KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Lorenz Ransomware exploits Mitel VoIP systems

Tracker ID: TN0921 **Date:** 22/Sept/2022 **Category:** Malware **Industry:** All **Region**: Asia, N. America

Background

The developers of the Lorenz Ransomware operation used a now-patched security vulnerability in Mitel MiVoice Connect to obtain access to target environments for subsequent malicious actions. The first malicious activity originated from a Mitel device on the network's perimeter, where the threat actor gained a reverse shell by exploiting CVE-2022-29499, a remote code execution vulnerability affecting the Mitel Service Appliance component of MiVoice Connect. It also used a Chisel as a tunnelling tool to pivot into the environment.

Lorenz Ransomware operators primarily targeted small and medium-sized businesses (SMBs) in the United States, with a lesser degree in China and Mexico. Lorenz, like many other ransomware operators, is infamous for double extortion by first stealing data and then encrypting systems. It's an "evolving ransomware" that's thought to be a rebranded version of the ".sZ40" malware identified in October 2020.

Mitel VoIP appliances are being used in ransomware attacks to gain remote code execution against an unidentified victim. Mitel VoIP solutions are a potential entry point given that there are around 20,000 internet-exposed devices online, rendering them vulnerable to malicious attacks. In one such attack, the threat actor utilized the remote code execution issue to construct a reverse shell and download the Chisel proxy tool.

The initial access was either made feasible with the help of an initial access broker (IAB) exploiting CVE-2022-29499 or the threat actors can initiate such a connection on their own. It's also worth noting that the Lorenz gang took about a month after acquiring initial access to execute post-exploitation operations like establishing persistence via a web shell, harvesting credentials, network reconnaissance, privilege escalation, and lateral movement. The attack eventually resulted in data exfiltration using FileZilla, and the hosts were then encrypted via Microsoft's BitLocker service, showing adversaries' continuous exploitation of LOLBINs.

The ransomware operators predominantly target victims in English-speaking nations. According to their website, they have published stolen data from 20 victims. However, the actual number of successful assaults is estimated to be higher. Enterprise security teams should keep a close watch on all internet-facing assets, including VoIP and IoT devices, for any indicators of malicious behavior. Since merely monitoring critical assets is unsustainable, as the threat actors are beginning to target less monitored assets to avoid discovery.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Lorenz Ransomware exploits Mitel VoIP systems

Tracker ID: TN0921 **Date:** 22/Sept/2022 **Category:** Malware **Industry:** All **Region**: Asia, N. America

MITRE ATT&CK Tactics

Initial Access, Lateral Movement, Execution, Defense Evasion, Credential Access, Discovery, Collection and Impact.

Indicators of Compromise

Please refer to the attached sheet for IOCs.

Recommendations

- Validate the IOCs attached and implement the detection & prevention accordingly. Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Immediately identify the vulnerable instances of Mitel MiVoice Connect:
    - R19.2 SP3 and earlier
    - R14.x and earlier
- Upgrade to the fixed version MiVoice Connect R19.3.
- Enforce strong passwords and maintain regular data backups.
- Use endpoint detection and response systems that can detect and remediate suspicious activity automatically.
- Monitor all internet-facing devices for potential malicious activity, including VoIP and IoT devices.
- Collect and review relevant logs, data, and artifacts to ensure the threat is eradicated from the network and thwart residual issues that could enable follow-on exploitation.

References

- Markus Neis, Ross Phillips, Steven Campbell, Teresa Whitmore, Alex Ammons, and Arctic Wolf Labs Team, Chiseling In: Lorenz Ransomware Group Cracks MiVoice And Calls Back For Free, Arctic Wolf, 12th September 2022, External Link (arcticwolf.com).
- Jeff Burt, Patch your Mitel VoIP systems, Lorenz ransomware gang is back on the prowl, The Register, 13th September 2022, External Link (www.theregister.com).
- Ravie Lakshmanan, Lorenz Ransomware Exploit Mitel VoIP Systems to Breach Business Networks, The Hacker News, 14th September 2022, External Link (thehackernews.com).

KPMG in India Cyber Response Hotline : +91 9176471471

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Lorenz Ransomware exploits Mitel VoIP systems

Tracker ID: TN0921 **Date:** 22/Sept/2022 **Category:** Malware **Industry:** All **Region**: Asia, N. America

*

SHA-256	IP
71cdbbc62e10983db183ca60ab964c1a3dab0d279c5326b2e920522480780956	157[.]90[.]147[.]28
4b1170f7774acfdc5517fbe1c911f2bd9f1af498f3c3d25078f05c95701cc999	172[.]86[.]75[.]63
8ea6a6d4578029c7b2dbbfb525ec88b2cb309901ec5a987847471b6101f0de41	162[.]33[.]179[.]45
971f0a32094b8ac10712503305ac6789048d190a209c436839e2e6b0acb016f3	172[.]86[.]75[.]63
cef17b9289ba18c979b704648c0f2b736f65f9f9158b471bc2486b6c14e14a4d	65[.]21[.]187[.]237
edc2070fd8116f1df5c8d419189331ec606d10062818c5f3de865cd0f7d6db84	167[.]99[.]186[.]156
a0ccb9019b90716c8ee1bc0829e0e04cf7166be2f25987abbc8987e65cef2e6f	157[.]90[.]147[.]28
1264b40feaa824d5ba31cef3c8a4ede230c61ef71c8a7994875deefe32bd8b3d	143[.]198[.]117[.]43
40ff1ab8ac09057421079dae83fb675d7a2a3da6c7d0cd6400a0d720c5b0f58c	45[.]61[.]139[.]150
a9fdbc6d20b780ca42660ad4803f391308fa0243fbc515fd3c1acf935dd43c1e	
7275034886da11ca6d828547f15cab259e22ba624c5f5762afd237aa686455dd	
5b03b861884cb3e14a8b888c7dee2ee0d494933df863d504882345fa278d1ea5	
71cdbbc62e10983db183ca60ab964c1a3dab0d279c5326b2e920522480780956	
4b1170f7774acfdc5517fbe1c911f2bd9f1af498f3c3d25078f05c95701cc999	
c0c99b141b014c8e2a5c586586ae9dc01fd634ea977e2714fbef62d7626eb3fb	