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 Extended Detection and Response customers.

Executive summary

Once a malicious actor has gained initial access to an internal asset, they may attempt to conduct command and control activity. The 'Command and Control' (C&C) tactic, as identified by the MITRE ATT&CK© Framework, consists "of techniques that adversaries may use to communicate with systems under their control within a victim network." Cobalt Strike is an effective adversary simulation tool used in security assessments but has been abused by malicious actors for Command and Control of victim networks. If configured by attackers, it can be used to deploy malicious software, execute scripts, and more.

This investigation began when the Managed Extended Detection and Response (MXDR) analyst team received multiple alarms involving the detection of Cobalt Strike on an internal customer asset. Within ten minutes of this activity, the attacker launched a Meterpreter reverse shell and successfully installed remote access tools Atera and Splashtop Streamer on the asset. These actions allowed the attacker to establish multiple channels of command and control. In response, the MXDR team created an investigation and informed the customer of this activity. The customer determined that an endpoint detection and response (EDR) agent was not running on this asset, which could have prevented this attack from occurring. This threat was remediated by isolating the asset and scanning it with SentinelOne to remove indicators of compromise. Additionally, Cobalt Strike, Atera, and Splashtop Streamer were added to SentinelOne's blacklist to prevent unauthorized execution of this software in the customer environment.

Investigation

Initial alarm review

Indicators of Compromise (IOC)

An initial alarm was triggered by a Windows Defender detection of Cobalt Strike on an internal customer asset. The associated log was provided to USM Anywhere using NXLog and was detected using a Windows Defender signature. Multiple processes related to Cobalt Strike were attached to this alarm.

Cobalt Strike, as mentioned previously, is a legitimate security tool that can be abused by malicious actors for Command and Control of compromised machines. In this instance, a Cobalt Strike beacon was installed on the compromised asset to communicate with the attacker's infrastructure. Windows Defender took action to prevent these processes from running.

Immediately following the Cobalt Strike detection, an additional alarm was triggered for a Meterpreter reverse shell.

Meterpreter

A Meterpreter reverse shell is a component of the Metasploit Framework and requires the attacker to set up a remote 'listener' on their own infrastructure that 'listens' for connections. Upon successful exploitation, the victim machine connects to this remote listener, establishing a channel for the attacker to send malicious commands. A Meterpreter reverse shell can be used to allow an attacker to upload files to the victim machine, record user keystrokes, and more. In this instance, Windows Defender also took action to prevent this process from running.

Expanded investigation

Events search

During post-exploitation, an attacker may leverage scheduled tasks to run periodically, disable antivirus, or configure malicious applications to execute during startup. To query for this activity, specific event names, such as 'Windows Autostart Location', 'New Scheduled Task', and events containing 'Windows Defender', were added to a filter in USM Anywhere. An additional filter was applied to display events occurring in the last 24 hours. This expanded event search provided context into attacker activity around the time of the initial Cobalt Strike and Meterpreter alarms.

context for Cobalt Strike

Event deep dive

Just after the Cobalt Strike and Meterpreter detections, a scheduled task was created named "Monitoring Recovery." This task is identified by Windows Event ID 106: log Cobalt Strike

This scheduled task was used to install two remote monitoring and management (RMM) applications: Atera and Splashtop Streamer. Shortly after this task was created and executed, an event was received indicating "AteraAgent.exe" was added as a Windows auto-start service. AlteraAgent

AteraAgent.exe is associated with Atera, a legitimate computer management application that allows for remote access, management, and monitoring of computer systems, but has been abused by attackers for command and control of compromised systems.

This change was followed by an event involving "SRService.exe" being added as a Windows auto-start service on this asset: SRServer SRService.exe is associated with Splashtop Streamer Service, a remote access application commonly used by IT support, also abused by attackers for C&C communications. At this point, the attacker attempted to create multiple channels for command and control using Cobalt Strike, Meterpreter, Atera, and Splashtop Streamer. While the Cobalt Strike and Meterpreter sessions were terminated by Windows Defender, Atera and Spashtop Streamer were successfully added as startup tasks. This allowed the attacker to establish persistence in the customer environment. Persistence, as identified by the MITRE ATT&CK framework, allows the attacker to maintain "access to systems across restarts, changed credentials, and other interruptions that could cut off their access."

Response

Building the investigation

All alarms and events were carefully recorded in an investigation created in USM Anywhere. The customer was immediately contacted regarding this compromise, which lead to an 'all-hands-on-deck' call to remediate this threat. This compromise was escalated to the customer's Threat Hunter, as well as management and Tier 2 analysts.

Customer interaction

The MXDR team worked directly with the customer to contain and remediate this threat. This asset was quarantined from the customer network where it was scanned for malicious indicators using SentinelOne. The customer installed the SentinelOne EDR agent on this asset to protect it from any current threats. Additionally, the unauthorized applications Cobalt Strike, Meterpreter, Atera, and Splashtop Streamer were added to SentinelOne's blacklist to prevent future execution of these programs in the customer environment.

Limitations and opportunities

Limitations

While this compromise was quickly detected and contained, the customer lacked the protection required to prevent the applications Atera and Splashtop Steamer from being installed and added as Windows auto-start programs.

Opportunities

To protect an enterprise network from current threats, a multi-layered approach must be taken, otherwise known as 'Defense in Depth.' This entails multiple layers of protection, including Endpoint Detection and Response, implementation of a SIEM (Security Information and Event Management System), and additional security controls. With the addition of an EDR agent installed on this asset, this malicious behavior would have been prevented. AT&T's Managed Endpoint Security (MES) provides endpoint detection and response and can be utilized along with USM Anywhere to actively detect, prevent, and notify the customer of malicious activity in their environment.