Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

14 JANUARY 2021

PIN Number

20210114-001

Please contact the FBI with any questions related to this Private Industry Notification at your local **Cyber Task Force**.

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 product has been coordinated with DHS – CISA.

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

Cyber Criminals Exploit Network Access and Privilege Escalation

Summary

Cyber criminals are focusing their operations to target employees of companies worldwide who maintain network access and an ability to escalate network privilege. During COVID-19 shelter-in-place and social distancing orders, many companies had to quickly adapt to changing environments and technology. With these restrictions, network access and privilege escalation may not be fully monitored. As more tools to automate services are implemented on companies' networks, the ability to keep track of who has access to different points on the network, and what type of access they have, will become more difficult to regulate.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat

Cyber criminals have changed techniques and tactics when compromising employee accounts or credentials. Cyber criminals are trying to obtain all employees' credentials, not just individuals who would likely have more access based on their corporate position. According to FBI case information, as of December 2019, cyber criminals collaborated to target both US-based and international-based employees' at large companies using social engineering techniques. The cyber criminals vished these employees through the use of VoIP platforms. Vishing attacks are voice phishing, which occurs during a phone call to users of VoIP platforms. During the phone calls, employees were tricked into logging into a phishing webpage in order to capture the employee's username and password. After gaining access to the network, many cyber criminals found they had greater network access, including the ability to escalate privileges of the compromised employees' accounts, thus allowing them to gain further access into the network often causing significant financial damage.

In one instance, the cyber criminals found an employee via the company's chatroom, and convinced the individual to log into the fake VPN page operated by the cyber criminals. The actors used these credentials to log into the company's VPN and performed reconnaissance to locate someone with higher privileges. The cyber criminals were looking for employees who could perform username and e-mail changes and found an employee through a cloud-based payroll service. The cyber criminals used a chatroom messaging service to contact and phish this employee's login credentials.

Recommended Mitigations

- Implement multi-factor authentication (MFA) for accessing employees' accounts in order to minimize the chances of an initial compromise.
- When new employees are hired, network access should be granted on a least privilege scale. Periodic review of this network access for all employees can significantly reduce the risk of compromise of vulnerable and/or weak spots within the network.
- Actively scanning and monitoring for unauthorized access or modifications can help detect a possible compromise in order to prevent or minimize the loss of data.

- Network segmentation should be implemented to break up one large network into multiple smaller networks which allows administrators to control the flow of network traffic.
- Administrators should be issued two accounts: one account with admin privileges to make system changes and the other account used for email, deploying updates, and generating reports.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. 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: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 your local FBI field office.

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