HC3: Sector Alert

April 3, 2024 TLP:CLEAR Report: 202404031000

Social Engineering Attacks Targeting IT Help Desks in the Health Sector

Executive Summary

HC3 has recently observed threat actors employing advanced social engineering tactics to target IT help desks in the health sector and gain initial access to target organizations. In general, threat actors continue to evolve their tactics, techniques, and procedures (TTPs) to achieve their goals. HC3 recommends various mitigations outlined in this alert, which involve user awareness training, as well as policies and procedures for increased security for identity verification with help desk requests.

Report

Social engineering is being used across the Healthcare and Public Health (HPH) sector to gain unauthorized access to systems. Threat actors are employing sophisticated social engineering techniques to target an organization's IT help desk with phone calls from an area code local to the target organization, claiming to be an employee in a financial role (specifically in revenue cycle or administrator roles). The threat actor is able to provide the required sensitive information for identity verification, including the last four digits of the target employee's social security number (SSN) and corporate ID number, along with other demographic details. These details were likely obtained from professional networking sites and other publicly available information sources, such as previous data breaches. The threat actor claimed that their phone was broken, and therefore could not log in or receive MFA tokens. The threat actor then successfully convinced the IT help desk to enroll a new device in multi-factor authentication (MFA) to gain access to corporate resources.

After gaining access, the threat actor specifically targeted login information related to payer websites, where they then submitted a form to make ACH changes for payer accounts. Once access has been gained to employee email accounts, they sent instructions to payment processors to divert legitimate payments to attacker-controlled U.S. bank accounts. The funds were then transferred to overseas accounts. During the malicious campaign, the threat actor also registered a domain with a single letter variation of the target organization and created an account impersonating the target organization's Chief Financial Officer (CFO).

Analysis

There was a recent high profile incident leveraging these social engineering techniques to target an organization in the hospitality and entertainment industry in September 2023. While the threat actor Scattered Spider (also known as UNC3944) claimed responsibility for this attack, which led to the deployment of ALPHV (also known as BlackCat) ransomware, there is currently no public attribution for the incident in the health sector.

While these recent campaigns in the health sector did not involve ransomware, both of these incidents did leverage spearphishing voice techniques and impersonation of employees with specific access related to the threat actors' end goals. Spearphishing voice (T1566.004) is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of manipulating a user into providing access to systems through a phone call or other forms of voice communications. Spearphishing frequently involves social engineering techniques, such as posing as a trusted source (impersonation) and/or creating a sense of urgency or alarm for the recipient.

It is important to note that threat actors may also attempt to leverage AI voice impersonation techniques to social engineer targets, making remote identity verification increasingly difficult with these technological

advancements. A recent global study found that out of 7,000 people surveyed, one in four said that they had experienced an AI voice cloning scam or knew someone who had.

Patches, Mitigations, and Workarounds

Various mitigations may be implemented by healthcare organizations, including requiring callbacks to the phone number on record for the employee requesting a password reset and enrollment of a new device. It is important to note that when attempting callbacks for verification, the threat actor may claim to be too busy to take a phone call. Other mitigations may involve monitoring for any suspicious ACH changes and revalidating all users with access to payer websites. Some hospitals have implemented procedures that require employees to appear in person at the IT help desk for such requests. Another suggestion is implementing policies that require the supervisor of the employee to be contacted to verify these requests. Additionally, users can be trained to identify and report social engineering techniques and spearphishing attempts, while also being suspicious of and verifying the identify of callers (M1017).

For organizations that are utilizing Entra ID (formerly Microsoft Azure Active Directory), the following recommendations from Mandiant have proven effective in mitigating against common UNC3944 TTPs, such as MFA abuse and unauthorized use of privileged accounts within the Microsoft cloud environment:

- Enforce Microsoft Authenticator with number matching and remove SMS as an MFA verification option.
- Remove SMS as a MFA verification option by clearing the checkbox for “Text message to phone” in the multi-factor authentication service settings dialog.
- To restrict MFA to only utilize Microsoft Authenticator with number matching, organizations will need to ensure they are at least in the “Migration In Progress” stage for leveraging authentication methods, and then appropriately configure the Microsoft Authenticator authentication method.
- Configure Microsoft Authenticator to require number matching for push notifications.
- Create a custom authentication strength that specifies **only** “Password + Microsoft Authenticator (Push Notification).”
- Create a new or edit an existing Conditional Access Policy to grant access only for the newly created authentication strength.
- Ensure MFA and SSPR registration is secure by requiring users to authenticate from a trusted network location and/or ensuring device compliance. Microsoft has documented how to accomplish this.
- Block external access to Microsoft Azure and Microsoft 365 administration features by creating a Conditional Access Policy that only allows access if users are authenticating from a trusted network location and/or ensuring device compliance. Read Microsoft’s documentation for securing MFA and SSPR registration as a template, except specify specific cloud apps instead of the User action. Add the following cloud apps to include: Microsoft Admin Portals (Preview), and Microsoft Azure Management. This can also be leveraged to further secure other capabilities, such as restricting access to Graph Explorer and Microsoft Graph PowerShell.

Relevant HC3 Products

HC3 Analyst Note, How to Identify Vishing/Phishing (August 19, 2022)
https://www.hhs.gov/sites/default/files/vishing-attacks-on-the-hph-sector-analyst-note.pdf

References

European Union Agency for Cybersecurity. "What is "Social Engineering"?" https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

Obsidian Security. "Behind The Breach: Social Engineering of Helpdesk Agents." Accessed January 19, 2024. https://www.obsidiansecurity.com/blog/behind-the-breach-social-engineering-helpdesk-agents/

Elevate Security. "How to Safeguard Your Help Desk from Social Engineering Attacks." https://elevatesecurity.com/how-to-safeguard-your-help-desk-from-social-engineering-attacks/

CyberTalk. "IT service desks targeted by social engineers." November 3, 2023. https://www.cybertalk.org/it-service-desks-targeted-by-social-engineers/

ThriveDX. "Investigating the MGM Cyberattack – How social engineering and a help desk put the whole strip at risk." October 6, 2023. https://thrivedx.com/resources/article/investigating-the-mgm-cyberattack-how-social-engineering-and-a-help-desk-put-the-whole-strip-at-risk

Ragan, Steve. "Why help desk employees are a social engineer's favorite target." July 17, 2013. https://www.csoonline.com/article/539410/social-engineering-why-help-desk-employees-are-a-social-engineer-s-favorite-target.html

Jones, David. "MGM, Caesars attacks raise new concerns about social engineering tactics." September 18, 2023. https://www.cybersecuritydive.com/news/mgm-caesars-attacks-social-engineering/693956/

American Hospital Association. "Hospital IT help desks targeted by sophisticated social engineering schemes." January 12, 2024. https://www.aha.org/news/headline/2024-01-12-hospital-it-help-desks-targeted-sophisticated-social-engineering-schemes

Service Desk Institute. "Protecting the IT Service Desk from Social Engineering Attacks." February 27, 2023. https://www.servicedeskinstitute.com/protecting-the-it-service-desk-from-social-engineering-attacks/

Bunn, Amy. "Artificial Imposters—Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam." May 15, 2023. https://www.mcafee.com/blogs/privacy-identity-protection/artificial-imposters-cybercriminals-turn-to-ai-voice-cloning-for-a-new-breed-of-scam/

Mandiant Intelligence. "Why Are You Texting Me? UNC3944 Leverages SMS Phishing Campaigns for SIM Swapping, Ransomware, Extortion, and Notoriety." September 15, 2023. https://www.mandiant.com/resources/blog/unc3944-sms-phishing-sim-swapping-ransomware

Mitre. "Phishing: Spearphishing Voice." Last modified October 15, 2023. https://attack.mitre.org/techniques/T1566/004/

Alder, Steve. "Hospital IT Help Desks Targeted in Sophisticated Payment Fraud Scam." https://www.hipaajournal.com/hospital-it-help-desk-scam/

Contact Information

HC3: Sector Alert

April 3, 2024 TLP:CLEAR Report: 202404031000

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback