Stories from the SOC is a blog series that describes recent real-world security incident investigations conducted and reported by the AT&T SOC analyst team for AT&T Managed Threat Detection and Response customers.

Executive summary

The Windows 'Administrator' account is a highly privileged account that is created during a Windows installation by default. If this account is not properly secured, attackers may leverage it to conduct privilege escalation and lateral movement. When this account is used for administrative purposes, it can be difficult to distinguish between legitimate and malicious activity. Security best practice is to create and implement user accounts with limited privileges and disable the default 'Administrator' account on all machines.

The Managed Threat Detection and Response (MTDR) analyst team received 82 alarms involving the default 'Administrator' account successfully logging into multiple assets in the customer environment. The source asset attempting these logons was internal, successfully logging into multiple other internal assets within a short timeframe. Further investigation revealed the use of PowerShell scripts used for network share enumeration, account enumeration, and asset discovery.

Investigation

Initial alarm review

Indicators of Compromise (IOC)

An initial alarm was triggered by a built-in USM Anywhere rule named "Successful Logon to Default Account." This rule was developed by the Alien Labs team to trigger based on successful login attempts to default Windows accounts, captured by Windows Event Log. This alarm was the first indicator of compromise in this environment which prompted this investigation.

IoC initial

Expanded investigation

Events search

The customer confirmed in prior investigations that the default Administrator account is widely used for legitimate administrative purposes in this environment. How does one distinguish between administrative activity and malicious activity? Additional event searching must be conducted to provide more context into this login and the actions surrounding it. To do this, filters were utilized in USM Anywhere to query for events associated with the Administrator account on the affected asset.

Event deep dive

First, the account Security Identifier (SID) was used to confirm which account was being used for this login. The SID Is a Globally Unique Identifier (GUID) that is unique to each account on a Windows System. The default Administrator Security Identifier (SID) typically ends with the Relative Identifier (RID) of 500 on Windows Systems.

A review of the event attached to this alarm confirms that the default Administrator account was used to sign in, with a SID ending with the RID of 500.

Alarm default admin

To provide more context, events originating from the source asset were queried within the last 24 hours. 40 successful logins using the Administrator account were seen from this source to other internal assets in less than 10 minutes. default alarm events

These events were captured by the AlienVault Agent, which was installed directly on the source asset to forward events to USM Anywhere.

Reviewing for additional indicators

Further review into the activity originating from the source asset reveals the use of an encoded and compressed PowerShell script. Encoding and compression effectively allow the attacker to obfuscate scripts being executed, evading detection.

Using open-source tools, we were able to decode and decompress the underlying PowerShell script:

default account PowerShell

The decoded 'Invoke-ShareFinder' script seen above is a function used to query for exposed network shares in a Windows domain. This tool can also be used to determine which users have access to each network share. Exposed and insecure network shares could allow an attacker to obtain sensitive information or conduct lateral movement. An additional event was found for the PowerShell script "Discovery.psm1" being executed on this asset. This script is used for internal network discovery using various scanning techniques.

PowerShell script

Response

Building the investigation

With all events gathered and analysis completed, an investigation was created and submitted to the customer for review. Due to the severity of this incident and for situational awareness, a call was made to the customer to inform them of this activity.

Customer interaction

The customer took quick action to isolate the source asset, preventing further lateral movement attempts. Additionally, all affected assets were scanned using SentinelOne to ensure they were not infected with malware. Lastly, the default 'Administrator' account was disabled on all assets in this environment, effectively preventing future abuse of this account.

Limitations and opportunities

Limitations

The MTDR team lacked visibility into the customer's SentinelOne EDR environment, which would have allowed for additional context and quicker response action.

Opportunities

AT&T offers Managed Endpoint Security (MES), a tool that provides comprehensive endpoint protection against malware, ransomware, and fileless attacks. MES utilizes behavioral analysis, which would have alerted analysts of malicious activity and prevented the "Discovery" and "Invoke-ShareFinder" scripts from executing on the asset. MES can also be used to conduct response actions such as isolating and scanning affected assets.