Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

12 May 2021

PIN Number
20210512-001

Please contact the FBI with any questions related to this Private Industry Notification at your local **FBI Field Office**.

Local Field Offices:
www.fbi.gov/contact-us/field-offices

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 has been coordinated with DHS-CISA.

This PIN has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Spear-Phishing Attack Directing Recipients to Download a Fake Windows Application Impersonating a Financial Institution

Summary

In a recent spear-phishing campaign, cyber actors impersonated a US-based financial institution's brand in an attempt to get recipients to download a Windows application unaffiliated with the financial institution. The unknown cyber actors tailored the campaign to spoof the financial institution through registered domains, email subjects, and an application, all appearing to be related to the institution.

Threat Overview

In February 2021, a US-based financial institution was notified of a spear-phishing attempt which impersonated the financial institution's brand to target a renewable energy company. The phishing e-mail's theme involved funding for a loan and instructed the recipient to download a Windows application to complete the loan process to receive more than $62 million. The fraudulent loan amount was in line with the victim's business model. The phishing e-mail appeared to

originate from a United Kingdom–based financial institution, stating the US financial institution's loan to the victim was confirmed and could be accessed through an application which appeared to represent the US financial institution. The phishing e-mail included two `.pdf` files, one of which spoofed the name and likeness of the UK's National Crime Agency and another which appeared to contain SWIFT information. The phishing e-mail also contained a link to download the application and a username and password for access.

As part of this spear-phishing campaign, the cyber actors also registered a fraudulent domain impersonating the US financial institution. This domain hosted the executable purporting to be the Windows application which the recipient received the link for in the original spoofed email.

The below indicators were observed in conjunction with this spear-phishing campaign. These suspicious activities/indicators should be observed in context and not individually.

The following files were attached to the spear-phishing e-mail:

Filename: Computer Feeder Message(Name Redacted).pdf
MD5: 57865182db4f963cf9ea7709384dd750
SHA256: bd45ae2cbc302bd219d4c59469d1ebb1f8049f3bd025bd19eb4572176b5176f5

Filename: Swift Copy(Name Redacted).pdf
MD5: fadcde66f6edf79442dce2be4f11ef60
SHA256: 375a0566bdfc04f8d24fae429a415434c679d3b5e7a7c97b8ddd5cea98e0aa0c

The following file was downloaded if the recipient clicked on the malicious link in the spear-phishing e-mail:

Filename: (Name Redacted).exe
MD5: 3d1111389aac89274f0eaf87c30732fe
SHA256: e09ae3c1ff5489f300ec9ecfc76ffdab90b6dab07eff1a0edf38285ab1e2b801

The malicious .exe file downloaded from the link embedded in the spear-phishing e-mail calls out to the domain **`secureportal(.)online`**.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Recommendations

- Ensure anti-virus and anti-malware software are enabled and signature definitions are updated regularly in a timely manner. Well-maintained anti-virus software may prevent use of commonly deployed attacker tools delivered via spear-phishing.
- Deploy application control software to limit which applications and executable code can be run by users. Email attachments and files downloaded via links in emails often contain executable code. Application control software limits users to only execute applications and code allowed by the organization, rendering malicious executables delivered via spear-phishing unable to execute.
- Limit the use of administrator privileges. Users who browse the internet, use email, and execute code with administrator privileges make spear-phishing much more effective by enabling attackers to move laterally across a network, gain additional accesses, and access highly sensitive information.
- Be suspicious of unsolicited contact via email or social media from any individual you do not know personally.
- Be suspicious of unsolicited or unexpected email or social media messages enticing recipients to open an attached or hosted file.
- Closely verify the spelling of web addresses, websites, and email addresses that look trustworthy but may be imitations of legitimate websites.
- Ensure operating systems and applications are updated to the most current versions.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

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