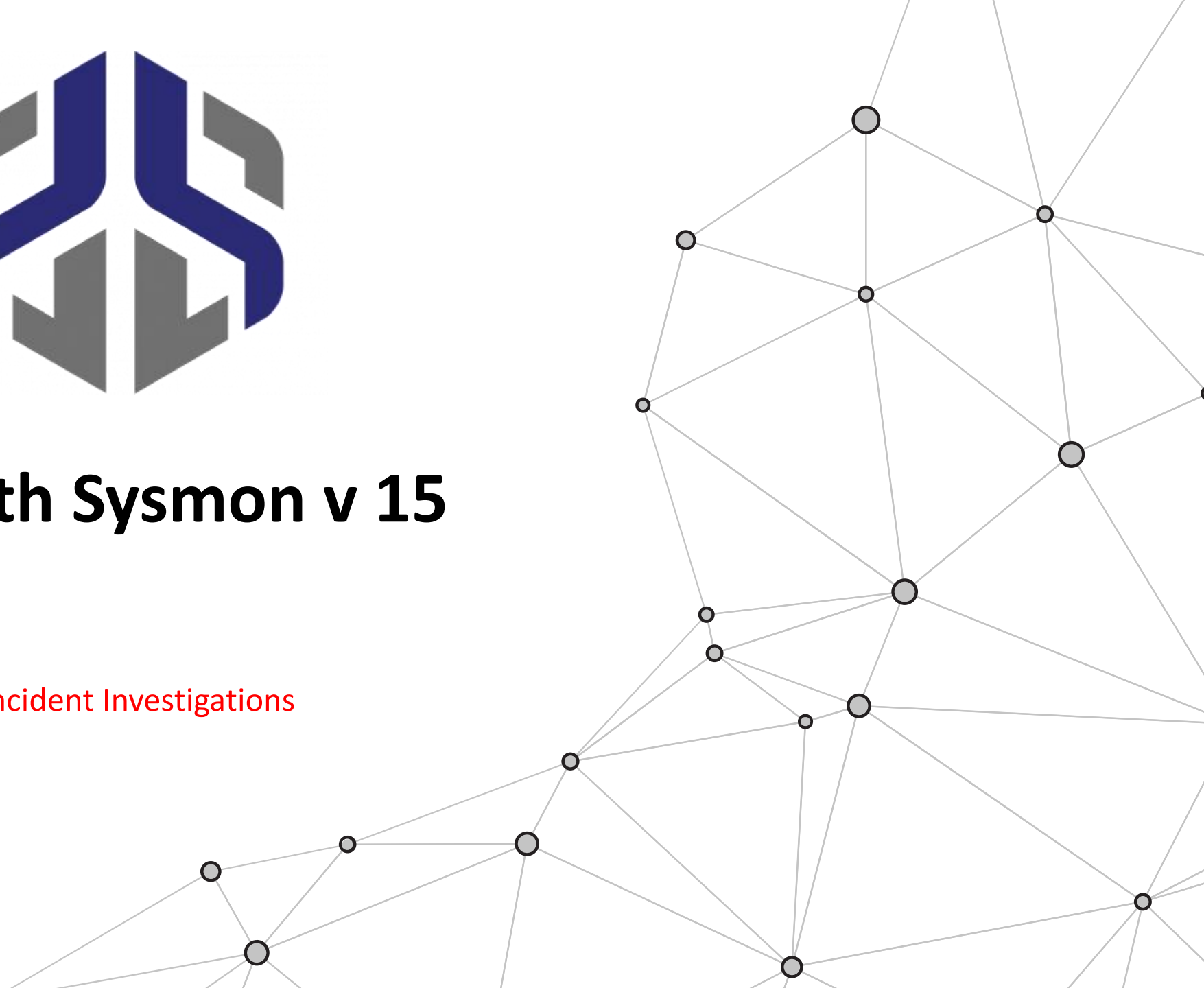




# What's new with Sysmon v 15

Leveraging System Monitor in Incident Investigations





Gerard Johansen  
**Principal Readiness  
Engineer**

 @irproactive



10+ Years of Incident Response,  
Digital Forensics and Threat  
Intelligence



BS – Justice and Law Admin, MA–  
Information Assurance, GCTI, GCFA,  
GNFA, GRID, CISSP Detective / Task  
Force Agent (FBI)



Rapid City, South Dakota

## Windows System Monitor (Sysmon)



- “System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, 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.”



<https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>

# Sysmon Capabilities



- Process creation command line & current/parent processes
- SHA1 hash value for process image files
- Process & Session GUIDs – aids in event correlation
- Logs driver or DLL loading with file signatures and hash values
- DNS and Network connection logging
- Insight into malware time creation modification
- Verbosity can be tailored
- Augment additional event logs and data sources (Prefetch, MFT) to aid in analysis



# What's new with System Monitor (Sysmon)



- Newly released version 15 (June 2023)
- New version includes:
  - Bug fixes (no surprise here)
  - Now runs as a PPL (Protected Process Lite)
  - New logging for FileExecutableDetected
  - Provides a much more targeted approach to addressing LOLBins and code that is brought into the environment



# The Good and the Bad with Sysmon



## The Good

- Deep visibility into endpoint behavior
- Verbose logs with additional insight
- Combine with other log entries (Security)
- Great first step in triage

## The Bad

- Very loud (depending on the configuration)
- Logs lots of legitimate behavior
- Can be difficult to craft SIEM alerts



# System Monitor Configuration and Setup



## Setting Up Sysmon (Locally)



1. Download Sysmon from the Microsoft site: <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>
2. Select Configuration: <https://raw.githubusercontent.com/olafhartong/sysmon-modular/master/sysmonconfig-with-filedelete.xml>
3. Command prompt:

```
C:\Users\ARTEvaluation\Downloads\Sysmon>Sysmon.exe -i C:\Users\ARTEvaluation\Downloads\sysmonconfig-with-filedelete.xml -accepteula
```

1. Increase Sysmon log file size: `wevtutil s1 Microsoft-Windows-Sysmon/Operational /ms:20971520`



# Setting Up Sysmon (Remotely)



- Velociraptor Remote Install

The screenshot displays the Velociraptor interface for configuring a client artifact. The main window shows the artifact name `Windows.Sysinternals.SysmonInstall` and its type `client`. A text box provides information about Sysmon and a note about the default configuration. Below this, a 'Tools' section lists `SysmonBinary` and `SysmonConfig`. On the right, the 'Client Artifacts' pane shows a list of installed artifacts, with `Windows.Sysinternals.SysmonInstall` highlighted.

Client Artifacts | sysmon

Windows.Sysinternals.SysmonInstall  
Type: client

Rectangular Snip

Sysmon is a kernel level system monitor written by Sysinternals. While we are not able to distribute Sysmon ourselves, Velociraptor can help you manage its deployment and installation.

NOTE: By default we install the sysmon config from SwiftOnSecurity - we recommend you review the config file and override it in the GUI with one that better suits your needs.

Tools

- SysmonBinary
- SysmonConfig

Generic.System.Pstree  
Windows.EventLogs.Evtx  
Windows.Sysinternals.SysmonInstall

# Velociraptor Sysmon Triage Demo



# Windows.Triage.Sysmon



## New Collection: Select Artifacts to collect ♥

sysmon

Generic.System.Pstree

Windows.EventLogs.Evtx

Windows.Sysinternals.SysmonInstall

**Windows.Triage.Sysmon**

### Windows.Triage.Sysmon

Type: client

Custom Artifact

Author: Matt Green - @mgreen27

This artifact allows collecting Sysmon Events for Triage around a timestamp.

By default collection will be 600 seconds from the current time and allows fast triage of a machine with recent telemetry.

#### Parameters

Name	Type	Default	Description
TargetTime	timestamp		the timestamp we want to box time around. Default is current time.
TargetTimeBox	int	600	the time box in seconds we want around TargetTime.

# Velociraptor Sysmon Collection Demo



# Manual Sysmon Triage Demo



# Analyzing Sysmon Log Files



# Initial Access



- T1566.001 Spear Phishing Attachment
- Event ID: 22 DNS Event (Query)

ProcessGuid: {d4e64a0a-4f0e-64b5-1e16-000000000800}

ProcessId: 5756

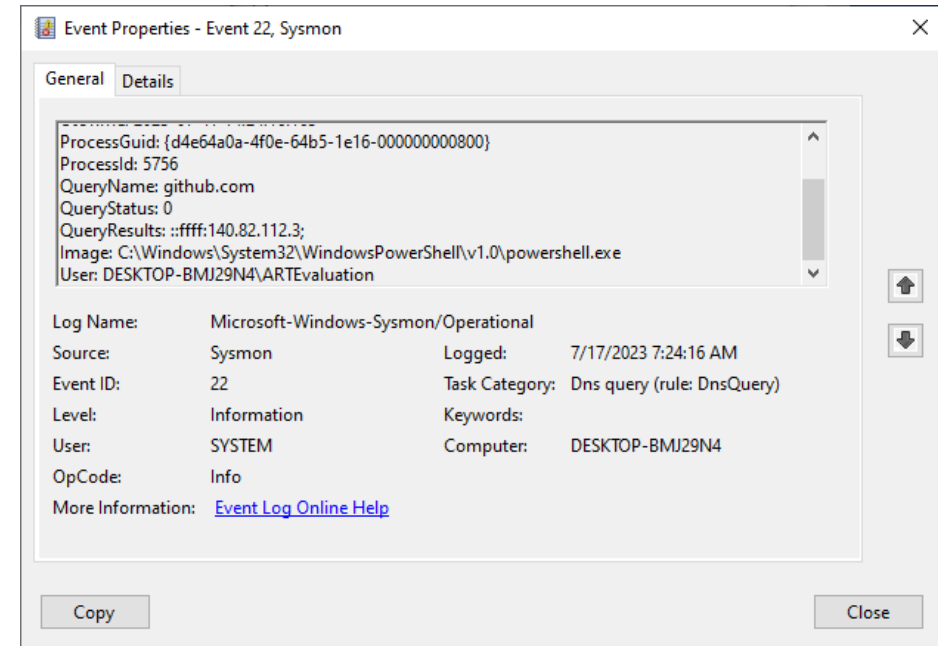
QueryName: github.com

QueryStatus: 0

QueryResults: ::ffff:140.82.112.3;

Image:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe



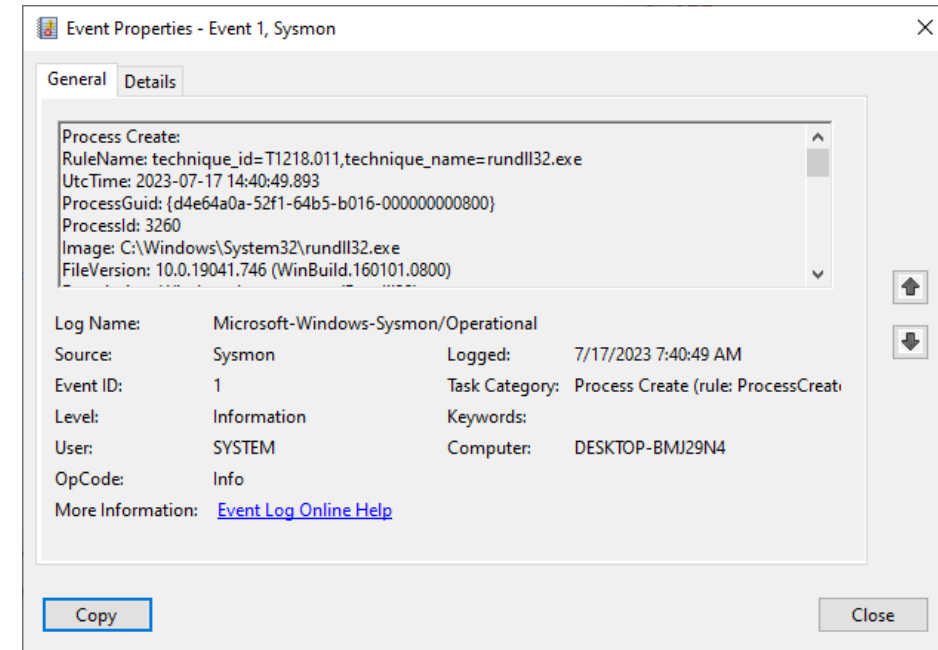
## Execution - Proxy



- T1218.011: Signed Binary Proxy Execution: Rundll32
- Event ID: 1 Process Creation

OriginalFileName: RUNDLL32.EXE

```
CommandLine: rundll32 vbscript:"\..\mshtml,#135  
"+String(CreateObject("WScript.Shell").Run("calc.exe")  
,0)
```





# Execution - WMI



- T1047 Windows Management Instrumentation
- Event ID 7: Image Loaded

Image: C:\Windows\System32\wbem\WmiPrvSE.exe

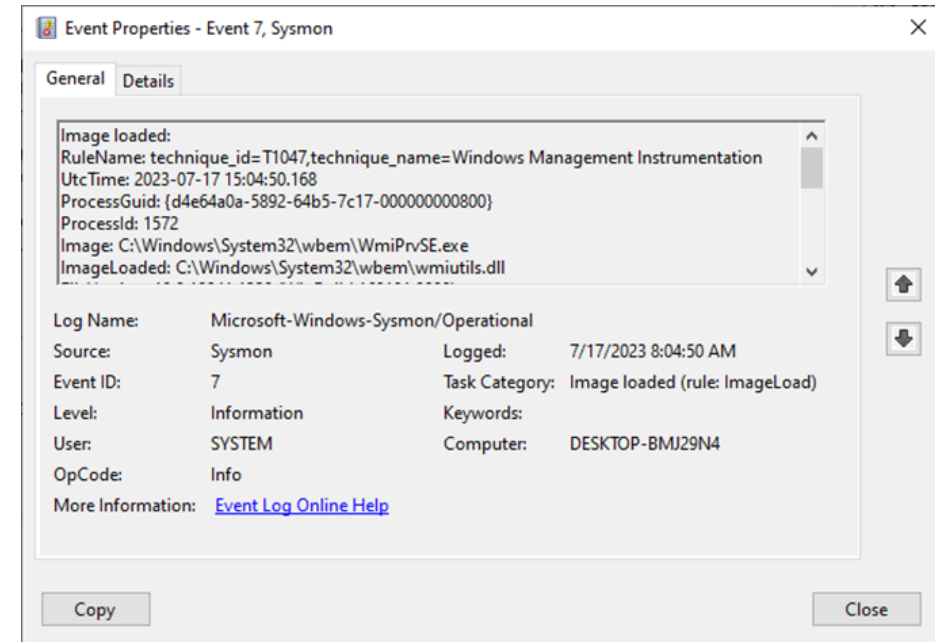
ImageLoaded:

C:\Windows\System32\wbem\wmiutils.dll

FileVersion: 10.0.19041.1320

(WinBuild.160101.0800)

Description: WMI

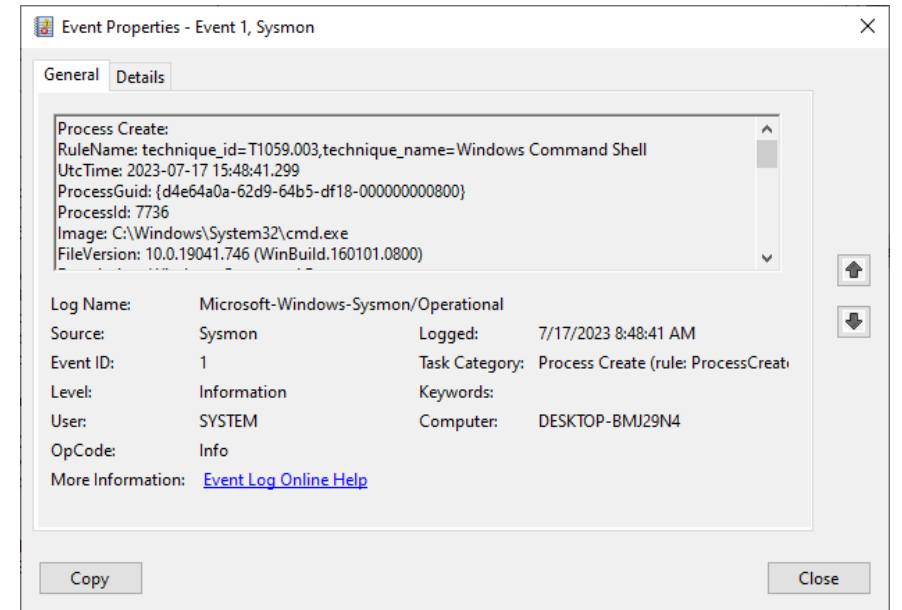


# Lateral Movement



- T1021.002 Remote Services / T1059.003 Command Shell
- Event ID 1: Process Create
- LOLBIN activity

```
CommandLine: "cmd.exe" /c  
"C:\AtomicRedTeam\atomics\..\ExternalPayloads\P  
sExec.exe \\localhost -accepteula -c  
C:\Windows\System32\cmd.exe"
```



# Command and Control



- T1071.004 Application Layer Protocol
- Event ID: 22 DNS Query
- Often large number of queries

UtcTime: 2023-07-17 15:37:39.554

ProcessGuid: {d4e64a0a-600a-64b5-7b18-00000000800}

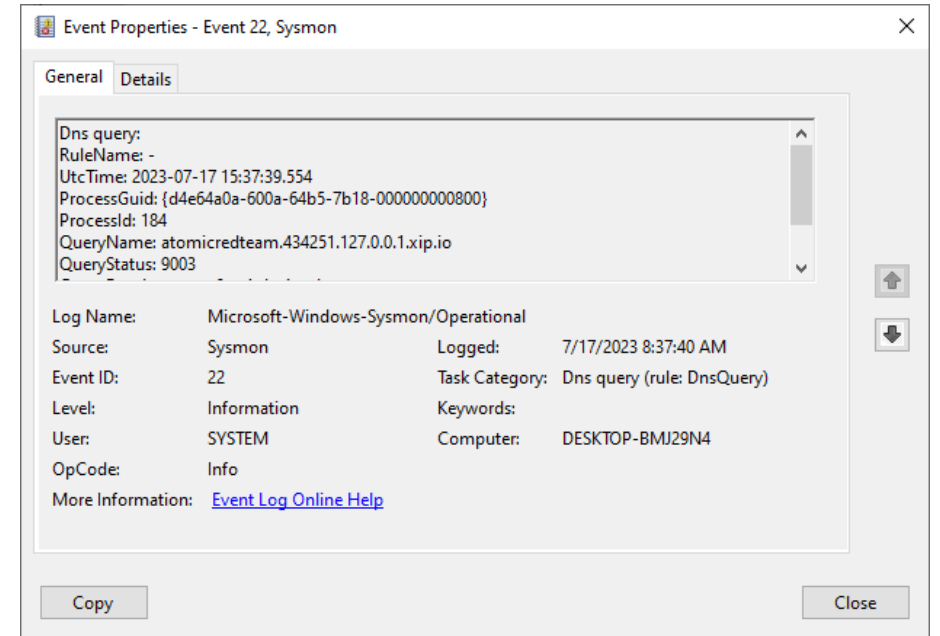
ProcessId: 184

QueryName:

atomicredteam.434251.127.0.0.1.xip.io

QueryStatus: 9003

QueryResults: type: 6 ns1.dnsimple.com;



# Command and Control



- T1105 Ingress Tool Transfer
- Event ID 29: FileExecutableDetected
- Post Exploitation tools: SharpHound, Mimikatz, Procdump

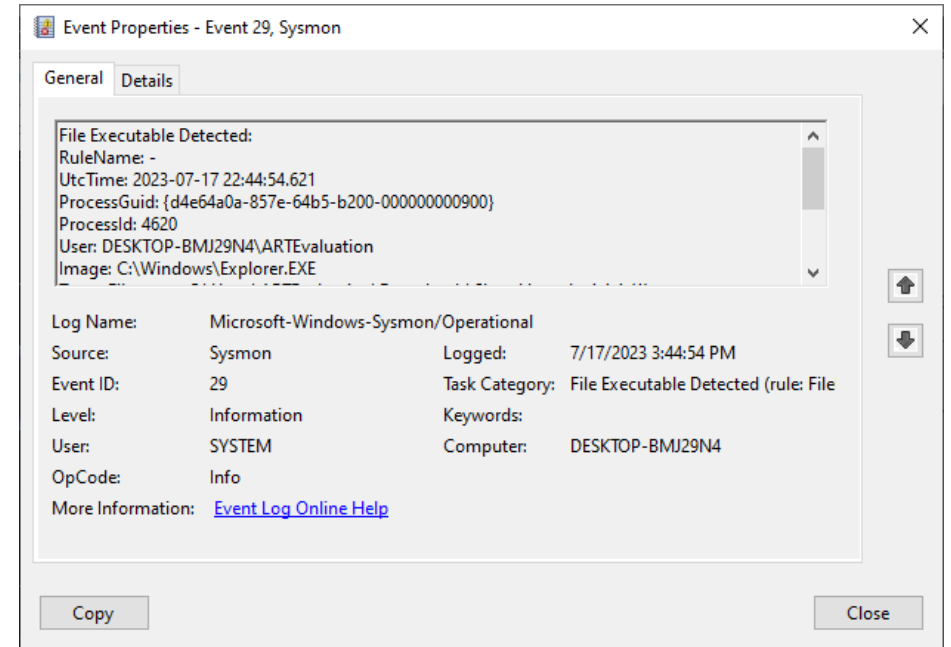
Image: C:\Windows\Explorer.EXE

TargetFilename:

C:\Users\ARTEvaluation\Downloads\SharpHound-v1.1.1 (1)\System.Diagnostics.Tracing.dll

Hashes:

SHA1=5340B1FC77E793D1FDDE49B14B7B426D0E448870,  
MD5=89C684EDAADCECF78C53E45DAE62E97E, SHA256=3A7  
F44E3B20A03CEF6FE8B164A5C193D50BD30EE0AAB26A785  
7D6B1944DA64FD,  
IMPHASH=DAE02F32A21E03CE65412F6E56942DAA



## Summary - Working with Sysmon



- Digital Forensics Analysis: Very good insight into endpoint behavior
- Combine with other evidence sources
- Start with high probability indicators
- May be difficult to use proactively for alerting across all system
- High Value Targets (HVTs) and Honeypots can provide early warning via Sysmon
- Include Acquisition and analysis into IR plans, playbooks and workflows



**PROACTIVE**



# Thank You

For Your Time & Attention

# Atomic Red Team Tests



- <https://atomicredteam.io/initial-access/T1566.001/#atomic-test-2---word-spawned-a-command-shell-and-used-an-ip-address-in-the-command-line>
- <https://atomicredteam.io/defense-evasion/T1218.011/#atomic-test-3---rundll32-execute-vbscript-command-using-ordinal-number>
- <https://atomicredteam.io/execution/T1047/#atomic-test-5---wmi-execute-local-process>
- <https://atomicredteam.io/lateral-movement/T1021.002/#atomic-test-3---copy-and-execute-file-with-psexec>

## Resources



- <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>
- <https://www.bleepingcomputer.com/news/microsoft/microsoft-sysmon-now-detects-when-executables-files-are-created/>
- <https://medium.com/@olafhartong/sysmon-15-0-file-executable-detected-40fd64349f36>
- <https://github.com/olafhartong/sysmon-modular/tree/master>
- <https://github.com/MHaggis/sysmon-dfir>