



Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

25 November 2020

PIN Number
20201125-001

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 actors. This product 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 Exploit Email Rule Vulnerability to Increase the Likelihood of Successful Business Email Compromise

Summary

The COVID-19 pandemic prompted a mass shift to telework among many US businesses, resulting in increased use of web-based email applications. According to recent FBI reporting, cyber criminals are implementing auto-forwarding rules on victims' web-based email clients to conceal their activities. The web-based client's forwarding rules often do not sync with the desktop client, limiting the rules' visibility to cyber security administrators. Cyber criminals then capitalize on this reduced visibility to increase the likelihood of a successful business email compromise (BEC). BEC schemes resulted in more than \$1.7 billion in worldwide losses^a reported to the Internet Crime Complaint Center (IC3) in 2019. The FBI is sharing this information to inform companies of this email rule forwarding vulnerability, which may leave businesses more susceptible to BEC.

^a Includes funds later recovered.

TLP: WHITE



Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat Overview

BEC is a sophisticated scam targeting businesses that perform electronic payments such as wire or automated clearing house transfers. A cyber criminal initially compromises a business email account through social engineering or computer intrusion techniques. Following the initial intrusion, the cyber criminal uses the system access to conduct reconnaissance on the victim's email communications. Using information gathered from the compromised accounts and reconnaissance efforts created by system access following the initial intrusion, the cyber criminal then impersonates an employee over email communications to redirect pending or future payments to fraudulent bank accounts. BEC actors create auto-forwarding rules within email accounts after they obtain employee credentials to decrease the victims' ability to observe fraudulent communications.

After obtaining access to a victim's email account, cyber criminals update the auto-forwarding email rules in the web-based client. If administrators do not actively sync their web and desktop email clients, the auto-forwarding rules may only appear in the web client, limiting the rules' visibility to security administrators. While IT personnel traditionally implement auto-alerts through security monitoring appliances to alert when rule updates appear on their networks, such alerts can miss updates on remote workstations using web-based email. If businesses do not configure their network to routinely sync their employees' web-based emails to the internal network, an intrusion may be left unidentified until the computer sends an update to the security appliance set up to monitor changes within the email application. This leaves the employee and all connected networks vulnerable to cyber criminals. Even after a financial institution or law enforcement contact warns a victimized business of a potential BEC, a system audit may not identify the updated email rules if it does not audit both applications, increasing the time a cyber criminal can retain email access and continue BEC activity. Cyber criminals may also use auto-forwarding rules to delete records from the recycle bin to further obfuscate their activities.

- In August 2020, cyber criminals created auto-forwarding email rules on the recently upgraded web client of a US-based medical equipment company. The webmail did not sync to the desktop application and went unnoticed by the victim company, which only observed auto-forwarding rules on the desktop client. RSS was also not enabled on the desktop application. After the BEC actors obtained access to the network, they impersonated a known international vendor. The actors created a domain with similar spelling to the victim and communicated with the vendor using a UK-based IP address to further increase the likelihood of payment. The actors obtained \$175,000 from the victim.



Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

- During another incident in August 2020, the same actor created three forwarding rules within the web-based email used by a company in the manufacturing industry. The first rule auto-forwarded any emails with the search terms "bank," "payment," "invoice," "wire," or "check" to the cyber criminal's email address. The other two rules were based off the sender's domain and again forwarded to the same email address.

For information on BEC actors targeting organizations that use Microsoft Office 365, please refer to the 3 March 2020 Private Industry Notification (PIN-20200303-001), "Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses Over Two Billion Dollars." Additionally, the 7 November 2019 Private Industry Notification (PIN-20191107-001), "Cyber Actors Leverage Subscription-based Commercial Database to Conduct Business Email Compromise Fraud against Construction Companies," details BEC actors registering similar domains to impersonate vendors with ongoing victim relationships.

Recommended Mitigations

- Ensure both the desktop and web applications are running the same version to allow appropriate syncing and updates.
- Be wary of last minute changes in established email account addresses.
- Carefully check email addresses for slight changes that can make fraudulent addresses appear legitimate and resemble actual clients' names.
- Enable multi-factor authentication for all email accounts.
- Prohibit automatic forwarding of email to external addresses.
- Frequently monitor the Email Exchange server for changes in configuration and custom rules for specific accounts.
- Create a rule to flag email communications where the "reply" email address differs from the "from" email address.
- Add an email banner to messages coming from outside your organization.
- Consider the necessity of legacy email protocols, such as POP, IMAP, and SMTP, that can be used to circumvent multi-factor authentication.
- Ensure changes to mailbox login and settings are logged and retained for at least 90 days.
- Enable security features that block malicious email, such as anti-phishing and anti-spoofing policies.



Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

- Encourage employees to request clarification of suspicious payment requests to their management prior to authorizing transactions.
- Immediately report any online fraud or BEC activity to the Internet Crime Complaint Center at ic3.gov/Home/BEC.

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

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>