JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP: CLEAR Product ID: 20240624-001

June 24, 2024

Social Engineering Tactics Targeting Healthcare & Public Health Entities and Providers

SUMMARY

The Federal Bureau of Investigation (FBI) and the Department of Health and Human Services (HHS) are releasing this joint Cybersecurity Advisory (CSA) to disseminate known indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) used in a social engineering campaign targeting healthcare, public health entities, and providers. Threat actors are using phishing schemes to steal login credentials for initial access and the diversion of automated clearinghouse (ACH) payments to US controlled bank accounts. Healthcare organizations are attractive targets for threat actors due to their size, technological dependence, access to personal health information, and unique impacts from patient care disruptions. The FBI and HHS encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of social engineering incidents.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 14.1. See the MITRE ATT&CK® Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK® tactics and techniques with corresponding mitigation and/or detection recommendations. For assistance with mapping malicious cyber activity to the MITRE ATT&CK® framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK® Mapping and CISA's Decider Tool.

Overview

Based on previous cyber attack and forensic analysis reports, the FBI and HHS observed consistency in TTPs used in cyber attacks against the Healthcare sector. Unknown threat actors gained initial

---

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

access to employees' email accounts, and then pivoted to specifically target login information related to the processing of reimbursement payments to insurance companies, medicare, or similar entities. To gain initial access to victim networks, the threat actor acquired credentials through social engineering or phishing. In some observed instances, the threat actor called an organization's IT Help Desk posing as an employee of the organization, and triggered a password reset for the targeted employee's organizational account [T1566.004]. In some instances, by manipulating the IT Help Desk employees, the threat actor was able to bypass multifactor authentication (MFA) [T1556.006]. In another instance, the threat actors registered a phishing domain [T1556.001] that varied by one character from the target organization's true domain, and targeted the organization's Chief Financial Officer (CFO) [TA1656]. The threat actors often have personally identifiable information (PII) of the impersonated employee, obtained from data breaches, enabling the threat actor to confirm the targeted employees' identity over the phone. If a social engineering attempt is successful, the threat actor then logs onto the victim account and attempts to use living off the land techniques (LOTL). LOTL gives threat actors the ability to conduct their malicious cyber attacks discreetly as they can camouflage activity with typical system and network behavior. By using LOTL, threat actors were able to amend forms to make ACH changes to patients' accounts which enabled the diversion of legitimate payments to US bank accounts controlled by the actors [T1657], followed by a second transfer of funds to overseas accounts. In some instances, the threat actor also attempted to upload malware to victim systems without success.

INDICATORS OF COMPROMISE

Since August 2023, threat actors used voice over Internet protocol (VoIP) numbers to conduct a spearphishing campaign to obtain login credentials from healthcare networks, clinics, and healthcare providers.

Table 1: Observed VoIP Telephone Numbers Affiliated with Spearphishing Attacks. It is important to note that since the attacks use VoIP technology, these numbers can easily be changed.

VoIP Telephone Numbers
+18438888744
+18436660266
+16623301993
+14105535453
+13203073676
+16099040399
+12088005074
+18036215366
+15049000076
+18164000462
+12086202993
+18038888204
+14108884533
+15049000075

+15182848237

MITRE ATT&CK® TACTICS AND TECHNIQUES

See Tables 2 through 6 for all referenced threat actor tactics and techniques in this advisory.

Table 2: Initial Access

Technique Title	ID	Use
Phishing: Spearphishing Voice	T1566.004	Threat actor uses voice communications to ultimately gain access to victim systems. Spearphishing voice employs the use of manipulating a user into providing access to systems through a phone call or other forms of voice communications.

Table 3: Persistence

Technique Title	ID	Use
Modify Authentication Process: Multi-Factor Authentication	T1556.006	Threat actor disables or modifies multi-factor authentication (MFA) mechanisms to enable persistent access to compromised accounts.

Table 4: Impact

Technique Title	ID	Use
Financial Theft	T1657	Threat actor may steal monetary resources from targets through extortion, social engineering, technical theft, or other methods aimed at their own financial gain at the expense of the availability of these resources for victims.

Table 5: Defense Evasion

Technique Title	ID	Use
Domain Controller Authentication	T1556.001	Threat actor patches the authentication process on a domain controller to bypass the typical authentication mechanisms and enable access to accounts.

Impersonation	TA1656	Threat actor impersonates a trusted person or organization in order to persuade and trick a target into performing some action on their behalf.

MITIGATIONS

The FBI and HHS recommend organizations implement the mitigations below to improve your organization's cybersecurity posture based on the threat actor's activity. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

- **Implement multi-factor authentication (MFA) for every account.** While privileged accounts and remote access systems are critical, it is also important to ensure full coverage across SaaS solutions. Enabling MFA for corporate communications platforms (as with all other accounts) provides vital defense against these types of attacks and, in many cases, can prevent them.
- **Train IT Help Desk employees on this vulnerability.** MFA bypasses should not be allowed for any individual calling into the Help Desk.
- **Reduce threat of malicious actors** using remote access tools by:
    - **Auditing remote access tools** on your network to identify currently used and/or authorized software.
    - **Reviewing logs for execution of remote access software** to detect abnormal use of programs running as a portable executable [CPG 2.T].
    - **Using security software** to detect instances of remote access software being loaded only in memory.
    - **Requiring authorized remote access solutions** to be used only from within your network over approved remote access solutions, such as virtual private networks (VPNs) or virtual desktop interfaces (VDIs).
    - **Blocking both inbound and outbound connections** on common remote access software ports and protocols at the network perimeter.
    - **Applying recommendations** in the Guide to Securing Remote Access Software.

- Organizations are urged to check phone call logs to identify if their organization has been in contact with any of the above listed phone numbers. If contact was made, the organization should assess what access the UA was given and if the UA was successful in accessing sensitive information.

The authoring agencies also recommend HPH network defenders to read the full Mitigation Guide: Healthcare and Public Health (HPH) Sector and reference the HPH Cybersecurity

Performance Goals, which provide tailored best practices to combat pervasive cyber threats against that sector. Specifically, the authoring organizations recommend:

- **Email Security**: Reduce risk from common email-based threats, such as email spoofing, phishing, and fraud.
- **Multifactor Authentication**: Add a critical, additional layer of security, where safe and technically capable, to protect assets and accounts directly accessible from the Internet.
- **Basic Cybersecurity Training**: Ensure organizational users learn and perform more secure behaviors.
- **Centralized Log Collection**: Collection of necessary telemetry from security log data sources within an organization's network that maximizes visibility, cost effectiveness, and faster response to incidents.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, the FBI and HHS recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK® for Enterprise framework in this advisory. The FBI and HHS recommend testing your existing security controls inventory to assess how they perform against the ATT&CK® techniques described in this advisory.

To get started:

1. Select an ATT&CK® technique described in this advisory (see table 2-5).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The FBI and HHS recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK® techniques identified in this advisory.

RESOURCES

- Resource to mitigate a phishing attack: CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) "Phishing Guidance: Stopping the Attack Cycle at Phase One" (October 2023).
- Joint Cybersecurity Advisory: Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs (May 28, 2021).

- HC3 Sector Alerts: https://www.hhs.gov/sites/default/files/help-desk-social-engineering-sector-alert-tlpclear.pdf

REPORTING

The FBI and HHS do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, the FBI and HHS urge you to promptly report such cyber incidents to the FBI's Internet Crime Complaint Center(IC3), a local FBI Field Office, or CISA via the agency's Incident Reporting System or its 24/7 Operations Center (report@cisa.gov or (888) 282-0870).

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. FBI and HHS do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the FBI or HHS.

VERSION HISTORY

June 24, 2024: Initial version.