Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

04 June 2019

PIN Number
20190604-001

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:WHITE**: The information in this product may be distributed without restriction, subject to copyright controls.

Cyber Actors Leveraging Malvertising with Hybrid Obfuscation Techniques to Deliver Malware

Summary

The FBI has observed cyber actors leveraging malicious advertising (malvertising) with hybrid techniques such as digital steganography[a] and fileless[b] malware to evade detection and improve computer intrusion capabilities. These techniques often take advantage of administrative tools such as PowerShell, which are already present on a victim's system. Over the past year, cyber actors have used these hybrid techniques to steal personally identifiable information, financial information, deploy ransomware, and gain unauthorized accesses to US networks.

[a] Steganography is a method used by cyber actors to hide malicious code in the pixels of an image file.
[b] Fileless malware does not install malicious files on computer hard drives like traditional computer viruses, and instead runs in memory by taking advantage of common operating system administration tools to appear as normal automated administrative processes.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat

The FBI has observed cyber actors using advanced techniques such as steganography and fileless malware in malvertising campaigns that target US victims. These cyber attacks typically conceal malicious code within online banner advertisements which inject into common browser and administrative tools such as JavaScript and PowerShell. As such, no user interaction beyond surfing to an infected website is necessary to automatically trigger the malicious chain. As a fileless delivery technique, these malicious code injections can skirt many of the defenses used in anti-virus and other intrusion detection systems.

Malvertisers often use the following tactics and techniques to gain placement of and operate their malicious advertisements:

- Using social engineering techniques to challenge the blocking of malicious advertisements.
- Pretending to be associates of fake advertisement agencies inquiring about the blocking of their advertisement.
- Using a third party to clear their code and overcome blocking mechanisms.
- Maintaining an open directory cloud account containing multiple images and hidden code for malvertising purposes.
- Sending phishing emails containing images with malicious script concealed by steganography to bypass antivirus software.

Recommendations

- Allow only applications with trusted signatures from trusted vendors to further mitigate the risk of successful malvertising.
- Establish a current whitelist to reduce the denial of service risk from malicious ad-blocking contributors.
- Monitor outbound traffic and system behavior to identify the successful use of steganography in cyber attacks.

- Secure and monitor administrative tools to improve detection rates for fileless malware.
- Regularly review security software and operating systems for updates to prevent malware installation.

Victim Reporting

The FBI encourages recipients to report suspicious activity to their local FBI field office, located at https://www.fbi.gov/contact-us/field-offices, or to file a complaint online at https://www.ic3.gov/complaint/splash.aspx.

Administrative Note

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

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