Credential Theft Prevention: Understanding the Basics
Crime and theft, especially of information, have evolved over the past few years. The sheer frequency of cybercrime means that your information is never safe, especially if you do not go above and beyond in protecting it. One of the most common and most damaging forms of cybercrime is ransomware, which is commonly preceded by a credential-based attacker credential theft.

Credential theft is a type of cybercrime that involves the theft of a victim’s proof of identity. When the cybercriminal has access to this proof of identity, they get the same privileges as the victim. This theft places one’s data and systems in serious jeopardy. Cybercriminals typically target the victim’s critical administrative systems and their backups. Admin credentials give cybercriminals access to systems in ways that enable them to implant ransomware and malware. Further, access to one’s backup can also be devastating. It gives the cybercriminals the ability to destroy the backups before launching the ransomware attack, leaving the system with no recourse. Such cybercrimes are especially serious for attractive accounts.

Credential theft attacks will allow the cybercriminal to gain the highest privilege, the root, system, or administrator accounts depending on the operating system being used. They can then use various tools and techniques to extract credentials from other logged-on accounts. Some of the actions credential theft attackers can perform include the following:

- Run malicious software
- Install remote access software
- Lock administrators out of the backup software
- Delete backups
- Install rootkits
- Move laterally to then gain access to other, potentially higher privilege accounts
- Change backup job retention settings

From a business standpoint, credential theft prevention is very important. According to the US Securities and Exchange Commission (SEC), up to 60% of small and medium enterprises will go out of business within 6 months following a data breach. These kinds of businesses are the principal target of such types of cybercrimes, and often suffer the most significant reputational and financial hits from them. Therefore, it is important to understand what credential theft is and the various techniques that cybercriminals typically use.

### Types of Credential Theft and Techniques

There are many different techniques through which credential theft is perpetrated. Cybercrime techniques are always evolving, and this is by no means an exhaustive list. However, these are the major methods through which credential theft is perpetrated.

**Memory dump:** A memory dump is a process of taking all the content that is written on the RAM and writing it onto a storage device. In normal circumstances, developers use memory dumps to gather information in the case of an unrecoverable error. However, memory dumps can also be used in
cybercrimes, where the information is used to capture credentials.

**OS credential dumping:** Operating systems will store user credentials & passwords in memory so that users don’t have to repeatedly input their password to access system resources. Cybercriminals will dump this data from the memory. These credentials can then be used to perform lateral movement and gain access to other forms of restricted information.

**Signing in to unsecured computers with privileged accounts:** This is when cybercriminals gain access to a lower privileged user device, and then request IT support. When an IT admin signs in with their account to assist, the credentials are stolen from the less secure device.

**Signing in to compromised workstations:** When users or a system admin signs into a workstation that has been compromised they can then easily have their credentials harvested.

**Sharing administrative account credentials:** Sharing credentials is one of the easiest ways to compromise workstation and systems. When administrative account credentials are shared, they are easy to access by cybercriminals.

**Browsing the internet with privileged accounts:** Cybercriminals are constantly on the prowl for weaknesses, especially for those that have or use attractive accounts. When a user browses the internet using privileged accounts, this places them at risk of compromise and attacks. Such risks are also heightened when the user overuses privileged accounts in ways that make it easy for cybercriminals to understand their patterns of use.

**Access to too many privileged systems for the job:** When a user has access to too many privileged accounts there are more chances for an account to be compromised.

**Cookie theft:** Cookie theft can happen in situations where a third party uses or copies unencrypted session data. This is then used to impersonate the real user. This often happens in situations where a user accesses their accounts over an unprotected or public network where the traffic can be accessed by anyone.

**Amazon AWS access and security keys theft:** The theft of security keys or Amazon AWS credentials/access keys is another way through which credential theft happens. Keeping AWS keys safe is one of the most important things one can do. Security holes used to steal credentials leave systems and data under threat.

**Remote access application credential theft:** This is where credentials are stolen using applications that allow for remote access to a user’s account.

**Windows reboot, Safe Mode cybercrimes:** This is the kind of cybercrime that uses the Windows diagnostic feature Safe Mode. When cybercriminals have access to an already compromised PC or server, they can use a remote attack vector to steal credentials.

**Elevated permissions in automated systems:** Elevated permission cybercrimes in automated systems allow an individual to exploit systems for their own illicit benefits. The elevated permissions allow cybercriminals or individuals with limited access to the systems to increase the scope and scale of their access permissions.

**Phishing emails:** These are cybercrimes that take advantage of the human vulnerabilities of individuals. They will steal credentials by getting the individual to reveal themselves. The cybercriminals will typically pose as legitimate websites and when clicked, lead to the revelation of the information, often unknowingly.

**Pass the hash:** The cybercriminal steals the hashed credentials and uses them to create a new user session on the same network, without necessarily having to crack the password.

**Keyloggers:** Keylogging is when the keystroke entries made on a computer are logged revealing sensitive information, including IDs and passwords as they are typed.
Shoulder surfing: Shoulder surfing on the other hand makes use of physical observation techniques to get pertinent information.

Solutions and Best Practice
Having understood the various ways and techniques used to perpetrate credential theft cybercrimes, one should also understand the potential solutions and techniques that could be used to prevent these cybercrimes.

Dark Web Monitoring
One of the techniques used includes dark web monitoring and leaked password monitoring. This is where one monitors the dark web to determine whether their systems were compromised or breached. There are several websites and tools that allow one to scan the dark web and determine whether their personal information, including passwords and usernames, shows up in data breaches. Typically, ransomware attackers start with previously stolen credentials that they acquire from other attackers. Monitoring can provide you with an early warning that your systems are at risk.

 Restricted Admin for RDC
While the monitoring of the dark web is useful, it can only work after the fact. It is important to know about cybercrimes and compromised data as soon as the attacks happen. However, there are proactive potential solutions available, including the use of the restricted admin mode for remote desktop connections (RDC).

RDC refers to the technology that allows a local computer to connect to and control another computer over a network. Restricted admin mode prevents the transmission of reusable credentials to the remote system. Even if malware or a malicious user is active on the remote server, credentials will not be available on the remote desktop server for the malware to attack.

LSA Protection
Another proactive protection technique is LSA protection. LSA, or Local Server Authority protection, also includes the LSASS (Local Security Authority Server Service) process. This protection system validates users for local and remote sign-ins and helps enforce local security policies. The LSA also controls and manages user rights information and password hashes, among other sensitive bits of information in memory.

User Training & Password Management
A lot of breaches can be prevented with increased end user training and the recommended use of password management systems. Many users reuse passwords among many online systems and if one is breached then all their services are at risk. Encouraging strong password use, unique passwords for each service, and the use of a password management tool to help them comply can minimize this cross contamination. In addition to this, encouraging multi-factor authentication can prevent breaches and provide a warning that a credential has been compromised.
How Asigra Protects Your Backups From Compromised Credentials

Despite increasing your diligence, protection and training it’s still possible that your admin credentials could become compromised. In the worst-case scenario, if attackers have access to your admin credentials, they can create all kinds of havoc, especially to your backups.

This is where Asigra comes in with a hyper focus on backup security, anti-ransomware protection, and breach defense. Some of the strategies Asigra uses to prevent and protect clients from credential theft attacks include the following:

**MFA/MPA:** MFA/MPA is a multifactor authorization and multiperson approval system that can easily be used to protect systems and backups from ransomware attacks. It involves the addition of MFA/MPA to critical backup tasks that affect the data.

If a backup admin’s credentials are compromised and their MFA notification has been intercepted, additional MFA/MPA requests may notify the administrator that bad actors have access to the backup system. If an attacker tries to delete backup jobs an additional MFA/MPA request can also be sent to a senior admin, providing an increased chance the attack will be prevented.

**Soft Delete:** If attackers are intercepting all MFA notifications, they may have access to delete data. Asigra lets the attacker think they’ve succeeded, by creating a “false delete” or soft delete. This is where the data will be marked as unusable, without deleting the backup data.

An actual deletion takes a 2-step process that is hidden from unaware cybercriminals accessing the environment as administrators. This provides an additional layer of protection for the data in the recovery process.

**Variable Repository Naming:** Attackers typically look for known backup vendor naming conventions for backup repositories once they have access to systems and storage, both for data exfiltration and deletion. Asigra allows backup administrators to create unique names for the backup repositories or obfuscate the repository name entirely through the generation of random names. This way, they cannot easily be identified and are protected against intrusions.

**Cybercrime is damaging but preventative measures can be taken, contact us!**

The danger of cybercrime and theft, especially credential theft, is huge and is always evolving. While there is no perfectly secure system, you will come as close as you can with the trusted professionals from Asigra.

Let us help you manage cyberattacks while you focus on running your business. Contact us online today to learn more or call (416) 736-8111 or 1 (877) 736-9901.