HC3: Sector Alert

March 18, 2024 TLP:CLEAR Report: 202403181500

Credential Harvesting and Mitigations

Executive Summary

Cyberattacks against healthcare facilities can involve credential harvesting, which may lead to a disruption of operations. Credential harvesting, also known as credential stealing or credential phishing, is a technique that cybercriminals can use to obtain sensitive login credentials like usernames, passwords, and personal information. These credentials operate as the gateway to an individual's digital identity, and can grant access to various types of information, such as online accounts and health data. The methods employed for credential harvesting are diverse, ranging from sophisticated phishing emails to fake websites and social engineering tactics.

Report

The healthcare sector commonly makes use of digital technologies to manage patient data, streamline operations, and enhance medical services. Credential harvesting refers to the process of stealing user authentication credentials for malicious purposes. Attackers can employ various techniques to obtain these credentials, including phishing, keylogging, and brute force attacks. Once acquired, these credentials can be used to gain unauthorized access to sensitive data, systems, or networks. There are multiple ways attackers can accomplish credential harvesting, and their goal is to convince a user to enter their login credentials into a malicious outlet, enabling the attacker access to the user's account.

- **Phishing:** Phishing attacks involve sending deceptive emails or messages that appear to be from legitimate sources. These emails aim to trick users into providing their login credentials on fake websites or through other means.
- **Keylogging:** Keyloggers are malicious software or hardware that record keystrokes entered by users, capturing sensitive information such as usernames and passwords.
- **Brute Force Attacks:** In brute force attacks, attackers systematically try numerous combinations of usernames and passwords until they discover the correct credentials to access a system or account.
- **Person-in-the-Middle (PITM) Attacks:** In PITM attacks, hackers intercept communication between two parties, capturing login credentials exchanged during the authentication process.
- **Credential Stuffing:** Attackers use previously compromised credentials to gain unauthorized access to other accounts where users have recycled the same username and password.

Credential harvesting can lead to data breaches, exposing patients' confidential information, including medical records, personal details, and other types of data. These breaches are capable of impacting patient privacy, and can negatively impact healthcare operations by giving an attacker access to deploy malware or conduct other nefarious operations. Accessing healthcare systems through credential harvesting can disrupt critical services, such as patient care delivery and administrative functions. System downtime and compromised infrastructure can impede medical professionals' abilities to access essential resources and provide timely care.

Impact to the HPH Sector

Credential harvesting is capable of disrupting normal operations, impeding the delivery of vital services and patient care. When systems are compromised, entities may experience downtime, inability to access

critical patient data, and disruptions in communication. These actions can lead to delays in appointments, procedures, and administration services. Additionally, these harvested credentials can be used to manipulate data in entity systems.

Patches, Mitigations, and Workarounds

Credential harvesting poses a significant threat to the security and integrity of healthcare systems, potentially compromising patient confidentiality. By implementing a combination of technical controls, user awareness training, and proactive security measures, healthcare organizations can mitigate the risks associated with credential harvesting, and protect sensitive data from unauthorized access.

- **Employee Training and Awareness:** Educating healthcare staff about phishing threats and best practices for identifying suspicious emails and websites is crucial in mitigating the risk associated with credential harvesting.
- **Multi-Factor Authentication (MFA):** MFA adds an additional layer of security by requiring users to provide multiple forms of authentication, reducing the effectiveness of credential harvesting attacks.
- **Email Filtering and Spam Detection:** Deploying email filtering solutions can help identify and block phishing emails before they reach end-users.
- **Monitoring and Detection:** Implementing robust monitoring tools to detect suspicious login attempts, unusual user behavior, or unauthorized access can help identify credential harvesting attacks in real-time.
- **Endpoint Security Solutions:** Utilizing endpoint security solutions can help detect and prevent malware-based credential harvesting techniques like keylogging.
- **Patch Management:** Keeping software and systems up-to-date with the latest security patches and updates can help address known vulnerabilities that attackers may exploit to harvest credentials.
- **Incident Response Planning:** Developing comprehensive incident response plans can enable prompt and effective strategies to minimizing the impact on operations and patients.

References

Iato. June 1, 2023. https://iatro.health/top-phishing-scams-used-to-attack-healthcare-organisations/#:~:text=Credential%20harvesting%20phishing%20attacks%20focus,unauthorised%20access%20to%20healthcare%20systems.

Lenaerts-Bergmans, Bart. July 19, 2023. Crowdstrike. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/credential-harvesting/

Descope. November 27, 2023. https://www.descope.com/learn/post/credential-harvesting

DataDome. How to Detect & Prevent Credential Harvesting Attacks in 2024. https://datadome.co/learning-center/how-to-detect-prevent-credential-harvesting-attacks/

Sjouwerman, Stu. SecurityBoulevard. February 02, 2024. Credential Harvesting Vs. Credential Stuffing Attacks: What's the Difference?. https://securityboulevard.com/2024/02/credential-harvesting-vs-credential-stuffing-attacks-whats-the-difference/

Cybersecurity Incident Response Plans. HC3. October 12, 2023.
https://www.hhs.gov/sites/default/files/cybersecurity-incident-response-plans.pdf

Contact Information

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