Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

09 May 2016

PIN Number
160509-001

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@ic.fbi.gov

Phone:
1-855-292-3937

Android Malware SlemBunk and Marcher Actively Target US Financial Institutions' Customers

Summary

The FBI has identified two Android malware families, SlemBunk and Marcher, actively phishing for specified US financial institutions' customer credentials. The malware monitors the infected phone for the launch of a targeted mobile banking application to inject a phishing overlay over the legitimate application's user interface. The malware then displays an indistinguishable fake login interface to steal the victim's banking credentials. According to cyber threat industry reports, both malware families have targeted foreign financial institutions since 2014, gradually broadening the list to include Western banks, and offered the malware for lease or purchase, respectively, in underground forums. At least as of December 2015, the malware expanded its configuration to include the Android package names of US financial institutions.

Scope of Threat

Both malware families are capable of defeating two-factor authentication through their ability to monitor and intercept SMS messages, facilitating the attackers' ability to perform account takeovers using only the infected mobile device. However, the financial losses attributed to these malware families are difficult to assess because the indistinguishable format of the phishing overlay from the legitimate mobile banking application thwarts the victim's ability to detect the mobile device as the initial point of compromise. Additionally, the malware sends the stolen login credentials to a

The information in this notification was obtained through an FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in 42 USC § 10607

command and control server, further complicating identification of the intrusion vector.

Of note, the December 2015 leak of the GM bot source code, an early variant from the SlemBunk family, may embolden malicious cyber actors to create their own Android banking malware using parts of the exposed source code and control panel. Further, depending on how much of the GM bot source code is in later malware variants of the SlemBunk family, the author may be prompted to alter SlemBunk's existing source code or develop an entirely new Android banking malware family to secure differentiation of the malware and continued profitability from fraud activity. SlemBunk's developer has proven adept at releasing numerous mobile malware variants and, as of late 2015, also broadened SlemBunk's target list to include Android applications for common US social media and instant messaging platforms, applying the same overlay technique to prompt the user for login credentials and/or credit card information. The FBI assesses mobile malware targeting Android devices will continue to attract financially-motivated cyber criminal actors with the means and opportunity to manipulate the leaked source code or exploit the increasing attack surface in Android's mobile market.

Infection Vectors

Review of cyber threat industry reports on the two malware families reveals the following initial vectors of compromise, because the malware distribution method is not included in its lease or purchase:

- SMS or MMS phishing, to include messages requesting the user to install malicious Adobe Flash Player software;
- Malvertisements or pop-ups from adult Web sites prompting the user to download a malicious Adobe Flash update;
- Mobile applications downloaded from third-party mobile application platforms; and
- Phishing e-mails.

Recommendations for Private Sector Institutions

- Use static code analysis tools to review the hardcoded and configuration list of malware sample(s) to identify targeted mobile applications.
- Conduct device fingerprinting and login analysis to detect unauthorized access to accounts, and be willing to set alerts for unknown devices and IP addresses accessing the accounts.

The information in this notification was obtained through an FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in 42 USC § 10607

- Differentiate traffic from mobile and non-mobile devices to attribute intrusions and related losses.
- Educate consumers on appropriate preventive and reactive actions to known criminal schemes and social engineering threats, including how employees should respond in their respective position and environment.
- Educate consumers on when personally identifiable information, authentication credentials, or payment card industry information would be requested.
- Use security application program interfaces during application development to determine risk for fraud activity.
- Work with respective brand enforcement units to remove malicious applications from official and third-party application platforms.

Recommendations for Consumers

- Install mobile applications from trusted sources, and review the application vendor prior to download.
- Do not download software or applications from third-party application platforms or untrusted Web sites.
- Review application permissions during installation; ensure permissions requested are appropriate for the type of application being downloaded.
- Install and regularly update the Android operating system.
- Do not use jailbroken Android devices, as such devices will not receive automatic updates.
- Install and regularly update anti-virus or anti-malware software on Android devices.
- Do not open or click on hyperlinks in SMS, MMS, or e-mail messages from unknown or suspicious sources.
- Do not open attachments included in unsolicited e-mails.
- Consider downloading an ad blocker to enable the device's browser to block advertisements and pop-ups.
- Use only secured wireless connections to access the Internet, taking extreme caution when accessing public Wi-Fi connections.

The information in this notification was obtained through an FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in 42 USC § 10607

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@ic.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.

Administrative Note

This product is marked TLP: AMBER. Information contained in this product is for official use only and should not be further disseminated. Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information. No portion of it should be released to the media, the general public, or over non-secure Internet servers.

There is no additional information available on this topic at this time. 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

The information in this notification was obtained through an FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in 42 USC § 10607