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

One of the most prevalent threats today, facing both organizations and individuals alike, is the use of ransomware. In 2021, 37% of organizations said they were victims of some type of ransomware attack. Ransomware can render large amounts of important data inaccessible nearly instantly. This makes reacting to potential ransomware events in a timely and accurate manner extremely important. Utilizing an endpoint security tool is critical to help mitigate these threats. However, it is vital to maintain vigilance and situational awareness when addressing these threats, and not rely solely on one piece of information when performing analysis.

The AT&T Managed Extended Detection and Response (MXDR) analyst team received an alarm stating SentinelOne had detected ransomware on a customer's asset. The logs suggested the threat had been automatically quarantined, but further analysis suggested something more sinister was afoot. The same malicious executable had been detected on that asset twice before, both times reportedly being automatically quarantined. This type of persistent malware can be an indicator of a deeper infection such as a rootkit. After a more in-depth analysis and collaboration with the customer, the decision was made to quarantine and power off the asset, and replace the asset entirely due to this persistent malware.

Investigation

Initial alarm review

Indicators of Compromise (IOC)

The initial SentinelOne alarm alerted us to an executable 'mssecsvc.exe':

IoC persistent malware

The name of the executable as well as the file path is cleverly crafted to imitate a legitimate Windows program.

Expanded investigation

Events search

Searching events for the file hash revealed it had been repeatedly detected on the same asset over the last 2 weeks. In each instance the event log reports the executable being automatically quarantined by SentinelOne.

Persistent malware events

Additionally, a seach in USM Anywhere revealed two previous investigations opened for the same executable on the same asset. In both previous investigations the customer noted SentinelOne had automatically quarantined the file but did not take any further action regarding the asset.

Event deep dive

In the new instance of this alarm the event log reports SentinelOne successfully killed any processes associated with the executable and quarantined the file.

deep dive 1 Deep dive 2

This may lead one to believe there is no longer a threat. But the persistent nature of this file raises more questions than the event log can answer.

Reviewing additional indicators

It is important to not rely on a single piece of information when assessing threats and to go beyond just what is contained in the logs we are given. Utilizing open-source threat intelligence strengthens our analysis and can confirm findings. Virus Total confirmed the file hash was deemed malicious by multiple other vendors.

Persistent malware additional indicators

The executable was also analyzed in JoeSandbox. This revealed the file contained a device path for a binary string ‘FLASHPLAYERUPDATESERVICE.EXE which could be used for kernel mode communication, further hinting at a rootkit.

JoeSandbox

Response

Building the investigation

Despite the event log suggesting the threat had been automatically quarantined, the combination of the repeat occurrence and the findings on open-source threat intel platforms warranted raising an investigation to the customer. The customer was alerted to the additional findings, and it was recommended to remove the asset from the network.

Response for persistent malware

The customer agreed with the initial analysis and suspected something more serious. The analysts then searched through the Deep Visibility logs from SentinelOne to determine the source of the mssecsvc.exe. Deep Visibility logs allow us to follow associated processes in a storyline order. In this case, it appears the ‘mssecsvc.exe’ originated from the same ‘FlashPlayerUpdateService.exe’ we saw in the JoeSandbox analysis. Deep Visibility also showed us that mssecsvc.exe had a Parent Process of wininit.exe, which was likely to be the source of persistence.

customer response to persistent malware

Customer interaction

Another notable feature of USM Anywhere is the ability to take action from one centralized portal. As a result of the investigation, the analysts used the Advanced AlienApp for SentinelOne to place the asset in network quarantine mode and then power it off. An internal ticket was submitted by the customer to have the asset replaced entirely.

Limitations and opportunities

Limitations

A limiting factor for the SOC is our visibility into the customer's environment as well as what information we are presented in log data. The event logs associated with this alarm suggested there was no longer a threat, as it had been killed and quarantined by SentinelOne. Taking a single instance of information at face value could have led to further damage, both financially and reputationally. This investigation highlighted the importance of thinking outside the log, researching historical investigations, and combining multiple sources of information to improve our analysis.