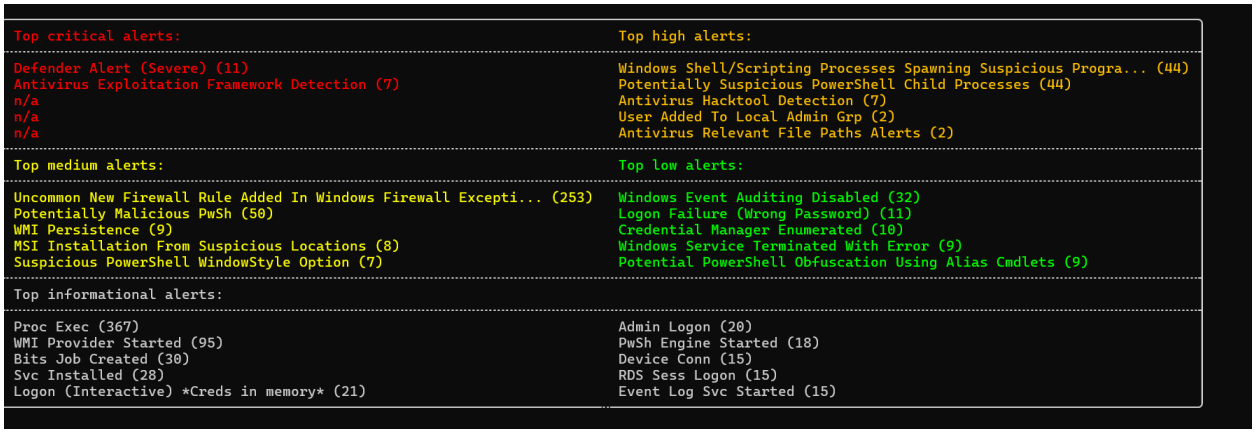
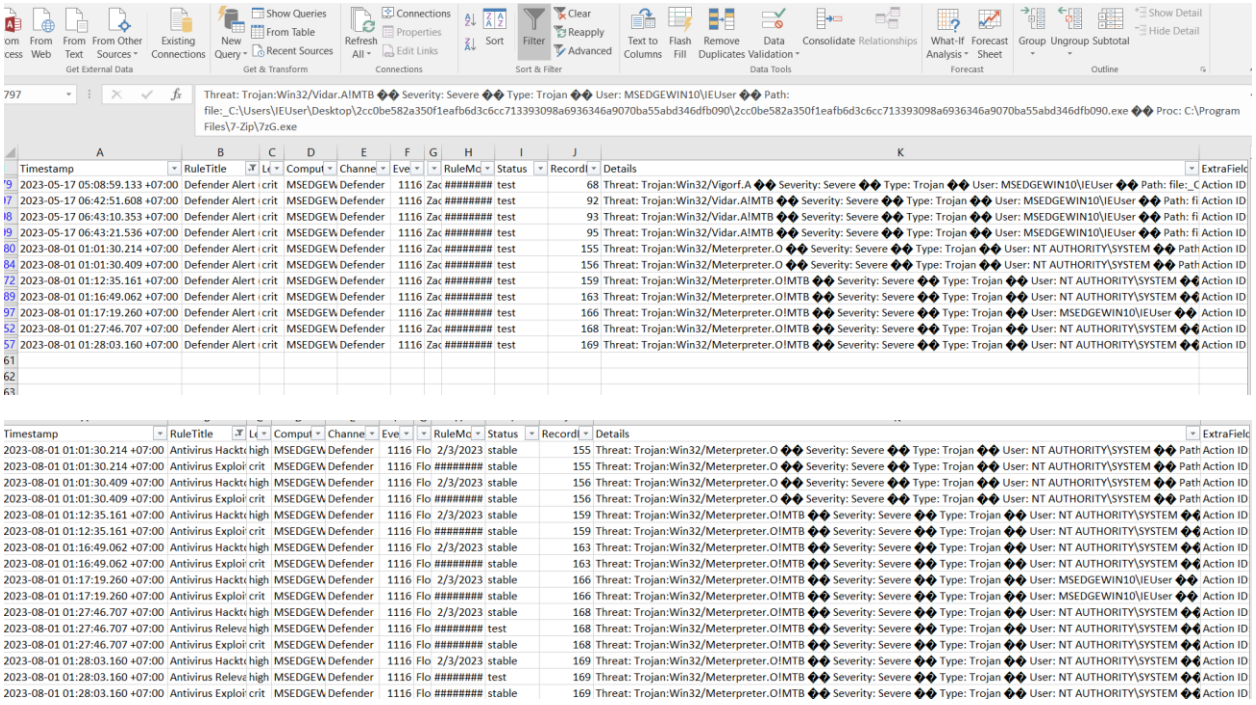
1.Phân tích luồng sự cố

Sử dụng opensource Hayabusa cho foder winevt log chúng ta được kết quả sau



Top critical alerts:	Top high alerts:
Defender Alert (Severe) (11)	Windows Shell/Scripting Processes Spawning Suspicious Progra... (44)
Antivirus Exploitation Framework Detection (7)	Potentially Suspicious PowerShell Child Processes (44)
n/a	Antivirus Hacktool Detection (7)
n/a	User Added To Local Admin Grp (2)
n/a	Antivirus Relevant File Paths Alerts (2)
Top medium alerts:	**Top low alerts:**
Uncommon New Firewall Rule Added In Windows Firewall Excepti... (253)	Windows Event Auditing Disabled (32)
Potentially Malicious PwSh (50)	Logon Failure (Wrong Password) (11)
WMI Persistence (9)	Credential Manager Enumerated (10)
MSI Installation From Suspicious Locations (8)	Windows Service Terminated With Error (9)
Suspicious PowerShell WindowStyle Option (7)	Potential PowerShell Obfuscation Using Alias Cmdlets (9)
Top informational alerts:	
Proc Exec (367)	Admin Logon (20)
WMI Provider Started (95)	PwSh Engine Started (18)
Bits Job Created (30)	Device Conn (15)
Svc Installed (28)	RDS Sess Logon (15)
Logon (Interactive) *Creds in memory* (21)	Event Log Svc Started (15)

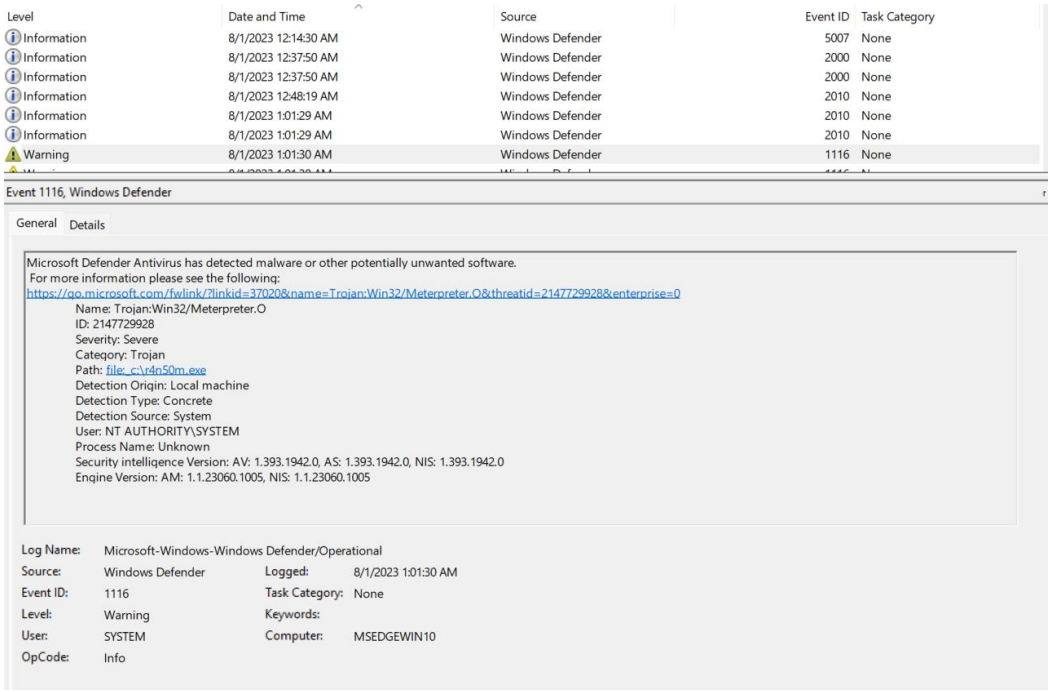
Chúng ta có thể thấy nó alerts rất nhiều ở mức critical và high như phát hiện AV Hacktool , AV Exploitation Framework , …..



Timestamp	RuleTitle	Details
2023-05-17 05:08:59.133 +07:00	Defender Alert	Threat: Trojan:Win32/Vigorf.A ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: MSEDGEWIN10\IEUser ◆◆ Path: file:_C
2023-05-17 06:42:51.608 +07:00	Defender Alert	Threat: Trojan:Win32/Vidar.A!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: MSEDGEWIN10\IEUser ◆◆ Path: fi
2023-05-17 06:43:10.353 +07:00	Defender Alert	Threat: Trojan:Win32/Vidar.A!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: MSEDGEWIN10\IEUser ◆◆ Path: fi
2023-05-17 06:43:21.536 +07:00	Defender Alert	Threat: Trojan:Win32/Vidar.A!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: MSEDGEWIN10\IEUser ◆◆ Path: fi
2023-08-01 01:01:30.214 +07:00	Defender Alert	Threat: Trojan:Win32/Meterpreter.O ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆ Path
2023-08-01 01:01:30.409 +07:00	Defender Alert	Threat: Trojan:Win32/Meterpreter.O ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆ Path
2023-08-01 01:12:35.161 +07:00	Defender Alert	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆
2023-08-01 01:16:49.062 +07:00	Defender Alert	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆
2023-08-01 01:17:19.260 +07:00	Defender Alert	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: MSEDGEWIN10\IEUser ◆◆
2023-08-01 01:27:46.707 +07:00	Defender Alert	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆
2023-08-01 01:28:03.160 +07:00	Defender Alert	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆

Timestamp	RuleTitle	Details
2023-08-01 01:01:30.214 +07:00	Antivirus Hackt	Threat: Trojan:Win32/Meterpreter.O ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆ Path
2023-08-01 01:01:30.214 +07:00	Antivirus Explo	Threat: Trojan:Win32/Meterpreter.O ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆ Path
2023-08-01 01:01:30.409 +07:00	Antivirus Hackt	Threat: Trojan:Win32/Meterpreter.O ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆ Path
2023-08-01 01:01:30.409 +07:00	Antivirus Explo	Threat: Trojan:Win32/Meterpreter.O ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆ Path
2023-08-01 01:12:35.161 +07:00	Antivirus Hackt	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆
2023-08-01 01:12:35.161 +07:00	Antivirus Explo	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆
2023-08-01 01:16:49.062 +07:00	Antivirus Hackt	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆
2023-08-01 01:16:49.062 +07:00	Antivirus Explo	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆
2023-08-01 01:17:19.260 +07:00	Antivirus Hackt	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: MSEDGEWIN10\IEUser ◆◆
2023-08-01 01:17:19.260 +07:00	Antivirus Explo	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: MSEDGEWIN10\IEUser ◆◆
2023-08-01 01:27:46.707 +07:00	Antivirus Hackt	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆
2023-08-01 01:27:46.707 +07:00	Antivirus Relea	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆
2023-08-01 01:27:46.707 +07:00	Antivirus Explo	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆
2023-08-01 01:28:03.160 +07:00	Antivirus Hackt	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆
2023-08-01 01:28:03.160 +07:00	Antivirus Relea	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆
2023-08-01 01:28:03.160 +07:00	Antivirus Explo	Threat: Trojan:Win32/Meterpreter.O!MTB ◆◆ Severity: Severe ◆◆ Type: Trojan ◆◆ User: NT AUTHORITY\SYSTEM ◆◆

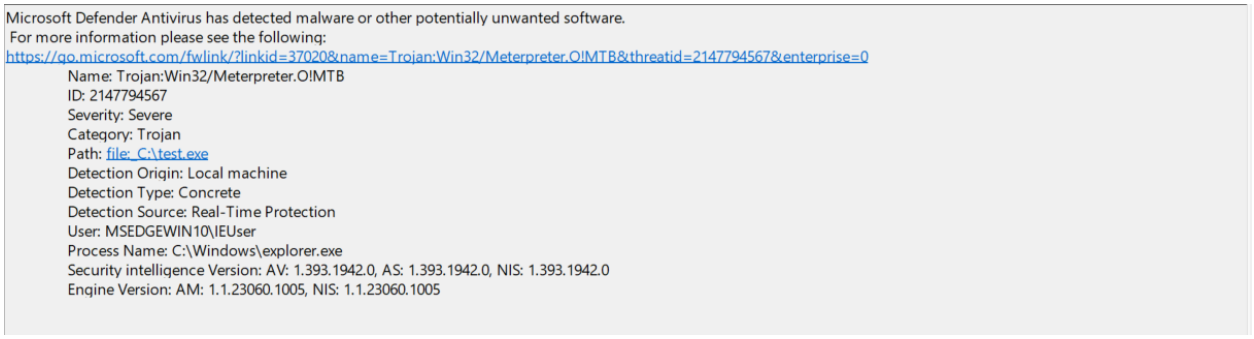
Phát hiện ra rất nhiều file đáng nghi windows defend detect là của Meterpreter gen ra.



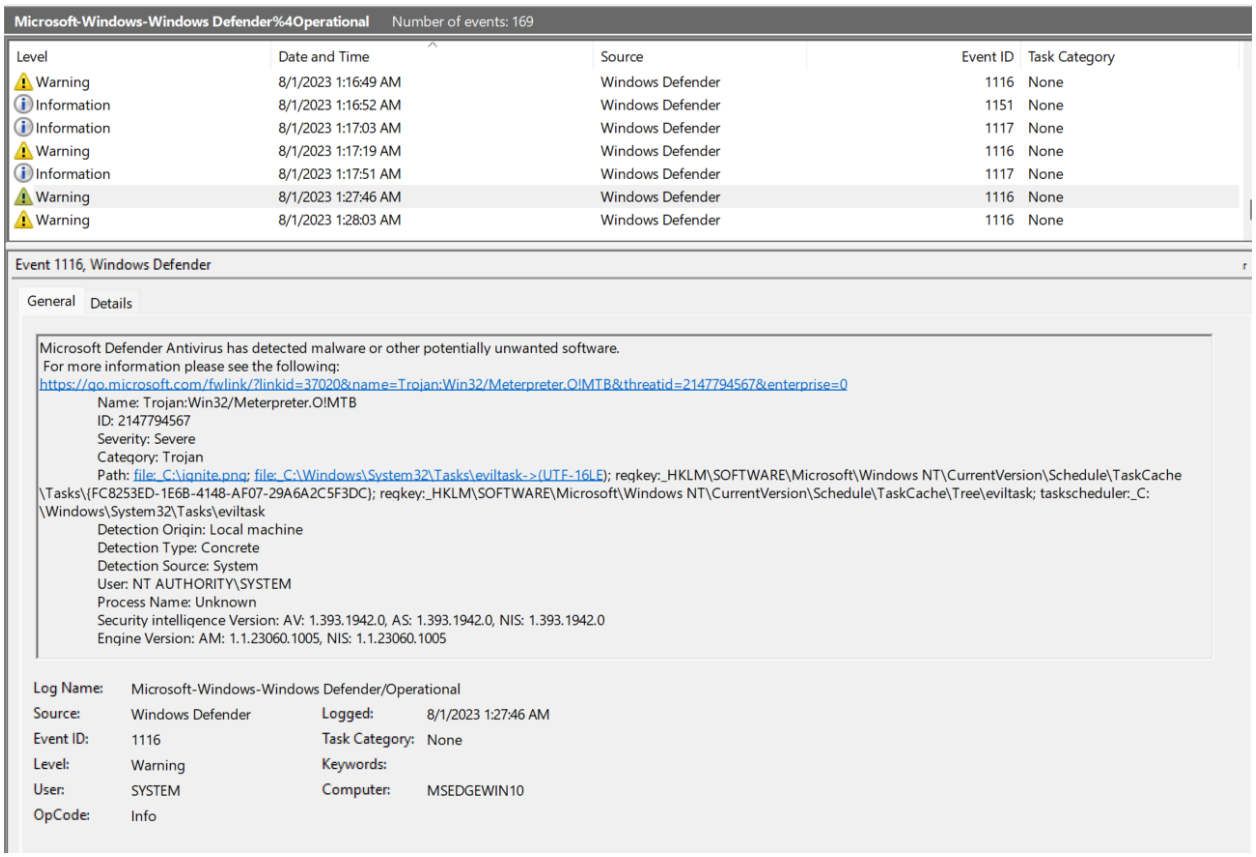
Level	Date and Time	Source	Event ID	Task Category
Information	8/1/2023 12:14:30 AM	Windows Defender	5007	None
Information	8/1/2023 12:37:50 AM	Windows Defender	2000	None
Information	8/1/2023 12:37:50 AM	Windows Defender	2000	None
Information	8/1/2023 12:48:19 AM	Windows Defender	2010	None
Information	8/1/2023 1:01:29 AM	Windows Defender	2010	None
Information	8/1/2023 1:01:29 AM	Windows Defender	2010	None
Warning	8/1/2023 1:01:30 AM	Windows Defender	1116	None

Kiểm tra trong WindowsDefend log . Vào lúc 1:01:30 Am ngày 8/1 windows defend phát hiện được 1 file đánh giá là Trojan .

Vào lúc 1:17:19AM phát hiện them 1 file test.exe bởi explorer.exe



Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Meterpreter.O!MTB&threatid=2147794567&enterprise=0
Name: Trojan:Win32/Meterpreter.O!MTB
ID: 2147794567
Severity: Severe
Category: Trojan
Path: file:_C:\test.exe
Detection Origin: Local machine
Detection Type: Concrete
Detection Source: Real-Time Protection
User: MSEDGEWIN10\IEUser
Process Name: C:\Windows\explorer.exe
Security intelligence Version: AV: 1.393.1942.0, AS: 1.393.1942.0, NIS: 1.393.1942.0
Engine Version: AM: 1.1.23060.1005, NIS: 1.1.23060.1005



Microsoft-Windows-Windows Defender%4Operational Number of events: 169

Level	Date and Time	Source	Event ID	Task Category
Warning	8/1/2023 1:16:49 AM	Windows Defender	1116	None
Information	8/1/2023 1:16:52 AM	Windows Defender	1151	None
Information	8/1/2023 1:17:03 AM	Windows Defender	1117	None
Warning	8/1/2023 1:17:19 AM	Windows Defender	1116	None
Information	8/1/2023 1:17:51 AM	Windows Defender	1117	None
Warning	8/1/2023 1:27:46 AM	Windows Defender	1116	None
Warning	8/1/2023 1:28:03 AM	Windows Defender	1116	None

Event 1116, Windows Defender

General Details

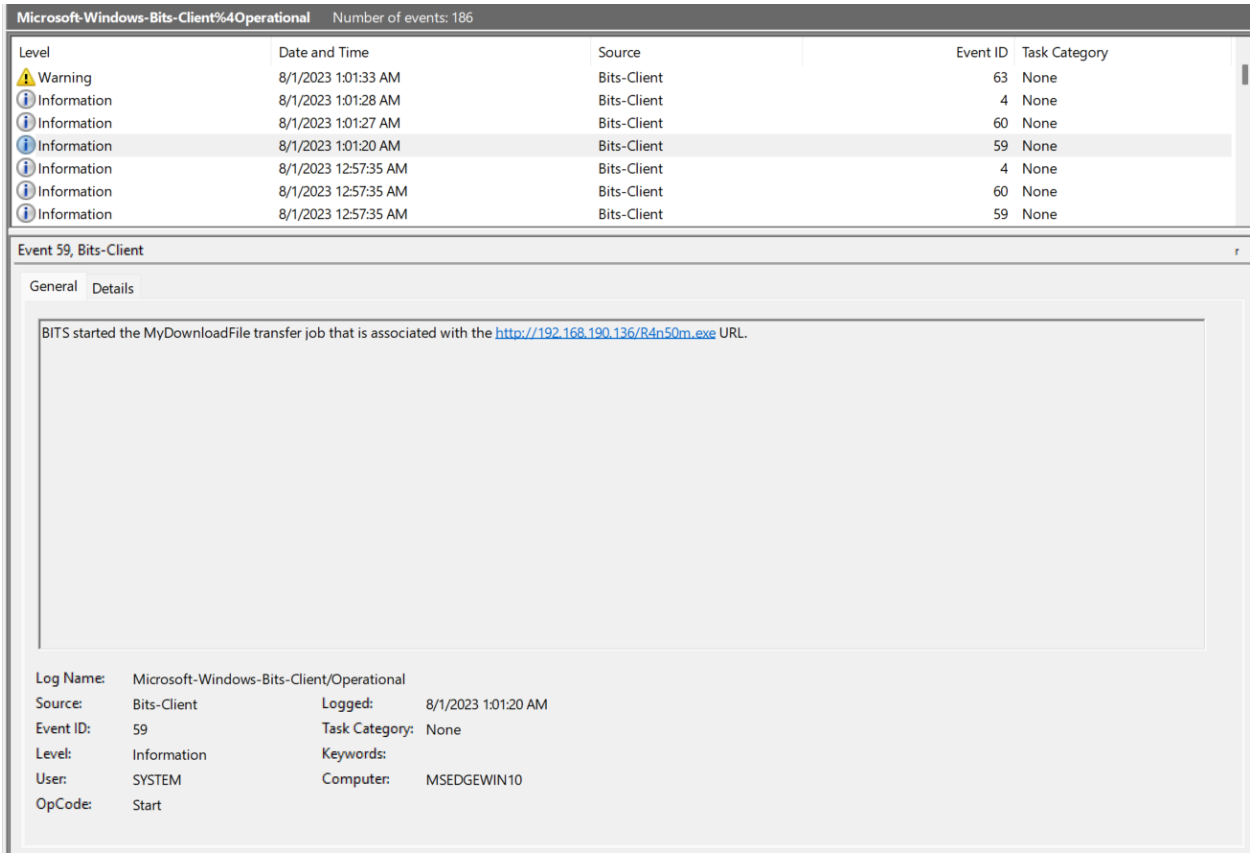
Microsoft Defender Antivirus has detected malware or other potentially unwanted software.
For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Meterpreter.O!MTB&threatid=2147794567&enterprise=0
Name: Trojan:Win32/Meterpreter.O!MTB
ID: 2147794567
Severity: Severe
Category: Trojan
Path: file:_C:\ignite.png; file:_C:\Windows\System32\Tasks\eviltask->(UTF-16LE); regkey:_HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{FC8253ED-1E6B-4148-AF07-29A6A2C5F3DC}; regkey:_HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\eviltask; taskscheduler:_C:\Windows\System32\Tasks\eviltask
Detection Origin: Local machine
Detection Type: Concrete
Detection Source: System
User: NT AUTHORITY\SYSTEM
Process Name: Unknown
Security intelligence Version: AV: 1.393.1942.0, AS: 1.393.1942.0, NIS: 1.393.1942.0
Engine Version: AM: 1.1.23060.1005, NIS: 1.1.23060.1005

Log Name: Microsoft-Windows-Windows Defender/Operational
Source: Windows Defender Logged: 8/1/2023 1:27:46 AM
Event ID: 1116 Task Category: None
Level: Warning Keywords:
User: SYSTEM Computer: MSEDGEWIN10
OpCode: Info

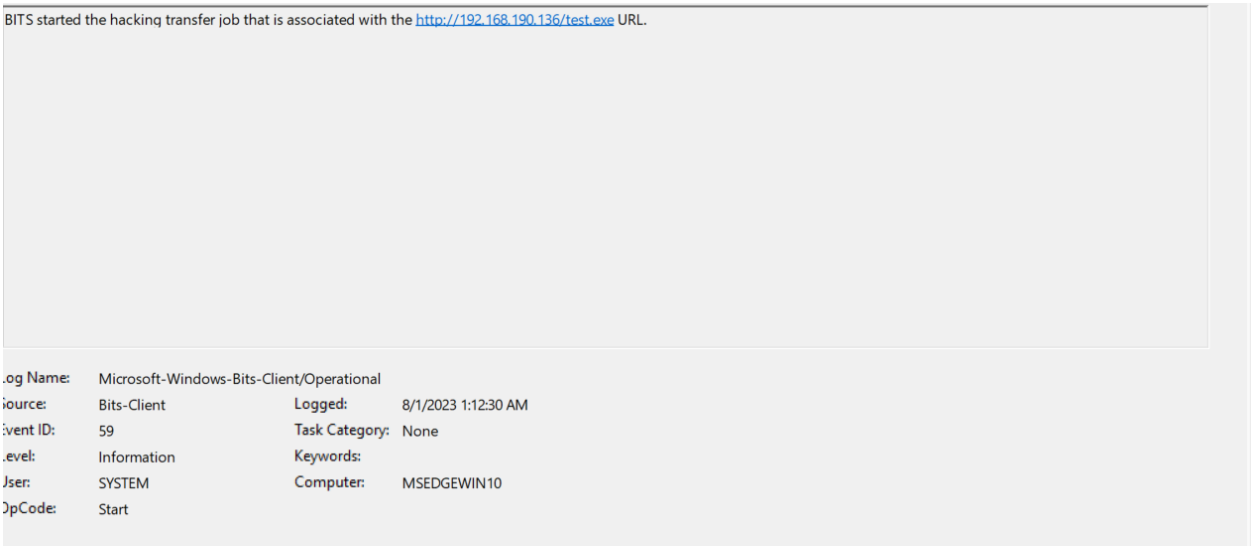
Đồng thời vào lúc 1:27:46 trong Schedule task detect them 1 eventask đã được thêm vào là eviltask có vẻ như nó đã được them bởi file độc hại

2023-08-01 01:09:32.439 +07:00	Potentially Susp	high	MSEDGEW	Sec	4688	Florian Ro	########	experimen	8265	Cmdline: ?? Proc: C:\Windows\System32\schtasks.exe ?? PID: 5432 ?? User: IEUser ?? LID: 0x2fbbc	M
2023-08-01 01:11:09.131 +07:00	Potentially Susp	high	MSEDGEW	Sec	4688	Florian Ro	########	experimen	8323	Cmdline: ?? Proc: C:\Windows\System32\bitsadmin.exe ?? PID: 7404 ?? User: IEUser ?? LID: 0x2fbbc	M
2023-08-01 01:11:44.563 +07:00	Potentially Susp	high	MSEDGEW	Sec	4688	Florian Ro	########	experimen	8359	Cmdline: ?? Proc: C:\Windows\System32\bitsadmin.exe ?? PID: 7880 ?? User: IEUser ?? LID: 0x2fbbc	M
2023-08-01 01:12:12.992 +07:00	Potentially Susp	high	MSEDGEW	Sec	4688	Florian Ro	########	experimen	8372	Cmdline: ?? Proc: C:\Windows\System32\bitsadmin.exe ?? PID: 1936 ?? User: IEUser ?? LID: 0x2fbbc	M
2023-08-01 01:12:30.884 +07:00	Potentially Susp	high	MSEDGEW	Sec	4688	Florian Ro	########	experimen	8385	Cmdline: ?? Proc: C:\Windows\System32\bitsadmin.exe ?? PID: 7424 ?? User: IEUser ?? LID: 0x2fbbc	M
2023-08-01 01:13:08.255 +07:00	Potentially Susp	high	MSEDGEW	Sec	4688	Florian Ro	########	experimen	8433	Cmdline: ?? Proc: C:\Windows\System32\schtasks.exe ?? PID: 5888 ?? User: IEUser ?? LID: 0x2fbbc	M
2023-08-01 01:23:20.317 +07:00	Potentially Susp	high	MSEDGEW	Sec	4688	Florian Ro	########	experimen	8950	Cmdline: ?? Proc: C:\Windows\System32\schtasks.exe ?? PID: 6336 ?? User: IEUser ?? LID: 0x2fbbc	M
2023-08-01 01:27:38.274 +07:00	Potentially Susp	high	MSEDGEW	Sec	4688	Florian Ro	########	experimen	9145	Cmdline: ?? Proc: C:\Windows\System32\schtasks.exe ?? PID: 5708 ?? User: IEUser ?? LID: 0x2fbbc	M

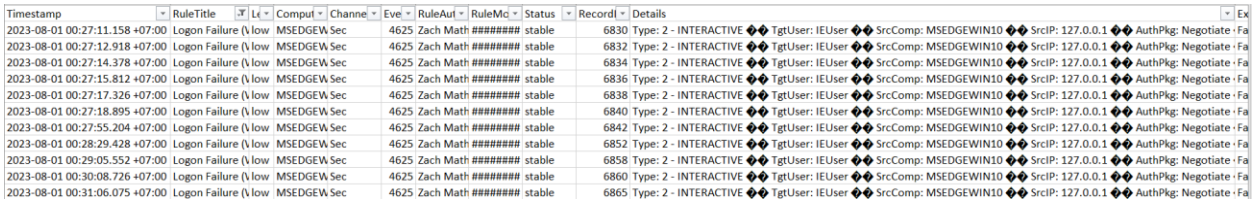
Vào khoảng thời gian mà mã độc được thực thi chúng ta có thể thấy các process có hoạt động đáng ngờ như schtasks.exe(tiến trình tạo lịch) với bitsadmin.exe là 1 tiến trình thực hiện BITS Job . Về cơ bản BITS job hoạt động gồm 2 trường URL sẽ chứa URL sử dụng để Download/Upload và Command sẽ chứa Command sẽ thực thi sau khi Download/Upload thành công



Đi vào Bits-Client log chúng ta có thể thấy thấy url mà nó đã download malware



Chúng ta có thể thấy user thực hiện những hành động đó là user IEUser . Có 1 dấu hiệu là thấy 11 lần đăng nhập thất bại có thể là dấu hiệu attacker cố gắng đăng nhập vào tài khoản đó nhưng đăng nhập có 11 lần thành công cho thấy dấu hiệu của việc password yếu dễ đoán cái này cần confirm lại



Timestamp	RuleTitle	L	Comput	Channe	Eve	RuleAut	RuleMo	Status	Record	Details	Ex
2023-08-01 00:27:11.158 +07:00	Logon Failure (\ low		MSEDGEW	Sec	4625	Zach Math	########	stable	6830	Type: 2 - INTERACTIVE ◆◆ TgtUser: IEUser ◆◆ SrcComp: MSEDGEWIN10 ◆◆ SrcIP: 127.0.0.1 ◆◆ AuthPkg: Negotiate	Fa
2023-08-01 00:27:12.918 +07:00	Logon Failure (\ low		MSEDGEW	Sec	4625	Zach Math	########	stable	6832	Type: 2 - INTERACTIVE ◆◆ TgtUser: IEUser ◆◆ SrcComp: MSEDGEWIN10 ◆◆ SrcIP: 127.0.0.1 ◆◆ AuthPkg: Negotiate	Fa
2023-08-01 00:27:14.378 +07:00	Logon Failure (\ low		MSEDGEW	Sec	4625	Zach Math	########	stable	6834	Type: 2 - INTERACTIVE ◆◆ TgtUser: IEUser ◆◆ SrcComp: MSEDGEWIN10 ◆◆ SrcIP: 127.0.0.1 ◆◆ AuthPkg: Negotiate	Fa
2023-08-01 00:27:15.812 +07:00	Logon Failure (\ low		MSEDGEW	Sec	4625	Zach Math	########	stable	6836	Type: 2 - INTERACTIVE ◆◆ TgtUser: IEUser ◆◆ SrcComp: MSEDGEWIN10 ◆◆ SrcIP: 127.0.0.1 ◆◆ AuthPkg: Negotiate	Fa
2023-08-01 00:27:17.326 +07:00	Logon Failure (\ low		MSEDGEW	Sec	4625	Zach Math	########	stable	6838	Type: 2 - INTERACTIVE ◆◆ TgtUser: IEUser ◆◆ SrcComp: MSEDGEWIN10 ◆◆ SrcIP: 127.0.0.1 ◆◆ AuthPkg: Negotiate	Fa
2023-08-01 00:27:18.895 +07:00	Logon Failure (\ low		MSEDGEW	Sec	4625	Zach Math	########	stable	6840	Type: 2 - INTERACTIVE ◆◆ TgtUser: IEUser ◆◆ SrcComp: MSEDGEWIN10 ◆◆ SrcIP: 127.0.0.1 ◆◆ AuthPkg: Negotiate	Fa
2023-08-01 00:27:55.204 +07:00	Logon Failure (\ low		MSEDGEW	Sec	4625	Zach Math	########	stable	6842	Type: 2 - INTERACTIVE ◆◆ TgtUser: IEUser ◆◆ SrcComp: MSEDGEWIN10 ◆◆ SrcIP: 127.0.0.1 ◆◆ AuthPkg: Negotiate	Fa
2023-08-01 00:28:29.428 +07:00	Logon Failure (\ low		MSEDGEW	Sec	4625	Zach Math	########	stable	6852	Type: 2 - INTERACTIVE ◆◆ TgtUser: IEUser ◆◆ SrcComp: MSEDGEWIN10 ◆◆ SrcIP: 127.0.0.1 ◆◆ AuthPkg: Negotiate	Fa
2023-08-01 00:29:05.552 +07:00	Logon Failure (\ low		MSEDGEW	Sec	4625	Zach Math	########	stable	6858	Type: 2 - INTERACTIVE ◆◆ TgtUser: IEUser ◆◆ SrcComp: MSEDGEWIN10 ◆◆ SrcIP: 127.0.0.1 ◆◆ AuthPkg: Negotiate	Fa
2023-08-01 00:30:08.726 +07:00	Logon Failure (\ low		MSEDGEW	Sec	4625	Zach Math	########	stable	6860	Type: 2 - INTERACTIVE ◆◆ TgtUser: IEUser ◆◆ SrcComp: MSEDGEWIN10 ◆◆ SrcIP: 127.0.0.1 ◆◆ AuthPkg: Negotiate	Fa
2023-08-01 00:31:06.075 +07:00	Logon Failure (\ low		MSEDGEW	Sec	4625	Zach Math	########	stable	6865	Type: 2 - INTERACTIVE ◆◆ TgtUser: IEUser ◆◆ SrcComp: MSEDGEWIN10 ◆◆ SrcIP: 127.0.0.1 ◆◆ AuthPkg: Negotiate	Fa

2.Mitre&ATTCK mapping

BITS Jobs [BITS Jobs, Technique T1197 - Enterprise | MITRE ATT&CK®]

Command and Scripting Interpreter: PowerShell [Command and Scripting Interpreter: PowerShell, Sub-technique T1059.001 - Enterprise | MITRE ATT&CK®]

Scheduled Task/Job [Scheduled Task/Job, Technique T1053 - Enterprise | MITRE ATT&CK®]

Account Manipulation [Account Manipulation, Technique T1098 - Enterprise | MITRE ATT&CK®]