|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | |  |   https://hisac-prod-csap.s3.amazonaws.com/tenant_media/66c393bf_WebAppWhiteBGLarge.png   |  | | --- | |  | |  | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  | | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | |  |  Threat Bulletins |  | |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | |  |   **FBI Warns of US Election Officals Targeting via Invoice-Themed Phishing Campaign to Harvest Credentials**   |  | | --- | |  | | | |  | | --- | |  | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  | | --- | |  | | |  | | --- | | https://hisac-prod-csap.s3.amazonaws.com/card_images/61bd7508_c86b0628_Default03.png | | |  | | --- | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | |  | | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  | | --- | |  |  |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | | https://cdn.cyware.com/email-templates/WHITE.png | | |  | | --- | | TLP:WHITE | | | | |  | | --- | | Mar 30, 2022 | | |  | | --- | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | |  | | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | |  | | --- | |  | |  |  |  | | --- | --- | | |  | | --- | | On March 29, 2022, the Federal Bureau of Investigation (FBI) released an FBI-PIN ([20220329-001](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ic3.gov%2FMedia%2FNews%2F2022%2F220329.pdf&data=04%7C01%7Cdsamuels%40AHA.ORG%7C26b3bf02bfe34dcda28908da1271040c%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C1%7C637842573874565815%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=DtO3egXB%2BJl6AMRAN02axs%2Bi0Yvhj%2B%2BOckhvzNmsJZk%3D&reserved=0)) 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.  The full report, also attached, can be accessed [here](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ic3.gov%2FMedia%2FNews%2F2022%2F220329.pdf&data=04%7C01%7Cdsamuels%40AHA.ORG%7C26b3bf02bfe34dcda28908da1271040c%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C1%7C637842573874565815%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=DtO3egXB%2BJl6AMRAN02axs%2Bi0Yvhj%2B%2BOckhvzNmsJZk%3D&reserved=0). | |  |  |  | | --- | --- | | |  | | --- | | 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 the 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 the report.” | | | | |  | | --- | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | |  | | |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | |  |  |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | | **Reference(s)** | | |  | | --- | | [IC3](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ic3.gov%2FMedia%2FNews%2F2022%2F220329.pdf&data=04%7C01%7Cdsamuels%40AHA.ORG%7C26b3bf02bfe34dcda28908da1271040c%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C1%7C637842573874565815%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=DtO3egXB%2BJl6AMRAN02axs%2Bi0Yvhj%2B%2BOckhvzNmsJZk%3D&reserved=0) | |  |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | | **Report Source(s)** | | |  | | --- | | FBI | | | | |  | | --- | |  | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | |  | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | |  |   **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 are 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 accounts, 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.   + 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. | |   **Sources**   |  |  | | --- | --- | | |  | | --- | | [FBI-PIN 20220329-001: Cyber Actors Target US Election Officials with InvoiceThemed Phishing Campaign to Harvest Credentials](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ic3.gov%2FMedia%2FNews%2F2022%2F220329.pdf&data=04%7C01%7Cdsamuels%40AHA.ORG%7C26b3bf02bfe34dcda28908da1271040c%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C1%7C637842573874565815%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=DtO3egXB%2BJl6AMRAN02axs%2Bi0Yvhj%2B%2BOckhvzNmsJZk%3D&reserved=0) | |  |  | | --- | |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | **Alert ID** f971d015 |  | |  |  | | |  | | --- | |  | | | | | | |  | | --- | |  | |  |  | | --- | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | |  | | |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | |  |  |  | | --- | |  |  |  | | --- | |  |   This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.  [**View Alert**](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fhealth-isac.cyware.com%2Fwebapp%2Fuser%2Fmyfeeds%2Ff971d015&data=04%7C01%7Cdsamuels%40AHA.ORG%7C26b3bf02bfe34dcda28908da1271040c%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C1%7C637842573874565815%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=AF%2BUn3WnCZUsik%2BQ2w2Ead9UpcGO32JU6Itkbd%2BEBWo%3D&reserved=0)   |  | | --- | |  |  |  |  | | --- | --- | | |  | | --- | | **Tags** FBI-PIN, FBI | |  |  |  | | --- | --- | | |  | | --- | | **TLP:WHITE** Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. | |  |  |  | | --- | --- | | |  | | --- | | **For Questions or Comments** Please email us at [toc@h-isac.org](mailto:toc@h-isac.org) | |  |  |  | | --- | --- | | |  | | --- | | **FBI** 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](http://www.fbi.gov/contact-us/field). Contact CyWatch by telephone at 855-292-3937 or by email at [CyWatch@fbi.gov](mailto:CyWatch@fbi.gov). | | | | |  | | --- | |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | |  | | |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | | Download Health-ISAC’s Information Sharing App. | | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | |  | | --- | |  |  |  |  |  |  | | --- | --- | --- | --- | | |  | | --- | | [https://cdn.cyware.com/email-templates/survey/applestore.png](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fitunes.apple.com%2Fin%2Fapp%2Fcyware-pro-for-organizations%2Fid1193942672%3Fmt%3D8&data=04%7C01%7Cdsamuels%40AHA.ORG%7C26b3bf02bfe34dcda28908da1271040c%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C1%7C637842573874565815%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=Xh3Cxs22%2B1Hephj0qpeU4lGz2Q9RYbpP08GsQihG1s8%3D&reserved=0) | | |  | | --- | | [https://cdn.cyware.com/email-templates/survey/googleplay.png](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fplay.google.com%2Fstore%2Fapps%2Fdetails%3Fid%3Dcom.cyware.enterprise.android%26hl%3Den&data=04%7C01%7Cdsamuels%40AHA.ORG%7C26b3bf02bfe34dcda28908da1271040c%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C1%7C637842573874565815%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=BRUg8KDx6yOKSM7XFYnOTdj4nypP90IjM%2FzLOwkZcho%3D&reserved=0) | | | | | | |  | | --- | |  | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  | | --- | |  | | |  |  | | --- | --- | | |  | | --- | |  |   For more update and alerts, visit: [**https://health-isac.cyware.com**](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fhealth-isac.cyware.com%2F&data=04%7C01%7Cdsamuels%40AHA.ORG%7C26b3bf02bfe34dcda28908da1271040c%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C1%7C637842573874565815%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=kvR6LOH3vWzQdhQzY7XAJgRQkGZl4GTSXD3K0o49eKo%3D&reserved=0) | | |  | | --- | |  | |  |  |  | | --- | --- | | |  | | --- | |  | |  |  | | --- | |  | | |  |  |  |  |  | | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | |  |   If you are not supposed to receive this email, please contact us at [**toc@h-isac.org**](mailto:toc@h-isac.org). |  | | |  |  |  |  |  | | --- | --- | --- | --- | | |  |  |  | | --- | --- | --- | | |  | | --- | |  |   Powered by [Cyware](https://nam11.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcyware.com%2F&data=04%7C01%7Cdsamuels%40AHA.ORG%7C26b3bf02bfe34dcda28908da1271040c%7Cb9119340beb74e5e84b23cc18f7b36a6%7C0%7C1%7C637842573874565815%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=65t5C8LQyXfNc%2FW4EW3kvn7JQ3k58TQHtu7kkUle1j8%3D&reserved=0) |  | |  |  | | --- | |  | |