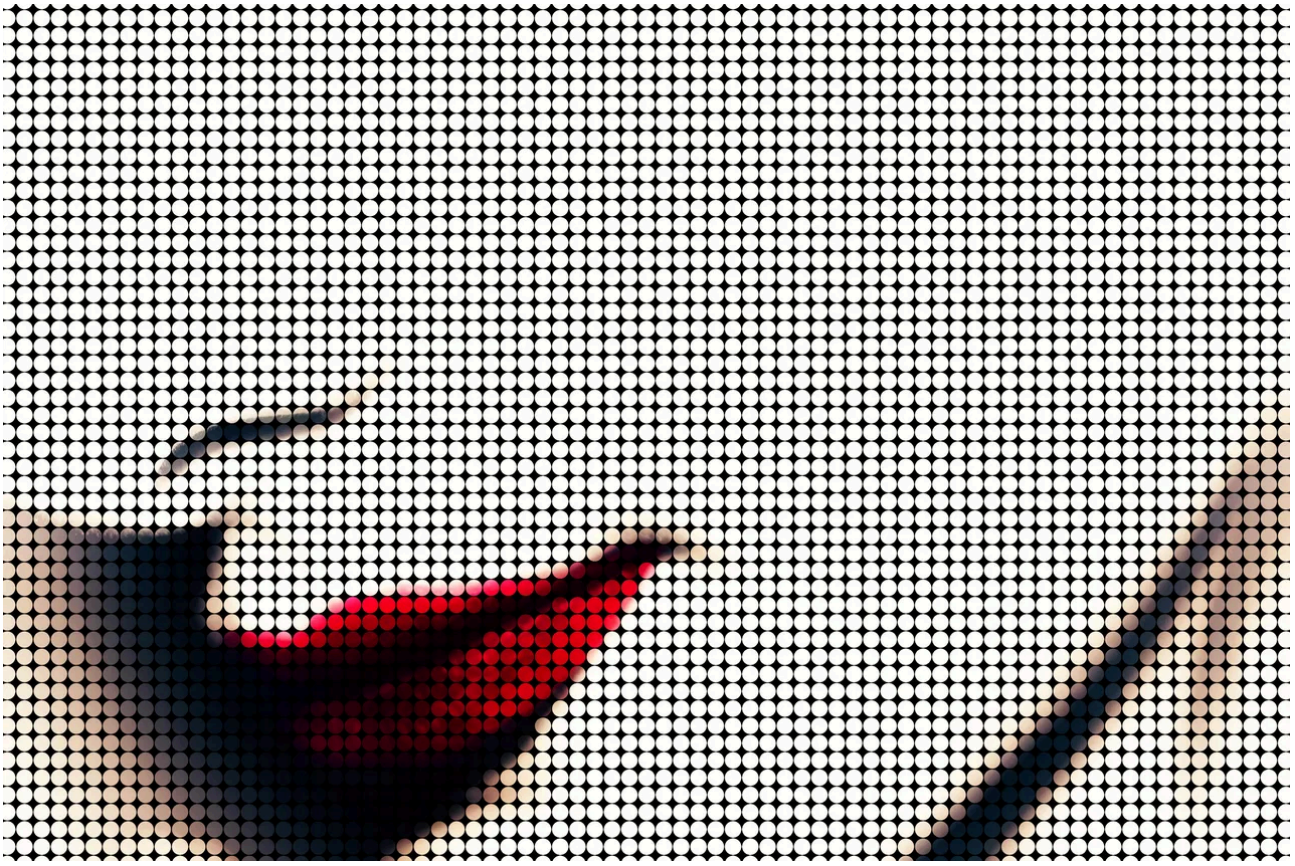
By Tara Seals

Published: 2024-04-04 · Archived: 2026-04-02 12:27:44 UTC

Tara Seals,Managing Editor, News,Dark Reading

April 4, 2024

4 Min Read



Source: Don McBailey/Stockimo via Alamy Stock Photo

What appears to be a fresh variant of the Babuk ransomware has emerged to attack VMware ESXi servers in several countries, including a confirmed hit on IxMetro PowerHost, a Chilean data center hosting company. The variant calls itself "SEXi," a play on its target platform of choice.

According to CronUp cybersecurity researcher Germán Fernández, PowerHost CEO Ricardo Rubem issued a statement confirming that a new ransomware variant had locked up the company's servers using the .SEXi file extension, with the initial access vector to the internal network as yet unknown. The attackers requested $140 million in ransom, which Rubem indicated would not be paid.

SEXi's emergence stands at the crossroads of two major ransomware trends: the rash of threat actors who have developed malware based on the Babuk source code; and a lust for compromising tantalizingly juicy VMware EXSi servers.

IX PowerHost Attack Part of Wider Ransomware Campaign

Meanwhile, Will Thomas, CTI researcher at Equinix, uncovered what he believes to be a binary related to that used in the attack, dubbed "LIMPOPOx32.bin" and tagged as a Linux version of Babuk in VirusTotal. At press time, that malware has a 53% detection rate on VT, with 34 out of 64 security vendors flagging it as malicious since it was first uploaded on Feb. 8. MalwareHunterTeam spotted it back on Valentine's Day, when it was being used without the "SEXi" handle in an attack on an entity in Thailand.

But Thomas further discovered other, related binaries. As he tweeted, "SEXi ransomware attack on IXMETRO POWERHOST linked to broader campaign that has hit at least three Latin American countries." These call themselves Socotra (used in an attack in Chile on March 23); Limpopo again (used in an attack in Peru on Feb. 9); and Formosa (used in an attack in Mexico on Feb. 26). Concerningly, at press time all three registered zero detections in VT.

Together, the findings showcase the development of a novel campaign using various SEXi iterations that all lead back to Babuk.

Shadowy TTPs Emerge in SEXi Attacks

There's no indication of where the malware operators originate from or what their intentions are. But slowly a set of tactics, techniques, and procedures are emerging. For one, the binaries' nomenclature comes from place names. Limpopo is the northernmost province of South Africa; Socotra is a Yemeni island in the Indian Ocean; and Formosa was a short-lived republic located on Taiwan in the late 1800s, after China's Qing Dynasty ceded its rule over the island.

And, as MalwareHunterTeam pointed out on X, "maybe interesting / worth to mention about this 'SEXi' ransomware that the communication method specified by the actors in the note is Session. While we['ve] seen some actors using it even years ago already, I [don't] remember seeing it in relation to any big/serious cases/actors."

Session is a cross-platform, end-to-end encrypted instant messaging application emphasizing user confidentiality and anonymity. The ransom note in the IX PowerHost attack urged the company to download the app and then send a message with the code "SEXi"; the earlier note in the Thai attack urged the Session download but to include the code "Limpopo."

EXSi Is Sexy to Cyberattackers

VMware's EXSi hypervisor platform runs on Linux and Linux-like OS, and can host multiple, data-rich virtual machines (VMs). It has been a popular target for ransomware actors for years now, partly because of the size of the attack surface: There are tens of thousands of ESXi servers exposed to the Internet, according to a Shodan

search, with most of them running older versions. And that doesn't take into account those that are reachable after an initial access breach of a corporate network.

Also contributing to ransomware gangs' growing interest in EXSi, the platform doesn't support any third-party security tooling.

"Unmanaged devices such as ESXi servers are a great target for ransomware threat actors," according to a report from Forescout released last year. "That's because of the valuable data on these servers, a growing number of exploited vulnerabilities affecting them, their frequent Internet exposure and the difficulty of implementing security measures, such as endpoint detection and response (EDR), on these devices. ESXi is a high-yielding target for attackers since it hosts several VMs, allowing attackers to deploy malware once and encrypt numerous servers with a single command."

VMware has a guide for securing EXSi environments. Specific suggestions include: Make sure ESXi software is patched and up-to-date; harden passwords; remove servers from the Internet; monitor for abnormal activities on network traffic and on ESXi servers; and ensure there are backups of the VMs outside the ESXi environment to enable recovery.

About the Author

Managing Editor, News, Dark Reading

Tara Seals has 20+ years of experience as a journalist, analyst and editor in the cybersecurity, communications and technology space. Prior to Dark Reading, Tara was Editor in Chief at Threatpost, and prior to that, the North American news lead for Infosecurity Magazine. She also spent 13 years working for Informa (formerly Virgo Publishing), as executive editor and editor-in-chief at publications focused on both the service provider and the enterprise arenas. A Texas native, she holds a B.A. from Columbia University, lives in Western Massachusetts with her family and is on a never-ending quest for good Mexican food in the Northeast.

Source: https://www.darkreading.com/threat-intelligence/sexi-ransomware-desires-vmware-hypervisors