Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

06 August 2019

PIN Number

20190806-001

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.

Technical Details of the Osiris Banking Trojan and How to Protect Against Fileless Malware Attacks

Summary

Fileless malware is a growing threat to the banking industry requiring sophisticated techniques to protect systems against cyber-criminal activity. The Osiris Banking Trojan, which is an upgraded version of the Kronos Banking Trojan, uses two fileless techniques, making it more difficult to detect using standard antivirus software. Its added features and enhanced functionality allow cyber criminals to gain remote access to financial customer profiles and cause the malware to be more effective in stealing funds.

Fileless Malware Attacks on the Rise

Based on reporting from a private security firm, between January and June 2018, fileless malware intrusion detections have increased 94 percent. Fileless malware operates partly or entirely from the computer's memory without placing malicious executables on the underlying file system. Using phishing and spearphishing as an initial vector, it can bypass the file system by loading and executing malicious code directly in memory, storing malicious scripts in the registry, or using legitimate system administration tools such as PowerShell.

Standard antivirus software detects malware by scanning the file system for files sharing characteristics with known malware, files which are variants of known malware "families" or are related to known malware by a common code base, and suspicious system behavior or file structures. Given the characteristics of fileless malware, most antivirus programs are unable to detect it on victim machines.

The Osiris malware, sold as a Malware-as-a-service worldwide, combines two fileless techniques, Process Hollowing and Process Doppelgänging, which enable the malware to compromise legitimate software as it infects a targeted system. One of the techniques, Process Doppelgänging, which became public in December 2017, affects all versions of Microsoft Windows and bypasses most antivirus software. Process Hollowing occurs when a process is created in a suspended state, after which its memory is unmapped and replaced with malicious code. The execution of the malicious code is masked under a legitimate process and may evade defenses and detection analysis.

Technical Details of the Osiris Banking Trojan

Technical analysis on Osiris code shows the following: (Directory comparison between Osiris and Kronos)

```
Number of subdirectories: 87
Number of equal files: 309
Number of different files: 883
```

Osiris contains a new table called `cclogs`, `browser_passwd`, `cc_data`, `running_jobs`; Once a victim's machine is infected, Osiris runs a SOCKS/proxy server on the machine. Those credentials are reported back to the Osiris C&C to store that information. Osiris has the following features activated or deactivated;

```
define("RVNC_ENABLED", FALSE); //Reverse VNC
define("SOCKS_ENABLED", FALSE); //Socks
define("KLOG_ENABLED", TRUE); //Key Logger
define("EMAIL_SPREAD_ENABLED", FALSE); //Email Spread
define("RHVNC_ENABLED", FALSE); //Reverse Hidden VNC
define("TV_ENABLED", FALSE); //TeamViewer
define("HVNC2_ENABLED", FALSE); //HVNC2
```

Recommendations

The FBI recommends monitoring system behavior, securing administrative tools, and adopting advanced network event collection and visualization technologies to improve detection rates for fileless malware.

—Security solutions which do not rely solely on file system activity by also conducting behavior monitoring, memory scanning, and boot sector protection can help to protect networks from fileless attacks.

—Fileless attacks have used administrative tools already present in a victim network, including PowerShell, in various ways during cyber operations. Securing and monitoring the use of such tools could reduce cyber actors’ ability to exploit them in conjunction with fileless malware.

—Security Incident and Event Management (SIEM) technologies—which aggregate, store, visualize, and create automated reports and alerts based on customized queries—

can help identify and craft signatures for malicious system behavior in lieu of a file signature to identify evolving adversary tactics, including fileless malware.

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