Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

03 August 2018

PIN Number

180803-001

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.

Cybercriminals Utilize Social Engineering Techniques to Obtain Employee Credentials to Conduct Payroll Diversion

This notification was created jointly by the FBI and the National Cyber Forensics & Training Alliance (NCFTA).

Summary

The FBI has observed an increase in cybercriminal actors using widespread tactics to gain access to companies' employee payroll data. In 2017, the FBI and IC3 identified approximately 17 cases. As of July 2018, the FBI and IC3 have identified approximately 47 payroll diversion cases, with losses totaling approximately $1million. Various institutions most affected by the outcomes of this cyber focused scheme include but are not limited to: universities, local school districts, healthcare, and commercial airway transportation. The FBI has observed two main social engineering methods in which the cybercriminal actors gain access to and alter employees' information, either via online phishing email or through telephone solicitation.

Methodologies

Cyber criminals use Payroll Diversion to obtain credentials from victim companies, utilizing the login credentials of employees to access payroll

portals and reroute direct deposits to fraudulent accounts owned by the actors. Cybercriminal actors divert payroll funds to prepaid bank cards which are controlled by the actors. Often the fraudulent payroll deposits arrive from multiple victims' accounts into the cybercriminal controlled accounts.

For the first observed social engineering method, victim credentials are targeted with a customized email that contains either a link to a phishing website or a .pdf file that redirects the user to the phishing site. In most cases, this phishing site is made to look like the legitimate HR software service the victim company provides. The victim is prompted to enter their login credentials which are captured by the actor. The actor logs into the employee's account and changes the bank account information to an account controlled by the actor. When the next deposit is made, the funds are routed to the actor as opposed to the employee's account.

The second observed social engineering method involves the cybercriminal actor calling the employees' resource hotline and providing the employee ID number and last four numbers of the Social Security number to reset the victim's password.

NCFTA intelligence analysts reviewed transactional data related to this activity and determined there were a total of approximately 205 fraudulent payroll deposits made to the pre-paid cards. In addition, the average time frame between when a card is activated and used to receive the fraudulent direct deposits is 54 days, with the minimum being one day. The cybercriminal actors tend to use the bank cards to receive cash withdrawals from ATM machines, or make purchases at gas stations, grocery stores, retail stores, fast food restaurants, and wireless phone carrier providers.

Recommendations

To mitigate the threat of payroll diversion:

- Alert your workforce to this scheme.
- Apply heightened scrutiny to bank information initiated by the employees seeking to update or change direct deposit credentials.
- Educate personnel on appropriate preventative and reactive actions to known criminal schemes and social engineering threats.
- Instruct employees to refrain from supplying log-in credentials or personally identifying information in response to any email.
- Direct employees to forward any suspicious requests for personal information to the information technology or human resources department.

- Ensure that log-in credentials used for payroll purposes differ from those used for other purposes, such as employee surveys.
- Monitor employee logins that occur outside of normal business hours.
- Restrict access to the Internet on systems handling sensitive information.
- Implement two-factor authentication for access to sensitive systems and information.
- Only allow required processes to run on systems handling sensitive information.

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 ww.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.

Administrative Note

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