Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

4 November 2024

PIN Number

20241104-001

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: CLEAR**

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

Easy Access to Information for Conducting Fraudulent Emergency Data Requests Impacts US-Based Companies and Law Enforcement Agencies

Summary

The Federal Bureau of Investigation (FBI) is releasing this Private Industry Notification to highlight a trend of compromised US and foreign government email addresses used to conduct fraudulent emergency data requests[a][b] to US-based companies, exposing personally identifying information (PII). While the concept of fraudulent emergency data requests was previously used by other threat actors, such as Lapsus$, the increase in postings on criminal forums regarding the process of emergency data requests and sale of compromised credentials has led to an increase of their use. The FBI encourages organizations to implement the recommendations in the Mitigations section to reduce the likelihood and impact from submission of fraudulent emergency data requests to attempt to gain unauthorized access to

[a] An emergency data request can be used in emergency circumstances to request information immediately from a business and bypassing additional reviews of the request for legitimacy.

[b] While emergency data requests are viewed within the law enforcement community as entirely separate data requests, many cyber-criminals use this terminology along with letterhead memorandums (LHM), subpoenas, and Mutual Legal Assistance Treaties (MLAT) interchangeably.

PII**.** Enhanced password protocols implemented in early 2023 highlighted that a mandated increase in password length, the use of multi-factor-authentication (MFA) for users with administrative rights, policy controls directed at vishing, and improved baseline monitoring worked together to decrease successful attempts at cracking passwords and made networks more resilient to a threat actor's initial intrusion and persistence.

Threat

As of August 2024, FBI noted an uptick in criminal forum posts regarding conducting fraudulent emergency data requests and is releasing this notification for industry awareness. Cyber-criminals are likely gaining access to compromised US and foreign government email addresses and using them to conduct fraudulent emergency data requests to US based companies, exposing the personal information of customers to further use for criminal purposes.

- In August 2024, a known cyber-criminal on an online forum posted their sale of "High Quality .gov emails for espionage/social engineering/data extortion/Dada requests, etc", which included US credentials. The poster indicated they could guide a buyer through emergency data requests and sell real stolen subpoena documents to pose as a law officer.
- In March 2024, a known cyber-criminal on an online forum indicated they "owned" government emails from over 25 countries, and that through a successful subpoena, the requestor could gain access to usernames, emails, phone numbers, and other private client information.
- In March 2024, a known cyber-criminal posted photos on an online forum of a fraudulent emergency data request submitted to Paypal. According to PayPal, the threat actor submitted a fraudulent Mutual Legal Assistance Treaty (MLAT) regarding a local ongoing investigation into child trafficking, which included a case number and legal code for verification, but the request was ultimately denied by PayPal.
- In December 2023, cyber-criminals would send a fake emergency data request, along with a statement to provide the requested information immediately, indicating an individual would suffer greatly or die unless the requested information was provided by the company.
- In October 2023, a known cyber-criminal stated on an online forum that .gov emails could be used to carry out emergency data requests on users, and allow a user to "become" a law enforcement officer or government entity. They further stated that the data obtained could be used to carry out phishing or malware attacks against the government sector and become an initial access vector.

- In August 2023, a cyber-criminal stated they were teaching individuals how to create and submit their own emergency data requests to get information on any social media account for 100USD.

Mitigations

FBI recommends government and other organizations that receive emergency data requests take the steps below to improve their security posture in response to the noted attack trends and possible outcomes using more resilient security protocols. FBI recommends organizations establish and maintain strong liaison relationships with the FBI Field Office in their region. The location and contact information for FBI Field Offices can be located at www.fbi.gov/contact-us/field-offices. Through these partnerships, FBI can assist with identifying vulnerabilities and mitigating potential threat activity. FBI further recommends organizations review and, if needed, update incident response and communication plans that list actions an organization will take if impacted by a cyber incident.

The cybersecurity landscape is ever-evolving, and cyber threats are becoming increasingly sophisticated. Organizations need to stay ahead of the curve using proactive approaches to mitigate risks. FBI recommends applying the following common industry best practices:

Mitigation for Cyber Incidents -

- Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.
- Document and monitor external remote connections. Organizations should document approved solutions for remote management and maintenance, and immediately investigate if an unapproved solution is installed on a workstation.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (that is, a hard drive, other storage device, or the cloud).
- Private Sector Companies receiving Law Enforcement requests should apply critical thinking to any emergency data requests received. Cyber-criminals understand the need for exigency, and use it to their advantage to shortcut the necessary analysis of the emergency data request. FBI recommends reviewers pay close attention to doctored images such as signatures or logos applied to the document. In addition, FBI recommends looking at the legal codes referenced in the emergency data request, as they should match what would be expected from the originating authority. For example, if this request is coming from a country outside of the United States, it should not appear to be copied and pasted language from the U.S. Title Code. Similarly, a foreign country's law enforcement would not be attaching a U.S. subpoena. If suspicion and the

need for validation arises, the FBI recommends contacting the sender and originating authority to discuss the request further.

- **Develop and implement strong password protocols.**
  - Passwords should use at least 16 characters; even longer passwords are better and significantly reduce risk. Password length is the greater mitigating factor, compared to complexity. Encourage a combination of two, or more, of the following within passwords: uppercase letters, lower-case letters, numbers, and symbols;
  - Encourage unique passwords (a password used for only one account);
  - Prevent common words that could be found in the dictionary, and blacklist specific words relating to the names of persons, characters, products, or the organization;
  - Check passwords against a blacklist of characteristics, such as those previously mentioned in a breach, containing repetitive characters or symbols, or have context-specific information, like derivatives of the service or a username;
  - Encourage a string of mixed-case letters, numbers, and symbols, or a passphrase of 5-7 random words.
  - For additional guidance on developing strong password policies, refer to the Cybersecurity & Infrastructure and Security Agency's (CISA) password guidance: Use Strong Passwords | CISA
- **Use Secure Password Storage: Require all accounts** with password logins (for example, service account, admin accounts, and domain admin accounts) to comply with National Institute of Standards and Technology (NIST) standards for developing and managing password policies.
  - Store passwords in hashed format using industry-recognized password managers;
  - Add password user "salts" to shared login credentials;
  - Avoid reusing passwords;
  - Implement multiple failed login attempt account lockouts;
  - Disable password "hints";
  - Refrain from requiring password changes more frequently than once per year unless a password is known or suspected to be compromised (Note: NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password "patterns" cyber criminals can easily decipher.); and
  - Require administrator credentials to install software.
- **Implement Password Management Tools** such as password manager and SSO.
- **Assess user passwords for compliance** with organizational policies, and to ensure they meet certain standards and criteria.
- **Require default credentials be changed** on all hardware and software products.
- **Require phishing-resistant multifactor authentication** for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.

- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts.
- **Audit user accounts with administrative privileges,** and configure access controls according to the principle of least privilege.
- **Implement time-based access for accounts set at the admin level and higher.** For example, the Just-in-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.
- **Generate compliance reports** to better assess your organization's password compliance status, in particular highlighting areas of non-compliance, vulnerabilities, and potential risks related to password security.
- **Secure and closely monitor remote desktop protocol (RDP) use.**
- **Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure.** If RDP is deemed operationally necessary, restrict the originating sources and require MFA to mitigate credential theft and reuse. If RDP must be available externally, use a VPN, virtual desktop infrastructure, or other means to authenticate and secure the connection before allowing RDP to connect to internal devices. Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force campaigns, log RDP login attempts, and disable unused remote access/RDP ports.
- **Segment networks to prevent the spread of malware/ransomware**. Network segmentation can help prevent the spread of malware/ransomware by controlling traffic flows between—and access to—various subnetworks, and by restricting adversary lateral movement.
- **Identify, detect, and investigate abnormal activity and potential traversal of any indicated malware/ransomware with a networking monitoring tool.** To aid in detecting malware/ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- **Install, regularly update, and enable real time detection for antivirus software on all hosts.**

Vulnerability and Configuration Management -

- **Keep all operating systems, software, and firmware 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. Organizations should prioritize patching of vulnerabilities on CISA's Known Exploited Vulnerabilities catalog.

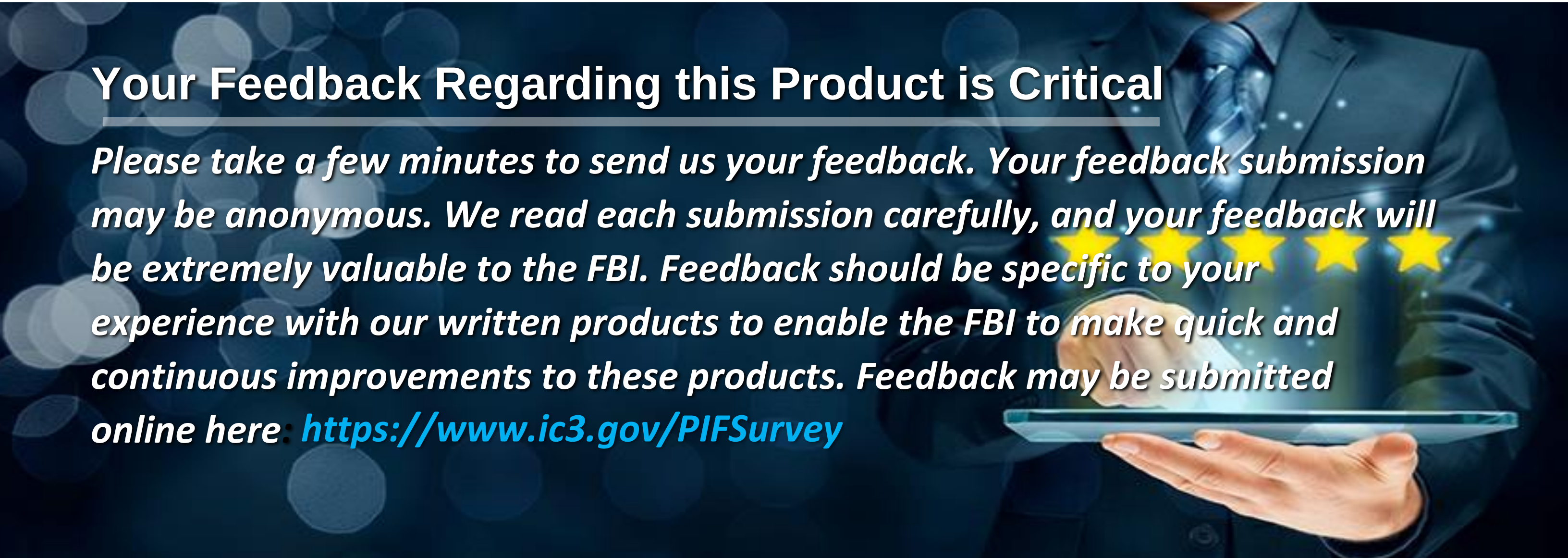
- **Disable command-line and scripting activities and permissions.** Privilege escalation and lateral movement often depend on software utilities running from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally.
- **Ensure devices are properly configured and that security features are enabled.**
- **Disable ports and protocols that are not being used for a business purpose** (such as RDP Transmission Control Protocol Port 3389).
- **Restrict Server Message Block (SMB) Protocol within the network to only access servers that are necessary, and remove or disable outdated versions of SMB** (such as SMB version 1). Threat actors use SMB to propagate malware across organizations.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or ic3.gov. 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, 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:CLEAR**. Subject to standard copyright rules, the information is this product may be shared without restrictions.



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