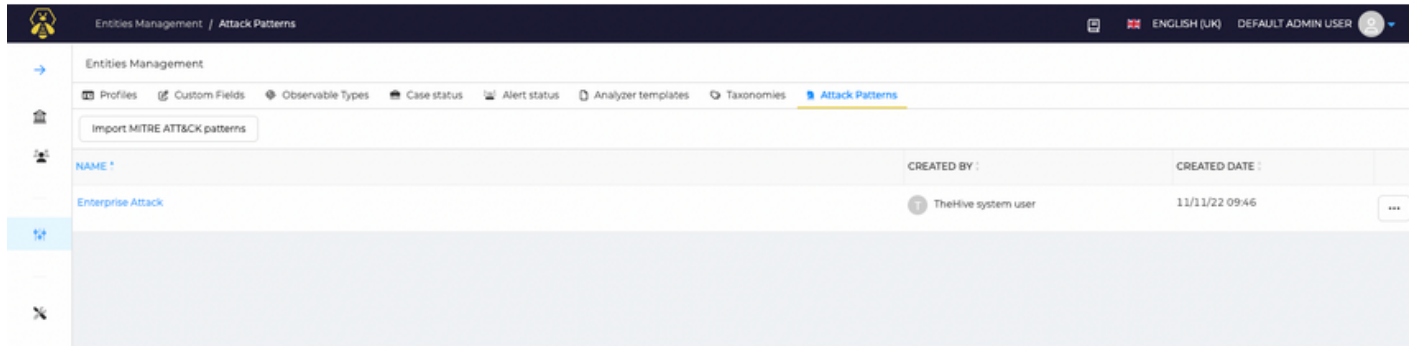


Att&ck Modelleri

Att&ck modelleri yapılandırması, Yönetici alanında mevcuttur: Varlıklar Yönetimi'ni açın, ardından Att&ck Modelleri sekmesine tıklayın.

Giriş

Varsayılan olarak, TheHive, MITRE'den Enterprise ATT&CK modelleri ile birlikte gelir. Bu, kurulum süreci sırasında yüklenir ve ilgili tüm tekniklerle birlikte Katalog adı Enterprise Attack oluşturulur.



Modelleri Görüntüle

Bir kataloğa dahil edilen modellerin ayrıntılarını görmek için bir kataloğa tıklayın.

The screenshot shows the 'Enterprise Attack' model details in the TheHive interface. The table lists various attack techniques with their IDs, names, sub-techniques, tactics, and descriptions.

ID	NAME	SUB-TECHNIQUE OF	TACTICS	DESCRIPTION
T1003.008	/etc/passwd and /etc/shadow	T1003	credential-access	Adversaries may attempt to dump the contents of /etc/passwd and /etc/shadow to enable offline password cracking. Most modern Linux operating systems use a combination of /etc/passwd and /etc/shadow [...]
T1557.002	ARP Cache Poisoning	T1557	collection, credential-access	Adversaries may poison Address Resolution Protocol (ARP) caches to position themselves between the communication of two or more networked devices. This activity may be used to enable follow-on behaviors such as
T1558.004	AS-REP Roasting	T1558	credential-access	Adversaries may reveal credentials of accounts that have disabled Kerberos preauthentication by Password Cracking Kerberos messages.(Citation: Harmj0y [...])
T1548	Abuse Elevation Control Mechanism		defense-evasion, privilege-escalation	Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. [...]
T1134	Access Token Manipulation		defense-evasion, privilege-escalation	Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access [...]

Her bir modelin tüm ayrıntıları teknik kimliğine tıklanarak incelenebilir

Entities Management / Attack Patterns / Enterprise Attack

Entities Management

ProfilesCustom FieldsObservable TypesCase statusAlert statusAnalyzer templatesTaxonomie

default

ID	NAME	SUB-TECHNIQUE OF	TACTIC
T1003.008	lsc/passwd and lsc/shadow	T1003	credential
T1557.002	ARP Cache Poisoning	T1557	collect
T1558.004	AS-REP Roasting	T1558	credential
T1548	Abuse Elevation Control Mechanism		defense, privilege
T1134	Access Token Manipulation		defense, privilege
T1015	Accessibility Features		
T1546.008	Accessibility Features	T1546	persist
T1531	Account Access Removal		impact
T1087	Account Discovery		discover
T1098	Account Manipulation		persist
T1583	Acquire Infrastructure		resource

T1546.008 - Accessibility Features

ID

T1546.008

Sub-technique Name

Accessibility Features

Sub-Technique of

Event Triggered Execution

Data Sources

Process: Process Creation
Windows Registry: Windows Regist...
Command: Command Execution
File: File Creation
File: File Modification

Permissions Required

Administrator

Remote Support

FALSE

Description

Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by accessibility features. Windows contains accessibility features that may be launched with a key combination before a user has logged in (e.g. when the user is on the Windows login screen). An adversary can modify the way these programs are launched to get a command prompt or backdoor without logging in to the system.

Two common accessibility programs are `C:\Windows\System32\sethc.exe`, launched when the shift key is pressed five times and `C:\Windows\System32\utilman.exe`, launched when the Windows + U key combination is pressed. The sethc.exe program is often referred to as "sticky keys", and has been used by adversaries for unauthenticated access through a remote desktop login screen. (Citation: FireEye Hikit Rootkit)

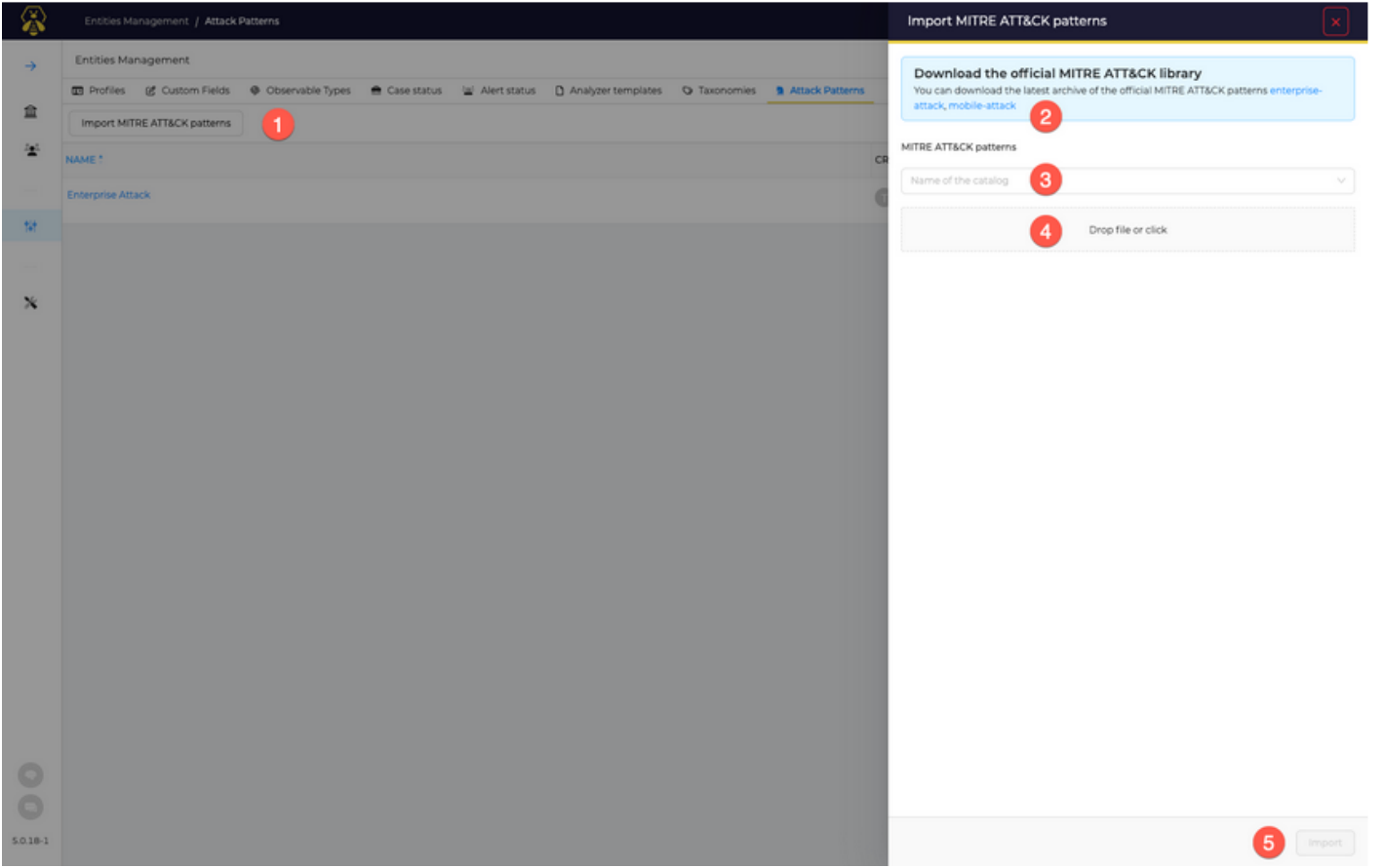
Depending on the version of Windows, an adversary may take advantage of these features in different ways. Common methods used by adversaries include replacing accessibility feature binaries or pointers/references to these binaries in the Registry. In newer versions of Windows, the replaced binary needs to be digitally signed for x64 systems, the binary must reside in `%systemdir%`, and it must be protected by Windows File or Resource Protection (WFR/WRP). (Citation: DEFCON2016 Sticky Keys) The `Image File Execution Options Injection` debugger method was likely discovered as a potential workaround because it does not require the corresponding accessibility feature binary to be replaced.

For simple binary replacement on Windows XP and later as well as Windows Server 2003/R2 and later, for example, the program (e.g., `C:\Windows\System32\utilman.exe`) may be replaced with "cmd.exe" (or another program that provides backdoor access). Subsequently, pressing the appropriate key combination at the login screen while sitting at the keyboard or when connected over `Remote Desktop Protocol` will cause the replaced file to be executed with SYSTEM privileges. (Citation: Tibbory 2014)

Other accessibility features exist that may also be leveraged in a similar fashion: (Citation: DEFCON2016 Sticky Keys) (Citation: Narrator Accessibility Abuse)

- * On-Screen Keyboard: `C:\Windows\System32\osk.exe`
- * Magnifier: `C:\Windows\System32\Magnify.exe`
- * Narrator: `C:\Windows\System32\Narrator.exe`
- * Display Switcher: `C:\Windows\System32\DisplaySwitch.exe`
- * App Switcher: `C:\Windows\System32\AtBroker.exe`

Kataloglar otomatik olarak güncellenmez, kurulum sırasında gelen Enterprise kataloğu da güncellenmez. Dolayısıyla, çerçevenin en son sürümlerinden yararlanmak istiyorsanız, bunları güncellemeniz gerekir.



Yeni bir katalog eklemek için:

1. "MITRE ATT&CK desenlerini içe aktar" üzerine tıklayın.
2. Kurmak istediğiniz desenleri seçin.
3. Yeni bir katalog oluşturuyorsanız bir katalog adı ekleyin veya güncellemek istediğiniz mevcut bir adı seçin.
4. İndirilen dosyayı sürükleyip bırakın.
5. İçe Aktar düğmesine tıklayın.

Bu işlemler biraz zaman alabilir.

Revision #2

Created 9 April 2024 11:07:20 by Güldeniz Akca

Updated 9 April 2024 18:14:05 by Güldeniz Akca