FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

09 SEP 2019

Alert Number

MC-000106-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**.

Email:

cywatch@fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

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

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.

Increased Number of Emotet Command and Control IP Addresses Identified

Summary

In early June 2019, Emotet, an advanced modular banking Trojan, attempted to communicate with 214 command and control (C2) IP addresses for initial instructions, indicating cyber actors recently made modifications or updates to Emotet malware or infrastructure. Immediately following, the Emotet malware ceased communication with the previously known C2 IP addresses. The FBI is providing the following attached internet protocol (IP) addresses to assist receiving organizations' computer network defense. System administrators should immediately block these IP addresses to prevent Emotet from exploiting their systems.

Technical Details

The Emotet banking Trojan primarily functions as a downloader or "dropper" of other banking Trojans and is distributed via phishing campaigns. Initial infection occurs when a user opens or clicks the malicious download link, PDF, or macro-enabled document included in the malspam, originating from the Emotet spam module. Malspam is a method for delivering emails in bulk which contain infected documents or links that redirect users to websites which contain

exploit kits. Once downloaded, Emotet establishes persistence, attempts to propagate within the local network through incorporated spreader modules that leverage Server Message Block (SMB), and steals web browser credentials and Outlook contacts. Then, Emotet downloads a secondary payload, usually another banking Trojan or ransomware.

Beginning in early June 2019, the Emotet malware ceased communication with the known C2 IP addresses. While older versions of Emotet only contacted approximately 10 IP addresses, the most recent update attempted communication with 214 C2 IP addresses, indicating cyber actors made modifications or updates to Emotet malware or infrastructure. Following a successful compromise, Emotet will attempt to contact these specific 214 IP addresses. A full list of the IP addresses and port combinations is attached to this FLASH.

Additional information on Emotet can be found on the MS-ISAC US-CERT report: https://www.us-cert.gov/ncas/alerts/TA18-201A.

Recommended Mitigations

- System administrators can use these IP and port combinations in the attached list to detect and block Emotet activity should the malware resume communication with C2 IP addresses.
- Contact the FBI upon discovery of infection to report an intrusion and request assistance.
- Maintain and provide relevant logs to FBI to enable effective investigation and attribution.
- Follow additional guidance in TA18-201A.

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. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

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.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.