Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

31 October 2018

PIN Number

20181031-001

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@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.

Cyber Criminals Likely To Shift Toward Sophisticated Small-Scale, Targeted Campaigns and Cryptocurrency Mining

Summary

Ransomware and cryptocurrency mining malware are ongoing threats to private industry. The FBI assesses cyber criminals are shifting toward more sophisticated, small-scale ransomware campaigns in parallel with large-scale campaigns using cryptocurrency mining malware. The small-scale campaigns are targeting specific organizations in order to maximize the impact on the victim and extort higher ransoms. In the past, large-scale ransomware campaigns sought high revenues in smaller increments via infection of as many victims as possible through less sophisticated attacks. In recent large-scale campaigns, the FBI has observed an increase in cyber criminals using cryptocurrency mining malware over ransomware, because it produces comparable revenues while drawing less scrutiny from law enforcement.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat

Between late 2017 and early 2018, at least six private sector cybersecurity firms observed relative rises in cryptocurrency mining and declines in ransomware, according to private sector cybersecurity researchers as of 17 April 2018. This trend reflects a shift away from large-scale ransomware campaigns, toward more sophisticated, small-scale ransomware campaigns. While ransomware remains a serious threat, it is not as broadly distributed as it once was, and instead focuses on smaller numbers of higher impact victims, such as large organizations. Small-scale campaigns allow cyber criminals to dedicate more time and resources to individual attacks in order to maximize the impact of the infection.

Cyber criminals target larger organizations, including small to medium-size businesses, rather than individuals, because such organizations have more valuable data and are more likely to have the funds on hand necessary to pay larger ransoms. High impact infections on large organizations are far more likely to produce victims willing and able to pay large ransoms, creating the opportunity to produce revenues equal to or greater than small-scale campaigns with far fewer victims. The resulting decline in large-scale ransomware campaigns have led large-scale malware campaigns to seek alternative payloads, most frequently cryptocurrency miners.

For large-scale campaigns, cryptocurrency miners have multiple advantages over ransomware.

- Cryptocurrency miners are quiet, operating in the background with little indication to the victim there is a problem, allowing the miner to operate uninterrupted for days, weeks, or even months at a time before removal.

- The costs are equally subtle as they are most often represented by incremental decreases in computing power and increases in electricity use. Further, unlike ransomware, cryptocurrency mining produces guaranteed returns.
- Cryptocurrency mining does not require a victim to pay a ransom to produce a return, while cryptocurrency mining's highest cost is transferred to the victim in the form of energy usage and stress on the computing device.

As a result, large-scale cryptocurrency mining campaigns are capable of comparable financial returns to large-scale ransomware campaigns, all while drawing less law enforcement scrutiny as victims are far less likely to report cryptocurrency mining infections.

In the near and long term, the FBI assesses cyber criminal groups, particularly those operating within real or perceived safe havens, will likely conduct sophisticated, small-scale ransomware campaigns seeking large, one-time payouts in parallel with large-scale passive campaigns.

Recommendations

Most active ransomware campaigns rely on Remote Desktop Protocol (RDP) implementations or spear phishing for its initial infection vector. While many ransomware campaigns rely on a victim completing an action, such as opening an e-mail or visiting a compromised Web site, RDP allows cyber actors to infect victims with minimal detection.

Precautionary measures to mitigate ransomware threats include:

- Back up data regularly.
- Verify integrity of back up process.
- Use strong passwords to protect RDP credentials.
- If possible, use two factor authentication.

- Audit who accesses RDP.
- Establish whitelist access for RDP.
- Consider disabling RDP if not in use.
- Change RDP port from the default to another unused port.
- Block RDP via firewall.
- Audit logs for all remote connection protocols.
- Audit logs to ensure all new accounts were intentionally created.
- Maintain operating system updates and patches for all machines.
- Employ ransomware protection software built-in to modern operating systems (Windows Controlled Folder Access).
- Scan for open or listening ports, and mediate.

Best practices to protect against cryptocurrency mining infections:

- Network administrators should continuously monitor for:
    - Elevated CPU activity on computer networks and servers.
    - Decrease processing speed on workstations.
    - Security industry reporting of malware being distributed through add-ons or applications running on their networks.
- Educate employees to recognize CPU overprocessing.
- Monitor network activity associated with cryptocurrency miners.
- Monitor and investigate suspicious processes.
- Limit access to server rooms to prevent physical installation of mining software.
- Maintain operating system updates and patches for all machines.

- Update and patch Web browsers enabling cryptocurrency mining blocking features.
- Continue to educate employees to scrutinize e-mail attachments and Web site hyperlinks, and do not open attachments included in unsolicited e-mails.
- Continue to educate employees on browsing Web sites which may have malicious cryptocurrency mining malware in advertisements.
- Install and regularly update anti-virus or anti-malware software on hosts.
- Network administrators review security reporting pertaining to third-party or free software used by their organization. This reporting can often identify when this software has been incorporated in a malicious scheme.

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.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

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