KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Prevalent Ransom Attacks by Iranian Phosphorus Hackers

Tracker ID: TN0915 **Date:** 21/Sept/2022 **Category:** Threat Actor **Industry:** All **Region**: All

Background

Phosphorus, an Iranian threat actor, is known for launching ransomware attacks for private gain as a "form of moonlighting." The group is tracked as DEV-0270, aka "Nemesis Kitten," and is suspected of being managed by corporations Secnerd and Lifeweb, as their infrastructure overlaps. DEV-0270 gets access to systems by exploiting high-severity vulnerabilities and is well-known for its early adoption of newly disclosed vulnerabilities.

DEV-0270 additionally prominently employs living-off-the-land binaries (LOLBINs) throughout the attack chain for credential access and discovery. This includes encrypting files on infected PCs with the built-in BitLocker program. The utilization of BitLocker and DiskCryptor by Iranian actors for opportunistic ransomware attacks was uncovered earlier this May when a threat organization known as Cobalt Mirage, which has ties to Phosphorus (aka Cobalt Illusion) and TunnelVision, carried out a series of assaults.

DEV-0270 performs network reconnaissance and credential theft activities to get initial access after scanning the Internet for servers and devices vulnerable to Microsoft Exchange Server, Fortinet FortiGate SSL-VPN, and Apache Log4J weaknesses. It establishes persistence through a scheduled procedure to acquire access to the compromised network. DEV-0270 then escalates privileges to the system level to perform post-exploitation tasks such as disabling Microsoft Defender Antivirus to prevent detection, lateral movement, and file encryption. To maintain operational security and stealth, it usually employs registry configurations, native WMI, NET, CMD, and PowerShell commands. It hides its presence by installing and masquerading as legitimate processes to use its modified binaries.

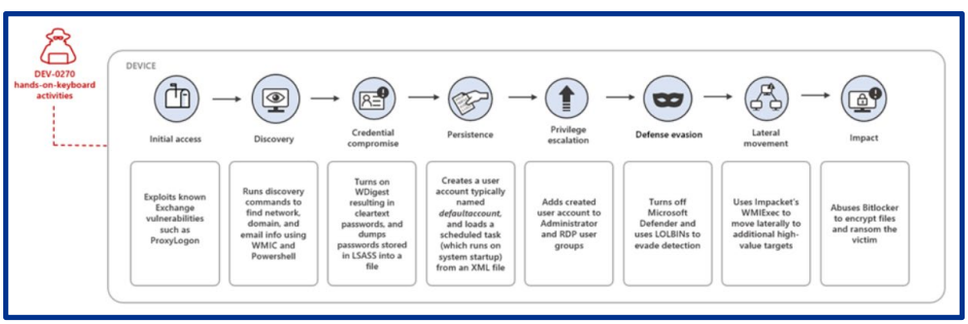

Fig.1 DEV-0270 attack chain

The organization dropped a ransom note demanding $8,000 for the decryption keys about two days after the first intrusion in some successful infections. When the victim organization refused to pay in one case, the actor chose to sell the stolen data. We advise enterprises to be cautious. Prioritize patching of internet-facing Exchange servers to limit risk, prevent network appliances such as Fortinet SSL-VPN devices from creating arbitrary internet connections, enforce strong passwords, and keep regular data backups.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Prevalent Ransom Attacks by Iranian Phosphorus Hackers

Tracker ID: TN0915 **Date:** 21/Sept/2022 **Category:** Threat Actor **Industry:** All **Region**: All

MITRE ATT&CK Tactics

Reconnaissance, Initial access, Discovery, Credential access, Persistence, Privilege Escalation, Defense Evasion, Lateral Movement and Impact.

Recommendations

- Prioritize patching for Internet-facing systems and products, predominantly for Log4J vulnerabilities.
- Ensure Microsoft Exchange Servers are patched for CVE-2021-26855, CVE-2021-26858, CVE-2021-26857 and CVE-2021-27065.
- Update Fortinet FortiGate SSL-VPN and Apache servers against known vulnerabilities.
- Restrict network appliances like Fortinet SSL-VPN devices from making arbitrary connections to the internet and downloads.
- Enforce strong passwords and maintain regular data backups.
- Use endpoint detection and response systems that can detect and remediate suspicious activity automatically.

References

- Ravie Lakshmanan, Microsoft Warns of Ransomware Attacks by Iranian Phosphorus Hacker Group, The Hacker News, 08th September 2022, External Link (thehackernews.com)
- Microsoft Security Threat Intelligence, Profiling DEV-0270: PHOSPHORUS' ransomware operations, Microsoft, 07th September 2022, External Link (microsoft.com)

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 in India Cyber Response Hotline : +91 9176471471