Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

17 March 2021

PIN Number
20210317-001

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-offices

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

Business Email Compromise Actors Targeting State, Local, Tribal, and Territorial Governments, Straining Resources

Summary

From 2018 through 2020, the FBI observed increases in business email compromise (BEC) actors targeting state, local, tribal, and territorial (SLTT) government entities for financial gain due to vulnerability exploitation and transparency requirements. The COVID-19 pandemic exacerbated these cybersecurity challenges as SLTTs shifted a significant portion of their workforce to remote work. These actors target SLTT victims with spoofed emails, phishing attacks, compromised vendor accounts, and credential harvesting to alter payment instructions for services rendered by vendors or employee payroll direct deposit information. From November 2018 to September 2020, the FBI observed losses ranging from $10,000 to $4 million, which have significantly impaired operational capabilities and imposed considerable resource strain on SLTT governments.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat Overview

BEC actors continue to target SLTT government entities with spoofed emails, phishing attacks, vendor email compromise, and credential harvesting techniques to manipulate payment or direct deposit information. These incidents not only can impair operational capabilities and cause reputational damage, but may also result in the loss of proprietary or sensitive information including personally identifiable information (PII), banking information, or employment data.

Cyber criminals often use open source information about SLTT government entities and readily obtainable malicious cyber tools to increase their capabilities and masquerade as trusted partners and vendors. The substantial amount of publicly available SLTT government operating information required by government transparency requirements enables cyber criminals to acquire information on SLTT leadership, vendor relationships, and associated contractors, allowing them to tailor attacks directly to victims. Cyber criminals may also determine those SLTT entities with inadequate cybersecurity protocols, such as a lack of personnel training, that they can compromise with the least amount of effort. Phishing kits—which bundle phishing tools and resources into user-friendly software—are increasingly available for purchase on the Dark Web, enabling even inexperienced cyber criminals with minimal technical skills to conduct more sophisticated attacks.

Rapid adoption of ad-hoc teleworking environments driven by the COVID-19 pandemic coupled with the ease of BEC operability against SLTT government entities and vendors has exacerbated cybersecurity challenges. This surge in teleworking has increased the use of potentially vulnerable services, such as Virtual Private Networks (VPN) and other remote support tools. In Fiscal Year 2020[a], DHS CISA conducted 25 Phishing Campaign Assessments of SLTT entities, which included 152 total campaigns. Of the more than 40,000 test emails sent during the assessments, CISA detected roughly 5,500 unique clicks of “malicious” links, constituting a 13.6% click rate. This highlights the need for defense in depth mitigations[b] in addition to phishing awareness training and email security efforts.

The FBI’s Internet Crime Complaint Center (IC3) notes BEC is an increasing and constantly evolving threat as criminal actors become more sophisticated and adapt to current events.

[a] Fiscal Year 2020 is from 1 October 2019 to 30 September 2020.
[b] Defense in depth represents instances where multiple layers of security controls are placed throughout an information technology system.

There was a 5 percent increase in adjusted losses[c] from 2019 to 2020, with over $1.7 billion adjusted losses reported to IC3 in 2019 and over $1.8 billion adjusted losses reported in 2020.

- In September 2020, a county government official received an email with new payment instructions from a legitimate vendor email address with whom the government had contracts. Upon failing to receive a $1.6 million payment, the vendor contacted the county who referred them to the email request. Upon forensic review, information technology personnel determined the vendor's email address had been compromised and the new payment instructions were fraudulent.
- In December 2019, unidentified malicious actors gained unauthorized access and modified rules for the email account of the financial coordinator of an identified US territory's government agency. The actors sent fraudulent financial transaction instructions to 146 government entities during their holiday leave. Four of the government entities transferred a total of $4 million to a fraudulent account after actors successfully intercepted and responded to further communications questioning the changes in banking information.
- In July 2019, a small city government received a spoofed email purporting to be from a known contractor requesting a change in payment method. The city complied with the request; however, after a delay in payment, the legitimate contractor contacted the city and informed them they had not requested the change. The adjusted loss to the city was approximately $3 million.
- In November 2018, a phishing attack targeting an identified county office resulted in a number of employees disclosing their account credentials. The criminal actors gained access to the system that maintained direct deposit information via the compromised accounts. The actors then diverted the employees' paychecks to unauthorized accounts, resulting in an approximate loss of $20,000.

Recommended Mitigations

General Mitigations:

- Educate employees about BEC scams, including preventative strategies such as how to identify phishing emails and how to respond to suspected compromises. The FBI has a BEC public service announcement video at: https://www.fbi.gov/video-repository/psa-business-e-mail-compromise-scam.mp4/view. The Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure ISAC (EI-ISAC) have also published

[c] Adjusted losses include funds recovered by law enforcement or banks.

beneficial reference material on BECs. Those can be found at: https://www.cisecurity.org/blog/business-email-compromise-cosmic-lynx/, https://www.cisecurity.org/white-papers/security-primer-business-email-compromise/, and https://cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-business-email-compromise-scam/.

- Be skeptical of unexplained urgency regarding payment requests.
- Be wary of last-minute changes in wire instructions or recipient account information as well as changes in established communication platforms or email account addresses.
- Be wary of unsolicited requests to verify account information.
- Be on the lookout for advance payment requests when not previously required.
- Verify all payment changes and transactions in person or via a known telephone number.
- Contact vendors through telephone numbers on file rather than through a number provided in emails.
- Look for grammar and spelling errors in emails.
- Verify email addresses and check for slight changes that can make fraudulent addresses appear legitimate and resemble actual clients' names. Look for additional punctuation, changes in the top-level domain (i.e. ".com" vs ".gov"), added prefixes or suffixes, or misspelling of the domain.
- Ensure company policies provide for verification of any changes to existing invoices, bank deposit routing information, or contact information.
- Do not make account changes from a link within emails.
- Report suspicious activity to security administrators.

Recommendations for information technology administrators:

- Consider conducting internal phishing campaigns to raise awareness.
- Encourage a skeptical cyber posture among employees.
- Require multi-factor authentication for all email accounts.
- Prohibit automatic forwarding of email to external addresses.
- Frequently monitor the company Email Exchange server for changes in configuration and custom rules for specific accounts.
- Add an email banner to messages coming from outside your organization.
- Consider if legacy email protocols, such as POP, IMAP, and SMTP1, that can be used to circumvent multi-factor authentication, are required.
- Ensure changes to mailbox login settings are logged and retained for at least 90 days.
- Enable alerts for suspicious activity, such as foreign IP address logins.
- Consider using or enabling email-filtering services.

- 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.
- Disable hyperlinks in received emails.
- Stay current on available patches for remote access features as well as VPN hardware and software.

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). BEC-specific complaints can also be filed through the FBI's Internet Crime Complaint Center (IC3) at ic3.gov/Home/BEC. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. 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