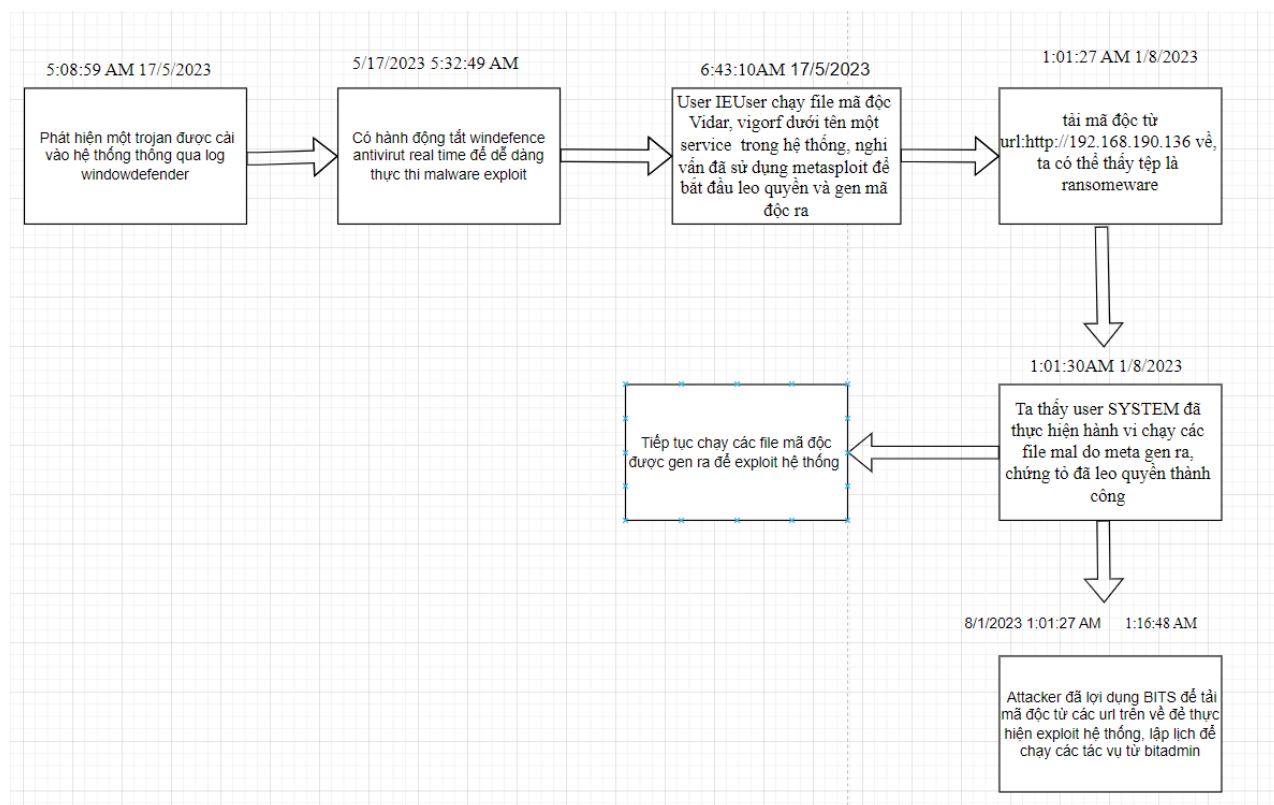


## Điều tra sự cố ZZZ

Sau khi điều tra, ta vẽ được luồng tấn công của hệ thống



## MITRE&ATTCK Mapping

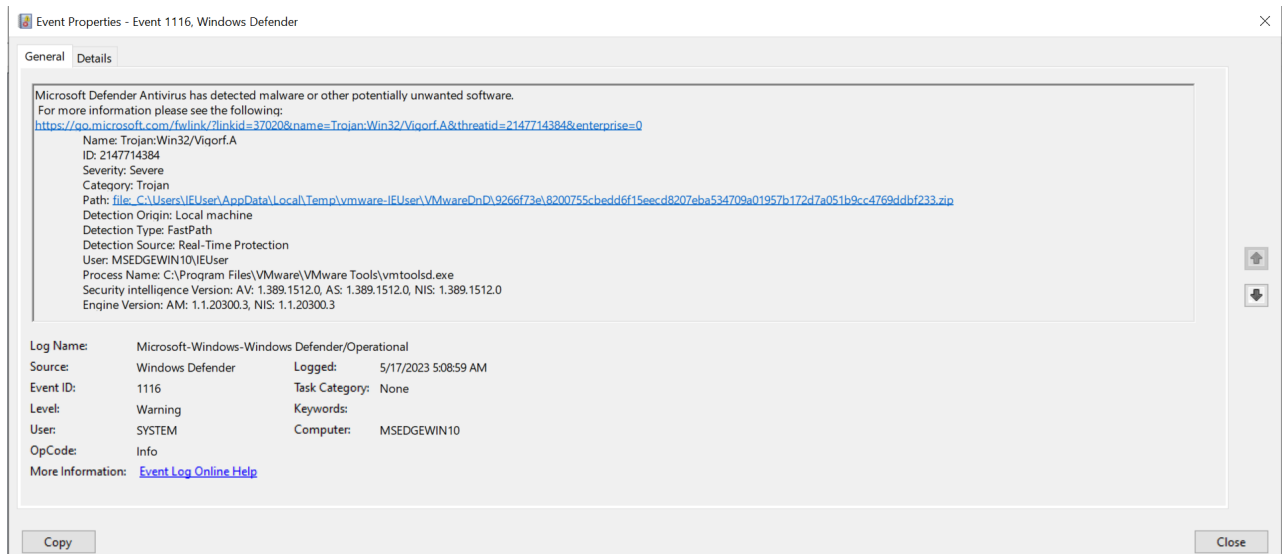
BITS Jobs [BITS Jobs, Technique T1197 - Enterprise | MITRE ATT&CK®](#)

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®](#)  
Privilege Escalation <https://attack.mitre.org/tactics/TA0004/>

Kiểm tra Log 1116, bắt đầu từ 5:08:59 AM ngày 17/5/2023, phát hiện mã độc trojan được cài vào hệ thống



Microsoft Defender Antivirus phát hiện một mối đe dọa Trojan:Win32/Vigorf.A, được xác định là mã độc nghiêm trọng (Severe). Mã độc này được phát hiện trong 1 tệp Zip ở trong 1 thư mục được tạo ra trong quá trình sử dụng VMware, thư mục này được lưu trong ổ C.

Ta thấy Process Name: C:\Program Files\VMware\VMware Tools\vmtoolsd.exe

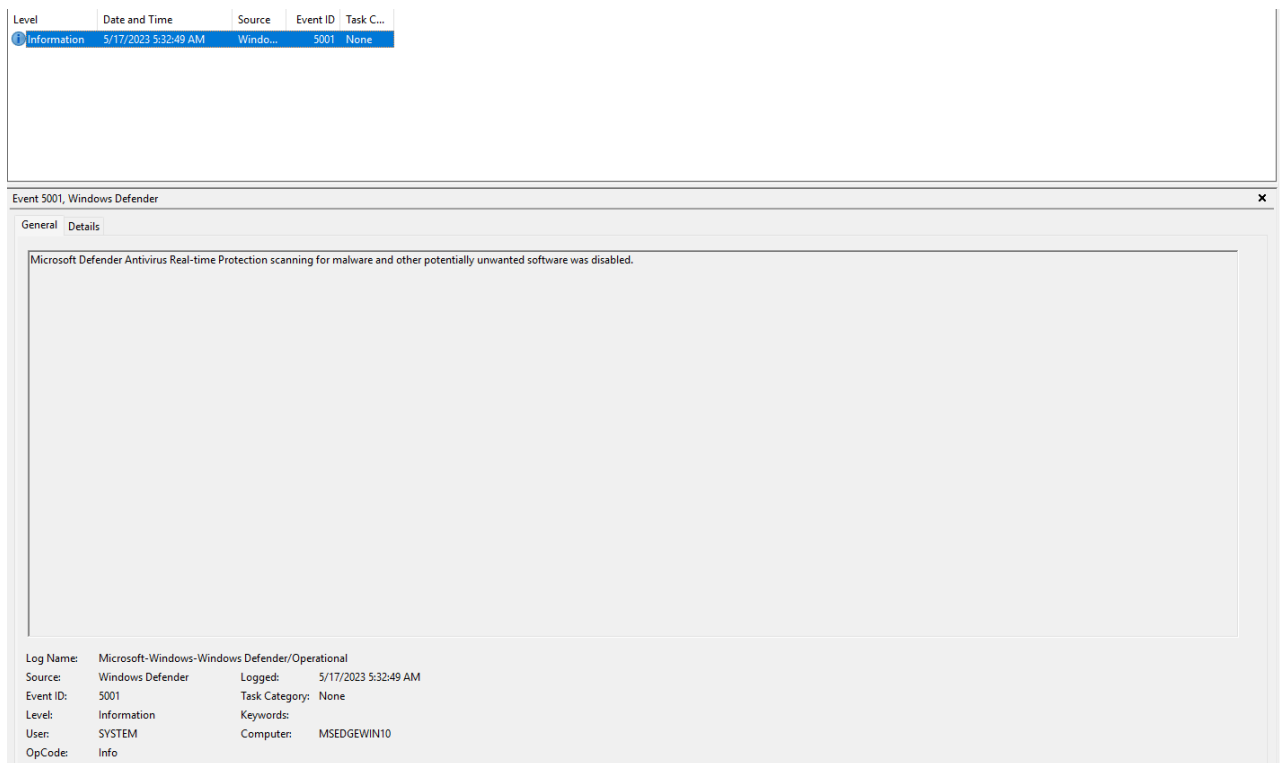
=> Mã độc liên quan đến tiến trình tiến trình vmtoolsd.exe, một phần mềm hỗ trợ cho VMware

Trojan này xâm nhập vào hệ thống thông qua một tệp ZIP khả nghi, có thể đã được truyền từ hệ thống chủ thông qua tính năng kéo-thả của VMware (VMwareDnD). Tiến trình vmtoolsd.exe có thể đã bị khai thác để chuyển tệp độc hại từ máy chủ chủ đến máy ảo thông qua chức năng kéo-thả.

Vigorf.A là một loại trojan được thiết kế để xâm nhập vào hệ thống bằng cách giả mạo như một phần mềm hợp lệ hoặc bị ẩn trong các tệp khác có thể download các mã độc khác, thu thập thông tin, mở backdoor, connect đến C2. Do ko có mẫu nên ko thể phân tích được nhưng cần phải kiểm tra lại chỉnh sửa registry và các config với defen

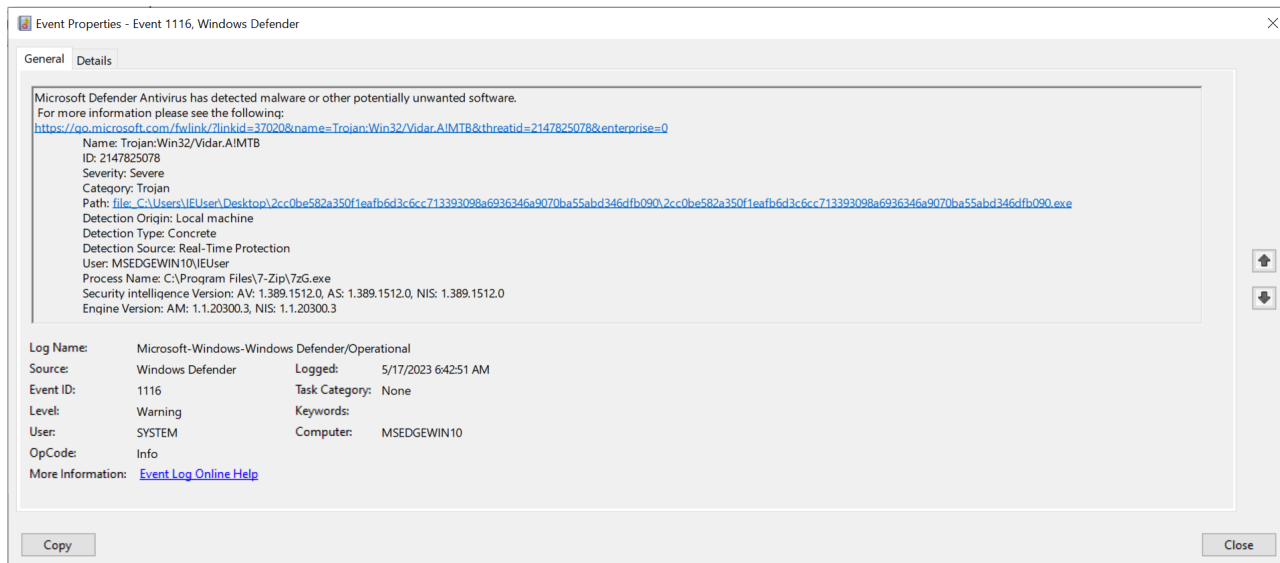
Ngoài ra ta thấy User thực hiện tiến trình này là IEUser (cần kiểm tra user này)

lúc 5h32:49 AM attacker có hành vi tắt Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software



=> đây có thể là hành động của malware tắt av nhằm exploit hệ thống

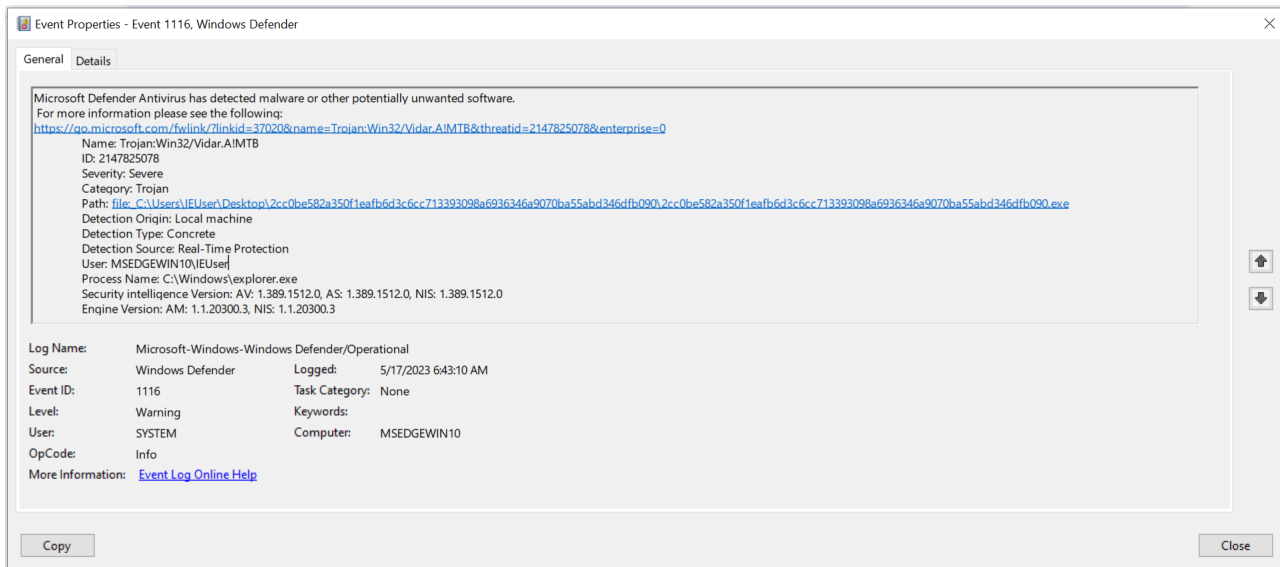
Lúc 6:42:51AM



Ta thấy tên của loại Trojan:Win32/Vidar.A!MTB. Vidar là một loại Trojan được sử dụng chủ yếu để đánh cắp thông tin nhạy cảm => có thể các dữ liệu nhạy cảm đã bị lộ

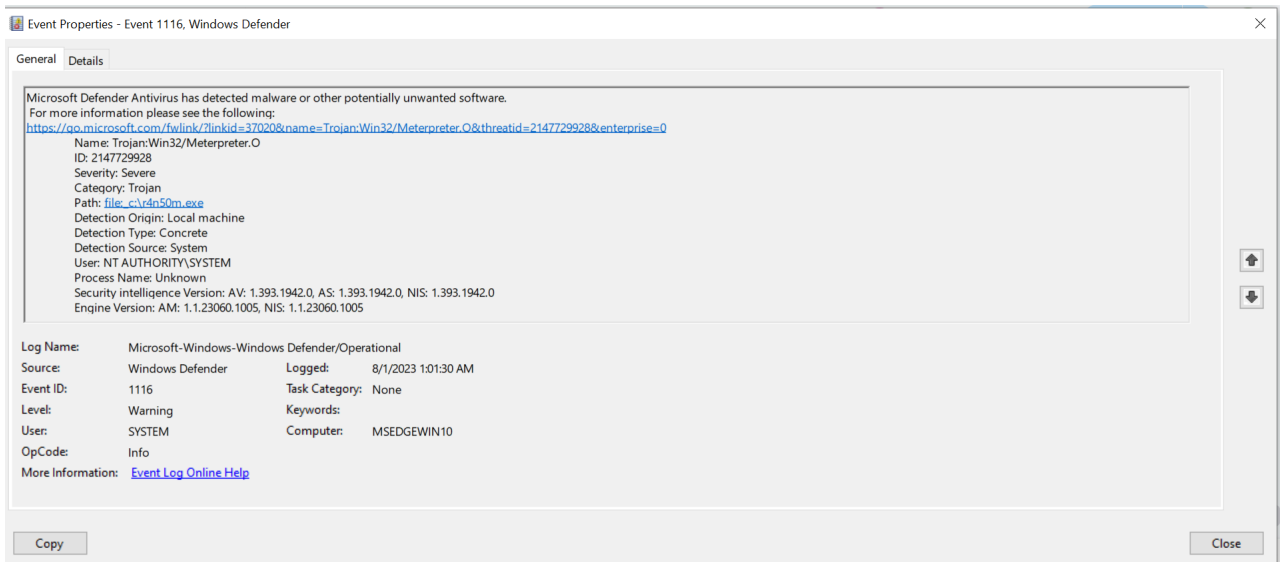
Nhìn vào Path, ta thấy mã độc đã được phát hiện ở Desktop của người dùng IEUser. Tập bị nhiễm có dạng .exe, là một loại tệp thực thi có khả năng hoạt động khi được chạy. Ta thấy Process Name:\Program Files\7-Zip\7zG.exe. => có thể mã độc đã lợi dụng quy trình giải nén này để thực thi mã độc và tránh được sự phát hiện vì giải nén tệp là 1 quy trình hợp pháp.=> có thể detect được bằng bộ sysinternals,mã độc này sẽ tiêu tốn cpu để hoạt động ngầm và tải xuống các mã độc khác nên sẽ dễ phát hiện

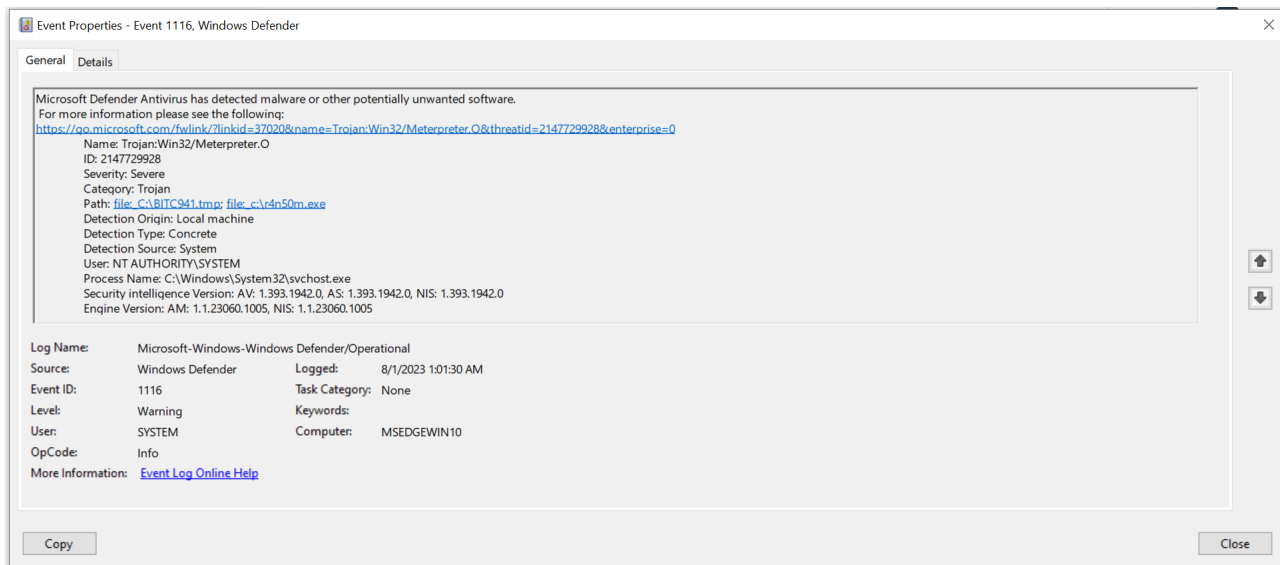
Lúc 6:43:10AM



Ta thấy người dùng IEUser tiếp tục chạy file mã độc Vidar được lưu ở Desktop thông qua quy trình C:\\Windows\\explorer.exe để tiếp tục đánh cắp thông tin.

Ngày 1/8/2023 lúc 1:01:30AM





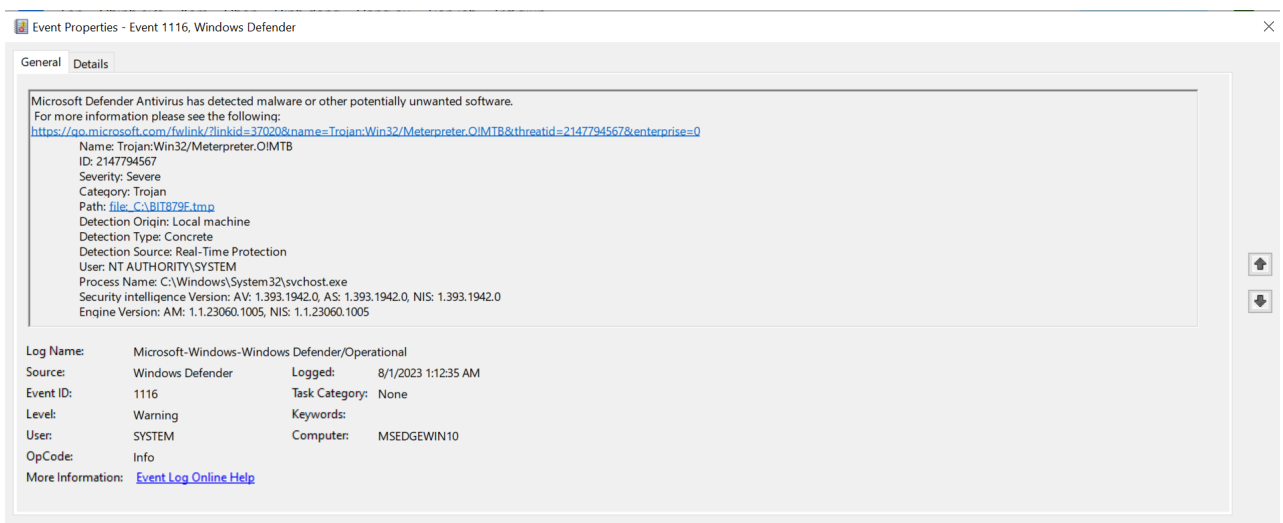
Ta thấy tên của loại Trojan:Win32/Meterpreter.O => Máy tính đã bị điều khiển từ xa và bị đánh cắp dữ liệu

Ta thấy Path:C:\BITC941.tmp(có thể là payload của mã độc) và c:\r4n50m.exe ( đây là vị trí tệp chứa mã độc). Ngoài ra mã độc được thực thi dưới User: NT AUTHORITY\SYSTEM => Mã độc đang chạy với quyền hệ thống cao nhất, có khả năng ảnh hưởng toàn bộ hệ thống.

Ta thấy Process Name: C:\Windows\System32\svchost.exe => mã độc đã inject payload vào tiến trình svchost.exe để tránh bị phát hiện do đây là 1 tiến trình hợp pháp.

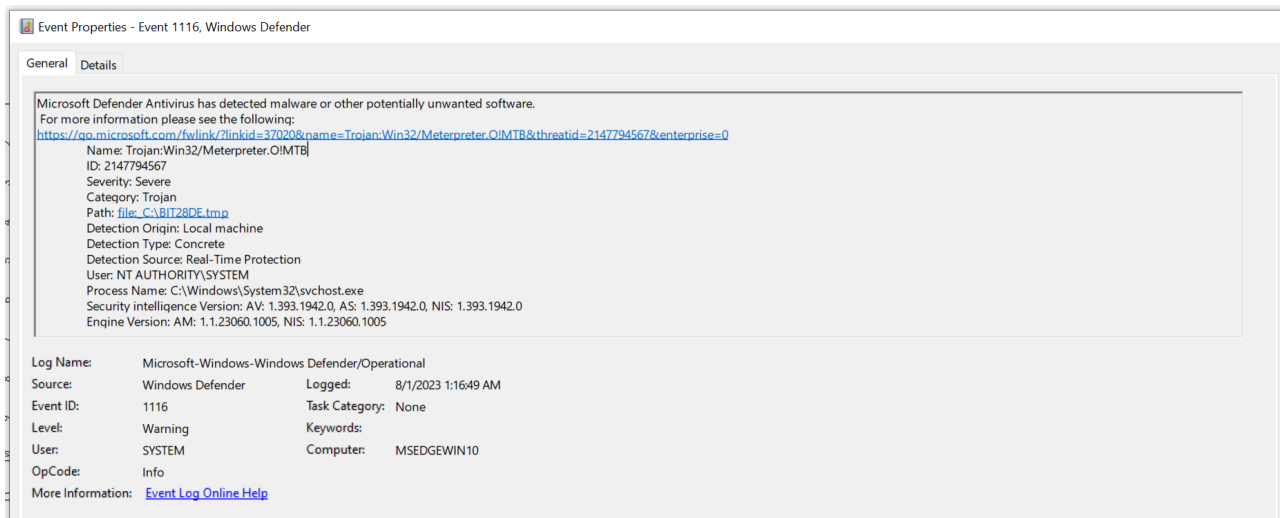
=> Có thể thấy những hành vi và các file mã độc trên do Meterpreter gen ra để exploit hệ thống. Sau khi attacker vào được hệ thống bằng 1 vul nào đó, nó sẽ triển khai meterpreter để exploit hệ thống.

Lúc 1:12:35AM



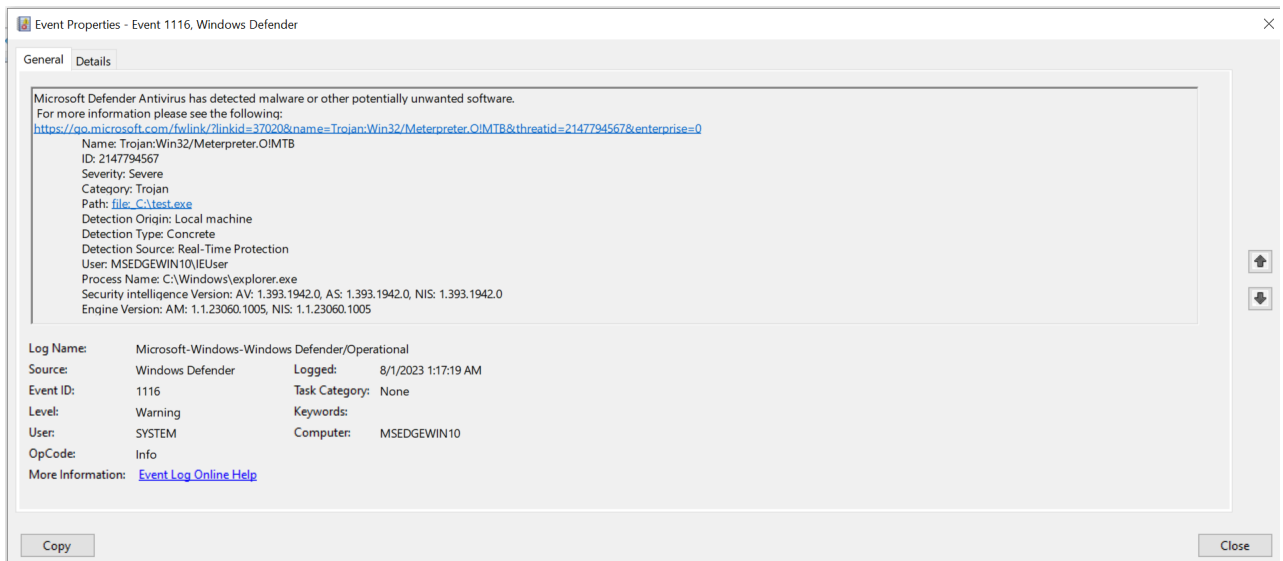
Ta thấy Path: file\_C:\BIT879F.tmp tiếp tục được thực thi qua tiến trình C:\Windows\System32\svchost.exe bằng User: NT AUTHORITY\SYSTEM.

Lúc 1:16:49AM



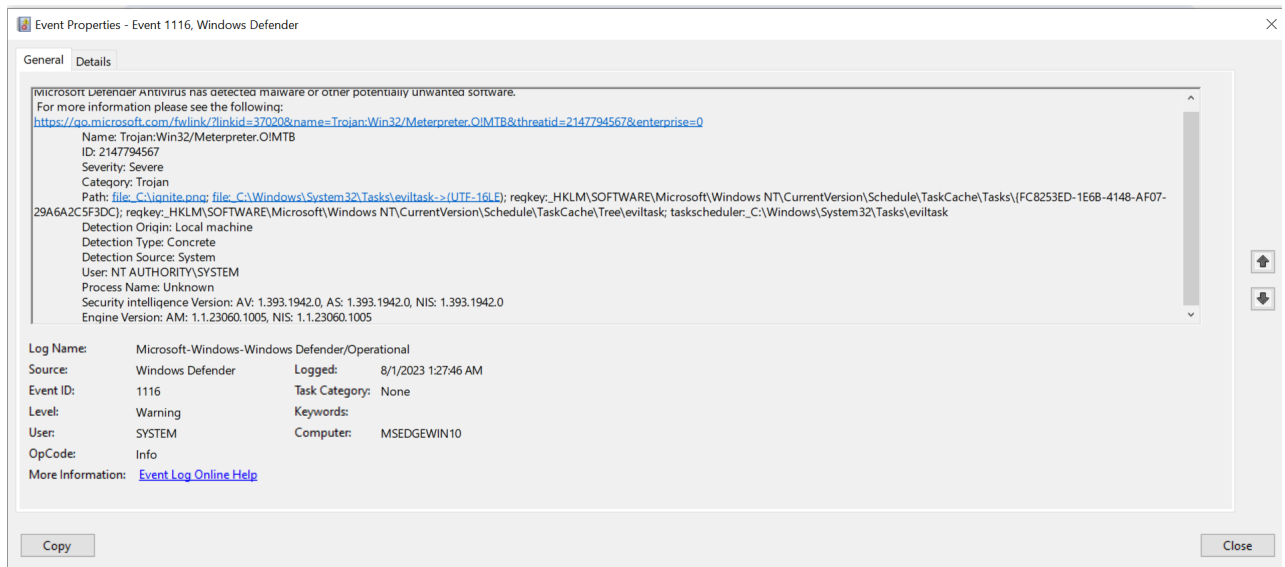
Ta tiếp tục thấy Path: file:\_C:\BIT28DE.tmp tiếp tục được thực thi qua tiến trình C:\Windows\System32\svchost.exe bằng User: NT AUTHORITY\SYSTEM.

Lúc 1:17:19AM



Ta tiếp tục thấy Path: file:\_C:\test.exe được thực thi qua tiến trình C:\Windows\explorer.exe bằng User: IEUser

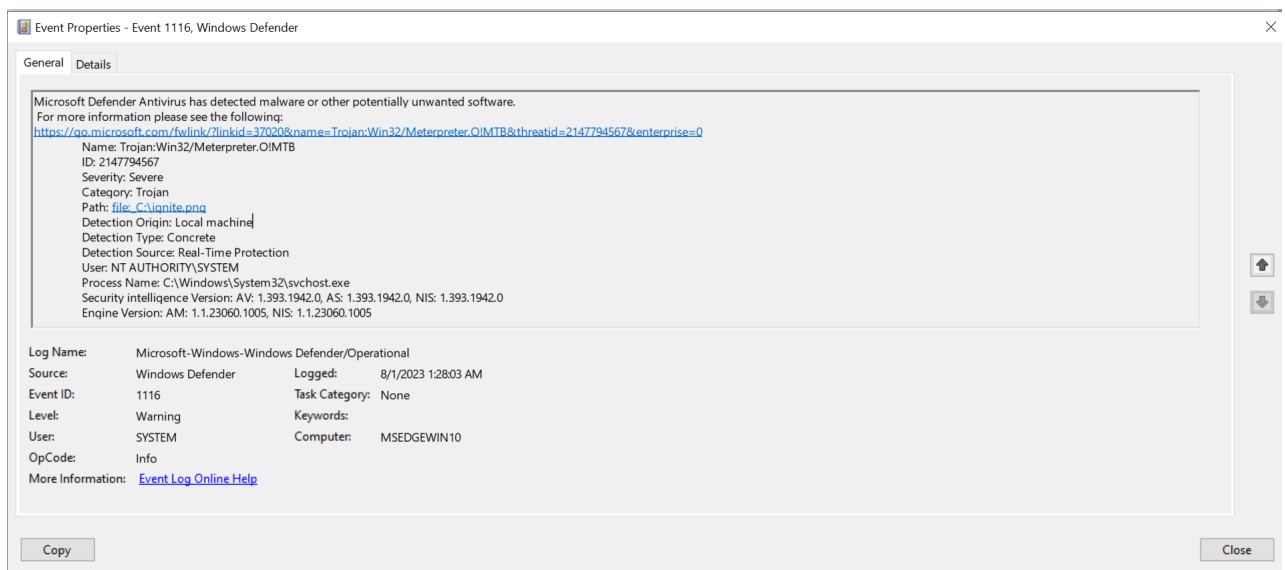
Lúc 1:27:46 AM



Ta thấy tệp file: \_C:\ignite.png (Tệp hình ảnh được sử dụng để ẩn payload ) và file: \_C:\Windows\System32\Tasks\eviltask (Tệp nhiệm vụ đã lên lịch có khả năng thực thi các hoạt động độc hại trên hệ thống) . Ngoài ra chúng còn được chạy bằng User: NT AUTHORITY\SYSTEM.

=> Mã độc dễ dàng vượt qua các cơ chế bảo vệ và thực hiện các hành vi độc hại.

Lúc 1:29:03 1/8/2023



Ta thấy tệp file: \_C:\ignite.png được thực thi qua tiến trình C:\Windows\System32\svchost.exe. Nó còn được chạy bằng User: NT AUTHORITY\SYSTEM.

=> Mã độc inject mã vào svchost.exe, một tiến trình hợp lệ và quan trọng của hệ điều hành Windows. Điều này giúp nó che giấu hoạt động và tránh bị phát hiện.

Kiểm tra event ID 4688

Vào thời điểm 8/1/2023 1:27:38 AM ta thấy một tiến trình lập lịch từ pwsh

Level	Date and Time	Source	Event ID	Task Ca...
Information	8/1/2023 1:27:38 AM	Micros...	4688	Process...
Information	8/1/2023 1:27:26 AM	Micros...	4688	Process...
Information	8/1/2023 1:27:26 AM	Micros...	4688	Process...
Information	8/1/2023 1:27:26 AM	Micros...	4688	Process...
Information	8/1/2023 1:27:00 AM	Micros...	4688	Process...
Information	8/1/2023 1:27:00 AM	Micros...	4688	Process...
Information	8/1/2023 1:26:00 AM	Micros...	4688	Process...
Information	8/1/2023 1:26:00 AM	Micros...	4688	Process...

Event 4688, Microsoft Windows security auditing.

General

Details

A new process has been created.

Creator Subject:

Security ID: S-1-5-21-321011808-3761883066-353627080-1000

Account Name: IEUser

Account Domain: MSEdgeWIN10

Logon ID: 0x2F8BC

Target Subject:

Security ID: NULL SID

Account Name: -

Account Domain: -

Logon ID: 0x0

Process Information:

New Process ID: 0x164c

New Process Name: C:\Windows\System32\schtasks.exe

Token Elevation Type: TokenElevationTypeFull (2)

Mandatory Label: Mandatory Label\High Mandatory Level

Creator Process ID: 0xc08

Creator Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Process Command Line:

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Log Name: Security

Source: Microsoft Windows security

Event ID: 4688

Level: Information

User: N/A

OpCode: Info

Logged: 8/1/2023 1:27:38 AM

Task Category: Process Creation

Keywords: Audit Success

Computer: MSEdgeWIN10

Trace tiếp với parent ta thấy sinh ra các tiến trình BITS job



Level	Date and Time	Source	Event ID	Task Category
Information	8/1/2023 1:12:56 AM	Microsoft Windows security auditing	4688	Process Creation
Information	8/1/2023 1:12:35 AM	Microsoft Windows security auditing	4688	Process Creation
Information	8/1/2023 1:12:32 AM	Microsoft Windows security auditing	4688	Process Creation
Information	8/1/2023 1:12:31 AM	Microsoft Windows security auditing	4688	Process Creation
Information	8/1/2023 1:12:31 AM	Microsoft Windows security auditing	4688	Process Creation
Information	8/1/2023 1:12:31 AM	Microsoft Windows security auditing	4688	Process Creation
Information	8/1/2023 1:12:30 AM	Microsoft Windows security auditing	4688	Process Creation
Information	8/1/2023 1:12:12 AM	Microsoft Windows security auditing	4688	Process Creation

Event 4688, Microsoft Windows security auditing.

General

Details

A new process has been created.

Creator Subject:

- Security ID: S-1-5-21-321011808-3761883066-353627080-1000
- Account Name: IEUser
- Account Domain: MSEDGEWIN10
- Logon ID: 0x2FBBC

Target Subject:

- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Process Information:

- New Process ID: 0x1d00
- New Process Name: C:\Windows\System32\bitsadmin.exe
- Token Elevation Type: TokenElevationTypeFull (2)
- Mandatory Label: Mandatory Label\High Mandatory Level
- Creator Process ID: 0xc08
- Creator Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
- Process Command Line:

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Log Name: Security

Source: Microsoft Windows security auditing

Event ID: 4688

Level: Information

User: N/A

OpCode: Info

Logged: 8/1/2023 1:12:30 AM

Task Category: Process Creation

Keywords: Audit Success

Computer: MSEDGEWIN10

Find

Find what: 0xc08

Find Next

Cancel

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. BITS job là các tác vụ truyền tải dữ liệu do các ứng dụng hoặc hệ điều hành tạo ra. Dưới đây là các loại chính:

### 1. Download Jobs:

- Tải xuống tệp từ máy chủ hoặc URL đến hệ thống cục bộ.

### 2. Upload Jobs:

- Tải tệp từ hệ thống cục bộ lên máy chủ.










### 3. Upload-Reply Jobs:

- Tải lên tệp và nhận phản hồi từ máy chủ (phổ biến trong các hệ thống xử lý dữ liệu trực tuyến).

Vào log của BITS client để kiểm tra khoảng thời gian trên.

Microsoft-Windows-Bits-Client%4Operational

Number of events: 186

Level	Date and Time	Source	Event ID	Task Ca...
 Information	8/1/2023 1:16:48 AM	Bits-Cli...	4	None
 Information	8/1/2023 1:16:48 AM	Bits-Cli...	60	None
 Information	8/1/2023 1:16:48 AM	Bits-Cli...	59	None
 Information	8/1/2023 1:16:48 AM	Bits-Cli...	3	None
 Warning	8/1/2023 1:12:34 AM	Bits-Cli...	63	None
 Information	8/1/2023 1:12:32 AM	Bits-Cli...	4	None
 Information	8/1/2023 1:12:31 AM	Bits-Cli...	60	None
 Information	8/1/2023 1:12:30 AM	Bits-Cli...	59	None
 Information	8/1/2023 1:11:09 AM	Bits-Cli...	3	None

Event 60, Bits-Client

General

Details

BITS stopped transferring the BITS Transfer transfer job that is associated with the <http://192.168.190.136/test.exe> URL. The status code is 0x0.

Log Name:

Microsoft-Windows-Bits-Client/Operational

Source:

Bits-Client

Logged:

8/1/2023 1:16:48 AM

Event ID:

60

Task Category:

None

Level:

Information

Keywords:

User:

SYSTEM

Computer:

MSEDGEWIN10

OpCode:

Stop

vào lúc 8/1/2023 1:16:48 AM attacker đã thực hiện tải mã độc từ url trên

Microsoft-Windows-Bits-Client%4Operational Number of events: 186

Level	Date and Time	Source	Event ID	Task Ca...
Information	8/1/2023 1:12:31 AM	Bits-Cli...	60	None
Information	8/1/2023 1:12:30 AM	Bits-Cli...	59	None
Information	8/1/2023 1:11:09 AM	Bits-Cli...	3	None
Information	8/1/2023 1:06:50 AM	Bits-Cli...	3	None
Warning	8/1/2023 1:01:33 AM	Bits-Cli...	63	None
Information	8/1/2023 1:01:28 AM	Bits-Cli...	4	None
Information	8/1/2023 1:01:27 AM	Bits-Cli...	60	None
Information	8/1/2023 1:01:20 AM	Bits-Cli...	59	None
Information	8/1/2023 12:57:35 AM	Bits-Cli...	4	None

Event 60, Bits-Client

General Details

BITS stopped transferring the MyDownloadFile transfer job that is associated with the <http://192.168.190.136/R4n50m.exe> URL. The status code is 0x0.

Log Name: Microsoft-Windows-Bits-Client/Operational  
Source: Bits-Client Logged: 8/1/2023 1:01:27 AM  
Event ID: 60 Task Category: None  
Level: Information Keywords:  
User: SYSTEM Computer: MSEDGEWIN10  
OpCode: Stop

vào lúc 8/1/2023 1:01:27 AM cũng thực hiện tải mã độc từ url trên về, ta có thể thấy tệp là ransomware  
=> Attacker đã lợi dụng BITS để tải mã độc từ các url trên về để thực hiện exploit hệ thống