Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

06 April 2020

Alert Number
I-040620-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than $2 Billion

Cyber criminals are targeting organizations that use popular cloud-based email services 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 more than $2.1 billion in actual losses from BEC scams using two popular cloud-based email services. While most cloud-based email services have security features that can help prevent BEC, many of these features must be manually configured and enabled. Users can better protect themselves from BEC by taking advantage of the full spectrum of protections that are available.

DEFINITIONS

Cloud-based email services are hosted subscription services that enable users to conduct business via tools such as email, shared calendars, online file storage, and instant messaging.

Business Email Compromise is a sophisticated scam targeting businesses that perform electronic payments such as wire or automated clearing house transfers. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques resulting in an unauthorized transfer of funds.

BACKGROUND

Over the last decade, organizations have increasingly moved from on-site email systems to cloud-based email services. Losses from BEC scams overall have increased every year since IC3 began tracking the scam in 2013. BEC scams have been reported in all 50 states and in 177 countries. Small and medium-size organizations, or those with limited IT resources, are most vulnerable to BEC scams because of the costs of robust cyber defense.

Federal Bureau of Investigation
Public Service Announcement

THREAT

There are a number of BEC scam variants. One of the most effective types is initiated through phishing emails designed to steal email account credentials. Cyber criminals use phishing kits that impersonate popular cloud-based email services. Many phishing kits identify the email service associated with each set of compromised credentials, allowing the cyber criminal to target victims using cloud-based services. Upon compromising victim email accounts, cyber criminals analyze the content of compromised email accounts for evidence of financial transactions. Often, the actors configure mailbox rules of a compromised account to delete key messages. They may also 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, to request pending or future payments be redirected to fraudulent bank accounts. Cyber criminals frequently access the address books of compromised accounts as a means to identify new targets to send phishing emails. As a result, a successful email account compromise at one business can pivot to multiple victims within an industry.

Depending upon the provider, cloud-based email services may provide security features such as advanced phishing protection and multi-factor authentication that are either not enabled by default or are only available at additional cost.

RECOMMENDATIONS 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 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,[1] 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 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, DomainKeys Identified Mail, and Domain-based Message Authentication Reporting and Conformance to prevent spoofing and validate email.
- Disable legacy account authentication.

[1] POP, IMAP and SMTP are the most commonly used email protocols that standardize the method for proper message transmittance.

Federal Bureau of Investigation
Public Service Announcement

WHAT TO DO IF YOU ARE A VICTIM

If you discover unauthorized payments, contact your financial institution immediately to request recall of the funds. Report attempted or actual fraudulent financial transfers to the Internet Crime Complaint Center at www.ic3.gov or to your local FBI field office, which can be found at www.fbi.gov/contact-us/field. The FBI may be able to assist financial institutions in the recovery of lost funds.