Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

19 August 2019

PIN Number
20190819-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Sodinokibi Ransomware Actors Target Management Service Providers' Clients

Summary

In June 2019, the FBI received notification of ransomware variant Sodinokibi, also known as "REvil" and "Sodin," compromising managed service providers (MSPs) by leveraging victim-installed remote monitoring and managing (RMM) software. Actors behind the Sodinokibi ransomware infection likely leveraged compromised network credentials to gain access to the system. Upon gaining access, Sodinokibi actors use PowerShell scripts to drop an executable containing Sodinokibi into the MSP's network infrastructure, infecting its customers' systems.

Threat

FBI investigative activity identified several Sodinokibi ransomware actors compromising MSPs as a means to spread ransomware throughout the MSPs' client networks. This tactic resulted in multiple US companies suffering infection and encryption of file systems as the

result of only one cyber intrusion. Once executed, Sodinokibi encrypts the victim files and produces a .txt file displaying the ransom note. The .txt file provides instructions on how to download and configure a TOR browser. Through the TOR browser, the victim accesses a unique uniform resource locator (URL) containing a chatroom, monitored by the actors responsible for Sodinokibi, for payment and decryption instructions.

Sodinokibi actors likely leveraged CVE-2018-8453 to conduct privilege escalation. Upon identification of the vulnerability, Microsoft released a patch for this CVE in October 2018.

Recommendations

- Regularly back up data and verify its integrity.
- Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Backups are critical in ransomware; if you are infected, backups may be the best way to recover your critical data.
- Patch the operating system, software, and firmware on devices. All endpoints should be patched as vulnerabilities are discovered.
- Monitor remote connections and software, such as remote desktop protocol (RDP).
- Apply two-factor authentication to user login credentials and implement least privilege for file, directory, and network share permissions. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.

Reporting Notice

If your company is a victim and/or you have knowledge of a potential ransomware incident, report it to your security office, your local FBI Field Office (www.fbi.gov/contact-us/field), and the Internet Crime Complaint Center (IC3) (https://www.ic3.gov). It is important to include the following details in any reported ransomware complaint:

- Victim Information
  - Impact statement (e.g., impacted services/operations)
  - Overall losses associated with the ransomware

- Any messages pertaining to the attack
  - Save correspondence in its original format
  - If a payment associated with the attack was sent, provide transaction details, including Bitcoin wallet addresses and any decryption keys

Administrative Note

This product is marked **TLP: GREEN**. Recipients may share **TLP: GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP: GREEN** information may not be released outside of the community.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey