Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 May 2020

PIN Number
20200521-003

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 actors. This PIN was coordinated with DHS-CISA.

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

Cyber Criminals Take Advantage of COVID-19 Pandemic to Target Teleworking Employees through Fake Termination Phishing Emails and Meeting Invites

Summary

In response to the recent increase in teleworking during the COVID-19 pandemic, cyber criminals are targeting teleworking employees with fraudulent termination phishing emails and VTC meeting invites, citing COVID-19 as the reason. Employees who are alarmed by the message may not scrutinize the spoofed email address that looks similar to their company's legitimate one. The emails entice victims to click on malicious links purporting to provide more information or online conferences pertaining to the victim's termination or severance packages. Companies should alert their employees to look for emails coming from Human Resources or management with spoofed email domains.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat Overview

The COVID-19 pandemic has led to an increase in teleworking, with businesses communicating and sharing information over the Internet. Scammers have seized on the increased telework environment and uncertainty surrounding the pandemic to target employees of companies with fake termination phishing emails and VTC meeting invites. As of early April 2020, the FBI learned some employees from a data security company received fraudulent emails that suggested the company was terminating the email's recipient. Messages included vague, attention-grabbing subject lines such as, "Termination Review Meeting." The emails cite the current COVID-19 pandemic as the reason for downsizing, give instructions describing how to process out from the company, and directs the employee to click a potentially malicious "hotlink" to receive termination benefits. The emails contained a spoofed domain address, and employees that clicked on the link received a black screen.

In another instance, FBI investigation determined attackers sent meeting notifications asking recipients to join a VTC meeting regarding their purported terminations. The emails contained links to a fake VTC service login page; and used hyperlinked text such as "Join this Live Meeting" to appear as a legitimate automated meeting notification. Recipients who fall victim to this attack have login credentials as well as any other information stored on the VTC platform compromised.

Indicators:

- Calls from employees who mistakenly believe themselves to be terminated.
- Employees reporting malware or ransomware infections.
- Employees reporting suspicious activity on legitimate accounts such as video conferencing accounts.
- Emergence of fake VTC applications installed on users' smartphones, tablets, or computers.

Recommendations:

- Alert employees to look for emails coming from Human Resources or management with spoofed email domains

- Select trusted and reputable telework software vendors; conduct additional due diligence when selecting foreign-sourced vendors.
- Require use of password or PIN for any teleconference or web meetings.
- Beware of social engineering tactics aimed at revealing sensitive information. Use tools that block suspected phishing emails or that allow users to report and quarantine them.
- Beware advertisements or emails purporting to be from telework software vendors.
- Always verify the web address of legitimate websites or manually type them into the browser.
- Do not share links to remote meetings, conference calls, or virtual classrooms on open websites or open social media profiles.
- Avoid opening attachments or click links within emails from senders you don't recognize.
- Only enable remote desktop access functions like Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC) when absolutely necessary.

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 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. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

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