Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

17 September 2019

PIN Number

20190917-001

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 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.

Cyber Criminals Use Social Engineering and Technical Attacks to Circumvent Multi-Factor Authentication

Summary

The FBI has observed cyber actors circumventing multi-factor authentication through common social engineering and technical attacks. This PIN explains these methods and offers mitigation strategies for organizations and entities using multi-factor authentication in their security efforts. Multi-factor authentication continues to be a strong and effective security measure to protect online accounts, as long as users take precautions to ensure they do not fall victim to these attacks.

Multi-factor authentication is the use of a variety of methods to confirm a user's identity instead of only using a username and password. Often this type of authentication uses a secondary token which changes over time to provide a one-time passcode, but many companies now employ biometrics or behavioral information—such as time of day, geolocation, or IP address—as a form of authentication.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat Overview

FBI reporting identified several methods cyber actors use to circumvent popular multi-factor authentication techniques in order to obtain the one-time passcode and access protected accounts. The primary methods are social engineering attacks which attack the users and technical attacks which target web code.

- In 2019 a US banking institution was targeted by a cyber attacker who was able to take advantage of a flaw in the bank's website to circumvent the two-factor authentication implemented to protect accounts. The cyber attacker logged in with stolen victim credentials and, when reaching the secondary page where the customer would normally need to enter a PIN and answer a security question, the attacker entered a manipulated string into the Web URL setting the computer as one recognized on the account. This allowed him to bypass the PIN and security question pages and initiate wire transfers from the victims' accounts.

- In 2016 customers of a US banking institution were targeted by a cyber attacker who ported their phone numbers to a phone he owned—an attack called SIM swapping. The attacker called the phone companies' customer service representatives, finding some who were more willing to provide him information to complete the SIM swap. Once the attacker had control over the customers' phone numbers, he called the bank to request a wire transfer from the victims' accounts to another account he owned. The bank, recognizing the phone number as belonging to the customer, did not ask for full security questions but requested a one-time code sent to the phone number from which he was calling. He also requested to change PINs and passwords and was able to attach victims' credit card numbers to a mobile payment application.

- Over the course of 2018 and 2019, the FBI's Internet Crime Complaint Center and FBI victim complaints observed the above attack—SIM swapping—as a common tactic from cyber criminals seeking to circumvent two-factor authentication. Victims of these attacks have had their phone numbers stolen, their bank accounts drained, and their passwords and PINs changed. Many of these attacks rely on socially engineering customer service representatives for major phone companies, who give information to the attackers.

- In February 2019 a cyber security expert at the RSA Conference in San Francisco, demonstrated a large variety of schemes and attacks cyber actors could use to circumvent multi-factor authentication. The security expert presented real-time examples of how cyber actors could use man-in-the-middle attacks and session hijacking to intercept the traffic between a user and a website to conduct these attacks and maintain access for as long as possible. He also demonstrated social engineering attacks, including phishing schemes or fraudulent text messages purporting to be a bank or other service to cause a user to log into a fake website and give up their private information.

- At the June 2019 Hack-in-the-Box conference in Amsterdam, cyber security experts demonstrated a pair of tools—Muraena and NecroBrowser—which worked in tandem to automate a phishing scheme against users of multi-factor authentication. The Muraena tool intercepts traffic between a user and a target website where they are requested to enter login credentials and a token code as usual. Once authenticated, NecroBrowser stores the data for the victims of this attack and hijacks the session cookie, allowing cyber actors to log into these private accounts, take them over, and change user passwords and recovery e-mail addresses while maintaining access as long as possible.

Mitigation Strategies

Defending against multi-factor authentication attacks requires awareness of the attacks which circumvent the security and constant vigilance for social engineering attacks.

- Educate users and administrators to identify social engineering trickery—how to recognize fake websites, not click on rogue links in e-mail, or block those links entirely—and teach them how to handle common social engineering tactics.

- Consider using additional or more complex forms of multi-factor authentication for users and administrators such as biometrics or behavioral authentication methods, though this may add inconvenience to these users.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

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.

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