Attractive Accounts for Credential Theft

By robinharwood

Archived: 2026-04-05 23:50:06 UTC

Credential theft attacks are those in which an attacker initially gains highest-privilege (root, Administrator, or SYSTEM, depending on the operating system in use) access to a computer on a network and then uses freely available tooling to extract credentials from the sessions of other logged-on accounts. Depending on the system configuration, these credentials can be extracted in the form of hashes, tickets, or even plaintext passwords. If any of the harvested credentials are for local accounts that are likely to exist on other computers on the network (for example, Administrator accounts in Windows, or root accounts in OSX, UNIX, or Linux), the attacker presents the credentials to other computers on the network to propagate compromise to additional computers and to try to obtain the credentials of two specific types of accounts:

1. Privileged domain accounts with both broad and deep privileges (that is, accounts that have administrator-level privileges on many computers and in Active Directory). These accounts may not be members of any of the highest-privilege groups in Active Directory, but they may have been granted Administrator-level privilege across many servers and workstations in the domain or forest, which makes them effectively as powerful as members of privileged groups in Active Directory. In most cases, accounts that have been granted high levels of privilege across broad swaths of the Windows infrastructure are service accounts, so service accounts should always be assessed for breadth and depth of privilege.

2. "Very Important Person" (VIP) domain accounts. In the context of this document, a VIP account is any account that has access to information an attacker wants (intellectual property and other sensitive information), or any account that can be used to grant the attacker access to that information. Examples of these user accounts include:

    1. Executives whose accounts have access to sensitive corporate information

    2. Accounts for Help Desk staff who are responsible for maintaining the computers and applications used by executives

    3. Accounts for legal staff who have access to an organization's bid and contract documents, whether the documents are for their own organization or client organizations

    4. Product planners who have access to plans and specifications for products in an company's development pipeline, regardless of the types of products the company makes

    5. Researchers whose accounts are used to access study data, product formulations, or any other research of interest to an attacker

Because highly privileged accounts in Active Directory can be used to propagate compromise and to manipulate VIP accounts or the data that they can access, the most useful accounts for credential theft attacks are accounts

that are members of Enterprise Admins, Domain Admins, and Administrators groups in Active Directory.

Because domain controllers are the repositories for the AD DS database and domain controllers have full access to all of the data in Active Directory, domain controllers are also targeted for compromise, whether in parallel with credential theft attacks, or after one or more highly privileged Active Directory accounts have been compromised. Although numerous publications (and many attackers) focus on the Domain Admins group memberships when describing pass-the-hash and other credential theft attacks (as is described in Reducing the Active Directory Attack Surface), an account that is a member of any of the groups listed here can be used to compromise the entire AD DS installation.

Because the target of credential theft is usually highly privileged domain accounts and VIP accounts, it is important for administrators to be conscious of activities that increase the likelihood of success of a credential-theft attack. Although attackers also target VIP accounts, if VIPs are not given high levels of privilege on systems or in the domain, theft of their credentials requires other types of attacks, such as socially engineering the VIP to provide secret information. Or the attacker must first obtain privileged access to a system on which VIP credentials are cached. Because of this, activities that increase the likelihood of credential theft described here are focused primarily on preventing the acquisition of highly privileged administrative credentials. These activities are common mechanisms by which attackers are able to compromise systems to obtain privileged credentials.

The core vulnerability that allows credential theft attacks to succeed is the act of logging on to computers that are not secure with accounts that are broadly and deeply privileged throughout the environment. These logons can be the result of various misconfigurations described here.

Although this is relatively uncommon, in assessing various AD DS installations, we have found IT employees using a single account for all of their work. The account is a member of at least one of the most highly privileged groups in Active Directory and is the same account that the employees use to log on to their workstations in the morning, check their email, browse Internet sites, and download content to their computers. When users run with accounts that are granted local Administrator rights and permissions, they expose the local computer to complete compromise. When those accounts are also members of the most privileged groups in Active Directory, they expose the entire forest to compromise, making it trivially easy for an attacker to gain complete control of the Active Directory and Windows environment.

Similarly, in some environments, we've found that the same user names and passwords are used for root accounts on non-Windows computers as are used in the Windows environment, which allows attackers to extend compromise from UNIX or Linux systems to Windows systems and vice versa.

When a highly privileged domain account is used to log on interactively to a compromised workstation or member server, that compromised computer may harvest credentials from any account that logs on to the system.

In many organizations, IT staff use multiple accounts. One account is used for logon to the employee's workstation, and because these are IT staff, they often have local Administrator rights on their workstations. In some cases, UAC is left enabled so that the user at least receives a split access token at logon and must elevate when privileges are required. When these users are performing maintenance activities, they typically use locally installed management tools and provide the credentials for their domain-privileged accounts, by selecting the **Run**

as Administrator option or by providing the credentials when prompted. Although this configuration may seem appropriate, it exposes the environment to compromise because:

- The "regular" user account that the employee uses to log on to their workstation has local Administrator rights, the computer is vulnerable to drive-by download attacks in which the user is convinced to install malware.
- The malware is installed in the context of an administrative account, the computer can now be used to capture keystrokes, clipboard contents, screenshots, and memory-resident credentials, any of which can result in exposure of the credentials of a powerful domain account.

The problems in this scenario are twofold. First, although separate accounts are used for local and domain administration, the computer is unsecured and does not protect the accounts against theft. Second, the regular user account and the administrative account have been granted excessive rights and permissions.

Users who log on to computers with accounts that are members of the local Administrators group on the computer, or members of privileged groups in Active Directory, and who then browse the Internet (or a compromised intranet) expose the local computer and the directory to compromise.

Accessing a maliciously crafted website with a browser running with administrative privileges can allow an attacker to deposit malicious code on the local computer in the context of the privileged user. If the user has local Administrator rights on the computer, attackers may deceive the user into downloading malicious code or opening email attachments that leverage application vulnerabilities and leverage the user's privileges to extract locally cached credentials for all active users on the computer. If the user has administrative rights in the directory by membership in the Enterprise Admins, Domain Admins, or Administrators groups in Active Directory, the attacker can extract the domain credentials and use them to compromise the entire AD DS domain or forest, without needing to compromise any other computer in the forest.

Configuring the same local Administrator account name and password on many or all computers enables credentials stolen from the SAM database on one computer to be used to compromise all other computers that use the same credentials. At a minimum, you should use different passwords for local Administrator accounts across each domain-joined system. Local Administrator accounts may also be uniquely named, but using different passwords for each system's privileged local accounts is sufficient to ensure that credentials cannot be used on other systems.

Granting membership in the EA, DA, or BA groups in a domain creates a target for attackers. The greater the number of members of these groups, the greater the likelihood that a privileged user may inadvertently misuse the credentials and expose them to credential theft attacks. Every workstation or server to which a privileged domain user logs on presents a possible mechanism by which the privileged user's credentials may be harvested and used to compromise the AD DS domain and forest.

Domain controllers house a replica of a domain's AD DS database. In the case of read-only domain controllers, the local replica of the database contains the credentials for only a subset of the accounts in the directory, none of which are privileged domain accounts by default. On read-write domain controllers, each domain controller maintains a full replica of the AD DS database, including credentials not only for privileged users like Domain Admins, but privileged accounts such as domain controller accounts or the domain's Krbtgt account, which is the

account that is associated with the KDC service on domain controllers. If additional applications that are not necessary for domain controller functionality are installed on domain controllers, or if domain controllers are not stringently patched and secured, attackers may compromise them via unpatched vulnerabilities, or they may leverage other attack vectors to install malicious software directly on them.

Regardless of the attack methods used, Active Directory is always targeted when a Windows environment is attacked, because it ultimately controls access to whatever the attackers want. This does not mean that the entire directory is targeted, however. Specific accounts, servers, and infrastructure components are usually the primary targets of attacks against Active Directory. These accounts are described as follows.

Because the introduction of Active Directory, it has been possible to use highly privileged accounts to build the Active Directory forest and then to delegate rights and permissions required to perform day-to-day administration to less-privileged accounts. Membership in the Enterprise Admins, Domain Admins, or Administrators groups in Active Directory is required only temporarily and infrequently in an environment that implements least-privilege approaches to daily administration.

Permanent privileged accounts are accounts that have been placed in privileged groups and left there from day to day. If your organization places five accounts into the Domain Admins group for a domain, those five accounts can be targeted 24-hours a day, seven days a week. However, the actual need to use accounts with Domain Admins privileges is typically only for specific domain-wide configuration, and for short periods of time.

An often overlooked target in Active Directory breaches is the accounts of "very important persons" (or VIPs) in an organization. Privileged accounts are targeted because those accounts can grant access to attackers, which allows them to compromise or even destroy targeted systems, as described earlier in this section.

"Privilege-attached" Active Directory accounts are domain accounts that have not been made members of any of the groups that have the highest levels of privilege in Active Directory, but have instead been granted high levels of privilege on many servers and workstations in the environment. These accounts are most often domain-based accounts that are configured to run services on domain-joined systems, typically for applications running on large sections of the infrastructure. Although these accounts have no privileges in Active Directory, if they are granted high privilege on large numbers of systems, they can be used to compromise or even destroy large segments of the infrastructure, achieving the same effect as compromise of a privileged Active Directory account.
