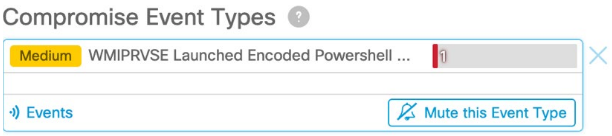
WMIPRVSE

Last Updated: November 3, 2020

INTRODUCTION

The Windows Management Interface (WMI) allows for the display and modification of local and remote computers, setting system variables, and executing scripts or processes. In this case, Behavioral Detection detected a related utility, WMIPRVSE, launching a new powershell process with parameters that contain further commands encoded in Base64. Various malware may use this as a Living Off the Land (LOLBin) method to disguise the true parent of the powershell process and perform a variety of malicious actions with utilities already located on the targeted computer.

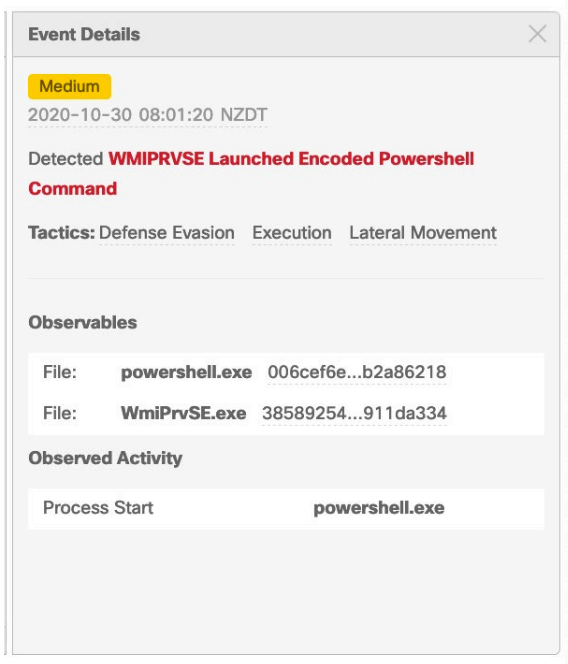


Compromise Event Types

Medium WMIPRVSE Launched Encoded Powershell ... 1

Events

Mute this Event Type



Event Details

Medium

2020-10-30 08:01:20 NZDT

Detected **WMIPRVSE Launched Encoded Powershell Command**

Tactics: Defense Evasion Execution Lateral Movement

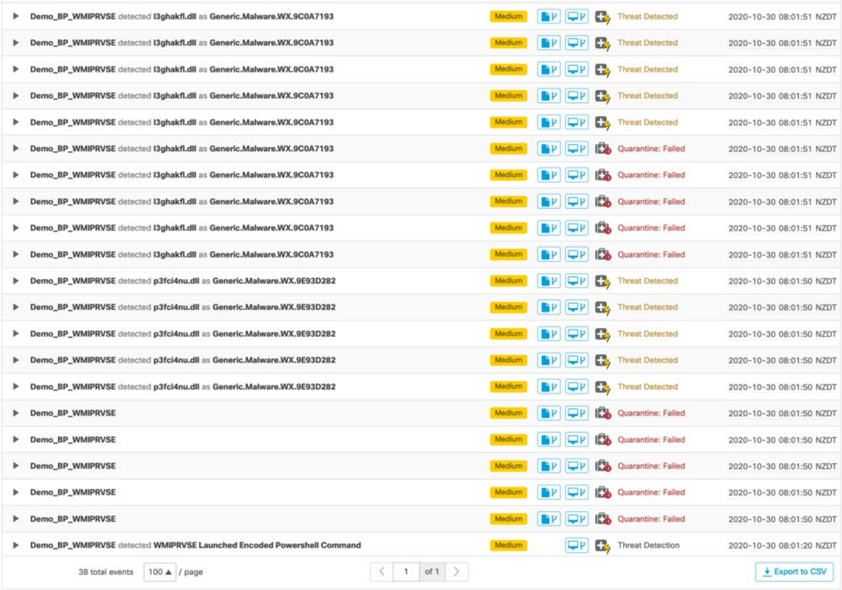
Observables

File:	**powershell.exe**	006cef6e...b2a86218
File:	**WmiPrvSE.exe**	38589254...911da334

Observed Activity

Process Start	**powershell.exe**

After loading the demo data, search for the compromise event.

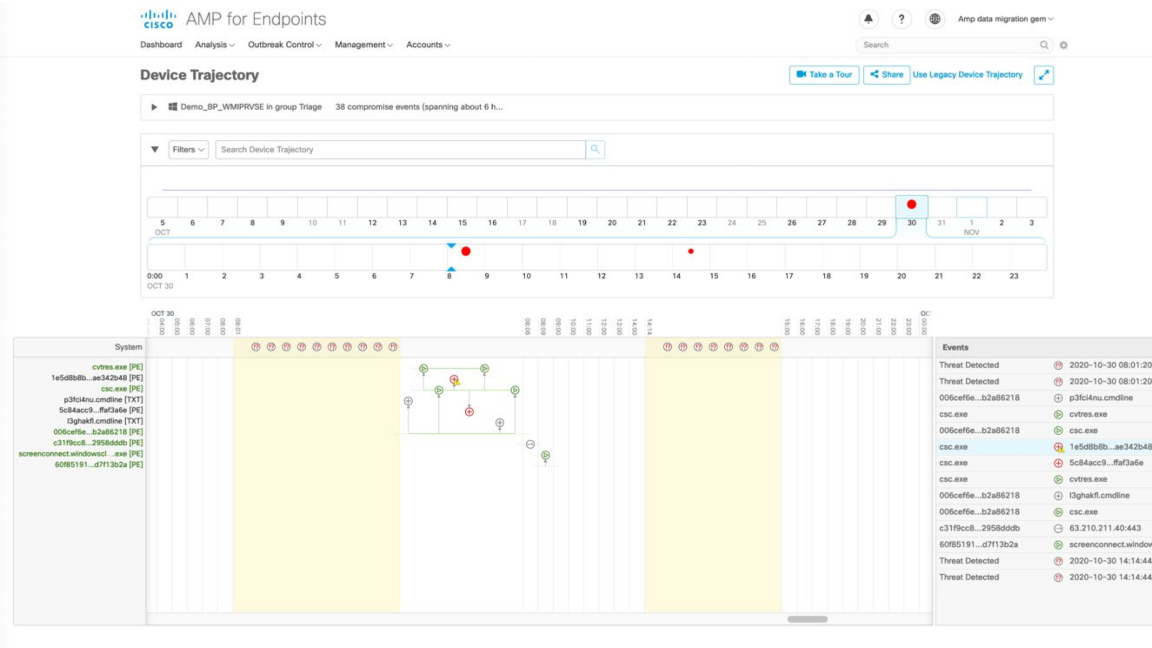


▶ **Demo_BP_WMIPRVSE** detected **l3ghakfl.dll** as **Generic.Malware.WX.9C0A7193**	Medium	Threat Detected	2020-10-30 08:01:51 NZDT
▶ **Demo_BP_WMIPRVSE** detected **l3ghakfl.dll** as **Generic.Malware.WX.9C0A7193**	Medium	Threat Detected	2020-10-30 08:01:51 NZDT
▶ **Demo_BP_WMIPRVSE** detected **l3ghakfl.dll** as **Generic.Malware.WX.9C0A7193**	Medium	Threat Detected	2020-10-30 08:01:51 NZDT
▶ **Demo_BP_WMIPRVSE** detected **l3ghakfl.dll** as **Generic.Malware.WX.9C0A7193**	Medium	Threat Detected	2020-10-30 08:01:51 NZDT
▶ **Demo_BP_WMIPRVSE** detected **l3ghakfl.dll** as **Generic.Malware.WX.9C0A7193**	Medium	Threat Detected	2020-10-30 08:01:51 NZDT
▶ **Demo_BP_WMIPRVSE** detected **l3ghakfl.dll** as **Generic.Malware.WX.9C0A7193**	Medium	Quarantine: Failed	2020-10-30 08:01:51 NZDT
▶ **Demo_BP_WMIPRVSE** detected **l3ghakfl.dll** as **Generic.Malware.WX.9C0A7193**	Medium	Quarantine: Failed	2020-10-30 08:01:51 NZDT
▶ **Demo_BP_WMIPRVSE** detected **l3ghakfl.dll** as **Generic.Malware.WX.9C0A7193**	Medium	Quarantine: Failed	2020-10-30 08:01:51 NZDT
▶ **Demo_BP_WMIPRVSE** detected **l3ghakfl.dll** as **Generic.Malware.WX.9C0A7193**	Medium	Quarantine: Failed	2020-10-30 08:01:51 NZDT
▶ **Demo_BP_WMIPRVSE** detected **l3ghakfl.dll** as **Generic.Malware.WX.9C0A7193**	Medium	Quarantine: Failed	2020-10-30 08:01:51 NZDT
▶ **Demo_BP_WMIPRVSE** detected **p3fci4nu.dll** as **Generic.Malware.WX.9E93D282**	Medium	Threat Detected	2020-10-30 08:01:50 NZDT
▶ **Demo_BP_WMIPRVSE** detected **p3fci4nu.dll** as **Generic.Malware.WX.9E93D282**	Medium	Threat Detected	2020-10-30 08:01:50 NZDT
▶ **Demo_BP_WMIPRVSE** detected **p3fci4nu.dll** as **Generic.Malware.WX.9E93D282**	Medium	Threat Detected	2020-10-30 08:01:50 NZDT
▶ **Demo_BP_WMIPRVSE** detected **p3fci4nu.dll** as **Generic.Malware.WX.9E93D282**	Medium	Threat Detected	2020-10-30 08:01:50 NZDT
▶ **Demo_BP_WMIPRVSE** detected **p3fci4nu.dll** as **Generic.Malware.WX.9E93D282**	Medium	Threat Detected	2020-10-30 08:01:50 NZDT
▶ **Demo_BP_WMIPRVSE**	Medium	Quarantine: Failed	2020-10-30 08:01:50 NZDT
▶ **Demo_BP_WMIPRVSE**	Medium	Quarantine: Failed	2020-10-30 08:01:50 NZDT
▶ **Demo_BP_WMIPRVSE**	Medium	Quarantine: Failed	2020-10-30 08:01:50 NZDT
▶ **Demo_BP_WMIPRVSE**	Medium	Quarantine: Failed	2020-10-30 08:01:50 NZDT
▶ **Demo_BP_WMIPRVSE**	Medium	Quarantine: Failed	2020-10-30 08:01:50 NZDT
▶ **Demo_BP_WMIPRVSE** detected **WMIPRVSE Launched Encoded Powershell Command**	Medium	Threat Detection	2020-10-30 08:01:20 NZDT

38 total events 100 ▲ / page

< 1 of 1 >

The demo data computer will appear along with several related events.



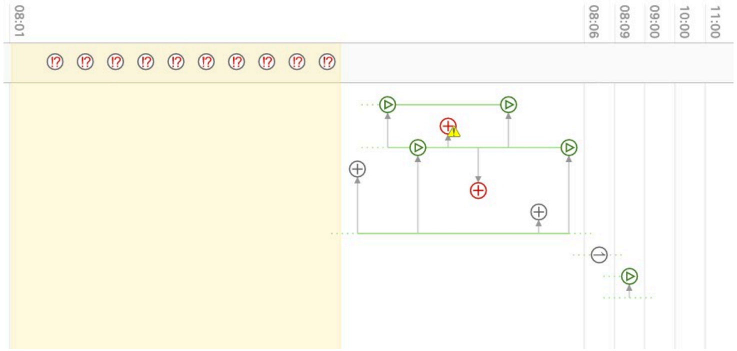
Device Trajectory

Demo_BP_WMIPRVSE in group Triage 38 compromise events (spanning about 6 h...

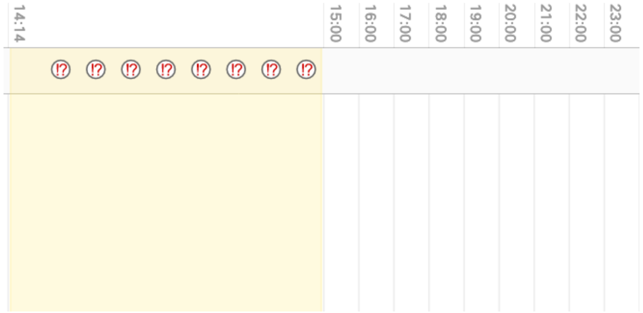
cvtres.exe [PE]
1e5d8b8b...ae342b48 [PE]
csc.exe [PE]
p3fci4nu.cmdline [TXT]
5c84acc9...ffaf3a6e [PE]
l3ghakfl.cmdline [TXT]
006cef6e...b2a86218 [PE]
c31f9cc8...2958dddb [PE]
screenconnect.windowscl....exe [PE]
60f85191...d7f13b2a [PE]

Events	
Threat Detected	2020-10-30 08:01:20
Threat Detected	2020-10-30 08:01:20
006cef6e...b2a86218	p3fci4nu.cmdline
csc.exe	cvtres.exe
006cef6e...b2a86218	csc.exe
csc.exe	1e5d8b8b...ae342b48
csc.exe	5c84acc9...ffaf3a6e
csc.exe	cvtres.exe
006cef6e...b2a86218	l3ghakfl.cmdline
006cef6e...b2a86218	csc.exe
c31f9cc8...2958dddb	63.210.211.40:443
60f85191...d7f13b2a	screenconnect.window
Threat Detected	2020-10-30 14:14:44
Threat Detected	2020-10-30 14:14:44

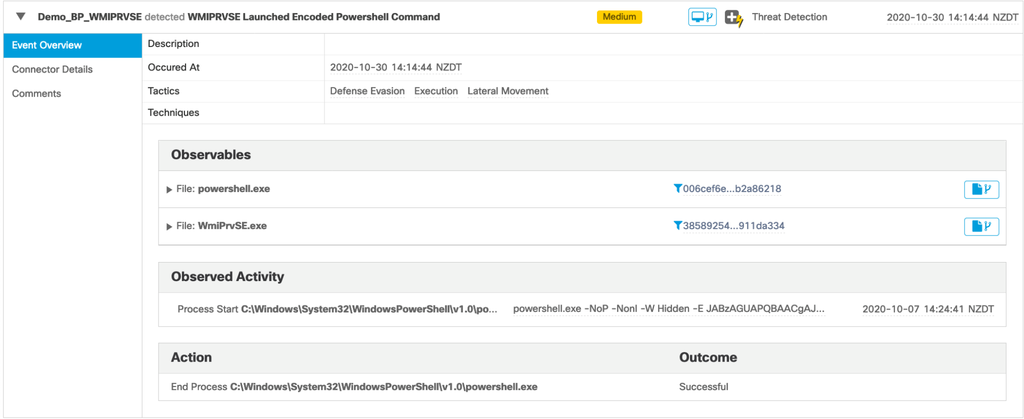
Multiple events are observed in Device Trajectory



When WMIPRVSE Launched Encoded Powershell initially triggers, Behavioral Protection is in audit mode. Although the signature is set to terminate an associated process, the action is currently disabled and follow-on events are observed. A handful of DLLs are also created and detected.



Hours later, the same attack is initiated again. This time the signature’s actions are active. Behavioral Protection immediately terminates the process to prevent further malicious activity.



▼ **Demo_BP_WMIPRVSE** detected **WMIPRVSE Launched Encoded Powershell Command** Medium Threat Detection 2020-10-30 14:14:44 NZDT

Description	
Occured At	2020-10-30 14:14:44 NZDT
Tactics	Defense Evasion Execution Lateral Movement
Techniques	

Observables

▶ File: **powershell.exe**	006cef6e...b2a86218
▶ File: **WmiPrvSE.exe**	38589254...911da334

Observed Activity

Process Start **C:\Windows\System32\WindowsPowerShell\v1.0\po...** powershell.exe -NoP -NonI -W Hidden -E JABzAGUAPQBAACgAJ... 2020-10-07 14:24:41 NZDT

Action	Outcome
End Process **C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe**	Successful

In this case the encoded portions of the Powershell command are related to a WannaMine attack. Subsequent steps of the attack are prevented because of the End Process action and no further activity is observed.