Health Care Social Engineering Campaign

By Hayden Evans 4 April 2024

Published: 2024-04-04 · Archived: 2026-04-06 01:54:36 UTC

Key Points

- In early April 2024, ReliaQuest investigated numerous similar incidents targeting customers in the health care sector.
- We concluded that these intrusions form part of a new campaign targeting health care organizations with the goal of accessing banking information.
- The attacks used social engineering techniques against help desk staff to bypass account access controls.
- Security teams should review the provided recommendations, which include introducing additional verification measures for help desk requests, to defend against similar attacks.

In early April 2024, ReliaQuest responded to multiple similar customer incidents in which an adversary targeted health care organizations. In this ongoing campaign, the attacker gained access to the impacted companies by using social engineering techniques against help desk employees, prompting them to reset multifactor authentication (MFA) credentials. The attacks were highly targeted and shared the same infrastructure, techniques, victim department, and likely motivation.

Campaign Identification

In early April 2024, ReliaQuest investigated several intrusions impacting health care organizations that all featured similar tactics and infrastructure:

- Focusing on user accounts from the healthcare companies' Revenue Cycle Management (RCM) departments
- Using social engineering techniques against the targets' help desk employees after MFA blocked account access efforts
- Attempting to access bank accounts, likely to alter routing information (indicating a financial motivation)

These commonalities indicate that the incidents almost certainly represent a campaign being conducted by the same threat group. This conclusion corresponds with a notification released by Health ISAC (H-ISAC) on April 3, 2024, which highlighted the same attacker techniques.

We identified that the attacker's infrastructure involved several different hosting providers with remote desktop protocol (RDP) enabled, enabling the adversary to pivot to other hosting providers to change source location

during authentication events.

Attack Flow

Authentication Attempts: In each of the incidents we investigated, the adversary first attempted to authenticate to the organization's VPN portal via several user accounts belonging to employees in the RCM department. The authentication attempts failed due to location-based conditional access policies and the attacker's use of expired credentials, suggesting these login details had been obtained from prior breaches. This suggests the adversary highly likely conducted extensive reconnaissance prior to the attack: targeting specific users in the RCM department and using gathered account credentials to execute the campaign.

MFA Block: We observed the adversary changing their infrastructure to match the target organization's location, effectively bypassing the targets' location conditional access policies. After using the correct location and credentials to authenticate, the threat actor was then blocked by the organization's MFA measures.

Help Desk Contact: The attacker then contacted the organization's help desk to request a reset of the account's MFA. The threat actor provided personal information associated with the target user to help desk staff (again highlighting the extensive resource development involved in the campaign). The adversary provided the last four digits of the user's social security number, their date of birth, and their address, satisfying validation requirements. Next, they registered a new MFA device or changed the MFA method to authenticate successfully and then reset the account's password to maintain persistence.

Bank Account Access: After compromising the targeted account, the attacker accessed the victim's Outlook inbox and deleted emails containing password reset notifications. The attacker proceeded to search through the account's emails and SharePoint for sensitive information. They then generated a one-time password to access a banking portal, likely to find and alter the bank account's routing information.

After the intrusion was identified, the ReliaQuest Threat Hunting team worked with the impacted customers to contain the incidents and eradicate the adversary's access.

Threat Forecast

As technical controls become more resilient and deny initial access, adversaries will adapt to use alternative techniques—such as social engineering—to compromise victims. By blending in as a regular user, attackers employing such methods effectively bypass security controls like endpoint detection and response (EDR) systems and behavioral analytics. It is realistically possible that voice-generated artificial intelligence will further enable attackers to target organizations and conduct social engineering by impersonating legitimate users, regardless of language barriers. This campaign emphasizes the need for organizations to adapt to the changing threat by implementing further verification for help desk requests and authentication from anomalous devices.

What ReliaQuest Is Doing

After identifying the shared attacker infrastructure, the ReliaQuest Threat Hunting team initiated hunts across the environments of customers in the healthcare industry and has notified impacted organizations. ReliaQuest has

added the IOCs we observed as part of this campaign to the GreyMatter threat feed, to enable customers to detect malicious activity associated with this campaign.

Recommendations and Best Practices

- Implement stricter controls for help desk requests with an emphasis on multifactor device resets. Additional controls could include video verification and verification by management.
- Introduce additional process controls around help desk requests for identity administrators (Okta, Entra, etc.), and extend these controls to finance and finance-adjacent roles for the immediate future. These controls could include additional identity verification steps and escalation to administrators for authorization.
- Use device certificate-based authentication for VPNs.
- Create device-based and location-based conditional access controls
- Refrain from directly providing the help desk phone number or hyperlinks to help desk and password reset procedures on login portals.

IOCs

- 74.50.79[.]78
- 45.126.208[.]87
- 66.23.206[.]199
- 170.130.55[.]159
- 69.50.92[.]18
- 105.112.179[.]134
