HC3: Analyst Note
December 17, 2024 TLP:CLEAR Report: 202412171700

Credential Harvesting

Executive Summary
Threat actors are currently conducting a credential harvesting campaign targeting grantees in the health sector, as well as across other industry verticals. Credential harvesting is a technique leveraged by cyberattackers to collect legitimate usernames and passwords from unwitting victims for the purposes of using them in future attacks. The end result can be fraud, data theft, disruption of critical systems, or other malicious impacts. This document includes defense and mitigation recommendations that will assist an organization in minimizing risk against such attacks.

Credential Harvesting
Credential harvesting refers to the process by which cyberattackers collect sensitive information, typically usernames, passwords, and other authentication data, from individuals or systems to gain unauthorized access to accounts, systems, networks, or services. This technique is often leveraged as the initial step of what is ultimately a more complex and egregious, larger-scale cyberattack. Credential harvesting can enable adversaries to obtain initial access, escalate privileges, exfiltrate sensitive data, disrupt systems, or engage in any number of additional malicious activities such as identity theft or financial fraud. Credential harvesting is often carried out via the following techniques:

- Phishing: The use of phony e-mails designed to look legitimate in order to entice the victim recipient to click a link or open an attachment in the e-mail, which would deliver malicious code to the victim's system and continue the cyberattack.
- Man-in-the-Middle Attacks: These are any attack where the user's credentials are captured while they are being transmitted for legitimate purposes as part of a valid login attempt.
- Keylogging: Malicious software can be deployed by cyberattackers to intercept a victim's keystrokes. This can include credentials as they are being entered as part of a valid login attempt.
- Credential Stuffing: Large datasets are frequently leaked, often as a result of a cyberattack. They can be posted for the public to access, or they can be bought and sold on the dark web. When a malicious actor obtains exposed credentials, they will use these same credentials in attempting to compromise another account associated with the same individual. This attack is predicated on the idea that individuals sometimes rely on password re-use, which is the tendency to re-use the same credentials, especially passwords, across many platforms due to the inability to memorize many different paswords. Credential stuffing is the use of compromised credentials associated with an individual to try and compromise other accounts associated with that individual.
- Social Engineering: This is the use of social manipulation techniques to convince unwitting individuals to reveal their credentials. Malicious actors often attempt to impersonate a help desk empolyee or an authority figure to conduct social engineering.
- Phony Login Webpages: Also known as pharming, or a watering hole attack, this is a webpage designed to look legitimate, often with a username/password login prompt. When a victim enters their credentials, they are often presented with a message that the site is temporarily down, all while their credentials have been recorded by the threat actor.
- Malware: This is malicious software that can collect victim credentials and report them back to the threat actor.

Credential harvesting can be tracked by the MITRE ATT&CK framework as Credential Access (ID: TA0006), Gather Victim Identity Information: Credentials (ID: T1589.001), OS Credential Dumping (ID: T1003).

HC3: Analyst Note
December 17, 2024 TLP:CLEAR Report: 202412171700

Defense and Mitigations

Credential harvesting is a technique leveraged by cyberattackers to collect legitimate usernames and passwords from unwitting victims for the purposes of using them in future attacks. The end result can be attacks that lead to data theft, disruption of critical systems, or other malicious impacts. There are a number of defense and mitigation steps to take when protecting against credential harvesting attacks, some of the more important are as follows:

- Educating Your Workforce: Ensure your workforce understands the following steps they can take to protect themselves as individuals, as well as your organization:
  - Use strong passwords (avoid personal details or anything easy to guess).
  - Do not re-use passwords across multiple accounts; this is a common practice that facilitates the success of credential harvesting.
  - Be reasonably sceptical and cautious when handling suspicious-looking e-mails; learn to recognize a phishing attack.
  - Be reasonably sceptical and cautious when handling suspicious phone calls; learn to recognize a social engineering attack.
  - Be cautious about suspicious-looking websites; always ensure you are submitting credentials to the proper site/application.
  - When in doubt of any form of communication, verify first.
- Multi-Factor Authentication (MFA): This requirement for multiple means of authentication can minimize the probability of a compromise, because if one factor (such as a password) is compromised, another is still required to access a system.
- E-mail/Malspam Filtering: Filters can be deployed and properly configured, which minimizes the amount of unwanted traffic flowing into your organization. Phishing is one of the most prolific infection vectors used by cyberattackers, and proper filtering can minimize associated risk.
- Endpoint Security: Utilizing endpoint security solutions can help detect and prevent malware-based credential harvesting techniques such as keylogging.
- Monitoring/Detection: Real time, comprehensive event and incident analysis across an enterprise infrastructure can help identify credential harvesting attacks as they occur. Leveraging appropriate tools and maintaining appropriately trained staff will improve this capability.
- Vulnerability/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. Maintaining a comprehensive and accurate inventory of all IT assets will improve the probability of success in this area.
- Incident Handling/Response: Developing and maintaining a full-lifecycle incident handling and response program (which should function closely with monitoring/detection above) can minimize the impact of credential harvesting on operations and patients.

HC3 has released a credential harvesting sector alert with additional analysis and recommendations.

References

HC3 Sector Alert: Credential Haarvesting and Mitigations
https://www.hhs.gov/sites/default/files/credential-harvesting-sector-alert-tlpclear.pdf

Digital Identity Guidelines

https://pages.nist.gov/800-63-3/

Using Rigorous Credential Control to Mitigate Trusted Network Exploitation
https://www.cisa.gov/news-events/alerts/2018/10/03/using-rigorous-credential-control-mitigate-trusted-network

What Is Credential Harvesting?
https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/credential-harvesting/?srsltid=AfmBOops_5_mPzlTp0lDNhgOOCNbc__xegSKCpyzW0pMR0-0tD0rWWIe

How does email security prevent credential harvesting?
https://www.trellix.com/security-awareness/email/how-does-email-security-prevent-credential-harvesting/

X-Force report reveals top cloud threats: AITM phishing, business email compromise, credential harvesting and theft
https://www.ibm.com/blog/x-force-cloud-threat-landscape/

BlueVoyant Identifies Credential Harvesting Campaign Targeting the Manufacturing Sector
https://www.bluevoyant.com/blog/credential-harvesting-campaign-targeting-the-manufacturing-sector

How a SOC Handles Credential Harvesting
https://datashieldprotect.hubspotpagebuilder.com/blog/how-datashield-handles-credential-harvesting

Analysing a Widespread Microsoft 365 Credential Harvesting Campaign
https://www.bridewell.com/insights/blogs/detail/analysing-widespread-microsoft365-credential-harvesting-campaign

Train End-Users to Report Credential Harvesting Attacks
https://5569894.fs1.hubspotusercontent-na1.net/hubfs/5569894/Marketing%20downloads/Credential%20Harvesting%20Simulations%20-%20data%20sheet.pdf

Credential Harvesting at Scale Without Malware
https://unit42.paloaltonetworks.com/credential-harvesting/

Department pf Health and Human Services: Health Industry Cybersecurity Practices
https://405d.hhs.gov/cornerstone/hicp

Healthcare data breaches hit all-time high in 2021, impacting 45M people
https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people

Contact Information

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

HC3: Analyst Note

December 17, 2024 TLP:CLEAR Report: 202412171700

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