Health-ISAC™
Collaborating for Resilience in Healthcare
SHARING SINCE 2010

THREAT BULLETINS

Social Engineering Tactics Targeting Healthcare and Public Health Entities and Providers

○○○ TLP:WHITE

Jun 25, 2024

On June 24, 2024, the Federal Bureau of Investigation (FBI) and the Department of Health and Human Services (HHS) released a joint Cyber Security Advisory (CSA). The alert includes known indicators of compromise (IoCs) and tactics, techniques, and procedures (TTPs) leveraged 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 fraudulent 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.

Health-ISAC is sharing this alert to help raise awareness regarding campaigns targeting help desks leveraging social engineering techniques to compromise networks. Attacks targeting help desks, most notably identified in a Cybersecurity and Infrastructure Security Agency (CISA) advisory, have been an ongoing challenge within the threat landscape.

All members are encouraged to review the attached joint Cyber Security Advisory for additional information, including indicators of compromise, observed tactics and techniques, and associated mitigations.

Unknown threat actors gained initial 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. The threat actor acquired credentials through social engineering or phishing to gain initial access to victim networks.

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. In some instances, by manipulating the IT Help Desk employees, the threat actor was able to bypass multifactor authentication (MFA). In another instance, the threat actors registered a phishing domain that varied by one character from the target organization’s true domain and targeted the organization’s Chief Financial Officer (CFO).

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 employee’s identity over the phone. If a social engineering attempt is successful, the threat actor then logs onto the victim's account and attempts to use living off the land techniques (LOTL). LOTL allows threat actors 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, 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.

Tactics-Techniques-Sub-techniques	• Enterprise - Initial Access - Phishing - Spearphishing Voice, Spearphishing Attachment • Enterprise - Persistence - Modify Authentication Process - Multi-Factor Authentication • Enterprise - Defense Evasion - Impersonation • Enterprise - Impact - Financial Theft

Alert ID 2f6a28f8

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Tags Help Desk Targeting, Social Engineering

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

HICP

The Health Industry Cybersecurity Practices (HICP) refer to a set of guidelines and recommendations developed by the U.S. Department of Health and Human Services (HHS) to help healthcare organizations improve their cybersecurity posture. The HICP was created in response to the increasing threat of cyberattacks and data breaches in the healthcare sector, which has been a target for cybercriminals due to the sensitive and valuable nature of healthcare data.

The HICP resources are aimed at helping healthcare organizations of all sizes, including small, medium, and large entities. It provides practical and actionable guidance for managing and mitigating cybersecurity risks in healthcare environments, with a focus on five key cybersecurity threats: ransomware, phishing, loss or theft of equipment or data, insider threats, and attacks against connected medical devices.

Access the Health-ISAC Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.