



What's new with Sysmon v 15

Leveraging System Monitor in Incident Investigations

Ο

PROACTIVE





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

Gerard Johansen

Principal Readiness Engineer

@irproactive



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



Rapid City, South Dakota

IP PROACTIVE

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."





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



PROACTIVE

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







Setting Up Sysmon (Locally)

- 1. Download Sysmon from the Microsoft site: https://learn.microsoft.com/enus/sysinternals/downloads/sysmon
- 2. Select Configuration: https://raw.githubusercontent.com/olafhartong/sysmonmodular/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

f		Client A	rtifacts		sysmon
¢	Windows Sysinternals SysmonInstall		Generic.S	System.Ps	tree
۶			Windows.	EventLogs	.Evtx
0	Type: client		Windows.S	Sysintern	als.SysmonInstall
	Sysmon is a kernel level system monitor written by Sysinternals. While we are not able to distribute Sysmon ourselves, Velociraptor can you manage its deployment and installation.	help			
•	NOTE: By default we install the sysmon config from SwiftOnSecurity - we recommend you review the config file and override it in the GU with one that better suits your needs.	I			
Ş	Tools				
<i>i</i> 4	• 🖸 SysmonBinary				
V	• C SysmonConfig				





Windows.Triage.Sysmon

New Collection: Select Artifacts to collect								
sysmon	Windows.Tr	iage.Sys	smon					
Generic.System.Pstree	Type: client							
Windows.EventLogs.Evtx	Custom Artifact							
Windows.Sysinternals.SysmonInstall	Author: Matt Green - Qmgreen27							
Windows.Triage.Sysmon	This artifact allo By default collec recent telemetry	ws collecting ction will be 6 y.	Sysmon Ev	ents for Triage around a timestamp. from the current time and allows fast triage of a machine with				
	Parameters	Туре	Nefeul+	Description				
	Name	iyhe	Delauit	DESCI 190101				
	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.				
	TargetTimeBox	int	600	the time box in seconds we want around TargetTime.				









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
```

ProcessGuid: {d4e	64a0a-4f0e-64b5-1e16-0000	00000800}		^	
ProcessId: 5756	uh com				
QueryStatus: 0	ableom				
QueryResults: ::fff	f:140.82.112.3;	CL III 1 0			
User: DESKTOP-R	vs\System32\WindowsPowe MI29N4\ARTEvaluation	erShell\v1.0\powers	hell.exe	~	
					1
Log Name:	Microsoft-Windows-Sysm	ion/Operational			L De
Source:	Sysmon	Logged:	7/17/2023 7:24:16 AM		
		Tack Catagons	Dos query (rule: DosQuery)		
Event ID:	22	lask category:	bills query (rule, billsQuery)		
Event ID: Level:	22 Information	Keywords:	bis query (rule bisedery)		
Event ID: Level: User:	22 Information SYSTEM	Keywords: Computer:	DESKTOP-BMJ29N4		
Event ID: Level: User: OpCode:	22 Information SYSTEM Info	Keywords: Computer:	DESKTOP-BMJ29N4		



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)
```

Process Create: RuleName: technique_id=T1218.011,technique_name=rundll32.exe UtcTime: 2023-07-17 14:40:49.893 ProcessGuid: {d4e64a0a-52f1-64b5-b016-00000000800} ProcessId: 3260 Image: C:\Windows\System32\rundll32.exe FileVersion: 10.0.19041.746 (WinBuild.160101.0800)						
Log Name:	Microsoft-Windows-Sysmon/Operational					
Source:	Sysmon	Logged:	7/17/2023 7:40:49 AM			
Event ID:	1	Task Category:	Process Create (rule: ProcessCre	eati		
la vali	Information	Keywords:				
Level:		Committee	DESKTOP-BMJ29N4			
Levei: User:	SYSTEM	Computer:				
Levei: User: OpCode:	SYSTEM Info	Computer:				



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

Image loaded:				^
RuleName: techn UtcTime: 2023-07	ique_id=T1047,technique_r -17 15:04:50.168	name=Windows Ma	inagement Instrumentation	
ProcessGuid: {d4e	e64a0a-5892-64b5-7c17-00	000000800}		
Image: C:\Windo	ws\System32\wbem\WmiF	PrvSE.exe		
ImageLoaded: C:	\Windows\System32\wben	n\wmiutils.dll		× 4
Log Name:	Microsoft-Windows-Sys	mon/Operational		
Courses	Sysmon	Logged:	7/17/2023 8:04:50 AM	
Source:				
Event ID:	7	Task Category	: Image loaded (rule: ImageLoad	d)
Event ID: Level:	7 Information	Task Category: Keywords:	: Image loaded (rule: ImageLoad	ł)
Event ID: Level: User:	7 Information SYSTEM	Task Category: Keywords: Computer:	: Image loaded (rule: ImageLoad DESKTOP-BMJ29N4	i)
Event ID: Level: User: OpCode:	7 Information SYSTEM Info	Task Category Keywords: Computer:	: Image loaded (rule: ImageLoad DESKTOP-BMJ29N4	4)



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"
```

RuleName: techni	^						
ProcessGuid: {d4e64a0a-62d9-64b5-df18-00000000800}							
Image: C:\Windo	ProcessId: //3b Image: C:\Windows\System32\cmd.exe						
FileVersion: 10.0.1	9041.746 (WinBuild.160101.0	800)		~			
Log Name:	Microsoft-Windows-Sysm	on/Operational					
Source:	Sysmon	Logged:	7/17/2023 8:48:41 AM				
Event ID:	1	Task Category:	Process Create (rule: Proce	ssCreat			
Level:	Information	Keywords:					
User:	SYSTEM	Computer:	DESKTOP-BMJ29N4				
OpCode:	Info						
M 1.6	Event Log Online Help						

PROACTIVE

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;
```

Dns query:				~			
RuleName: -	RuleName: - LiteTime: 2023-07-17 15:37:39 554						
ProcessGuid: {d4e64a0a-600a-64b5-7b18-00000000800}							
ProcessId: 184	Processid: 184						
QueryStatus: 9003	ncreateann.434231.127.0.0.1.3	apao		~			
					1		
Log Name:	Microsoft-Windows-Sysmo	on/Operational			4		
Source:	Sysmon	Logged:	7/17/2023 8:37:40 AM				
Event ID:	22	Task Category:	Dns query (rule: DnsQuery)				
Level:	Information	Keywords:					
User:	SYSTEM	Computer:	DESKTOP-BMJ29N4				
OpCode:	Info						
More Information:	Event Log Online Help						

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\SharpHoundv1.1.1 (1)\System.Diagnostics.Tracing.dll Hashes:

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

 ి Event	Properties -	Event 29, Sysmon				×
General File Exe RuleNa UtcTim Process User: D Image:	Details ecutable Det me: - e: 2023-07- sGuid: {d4e6 sld: 4620 ESKTOP-BM C:\Window	tected: 17 22:44:54.621 54a0a-857e-64b5-b200-000000 1J29N4\ARTEvaluation Is\Explorer.EXE	1000900}		~	•
Log Nar	ne:	Microsoft-Windows-Sysmon/Operational				
Source:		Sysmon	Logged:	7/17/2023 3:44:54 PM		
Event ID	:	29	Task Category:	File Executable Detected (rule:	File	
Level:		Information	Keywords:			
User:		SYSTEM	Computer:	DESKTOP-BMJ29N4		
OpCode	8	Info				
More In	formation:	Event Log Online Help				
_						
Сору					C	lose



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



For Your Time & Attention



Atomic Red Team Tests

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



Resources

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