TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

1 April 2020

PIN Number

20200401-001

Please contact the FBI with any questions related to this Private Industry Notification via your local Cyber Squad or FBI CyWatch.

www.fbi.gov/contact-us/field | **E-Mail:** cywatch@fbi.gov | **Phone: 1-855-292-3937**

Sodinokibi Ransomware Actors Adopt New Tactics

Summary

This notification updates PIN 20190819-001, Sodinokibi Ransomware Actors Target Management Service Providers' Clients (19 August 2019).

Sodinokibi ransomware actors have adopted new tactics with the potential to increase the number of victims and potential revenue generated from their attacks. These new tactics include examining data in compromised accounts for information that could provide leverage for extortion and searching for unpatched vulnerabilities in virtual private network (VPN) servers to facilitate deployment of malware.

Threat

Extortion Attempts Increase

As of early March 2020, Sodinokibi actors are directing some victims to pay ransoms under threat of extortion. This mimics the actions several ransomware groups adopted in late 2019—including Maze, Nemty, and DoppelPaymer—possibly in response to victim rejection of ransom demands. In this new variation of the ransomware scheme, Sodinokibi actors search through

compromised accounts for proprietary or potentially embarrassing information about the victim, vendors, or clients.

The actors threaten to pass the information to competitors or share with the general public under the assumption the release of sensitive information could cost potential victims more than any ransom demand.

Pulse Secure Servers Targeted

Since at least mid-2019, Sodinokibi actors used and continue to conduct mass port scans to identify Pulse Secure virtual private network (VPN) servers that still remain unpatched for CVE-2019-11510. The actors leverage the vulnerability to obtain private keys and passwords, which, when used in conjunction with a remote command injection vulnerability (CVE-2019-11539), permit entry to the victim's VPN. They use the compromised credentials to obtain administrative privileges, disable endpoint security tools, and install the Sodinokibi ransomware.

Attacks Against Managed Service Providers Persist

Sodinokibi actors continue to compromise Managed Service Providers (MSPs). This enables them to direct remote monitoring and managing (RMM) tools to spread ransomware, leading to the infection and encryption of multiple MSP clients.

Recommendations

- Audit user accounts regularly, particularly RMM accounts that are publicly accessible. Patch operating systems, software, firmware, and endpoints.
- Ensure backups are secure and are disconnected from the network at the conclusion of each backup session.
- Monitor inbound and outbound network traffic; set alerts for data exfiltration.
- Apply two-factor authentication to user login credentials, receiving responses by text rather than email as actors may be in control of victim email accounts.
- Implement least privilege for file, directory, and network share permission.
- Educate employees about ransomware tactics, including preventative strategies such as how to identify phishing emails and how to respond to suspected compromises.

- Ensure backups are secure and are disconnected from the network at the conclusion of each backup session.
- Monitor inbound and outbound network traffic; set alerts for data exfiltration.
- Apply two-factor authentication to user login credentials, receiving responses by text rather than email as actors may be in control of victim email accounts.
- Implement least privilege for file, directory, and network share permission.
- Educate employees about ransomware tactics, including preventative strategies such as how to identify phishing emails and how to respond to suspected compromises.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE** Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.