

Conti Ransomware - Splunk Threat Hunting

Execute Date: Jan 15, 2023

Incident Responder: Wen H.

Email: whsu05@nyit.edu

Description

[Conti](#), ransomware, compromised a Microsoft Exchange server in 2021. We have to investigate this incident as a SOC Tier 1 analyst through Splunk, finding the malicious artifacts to escalate to the incident responder team (IR).

Identify Where is the location of the Conti ransomware

Detect ransomware locations using Splunk and identify Sysmon event ID 11 (File Create). And there is a strange IMAGE location under Administrator's dictionary.

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** `index = main sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=11`
- Results:** 104 events (before 1/15/23 8:42:18.000 PM). No Event Sampling.
- Visualizations:** Events (104), Patterns, Statistics, Visualization.
- Fields List:** host 1, source 1, sourcetype 1, ComputerName 1, CreationUtcTime 87, EventCode 1, EventType 1, Image 10, index 1, Keywords 1, linecount 1, LogName 1, Message 100%.
- Modal Window (Image):** Displays the top 10 values for the 'Image' field.

Top 10 Values	Count	%
C:\Windows\system32\cleanmgr.exe	27	25.962%
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.exe	26	25%
C:\Windows\System32\svchost.exe	18	17.308%
c:\Users\Administrator\Documents\cmd.exe	18	17.308%
C:\Program Files\Windows Defender\MpCmdRun.exe	6	5.769%

index - main md5 Administrator

90 events (before 1/15/23 8:53:56.000 PM) No Event Sampling

Jobs

Events (90) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection x Deselect 1 hour per column

List Format 20 Per Page < Prev 1 2 3 4 5 Next >

Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS		>	9/8/21	09/08/2021 04:05:32 PM
host 1			1:05:32.000 PM	LogName-Microsoft-Windows-Sysmon/Operational
source 1				EventCode=1
sourcetype 1				EventType=4
INTERESTING FIELDS				ComputerName-WIN-AQKKG2AS2Q7.bellybear.local
CommandLine 54				User=NOT_TRANSLATED
Company 4				Sid=S-1-5-18
ComputerName 1				SidType=0
CurrentDirectory 4				SourceName-Microsoft-Windows-Sysmon
Description 16				Type=Information
EventCode 1				RecordNumber=3136
EventType 1				Keywords=None
FileVersion 8				TaskCategory=Process Create (rule: ProcessCreate)
Hashes 16				OpCode=Info
image 16				Message=Process Create:
index 1				RuleName= -
integrityLevel 4				UtcTime: 2021-09-08 20:05:32.431
Keywords 1				ProcessGuid: {72893ba8-178c-6139-b402-000000000c00}
linecount 1				ProcessId: 15540
logName 1				Image: C:\Users\Administrator\Documents\cmd.exe
				FileVersion: -

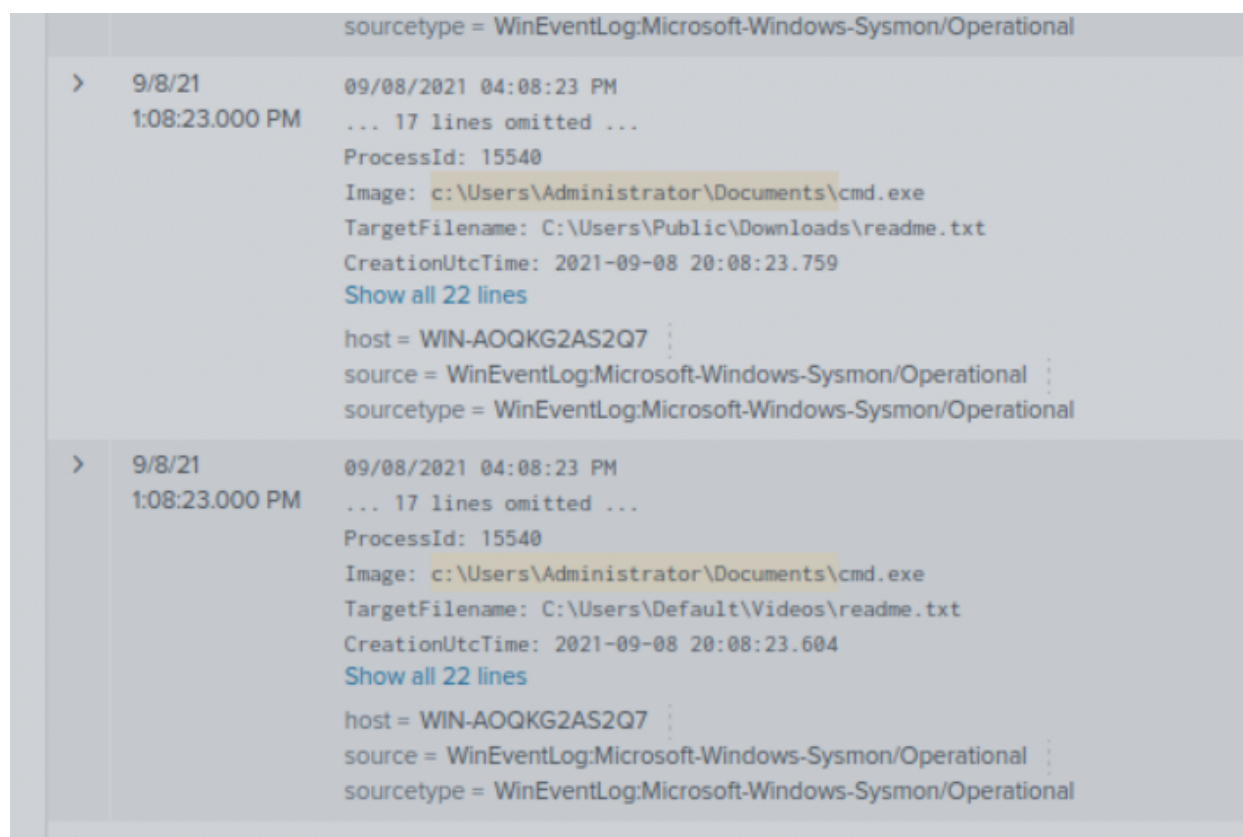
c:\Users\Administrator\Documents\cmd.exe

File Artifact Collection (Hash Value)

We know the ransomware is under the Administrator directory, so we can query “md5” “Administrator”

MD5: 290C7DFB01E50CEA9E19DA81A781AF2C

What files are saved in multiple folders?



Through “**stats count by Filename**” query or we can obviously see the “readme.txt” is under the “Videos” and “Downloads” directory.

readme.txt

How did the attacker compromise the Exchange server?

Persistence: Through adding a new user with the cmd command line [[net user](#)]

New Search

index - main sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" net user All time

52 events (before 1/15/23 9:04:50.000 PM) No Event Sampling Job Smart Mode

Events (52) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

Sep 6, 2021 12:00 PM 0 events at 6 PM on Monday, September 6, 2021 2 days 2 hours Sep 8, 2021 2:00 PM

List Format 20 Per Page Prev 1 2 3 Next

Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS				
host 1				
source 1				
sourcetype 1				
INTERESTING FIELDS				
CommandLine 14				
Company 1				
ComputerName 1				
CreationUtcTime 32				
CurrentDirectory 2				
Description 4				
EventCode 3				
EventType 2				

9/8/21 1:06:57.000 PM ... 5 lines omitted ... User=NOT_TRANSLATED ... 12 lines omitted ... ProcessId: 15540 Image: c:\Users\Administrator\Documents\cmd.exe TargetFilename: C:\Users\ADMINISTRATOR\Downloads\readme.txt CreationUtcTime: 2021-09-08 20:06:57.745 Show all 22 lines host = WIN-AOQKG2AS2Q7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

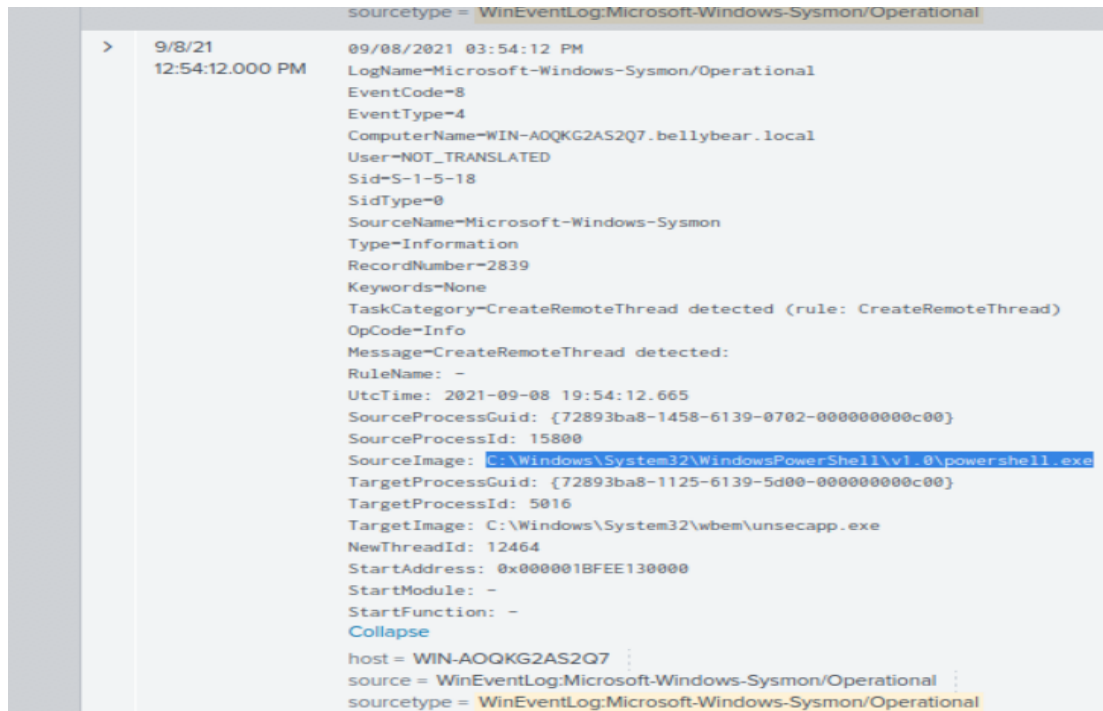
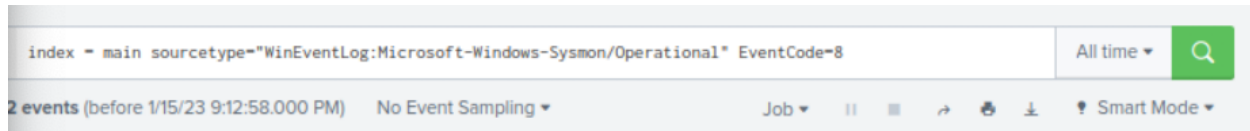
9/8/21 1:06:57.000 PM ... 5 lines omitted ... User=NOT_TRANSLATED ... 12 lines omitted ...

ParentCommandLine 8	C:\Windows\system32\cmd.exe	3	21.428%
ParentImage 5	"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\map_i_nspi\476099e8\44545f4d\ucfirypz.cmdline"	1	7.143%
ParentProcessGuid 9	c:\windows\system32\inetssrv\w3wp.exe -ap "MSEExchangeMapiAddressBookAppPool" -v "v4.0" -c "C:\Program Files\Microsoft\Exchange Server\V15\bin\MSEExchangeMapiAddressBookAppPool_CLRConfig.config" -a \\.\pipe\iisipm59e37a4a-8675-446b-94bf-267d59c79bf5 -h "C:\inetpub\temp\appools\MSEExchangeMapiAddressBookAppPool\MSEExchangeMapiAddressBookAppPool.config" -w "" -m 0	1	7.143%
ProcessGuid 45	c:\windows\system32\inetssrv\w3wp.exe -ap "MSEExchangeOWAAppPool" -v "v4.0" -c "C:\Program Files\Microsoft\Exchange Server\V15\bin\GenericAppPoolConfigWithGCServerEnabledFalse.config" -a \\.\pipe\iisipm02ecba3c-c3b8-4c36-b28a-0f20ecab4048 -h "C:\inetpub\temp\appools\MSEExchangeOWAAppPool\MSEExchangeOWAAppPool.config" -w "" -m 0	1	7.143%
ProcessId 44	net localgroup "Remote Desktop Users" "securityninja" /add	1	7.143%
Product 2	net localgroup administrators securityninja /add	1	7.143%
punct 3	net user /add securityninja hardToHack123\$	1	7.143%
RecordNumber 52			
RuleName 4			
Sid 1			
SidType 1			
SourceName 1			
splunk_server 1			
TargetFilename 32			
TaskCategory 3			
TerminalSessionId 1			
Type 1			
User 2			
UtcTime 52			

net user /add securityninja hardToHack123\$

We also can see the attacker add the “securityninja” user to the “Remote Desktop Users” and “administrators” groups.

Better Persistence: Process migration (Sysmon CreateRemoteThread: Event ID 8)




The original process is

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

Migrate to:

C:\Windows\System32\wbem\unsecapp.exe

What process to get the file hash with Event ID 8?

List ▾  Format 20 Per Page ▾		
Hide Fields	All Fields	
SELECTED FIELDS		
host 1		
source 1		
sourcetype 1		
INTERESTING FIELDS		
ComputerName 1		
EventCode 1		
EventType 1		
index 1		
Keywords 1		
linecount 1		
LogName 1		
Message 1		
NewThreadId 1		
OpCode 1		
punct 1		
RecordNumber 1		
RuleName 1		
Sid 1		
SidType 1		
SourceImage 1		
SourceName 1		
SourceProcessGuid 1		
SourceProcessId 1		
splunk_server 1		
StartAddress 1		
StartFunction 1		
StartModule 1		
TargetImage 1		
TargetProcessGuid 1		
TargetProcessId 1		

i	Time	Event
>	9/8/21	09/08/2021 03:55:30 PM
	12:55:30.000 PM	LogName=Microsoft-Windows-Sysmon/Operational
		EventCode=8
		EventType=4
		ComputerName=WIN-AOQKG2AS2Q7.bellybear.local
		User=NOT_TRANSLATED
		Sid=S-1-5-18
		SidType=0
		SourceName=Microsoft-Windows-Sysmon
		Type=Information
		RecordNumber=2915
		Keywords=None
		TaskCategory=CreateRemoteThread detected (rule: CreateRemoteThread)
		OpCode=Info
		Message=CreateRemoteThread detected:
		RuleName: -
		UtcTime: 2021-09-08 19:55:30.770
		SourceProcessGuid: {72893ba8-1125-6139-5d00-00000000c00}
		SourceProcessId: 5016
		SourceImage: C:\Windows\System32\wbem\unsecapp.exe
		TargetProcessGuid: {72893ba8-111d-6139-0c00-00000000c00}
		TargetProcessId: 672
		TargetImage: C:\Windows\System32\lsass.exe
		NewThreadId: 13980
		StartAddress: 0x000001D471950000
		StartModule: -
		StartFunction: -
		Collapse
		host = WIN-AOQKG2AS2Q7
		source = WinEventLog:Microsoft-Windows-Sysmon/Operational
		sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

C:\Windows\System32\lsass.exe

lsass.exe is a “Local Security Authentication Server” that can dump users' credentials ([OS Credential Dumping: LSASS Memory](#)) because lsass.exe stores not only a current user's OS credentials but also a domain admin's.

What is the web shell deployed on the system?

New Search

1 index = "*" sourcetype=iis post

862 events (before 1/15/23 9:29:07:000 PM) No Event Sampling

Events (862) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 day per column

cs_uri_stem

15 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
/powershell	216	25.058%
/napi/ensmdb/	208	24.13%
/ecp/DDI/DDIService.svc/GetList	177	20.534%
/OWA/auth.owa	101	11.717%
/owa/service.svc	67	7.773%
/Autodiscover/autodiscover.json	29	3.364%
/Microsoft-Server-ActiveSync/default.eas	27	3.132%
/owa/ev.owa2	15	1.74%
/owa/auth.owa	8	0.928%
/owa/auth/i3gfPctK1c2x.aspx	4	0.464%

i3gfPctK1c2x.aspx

What is the command line to execute this web shell?

splunk>enterprise Apps Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As Create Table View Close

1 index = "*" "i3gfPctK1c2x.aspx" All time

6 events (before 1/15/23 9:35:31.000 PM) No Event Sampling Job

Events (6) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 second per column

List Format 20 Per Page

Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 3 a sourcetype 3	INTERESTING FIELDS a c_ip 1 a cafeReqId 4 a ComputerName 1 a CorrelationID 1 a cs_method 1 a cs_uri_query 4 a cs_uri_stem 1 a cs_User_Agent 1 a date 1 # date_hour 1 # date_mday 1 # date_minute 1 # date_month 1 # date_second 3 a date_wday 1 # date_year 1		9/8/21 12:52:09.000 PM	09/08/2021 03:52:09 PM ... 22 lines omitted ... Company: Microsoft Corporation OriginalFileName: ATTRIB.EXE CommandLine: attrib.exe -r \\\\.win-aoqkg2as2q7.bellybear.local\C\$\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\i3gfPctK1c2x.aspx CurrentDirectory: c:\windows\system32\inetmgr\ Show all 37 lines host = WIN-AOQKG2AS2Q7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
			9/8/21 12:51:50.000 PM	2021-09-08 19:51:50 10.10.10.6 POST /owa/auth/i3gfPctK1c2x.aspx &CorrelationID=<empty>;&cafeReqId=3e3e86e0-0f1d-4a75-9719-de8fb42da4d9;&encoding=; 443 - 10.10.10.2 Mozilla/5.0 - 200 0 0 54 host = WIN-AOQKG2AS2Q7 source = C:\inetpub\logs\LogFiles\W3SVC1u_ex210908.log sourcetype = iis
			9/8/21 12:51:50.000 PM	2021-09-08 19:51:50 10.10.10.6 POST /owa/auth/i3gfPctK1c2x.aspx &CorrelationID=<empty>;&cafeReqId=3e3e86e0-0f1d-4a75-9719-de8fb42da4d9;&encoding=; 443 - 10.10.10.2 Mozilla/5.0 - 200 0 0 3759 host = WIN-AOQKG2AS2Q7 source = C:\inetpub\logs\LogFiles\W3SVC1u_ex210908.log sourcetype = iis

attrib.exe -r \\\\.win-aoqkg2as2q7.bellybear.local\C\$\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\i3gfPctK1c2x.aspx

Three CVEs did this leverage exploitation

CVE-2020-0796: Remote Code Execution vulnerability

CVE-2018-13374: An improper control in Fortinet OS 6.0.2, 5.6.7 and before.

CVE-2018-13379: a pre-authentication vulnerability that allows a threat actor to read arbitrary files by sending specially crafted HTTP requests to FortiOS devices.

Resources:

1. https://www.splunk.com/en_us/blog/industries/detecting-ransomware-attacks-with-splunk.html
2. <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>
3. <https://cybersecurityworks.com/blog/ransomware/is-conti-ransomware-on-a-roll.html>