Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

3 March 2020
PIN Number
20200303-001

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

Email:
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**: Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses Over Two Billion Dollars

Summary

Cyber criminals are targeting organizations who utilize Microsoft Office 365 and Google G Suite to conduct Business Email Compromise (BEC) scams. The scams are initiated through specifically developed phish kits designed to mimic the cloud-based email services in order to compromise business email accounts and request or misdirect transfers of funds. Between January 2014 and October 2019, the Internet Crime Complaint Center (IC3) received complaints totaling over $2.1 billion in actual losses from BEC scams targeting Microsoft Office 365 and Google G Suite.

Threat

Over the last decade, organizations have increasingly moved from on-premise email systems to cloud-based email services. Since 2014, cyber criminals have targeted two of the largest cloud-based email services, Microsoft Office 365 and Google G Suite, based on FBI complaint information. Between January 2014 and October 2019,

the Internet Crime Complaint Center (IC3) received complaints totaling over $2.1 billion in actual losses from BEC scams targeting the aforementioned platforms. Losses from BEC scams overall have increased every year since IC3 began tracking the scam in 2013 and have been reported in all 50 states and in 177 countries.

Cyber criminals develop and use specifically designed phishing kits that target the Microsoft Office 365 and Google G Suite platforms, particularly Office 365 given its dominant market share. These phishing kits are deployed in large batches of emails to US organizations and are able to identify the email service associated with each set of compromised credentials. This allows cyber criminals to target victims using cloud-based email services. Upon compromising victim email accounts, cyber criminals analyze the content to look for evidence of financial transactions. Often, the actors configure mailbox rules within a compromised account to delete key messages or enable automatic forwarding to an outside email account.

Using the information gathered from compromised accounts, cyber criminals impersonate email communications between compromised businesses and third parties, such as vendors or customers. The illicit actors then impersonate the compromised business, the third party, or both to request pending or future payments be redirected to fraudulent bank accounts. Cyber criminals use some or all of the following methods to impersonate these communications:

1. Send email from the compromised account to the target business or third party. Fraudulent email sent from a compromised account is difficult to detect.
2. Register a lookalike domain name which is used to impersonate a legitimate domain. For example, an employee with the email address janedoe@abccorporation.com could be impersonated through the email address janedoe@abccorp**a**ration.com.
3. Modify the “From” and “Reply-To” fields of email messages so they appear to have come from a particular sender. Replies sent to these spoofed messages are directed to the fraudulent sender.

Cyber criminals frequently access the address books of compromised accounts as a means to identify new targets to send additional phishing emails. As a result, a successful email account compromise at one business can pivot to multiple victims within an industry.

While Microsoft Office 365 and Google G Suite have security features that can help prevent BEC, many of these features must be manually configured and enabled. IT administrators can better protect their organizations from BEC by taking advantage of the full spectrum of protections available. Small and medium-size organizations, or those with limited IT resources, are most vulnerable to BEC scams.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

RECOMMENDATIONS FOR PROTECTION FOR END USERS

- Enable multi-factor authentication for all email accounts.
- Verify all payment changes and transactions in-person or via a known telephone number.
- Educate employees about BEC scams, including preventative strategies such as how to identify phishing emails and how to respond to suspected compromises.

RECOMMENDATIONS FOR PROTECTION FOR IT ADMINISTRATORS

- Prohibit automatic forwarding of email to external addresses.
- Add an email banner to messages coming from outside your organization.
- Prohibit legacy email protocols such as POP, IMAP, and SMTP that can be used to circumvent multi-factor authentication.
- Ensure mailbox logon and settings changes are logged and retained for at least 90 days.
- Enable alerts for suspicious activity such as foreign logins.
- Enable security features that block malicious email such as anti-phishing and anti-spoofing policies.
- Configure Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication Reporting and Conformance (DMARC) to prevent spoofing and to validate email.
- Disable legacy account authentication.

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 may be identified at www.fbi.gov/contact-us/field. Contact CyWatch by telephone at 855-292-3937 or by email at CyWatch@fbi.gov.

Administrative Note

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

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