Unlocking Active Directory with the Skeleton Key Attack

blog.netwrix.com/2022/11/29/skeleton-key-attack-active-directory

Skeleton Key is a particularly scary piece of malware that makes it alarmingly easy for attackers to hijack any identity in a Microsoft Windows domain, including accounts that provide privileged access. This malware implants itself into LSASS and creates a master password that will work for any Active Directory account in the domain. Since users' current passwords also continue to work, a Skeleton Key attack won't disrupt the authentication process, so attacks are difficult to spot unless you know what to look for.

Handpicked related content:

[Free Guide] Active Directory Security Best Practices

Using Skeleton Key enables adversaries to use lateral movement techniques to leverage their current access privileges to navigate around the target environment, as well as to use privilege escalation strategies to gain increased access permissions to data and other resources and achieve persistence in the Active Directory forest.

Skeleton Key is one of several methods of attack that are packaged and very easy to perform using mimikatz. Let's take a look at how it works.

Requirements for the Skeleton Key Attack

In order to perpetrate a Skeleton Key attack, the attacker must have Domain Admin rights. For complete compromise, the attack must be performed on every domain controller, but targeting even a single domain controller can be effective. Rebooting a domain controller will remove the malware.

Performing the Skeleton Key Attack

Performing the attack is very straightforward. You need only to run the following command on each domain controller: **misc::skeleton**.

After that, you can authenticate as any user by providing the same password, which by default is “mimikatz”. If the authentication is performed for a member of the Domain Admin group, you can get administrative access to a domain controller:

Note: You might get the message, “System error 86 has occurred. The specified network password is not correct.” In that case, try supplying the username in domainaccount format.

Preventing and Detecting Skeleton Key Attacks

The best way to defend against these attacks is to reduce the number of Domain Admin accounts available in your environment for attackers to hijack, and to implement proper security controls around the few accounts that remain. More broadly, you should eliminate all types of standing privileged accounts in your environment to minimize your attack surface area. The Netwrix Privilege Secure solution strengthens AD security by enabling you to replace privileged accounts with temporary accounts that provide just enough access to perform the task at hand and that are removed immediately when the job is complete.

Other mitigation and detection methods are provided by Sean Metcalf from ADSecurity and by Dell SecureWorks in Skeleton Key Malware Analysis.

FAQ

What is a Skeleton Key attack?

Skeleton Key is a post-exploitation hacking technique that involves exploiting the Windows LSASS process to give adversaries a password (a “skeleton key”) that can be used with any domain account.

What are requirements for the Skeleton Key attack?

Skeleton Key requires attacker to have Domain Admin credentials.

How to mitigate skeleton key attack?

The best prevention for these attacks is to reduce the number of privileged accounts in your environment. It’s also wise to track modifications to your encryption settings and monitor Event IDs 7045, 4673, 4611 and 4611 for abnormalities.

Jeff Warren