Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

23 April 2019

PIN Number
20190423-001

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:WHITE: The information in this product may be distributed without restriction, subject to copyright controls.

Cyber Insider Threat Actors Disrupt Networks and Steal Data, Inflicting Significant Losses to US Businesses

Summary

The FBI continues to observe U.S. businesses' reporting significant losses caused by cyber insider threat actors.[a] These cases often involve former or disgruntled employees exploiting their enhanced privileges—such as unfettered access to company networks and software, remote login credentials, and administrative permissions—to harm companies. Cyber insider threat actors most often are motivated by revenge, but they also conduct attacks to profit financially from stolen information, gain a competitive edge at a new company, engage in extortion, or commit fraud through unauthorized sales and purchases.

[a] (U) Cyber insider threat actors include former and current employees or contractors who use their unique accesses and knowledge of company networks or policies to disrupt network operations or steal proprietary or sensitive information for financial gain. Cyber insider threat actors are often investigated and/or charged for violations of the Computer Fraud and Abuse Act.

The FBI identified the following trends after reviewing cyber insider threat cases over the past three years:

- In most cases, actors held an Information Technology role (system administrators, technical support, network engineers, IT contractors, etc.).
- The actors' length of employment varied, but most had worked for the victim company for between one and 10 years.
- The damage actors caused most often led to network and operation disruption, data deletion, theft of proprietary information, or the compromise of personally identifiable information of customers and employees.
- The average reported loss due to a cyber insider threat incident was $3.5 million.
- Actors typically had a history of discipline for poor conduct or misusing company assets.

Cyber insider threat actors' methods often involved:

- Using existing or shared administrative credentials and knowledge of company networks and culture to steal data and disrupt operations. Some also used their inside knowledge to conceal their activities, with varying success.
- Establishing fake administrative accounts before leaving victim companies.
- Using their unique knowledge to maintain persistent access to networks and leveraging open source coding sites to troubleshoot access issues.
- Social engineering other employees, such as the Help Desk or other third-party contractors, to share or reset passwords.
- Creating backdoors into company networks and using remote access software or tools to log into company networks.
- Installing malware and keyloggers on company computers and devices.
- Stealing employee and customer data or exploiting their privileged access to profit from unauthorized sales.
- Contacting and bribing former coworkers to provide client lists, company data, or network access.
- Using their privileges as IT employees to activate accounts of other former employees, elevating the privileges of those accounts prior to their departure, and using those credentials to engage in criminal activities.
- Taking active steps to conceal their crimes, such as disabling relevant network or application logging functions.

Protection and Defense

- Ensure employee access to all company network systems and databases is revoked when employees leave the company. Coordinate employee terminations with the Human Resources and IT departments (including the Help Desk).
- Maintain an audit of administrative accounts before and after a major hiring or contracting event, and following the departure of key IT personnel.
- Monitor unusual employee network activity, especially in the weeks leading up to an employee's leaving the company.
- Monitor suspicious physical security habits of employees, especially the abnormal use of personal devices such as concealing devices in the workspace or using personal devices to photograph sensitive information.
- Change passwords to shared administrator network or remote login credentials regularly. Ensure passwords are changed when an employee with administrative access leaves the company.
- Maintain a robust and tiered backup strategy for computer networks and servers.
- Monitor data uploads to all media, email, or cloud storage outside of the company network.
- Regularly monitor online postings for proprietary products.
- Establish alerts for unusual activities on administrative accounts, and after all network-level access changes.
- Regularly review remote login sessions and unusual activity conducted outside of normal working hours.
- Establish and raise awareness of a reporting mechanism for violations of ethics, brand, or intellectual property rights.

Additional Resources

For additional information on the methodologies and impact of cyber insider threats, please refer to "Increase in Insider Threat Cases Highlight Significant Risks to Business Networks and Proprietary Information," available at https://www.ic3.gov/media/2014/140923.aspx.

Victim Reporting

The FBI encourages recipients to report suspicious activity to their local FBI field office, which can be located at https://www.fbi.gov/contact-us/field-offices, or to file a complaint online at https://www.ic3.gov/complaint/splash.aspx.

Administrative Note

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

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