Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

07 March 2019

PIN Number

20190307-001

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 Steal Funds from Retirement and Spending Accounts through Unauthorized Online Access

Summary

Since September 2017, the FBI has received numerous reports of cyber criminals creating new online accounts—or accessing existing online accounts—to gain access to a variety of victim retirement and health spending accounts. Examples of targeted accounts include 401(k), pension, health savings, and flexible spending accounts. Many of the victim reports indicated the criminals used stolen personally identifiable information (PII) to either create new accounts or access existing ones, while other attacks targeted multiple employee accounts which were managed by the employer or a third-party plan administrator.

In the attacks which targeted employers or plan administrators, cyber criminals gained unauthorized access to several individual accounts by compromising the company's system and attaining privileged access. For example, some of the recent reports received by the FBI indicated the employees of a company responded to phishing e-mails or the malicious actors exploited a security weakness in the company's or plan administrator's website.

Threat

The FBI has investigated multiple cases nationwide related to data breaches of retirement and spending accounts since September 2017. More recently, from July through November 2018, the FBI observed an increase in the number of confirmed victim reports for these types of accounts.

For existing online accounts, cyber criminals were able to access individual accounts by exploiting PII, to include name, date of birth, and social security number, derived from unknown sources. The criminals then changed the participants' e-mail addresses, phone numbers, home addresses, security questions and answers, and bank accounts to falsify information under their control. Cyber criminals also created new online accounts for individuals without previously established online accounts. After gaining control of the accounts, the criminals attempt to have funds directly deposited into bank accounts in their control by:

- initiating loans from accounts
- transferring/withdrawing funds
- initiating distribution of retirement accounts
- re-directing ongoing deposits into retirement or health spending accounts
- diverting existing 401(k) or pension payments
- submitting fraudulent claims for health spending account payments/ reimbursements

The FBI assesses cyber criminals will continue to target participant accounts as well as the systems managed by plan administrators with the intent to steal funds, and will remain an ongoing threat to private industry.

Recommendations

The FBI recommends taking precautionary measures to mitigate the threat and protect against exploitation. Employers and plan administrators responsible for managing participant accounts should:

- Alert their workforce personnel to this scheme and actively monitor accounts for unauthorized access, modification, and anomalous activities.
- Continue to educate employees on scrutinizing links contained in e-mails, and not opening attachments included in unsolicited e-mails.
- Ensure employees are aware of social engineering and phishing attacks (i.e., via phone or e-mail) by cyber criminals attempting to obtain user credentials.
- Instruct employees to refrain from providing log-in credentials or PII in response to any e-mail or phone call.
- Direct employees to report any suspicious requests for personal information to the Information Technology or Information Security Department.
- Establish company policies to contact the owner of the account to verify any changes to existing account information. Apply heightened scrutiny to bank information initiated by account holders seeking to update or change direct deposit credentials.
- Establish multi-factor authentication for creating new online accounts and for making account changes, such as password or bank account information.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

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@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: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