Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

4 June 2018

PIN Number
20180604-001

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 in order 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.

Identified Qakbot Malware Variant Found on Thumb Drive Manufactured in China

Summary

In March 2018, an identified financial services corporation received a thumb drive infected with the bank credential-stealing Qakbot malware variant, targeting information from networked computers and financial institution web sites. The financial services corporation purchased bulk thumb drives from a US online retailer of computer hardware. The thumb drives were originally manufactured in China. According to FBI forensic analysis, the Qakbot malware was on the infected thumb drive before the drive arrived in the United States. Qakbot is extremely persistent and requires removal of all malware from every device. Failure to remove even one node of malware may result in re-infecting previously sanitized systems possibly costing the victim hundreds of thousands of dollars in malware removal and system downtime.

Threat

Qakbot is an information stealing worm—originally discovered in 2007 with a major update in 2017—that propagates through removable drives, network

shares, and Web pages. The most common vector of intrusion for Qakbot is malicious attachments to phishing emails. Once executed, Qakbot spreads to other shared folders and uses Server Message Block (SMB) protocol to infect other machines. Qakbot has keylogging capabilities, and is able to propagate across network environments through a single instance within that network. It is capable of remaining on a device through the use of registry keys and by scheduling recurring tasks to run at timed intervals. Every device connected to the network and every piece of removable media which has been attached needs to be scanned for the malware and cleaned of the infection before it can be reconnected. The most recent updates in 2017 allows Qakbot to lock users out of the active directory, preventing them from being able to work. It also deploys malicious executables into network shares, registering them as services.

Cyber actors have the capability to infect devices with malware at nearly any point in the manufacturing process. The FBI has historically seen cases of infection with malware capable of stealing credentials, gathering data on the users of a computer or network, dropping other types of malware, and serving as a "backdoor" into a secure network. It is difficult to know at which point the malware infection occurred or whether the infection was intentional, due to the international nature of hardware manufacturing.

Recommendations

To mitigate the threat of a potentially infected thumb drive, the following measures should be taken at a minimum:

- Ensure the use of approved, trusted vendors for hardware purchases.
- Scan all hardware, especially removable storage media, on an external system prior to its insertion into a network environment.
- For signature-based intrusion detection systems, ensure that the hash value for known Qakbot variants are included. The MD5 value for the variant identified in this PIN was: ff0e3ec80faafd04c9a8b375be77c6b6. This hash value can change, so be prepared to use other advanced detection systems.
- Users should protect themselves and organizations by practicing good browsing habits, ensuring they do not respond to or click on unsolicited email, and to not plug unknown USB devices into their workstations.
- If you don't have the expertise to properly handle or identify potential cyber threats please seek out an expert who can provide the expertise needed to secure your organization.

Federal Bureau of Investigation, Cyber Division

Private Industry Notification

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