Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

23 April 2020

PIN Number
20200423-001

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 actors. This PIN was coordinated with DHS-CISA and US Treasury.

This PIN has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations with their sector or community, but should not be shared via publicly accessible channels.

Cyber Criminals Initiate Fraudulent SWIFT Messages via Third-Party Vendors Serving Small Businesses

Summary

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is the network used by financial institutions to transfer information securely and is a primary method for the transfer of financial messages. The FBI has observed at least two attempts by cyber criminals to initiate fraudulent SWIFT messages through third-party vendors who provide SWIFT messaging service to small businesses. The cyber criminals employ social engineering techniques against the targeted third-party vendors in order to initiate fraudulent money transfers. There was no evidence of a cyber intrusion into the SWIFT network.

Threat Overview

The SWIFT network allows banks and other financial institutions to quickly, accurately, and securely send and receive information, such as money transfer instructions. According to SWIFT, every day nearly 11,500 member institutions send approximately 36.7 million transactions through the network.

Between February and April 2020, the FBI observed at least two attempts by cyber criminals to initiate fraudulent SWIFT messages through third-party vendors who provide SWIFT messaging service to small businesses. The cyber criminals employed social engineering techniques against the targeted third-party vendors in order to initiate fraudulent money transfers and Standby Lines of Credit, a sum of money borrowed in part or in full from a credit granting institution.

Cyber criminals contacted the third-party SWIFT vendors to set up new accounts through web inquires or email. In some instances, the cyber criminals impersonated a person with which the provider already had an existing business relationship, while in others there was no prior business relationship. While communicating with the third-party SWIFT vendors, the actors also mimicked email domains to the businesses they purported to represent, but with minute differences. For example, the actors added the word "finance" at the end of the business's name (*acmebank.com vs. acmebankfinance.com*) or placed a "." between words (*acmebank.com vs. acme.bank.com*).

Cyber criminals are known to use Voice-over-Internet Protocol (VOIP) services, such as Bandwidth.com or TalkU (talktone.me), to call targeted third-party SWIFT vendors. Using VOIP and mimicked email domains of actual small businesses, the cyber criminals impersonate chief executive officers or other persons of authority of the small business in order to gain access to the SWIFT messaging service provided by the target third-party vendors. The same cyber criminals may call the employees of the SWIFT messaging service provider to ensure that their messages are delivered to their intended recipients. These calls typically take place in the morning to early afternoon Eastern Standard Time.

If successful in setting up an account with the SWIFT service provider, the cyber criminals may send out multiple messages through the newly established SWIFT accounts using various Message Types (MTs), including but not limited to:

- MT -103
- MT -795

- MT -199
- MT -760
- MT -767
- MT -796
- MT -799
- MT -999

In the majority of the messages observed, the cyber criminals used free format messaging ending in x99. These MTs are sent to accounts located around the world, and many MTs are sent to accounts the FBI has confirmed to be real accounts.

Recommendations for End Users

- Be aware of social engineering techniques employed by cyber criminals—including strategies to identify phishing emails, impersonated calls, and fraudulent businesses and domains—and how to respond to a suspected compromise.
- Verify all account and transaction information via a known telephone number or over secure video conference.
- Ensure proper Know Your Customer (KYC) procedures are in place for new or inactive customers requesting access to the SWIFT platform. When reviewing customer information:
  - Verify the documents provided through KYC to ensure their accuracy. For example, if the customer provided a business license, confirm the validity of the license with the state that issued it.
  - Independently verify that the business requesting the transaction authorized it by confirming through an alternative source. For example, rather than using the email or phone number provided, use the phone number or email address listed on the organization’s website.
  - Check the customer’s email domain name against the entity’s web domain name to ensure they’re the same.
- Avoid allowing customers to initiate transactions via VOIP calls without additional vetting and verification.

Recommendations for Users of SWIFT Platform

- Alert your workforce to this scheme.
- Provide regular training and develop internal guidance concerning social engineering techniques and Business Email Compromise.
- Verify any suspicious money transfers from unfamiliar SWIFT accounts.

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 email 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: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