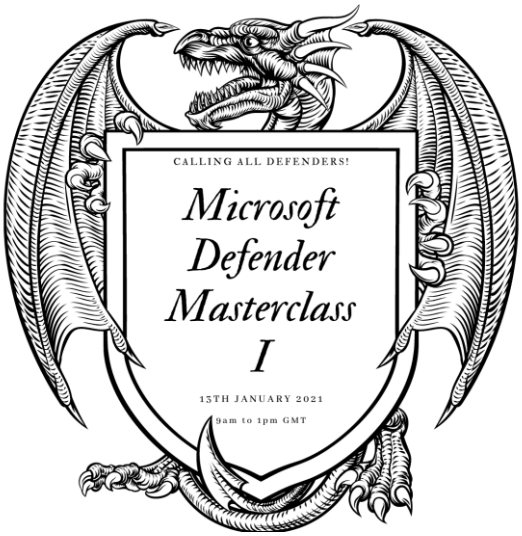


ATTACK SCENARIO CHALLENGES

A series of questions to challenge your knowledge

ABSTRACT

Within this document you will find a series of questions that correspond to specific attack scenarios that were made available during the Microsoft Defender Masterclass event series.

Mark Thomas

Microsoft Defender Masterclass I – a partner event created by James Graham

Scenario 1

1. **Has the device been fully remediated?**

Within the evidence tab we can see that the following files were remidated

pooler-cpuminer-2.5.1-win32.zip

File
Remediated

Open file page | Add Allowed/Blocked list rule for this file | Go hunt

File details

Verdict	Remediated Entity was pre-remediated by Windows Defender
Device	TRN-WIN10-3
File Name	pooler-cpuminer-2.5.1-win32.zip
File Path	c:\users\zack\downloads\pooler-cpuminer-2.5.1-win32.zip
Directory	c:\users\zack\downloads
Device Operating System	Windows10
Hashes	Show Hashes
Virus Total	46/66
Worldwide prevalence	3
Prevalence in organization	1

minerd.exe

File
Remediated

Open file page | Add Allowed/Blocked list rule for this file | Go hunt

File details

Verdict	Remediated Entity was pre-remediated by Windows Defender
Device	TRN-WIN10-3
File Name	minerd.exe
File Path	c:\users\zack\downloads\minerd.exe
Directory	c:\users\zack\downloads
Device Operating System	Windows10
Hashes	Show Hashes
Virus Total	42/70
Worldwide prevalence	3
Prevalence in organization	1

1 Point

2. **What Evidence has been collected?**

Check the Evidence tab within the incident.

Incidents > **Scenario 1 - Zack the Bitcoin Maniac**

Alerts (3) | Devices (1) | Investigations (2) | **Evidence (11)** | Graph beta

Evidence summary (11)
- Files (7)
- Processes (3)
- URLs (1)

Choose columns | 30 items per page

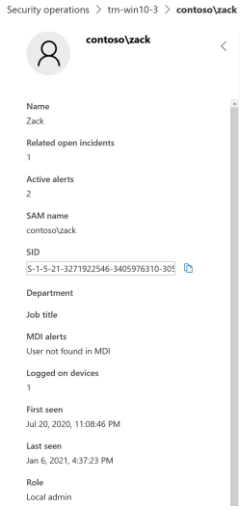
Files (7)

Verdict	Status Details	File Path
Remediated	Entity was pre-remediated by Windows Defend...	c:\users\zack\downloads\pooler-cpuminer-2.5.1-win32.zip
Remediated	Entity was pre-remediated by Windows Defend...	c:\users\zack\downloads\minerd.exe
Suspicious		C:\Users\zack\Downloads\pooler-cpuminer-2.5.1-win32.zip
Suspicious		C:\Users\zack\Downloads\minerd.exe
Suspicious		C:\Users\zack\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3c
Suspicious		C:\Users\zack\Downloads\minerd.exe
Suspicious		C:\Users\zack\Downloads\pooler-cpuminer-2.5.1-win32.zip

1 Point

3. What permission does Zach have on the device?

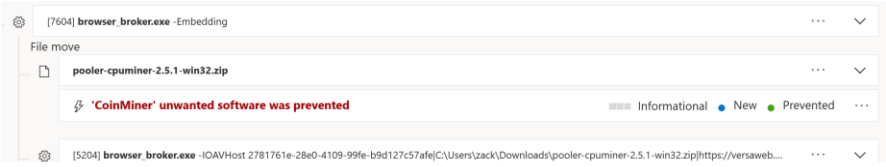
Local Admin



1 Point

4. How was pooler-cpuminder-2.5.1-win32.zip downloaded?

We can see browser_broker.exe (Microsoft Edge) was used to download the zip file.



2 Point

5. What URLs were used to download?

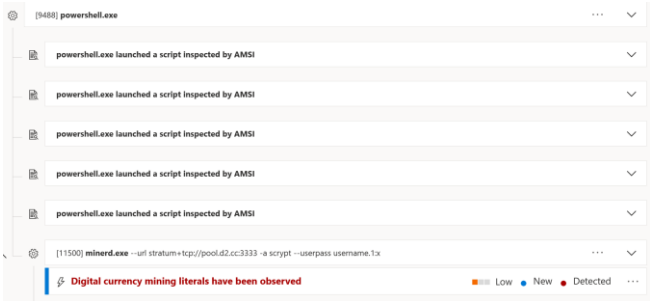
We can see the following URLs in the Alert story

- https://phoenixnap.dl.sourceforge.net/project/cpuminer/pooler-cpuminer-2.5.1-win32.zip
- https://versaweb.dl.sourceforge.net/project/cpuminer/pooler-cpuminer-2.5.1-win32.zip

1 Point for each

6. How was the CoinMiner executed?

Using PowerShell

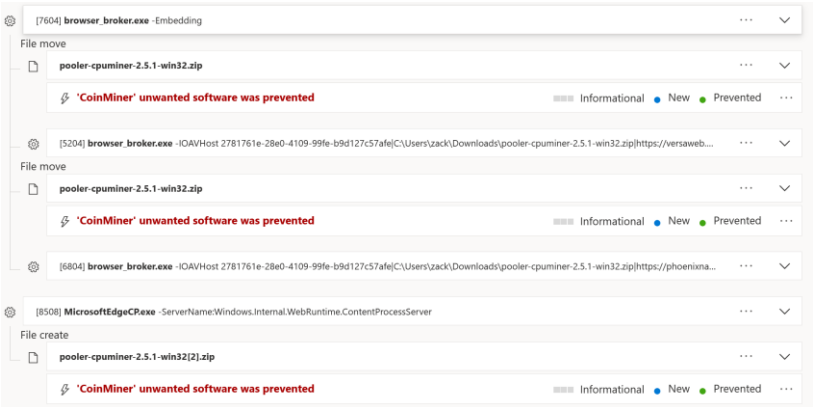


.\"minerd.exe" --url stratum+tcp://pool.d2.cc:3333 -a scrypt --userpass username.1:x

1 Point

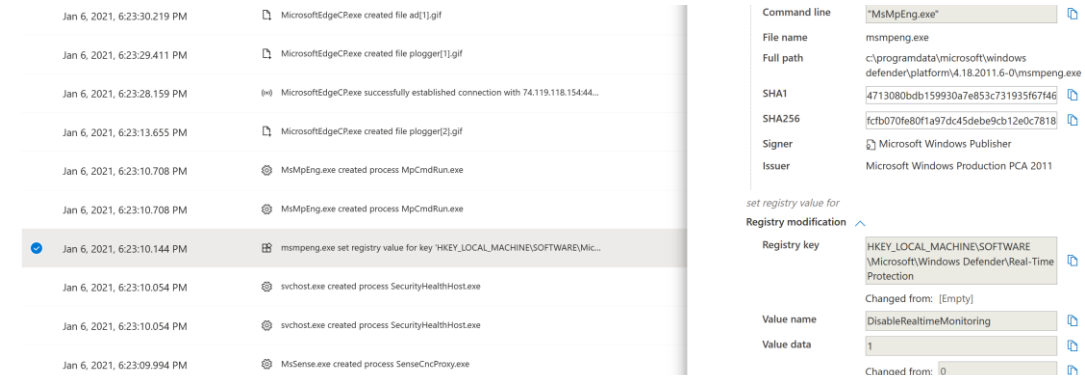
7. How was the CoinMiner able to execute on the device?

When looking at the Alerts we can see that the CoinMiner was originally prevented by Defender AV.



But we can see it running on the device later in the alert story.

When looking in the timeline we can see Defender AV settings were changed just before minerd.exe was downloaded again and executed.



5 Points

8. **How could this have been prevented?**

Tamper Protection – Stops Defender AV Real-time protection being disabled.

2 Points

9. **Advanced Hunting: How can we see if any other processes accessed sourceforge?**

```
DeviceNetworkEvents
| where RemoteUrl contains "sourceforge.net"
| project Timestamp, DeviceId, DeviceName, ActionType, RemoteIP,
RemoteUrl, InitiatingProcessFileName, InitiatingProcessFolderPath,
InitiatingProcessAccountUpn
```

5 Points

10. **Advanced Hunting: How can we see what users have disabled Real-time protection using the registry?**

```
DeviceRegistryEvents
| where RegistryValueName contains "DisableRealtimeMonitoring"
```

5 Points

Scenario 2

1. **What device does the incident start with?**

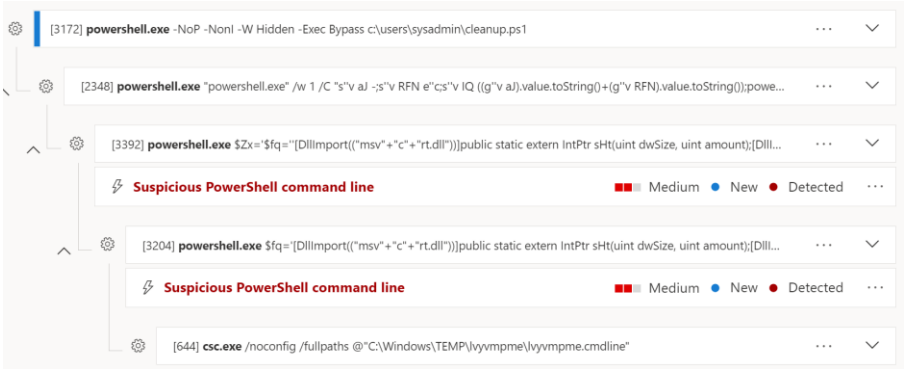
trn-w2k12-1

1 Point

2. **What is PowerShell running in the first Suspicious PowerShell Alert?**

Cleanup.ps1 is being ran and executing encoded PowerShell commands.

Microsoft.NET Framework module csc.exe is loaded.



2 Points

3. **On which machines does cleanup.ps1 exist?**

trn-w2k12-1

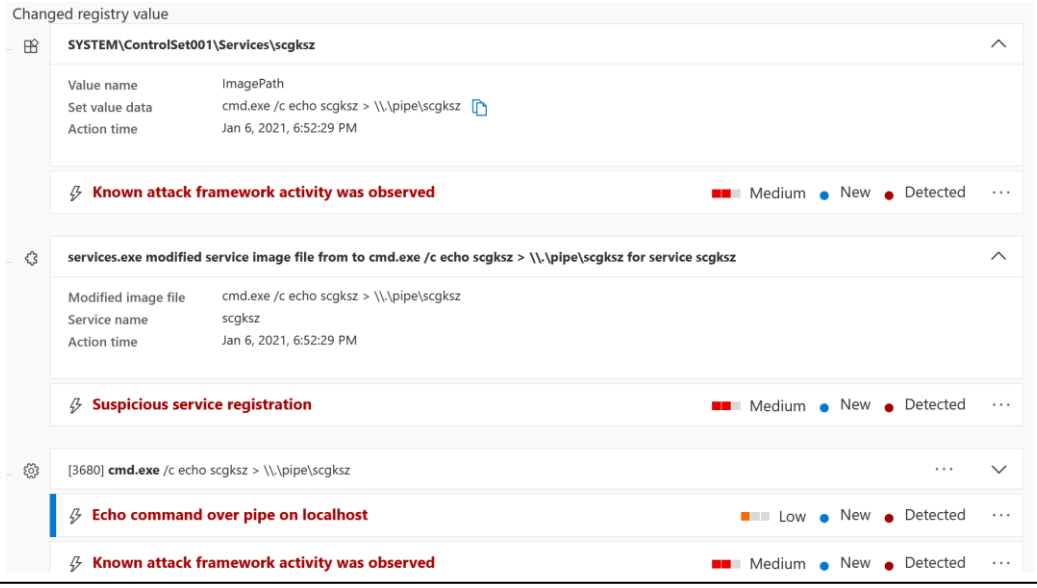
This can be found using the file search page or using the following Advanced Hunting query:

```
DeviceFileEvents
| where FileName contains "cleanup.ps1"
|project Timestamp, DeviceName, ActionType, FolderPath
```

1 Point

4. **How was the suspicious service registered on device trn-w2k12-1?**

Appears that an Attack Framework such as Metersploit is used. In this case the attacker is using named pipes to gain System privileges on this machine via meterpreter “getsystem”



1 Point

5. **What is the impact of the WDigest configuration change?**

Store credentials as plaintext in LSASS process memory. An attacker might be attempting to collect those credentials.

2 Points

6. **Advanced Hunting: Find all machines where HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\Wdigest\UseLogonCredential was changed from 0 to 1**

5 Points

```
DeviceRegistryEvents
|where RegistryKey contains
@"HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\Wdigest"
|where RegistryValueName == "UseLogonCredential"
|where RegistryValueData == "1"
|where PreviousRegistryValueData == "0"
|project Timestamp, DeviceName, InitiatingProcessAccountName,
InitiatingProcessParentFileName
```

7. **What users have logged into trn-w2k12-1? BONUS Advanced Hunting: Did any other users log on to the device within 30 minutes of Wdigest registry change?**

Users who have logged in: Sysadmin & margo

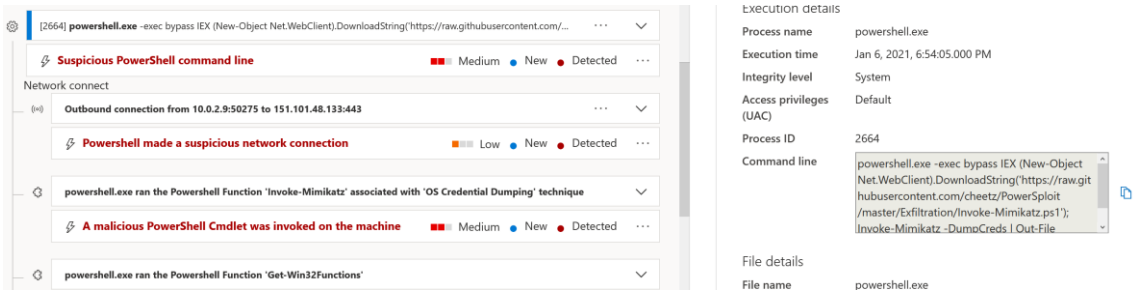
```
DeviceRegistryEvents
|where RegistryKey contains
@"HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SecurityProviders\Wdigest"
|where RegistryValueName == "UseLogonCredential"
|where RegistryValueData == "1"
|where PreviousRegistryValueData == "0"
|project DeviceRegistryTimestamp = Timestamp, DeviceName, InitiatingProcessAccountName,
InitiatingProcessParentFileName
|join (
DeviceInfo
| where Timestamp > ago(30d)
| project DeviceInfoTimestamp = Timestamp, LoggedOnUsers, DeviceName
) on DeviceName
| where (DeviceInfoTimestamp - DeviceRegistryTimestamp ) between (0min .. 30min)
```

1 Point (5 Points with AH)

8. **What URL did PowerShell make a suspicious network connection to on trn-w2k12-1 and what tool was executed?**

raw.githubusercontent.com/cheetz/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1

Mimikatz

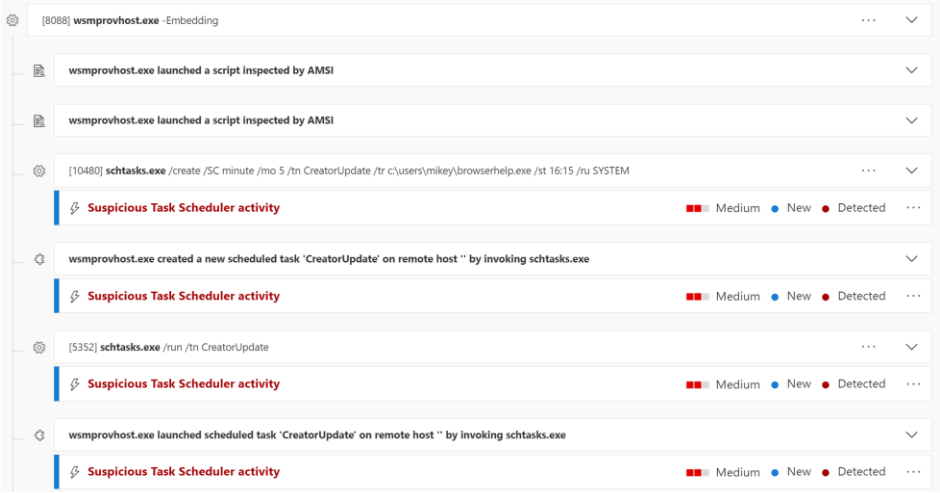


2 Points

9. **What devices have Suspicious Task Scheduler activity and what processes were involved?**

Devices: trn-win10-1, trn-win10-2

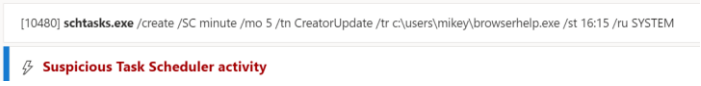
Processes: wsmprovhost.exe (Windows Remote PowerShell) & schtasks.exe (Scheduled Tasks)



2 Points

10. **What executable does the suspicious scheduled tasks run?**

Browserhelp.exe



1 Point

11. **In the device timeline what key actions does the file browserhelp.exe perform?**

browserhelp.exe successfully established connection with 13.84.168.153:80 (13.84.168.153/wiperpayload.exe)

browserhelp.exe set registry value for key 'HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\BITS'

Creates file funnygagwiper.exe

3 Points

12. **Advanced Hunting: Find PowerShell events that could involve a download.**

```
Shared queries > Execution > PowerShell downloads
// Finds PowerShell execution events that could involve a download
union DeviceProcessEvents, DeviceNetworkEvents
| where Timestamp > ago(14d)
// Pivoting on PowerShell processes
| where FileName in~ ("powershell.exe", "powershell_ise.exe")
// Suspicious commands
| where ProcessCommandLine has_any("WebClient",
"DownloadFile",
"DownloadData",
"DownloadString",
"WebRequest",
"Shellcode",
"BitsTransfer",
"http",
"https")
| project Timestamp, DeviceName, InitiatingProcessFileName,
InitiatingProcessCommandLine,
FileName, ProcessCommandLine, RemoteIP, RemoteUrl, RemotePort,
RemoteIPType
```

5 Points

13. **How could we stop the attack from its conclusion?**

What configuration changes could be made to improve the security posture to prevent this attack?

- Restrict WinRM
- Limit accounts with standing rights that could be used for lateral movement (Wendy)
- Don’t use easy to guess usernames and passwords
- Application Control (browserhelp.exe / funnygagwiper.exe)