Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

14 September 2022

PIN Number

20220914-001

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 and Oregon TITAN Fusion Center.

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 Criminals Targeting Healthcare Payment Processors, Costing Victims Millions in Losses

Summary

The FBI has received multiple reports of cyber criminals increasingly targeting healthcare payment processors to redirect victim payments. In each of these reports, unknown cyber criminals used employees' publicly-available Personally Identifiable Information (PII) and social engineering techniques to impersonate victims and obtain access to files, healthcare portals, payment information, and websites. In one case, the attacker changed victims' direct deposit information to a bank account controlled by the attacker, redirecting $3.1 million from victims' payments.

Threat

Cyber criminals are compromising user login credentials of healthcare payment processors and diverting payments to accounts controlled by the cyber criminals. Recent reporting indicates cyber criminals will continue targeting healthcare payment processors through a variety of techniques, such as phishing campaigns and social engineering, to spoof support centers and obtain user access.

- In April 2022, a healthcare company with more than 175 medical providers discovered an unauthorized cyber criminal posing as an employee had changed Automated Clearing House (ACH) instructions of one of their payment processing vendors to direct payments to the cyber criminal rather than the intended providers. The cyber criminal successfully diverted approximately $840,000 dollars over two transactions prior to the discovery.
- In February 2022, a cyber criminal obtained credentials from a major healthcare company and changed direct deposit banking information from a hospital to a consumer checking account belonging to the cyber criminal, resulting in a $3.1 million loss. In mid-February 2022, in a separate incident a different cyber criminal used the same method to steal approximately $700,000.
- From June 2018 to January 2019, cyber criminals targeted and accessed at least 65 healthcare payment processors throughout the United States to replace legitimate customer banking and contact information with accounts controlled by the cyber criminals. One victim reported a loss of approximately $1.5 million. The cyber criminals used a combination of publicly available PII and phishing schemes to gain access to customer accounts. Entities involved in processing and distributing healthcare payments through processors remain vulnerable to exploitation via this method.

The FBI has identified potential indicators of cyber criminals attempting to gain access to user accounts.

- Phishing emails, specifically targeting financial departments of healthcare payment processors.
- Suspected social engineering attempts to obtain access to internal files and payment portals.
- Unwarranted changes in email exchange server configuration and custom rules for specific accounts.
- Requests for employees to reset both passwords and 2FA phone numbers within a short timeframe.
- Employees reporting they are locked out of payment processor accounts due to failed password recovery attempts.

Recommendations

The FBI recommends network defenders apply the following mitigations to reduce the risk of compromise from cyber threats.

- Ensure anti-virus and anti-malware is enabled and security protocols are updated regularly and in a timely manner. Well-maintained anti-virus and anti-malware software may prevent commonly used attacker tools.
- Conduct regular network security assessments to stay up to date on compliance standards and regulations. These should include performing penetration tests and vulnerability scans to ensure the knowledge and level of current system and security protocols.
- Implement training for employees on how to identify and report phishing, social engineering, and spoofing attempts. As budget constraints allow, consider options in authentication or barrier layers to decrease or eliminate the viability of phishing.
- Advise all employees to exercise caution while revealing sensitive information such as login credentials through phone or web communications. Employees should conduct requests for sensitive information through approved secondary channels.
- Use multi-factor authentication for all accounts and login credentials to the extent possible. Viable choices such as hard tokens allow access to software and verifies identity with a physical device instead of authentication codes or passwords.
- Update or draft an incident response plan, in accordance with Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules.
- Mitigate vulnerabilities related to third-party vendors. Outside communication exchanges should contain email banners to alert employees of communications originating outside of the organization. Review and understand the vendor’s risk threshold and what comprises a breach of service.
- Verify and modify as needed contract renewals to include the inability to change both credentials and 2FA within the same timeframe to reduce further vulnerability exploitations.
- Ensure company policies include verification of any changes to existing invoices, bank deposits, and contact information for interactions with third-party vendors and organizational collaborations. Any direct request for account actions needs to be verified through the appropriate, previously established channels before a request is sanctioned.
- Create protocols for employees to report suspicious emails, changes to email exchange server configurations, denied password recovery attempts, and password resets including 2FA phone numbers within a short timeframe to IT and security departments for investigation.

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

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