Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

29 March 2022

PIN Number

20220329-001

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**

Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.

www.fbi.gov/contact-us/field-offices

Cyber Actors Target US Election Officials with Invoice-Themed Phishing Campaign to Harvest Credentials

Summary

The FBI is warning US election and other state and local government officials about invoice-themed phishing emails that could be used to harvest officials' login credentials. If successful, this activity may provide cyber actors with sustained, undetected access to a victim's systems. As of October 2021, US election officials in at least nine states received invoice-themed phishing emails containing links to websites intended to steal login credentials. These emails shared similar attachment files, used compromised email addresses, and were sent close in time, suggesting a concerted effort to target US election officials.

Threat

The FBI judges cyber actors will likely continue or increase their targeting of US election officials with phishing campaigns in the lead-up to the 2022 US midterm elections. Proactive monitoring of election infrastructure (including official email accounts) and communication between FBI and its state, local, territorial, and tribal partners about this type of activity will provide

opportunities to mitigate instances of credential harvesting and compromise, identify potential targets and information sought by threat actors, and identify threat actors. This assessment is based on reports of phishing attacks that occurred in October 2021 and had the characteristics of a coordinated, ongoing effort to target US election officials.

- On 5 October 2021, unidentified cyber actors targeted US election officials in at least nine states, and representatives of the National Association of Secretaries of State, with phishing emails. These emails originated from at least two email addresses with the same attachment titled, “INVOICE INQUIRY.PDF,” which redirected users to a credential-harvesting website. One of the email addresses sending the phishing emails was a compromised US government official’s email account.

- On 18 October 2021, cyber actors used two email addresses, purportedly from US businesses, to send phishing emails to county election employees. Both emails contained Microsoft Word document attachments regarding invoices, which redirected users to unidentified online credential harvesting websites.

- On 19 October 2021, cyber actors used an email address, purportedly from a US business, to send a phishing email containing fake invoices to an election official. The emails contained an attached Microsoft Word document titled, “Current Invoice and Payments for report.”

Recommendations

FBI recommends network defenders apply the following mitigations to reduce the risk of compromise.

- Educate employees on how to identify phishing, spear-phishing, social engineering, and spoofing attempts. Advise employees to be cautious when providing sensitive information – such as login credentials – electronically or over the phone, particularly if unsolicited or anomalous. Employees should confirm, if possible, requests for sensitive information through secondary channels.

- Create protocols for employees to send suspicious emails to IT departments for confirmation.

- Mark external emails with a banner denoting the email is from an external source to assist users in detecting spoofed emails.

- Enable strong spam filters to prevent phishing emails from reaching end users. Filter emails containing executable files from reaching end users.

- Advise training personnel not to open e-mail attachments from senders they do not recognize.

- Require all accounts with password logins (*e.g*., service account, admin accounts, and domain admin accounts) to have strong, unique passphrases. Passphrases should not be reused across multiple accounts or stored on the system where an adversary may have access. (Note: Devices with local administrative accounts should implement a password policy that requires strong, unique passwords for each administrative account.)

- Require multi-factor authentication for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.

- If there is evidence of system or network compromise, implement mandatory passphrase changes for all affected accounts.

- Keep all operating systems and software up to date. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. 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.

Administrative Note

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