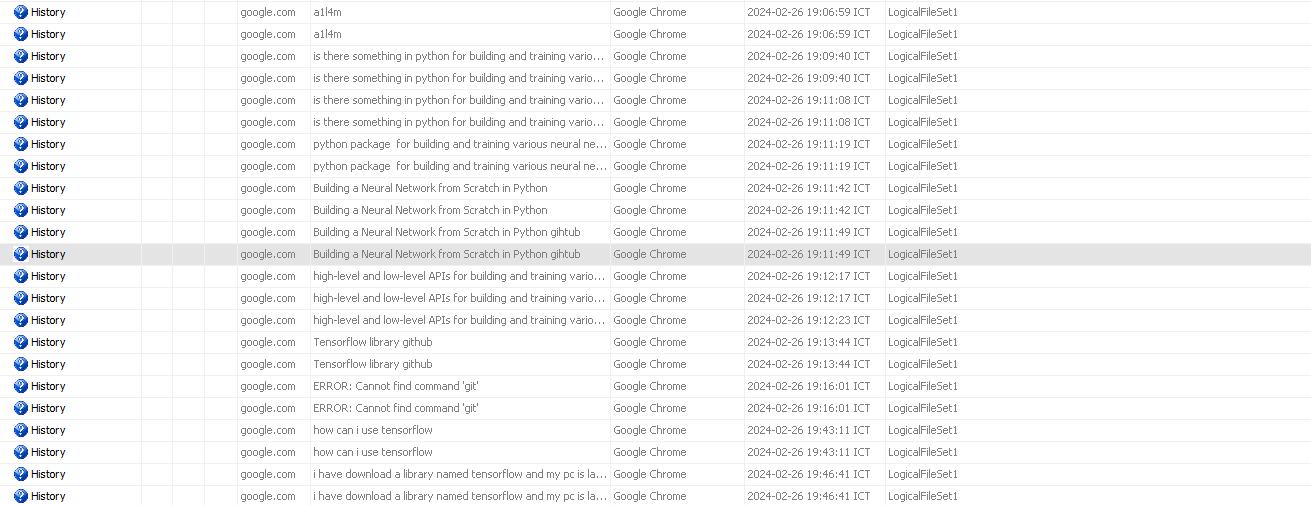
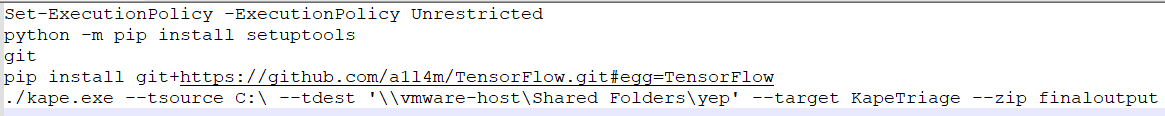
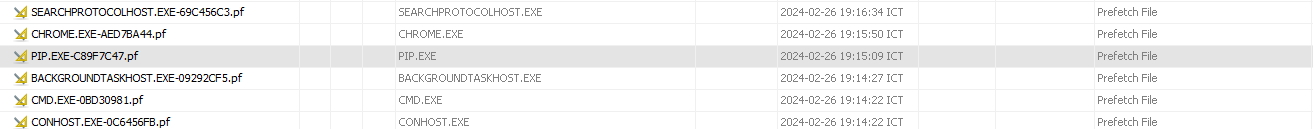
**1 Phân tích luồng sự cố**

****

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



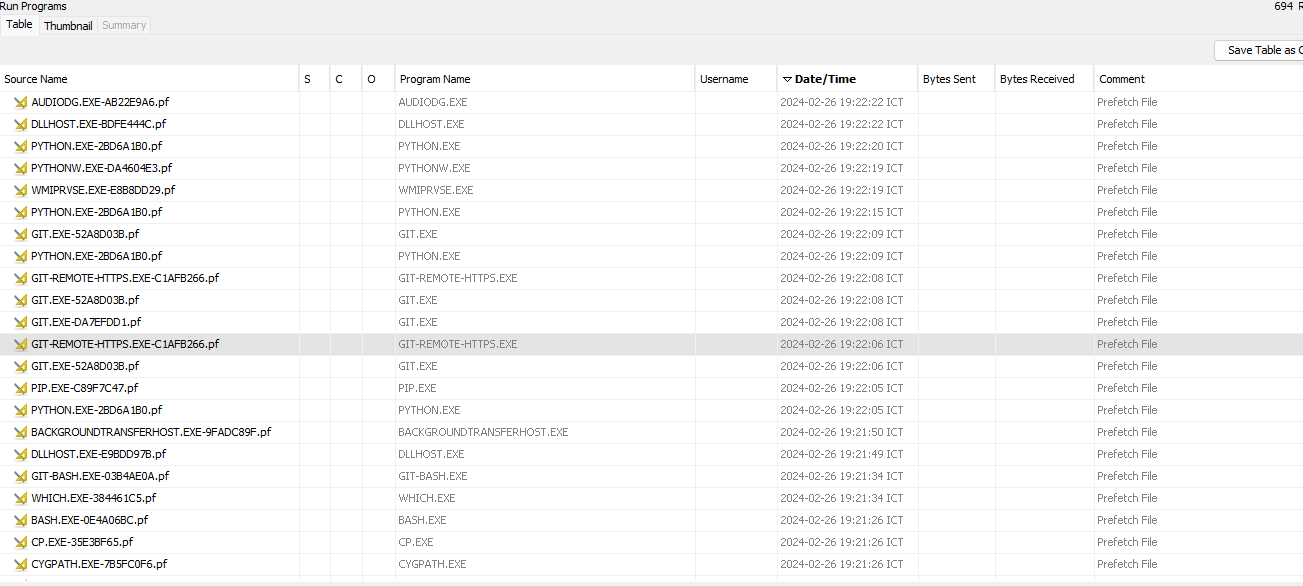
Check trong lịch sử command powershell chúng ta có thể thấy command Set-ExecutionPolicy -ExecutionPolicy Unrestricted thiết lập chính sách thực thi script (Execution Policy) của PowerShell thành "Unrestricted" có thể khiến powershell thực thi mọi loại script trên hệ thống . Chúng ta cũng có thể thấy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



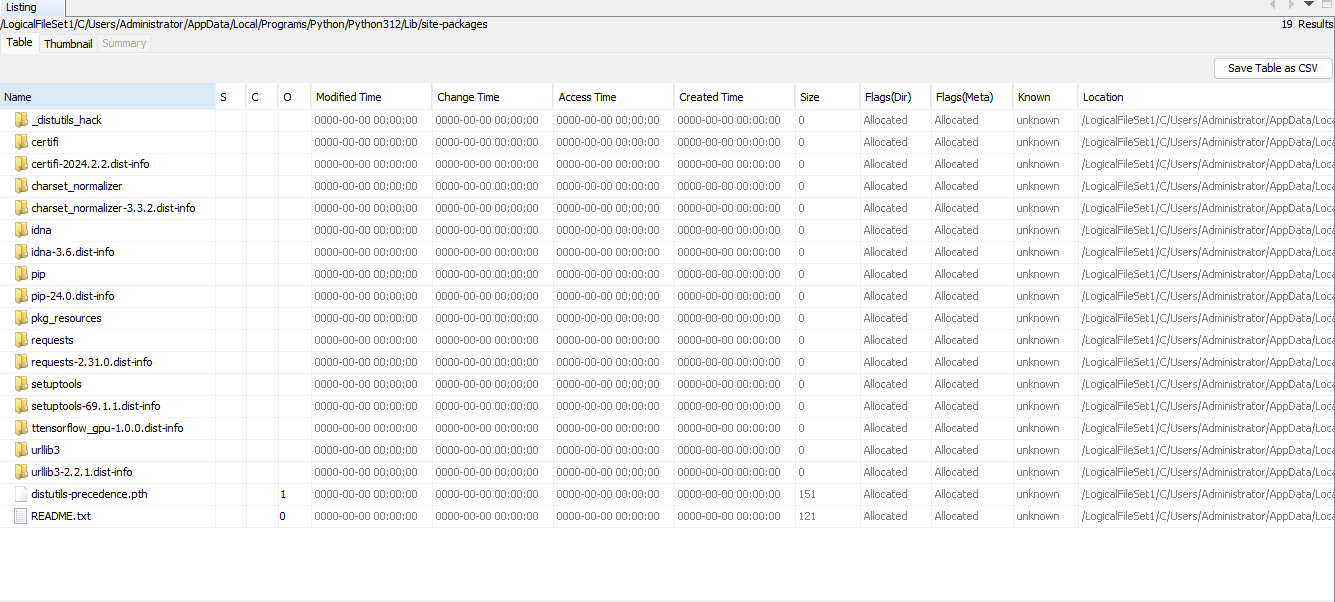
Nhìn vào tệp Prefetch chúng ta có thể thấy user đã chạy lệnh pip vào lúc 19:15 nhưng có vẻ như không được nên đã tìm kiếm trên trình duyệt



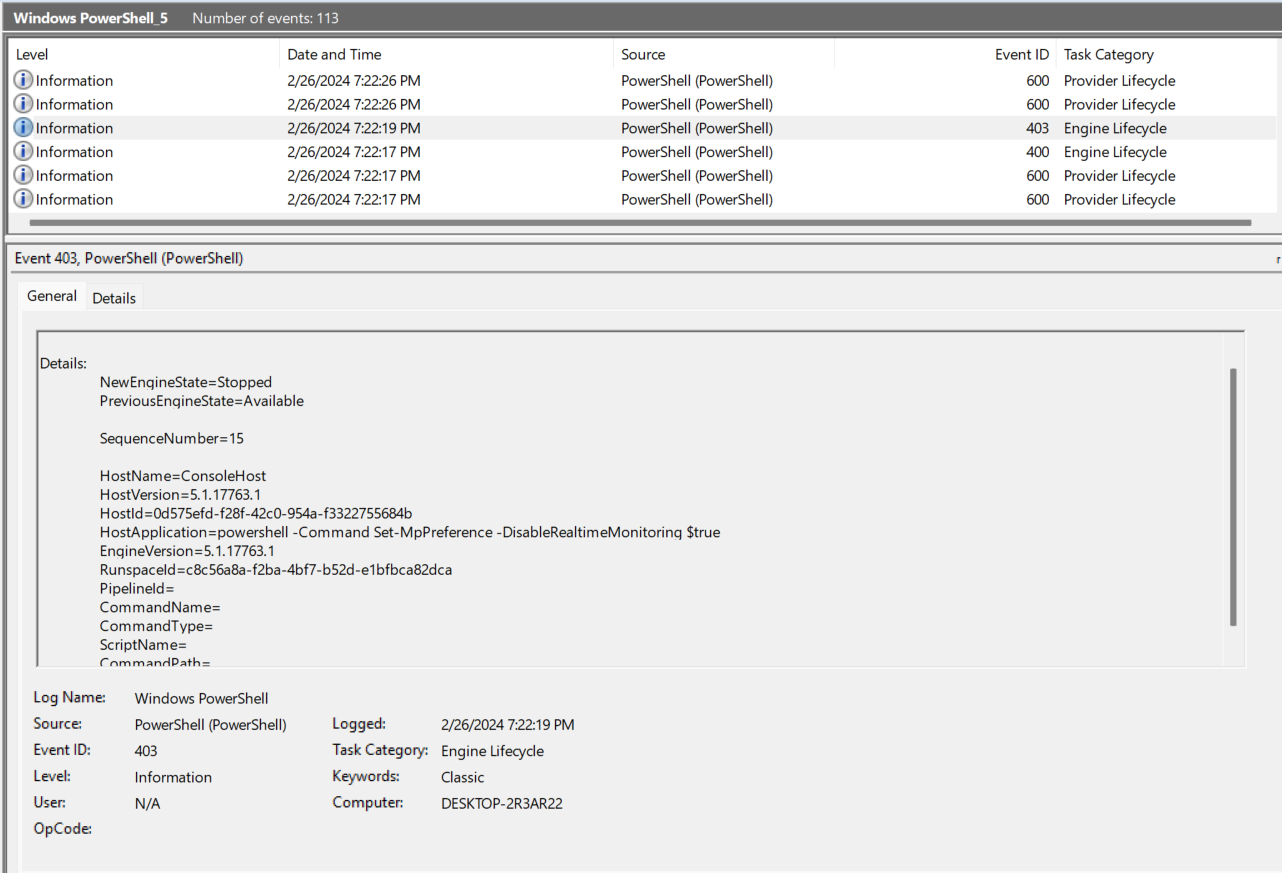
Vào lúc 19:16 user đã download git về để setup

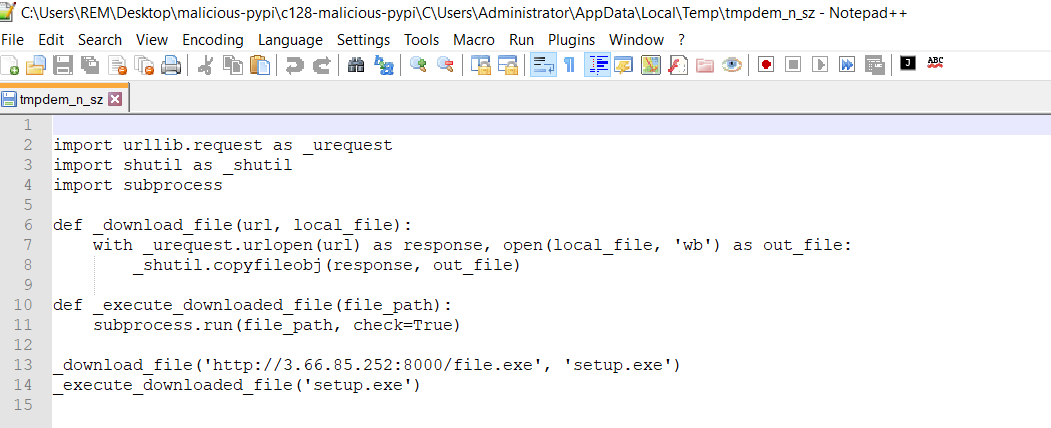


Lúc 19:22 user đã thực hiện command pip install từ URL https://github.com/all4m/TensorFlow.git #egg=TensorFlow . Tại thời điểm viết report này thì miền url này đã close nên không thể xem được source nguồn và source của package tải về cũng không thể được tìm thấy chỉ có thể tìm thấy folder chứa file config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



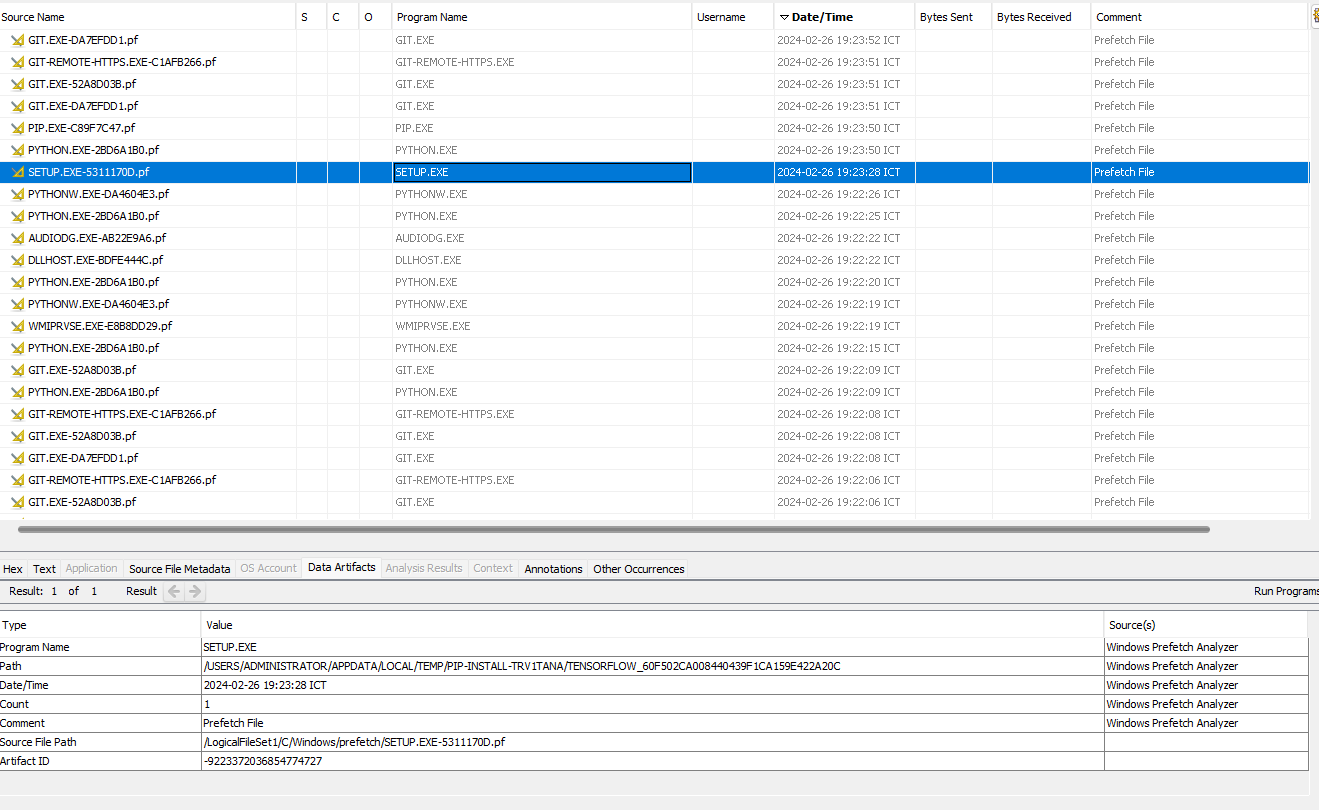
Vào lúc 19:22:09 sau khi thực thi download package kia về và thực thi lệnh git thì vào lúc 19:22:19 chúng ta có thể thấy là Windows defend bị disable đây là dấu hiệu có thể cho thấy đây là hành động của attacker

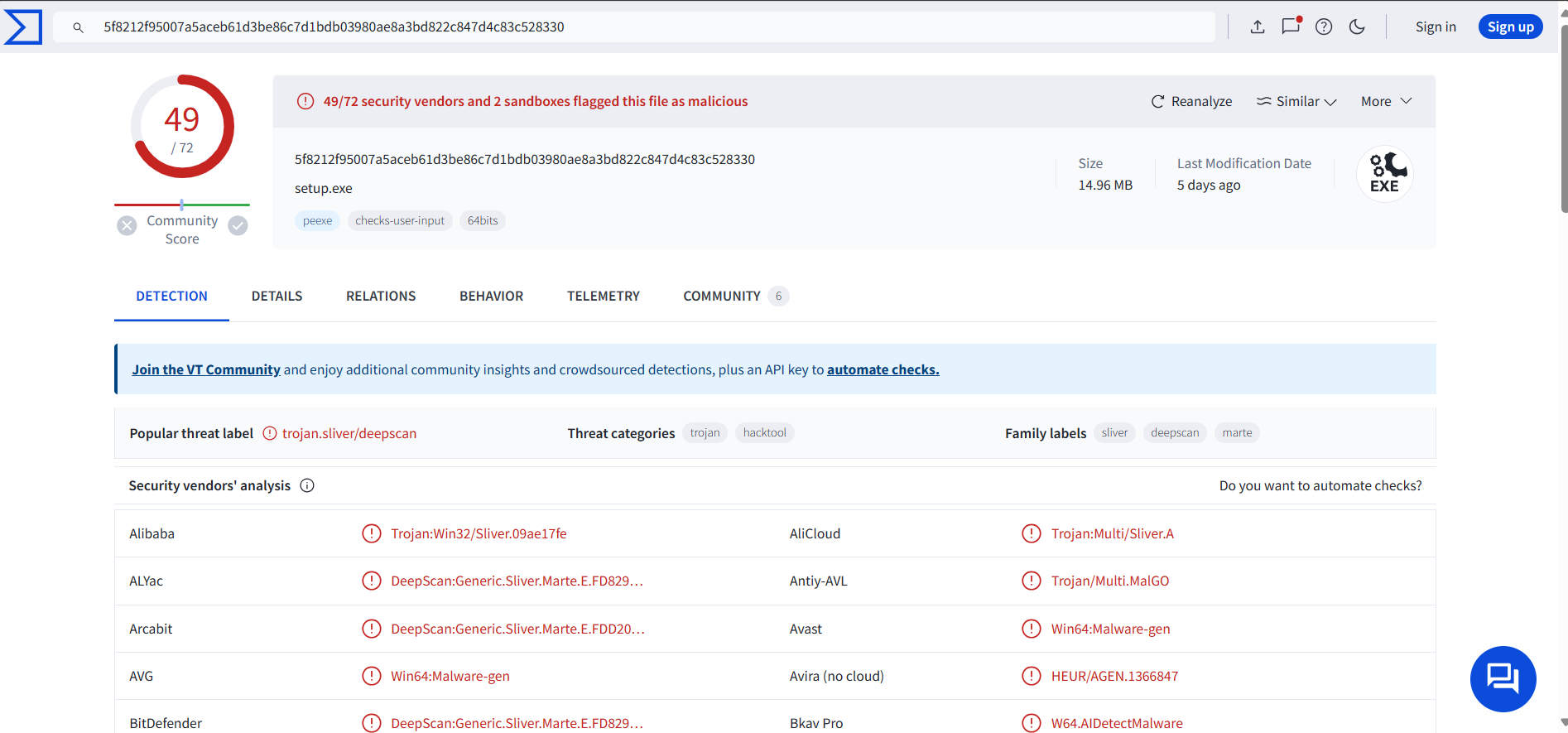




Tuy không tìm thấy source nguồn ở foder mặc định nhưng trong foder temp vẫn còn lưu trữ source của packages đã tải về kia để thực thi . Nó download 1 file ở URL [**http://3[.]66[.]85[.]252:8000/file.exe**](http://3[.]66[.]85[.]252:8000/file.exe) và rename file thành setup.exe vào lúc 19:22 và excute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



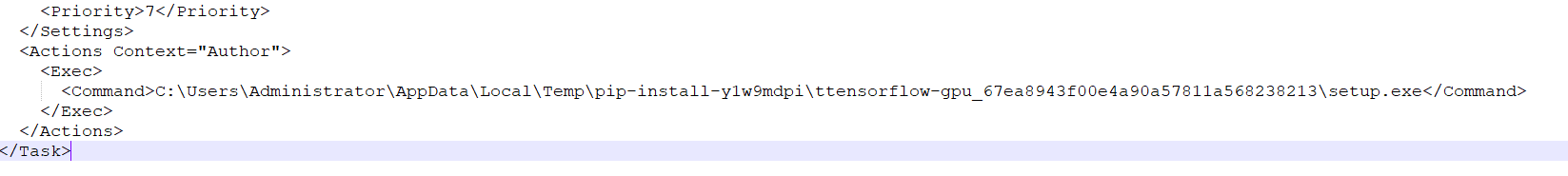
Check hash file đó trên VT chúng ta thấy 49/72 AV đánh giá là malware 

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

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





**2 Phân tích mẫu chi tiết mã độc**

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

**3 IOC**

URL :

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

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

File :

Filename : setup.exe

MD5 Hash : 23aadf3c98745cf293bff6b1b0980429

**4 Mitre&ATTCK mapping**

Command and Scripting Interpreter: PowerShell[Command and Scripting Interpreter: PowerShell, Sub-technique T1059.001 - Enterprise | MITRE ATT&CK®](https://attack.mitre.org/techniques/T1059/001/)

Scheduled Task/Job: Scheduled Task[Scheduled Task/Job: Scheduled Task, Sub-technique T1053.005 - Enterprise | MITRE ATT&CK®](https://attack.mitre.org/techniques/T1053/005/)

Impair Defenses: Disable or Modify Tools[Impair Defenses: Disable or Modify Tools, Sub-technique T1562.001 - Enterprise | MITRE ATT&CK®](https://attack.mitre.org/techniques/T1562/001/)

Supply Chain Compromise[Supply Chain Compromise, Technique T1195 - Enterprise | MITRE ATT&CK®](https://attack.mitre.org/techniques/T1195/)

**System Information Discovery** [System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®](https://attack.mitre.org/techniques/T1082/)

as the attacker concluded their intrusion , a specific file was left behind on the host . What is the name of the file