

SIEM vs EDR

The fight for a holistic and combined approach

Michel de Crevoisier
SOC / Detection lead

 mdecrevoisier

Bsides Zagreb 2024



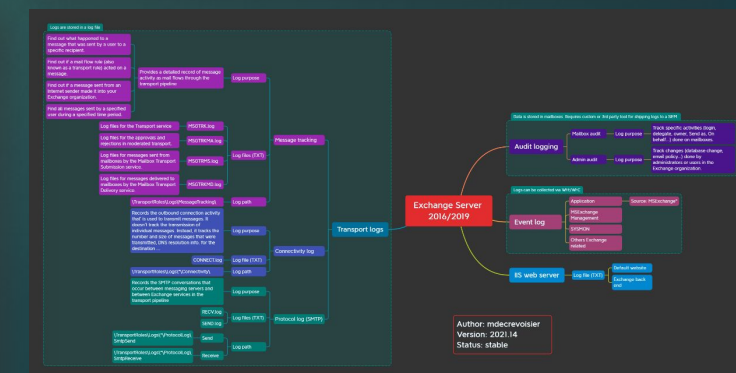
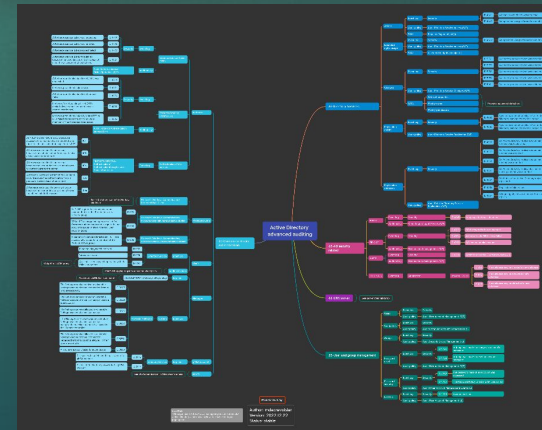
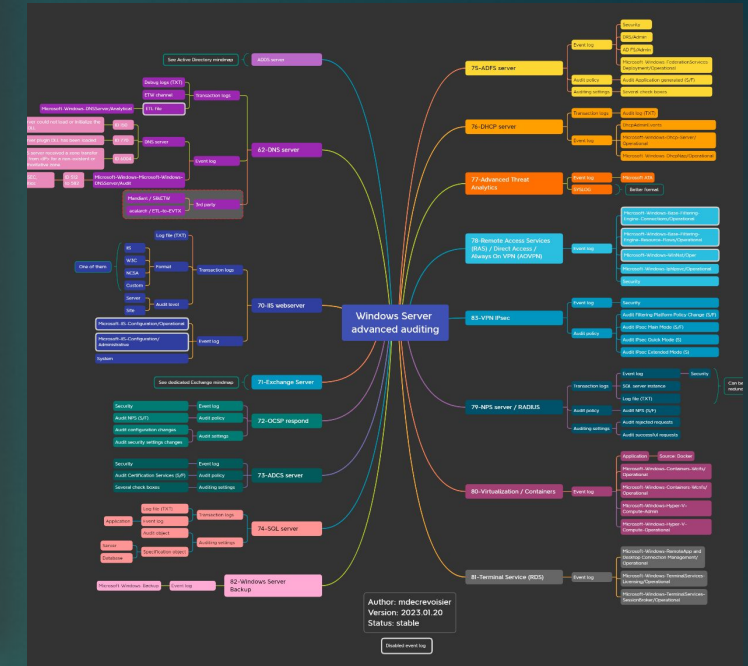
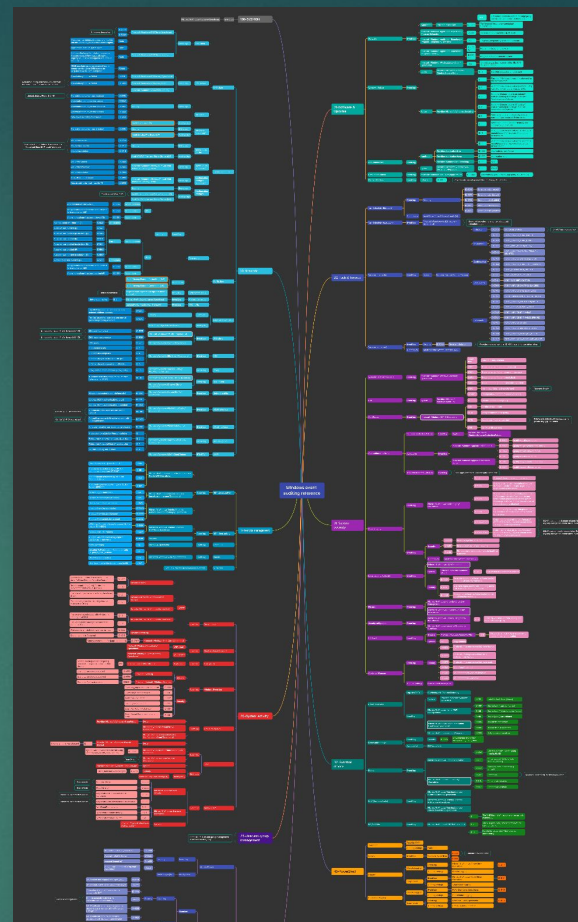
#whoami

SOC / Detection lead / Senior Security Analyst

- ▶ ex Network & System administrator
- ▶ Threat bounty developer at **SOC PRIME**
- ▶ Guest contributor at **redcanary**
- ▶ Frequent speaker at **BO SIDES**
- ▶ Author of several projects:
 - ▶ SIGMA-detection-rules (>320 rules)
 - ▶ EVTX-to-MITRE-Attack (>270 samples)
 - ▶ Microsoft-eventlog-mindmaps

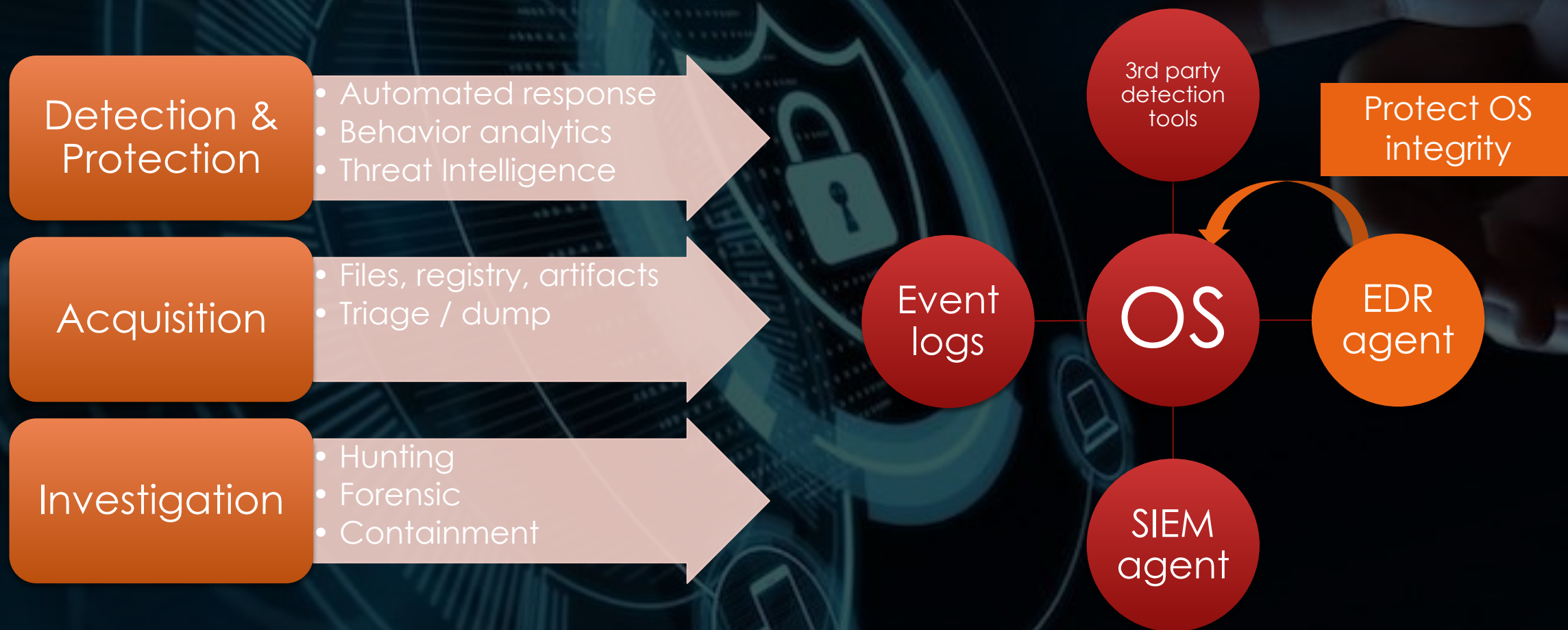


2



EDR at a glance

3



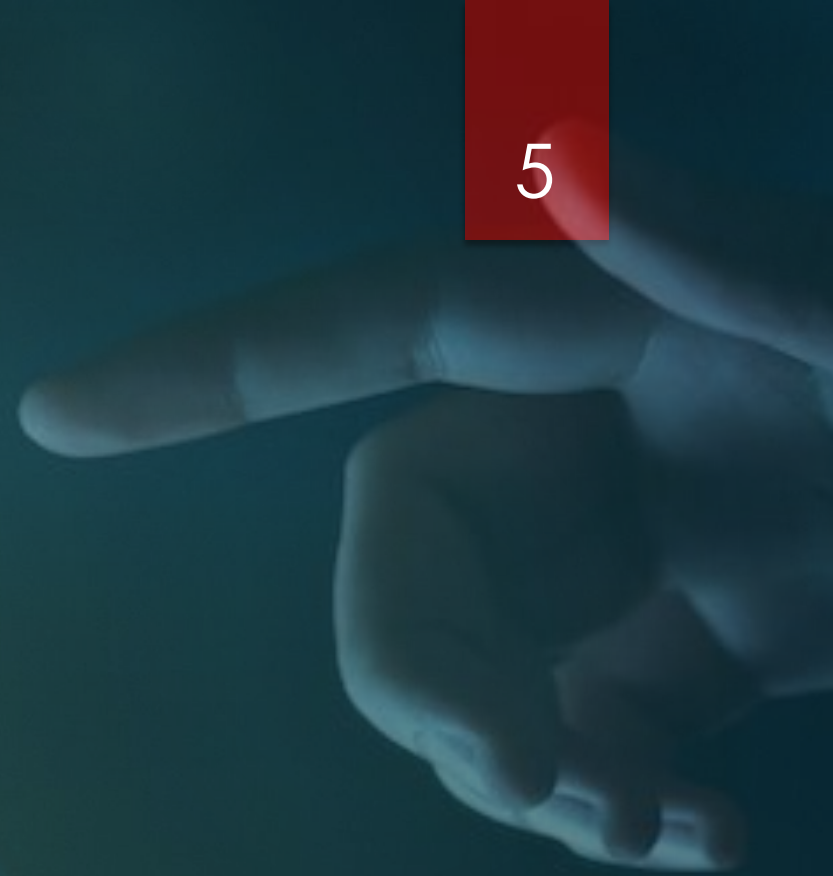
EDR: first prey ?

Focus on **evasion** operations

EDR evasion operations

5

Avoiding
the EDR



Hiding in hypervisors



2023-09: Johnson Controls International had a ransomware attack that targeted ESXi servers



2023-02: Akira ransomware groups targeted Windows Hyper-V servers

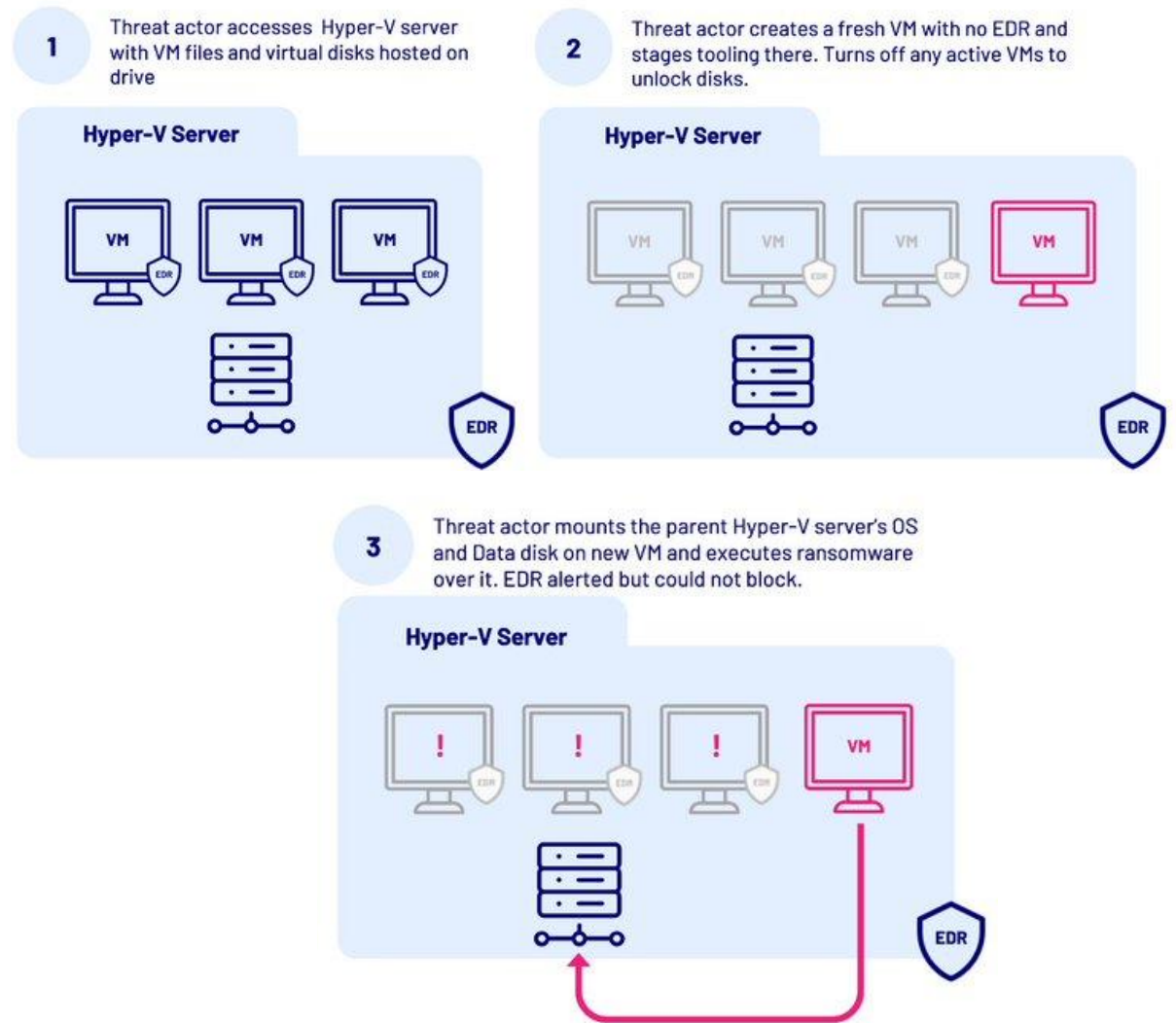


2022: Alpha Spidere used Cobalt strike variants on ESXi servers



2022: Scattered Spider used proxy tool RSOCX for persistence on ESXi servers

6



Source: Weaponising VMs to bypass EDR – Akira ransomware - CyberCX - September 2023

Hiding in network devices

2023-09: BlackTech hacking gang infiltrated Cisco devices (with firmware replacement and SSH backdoor)

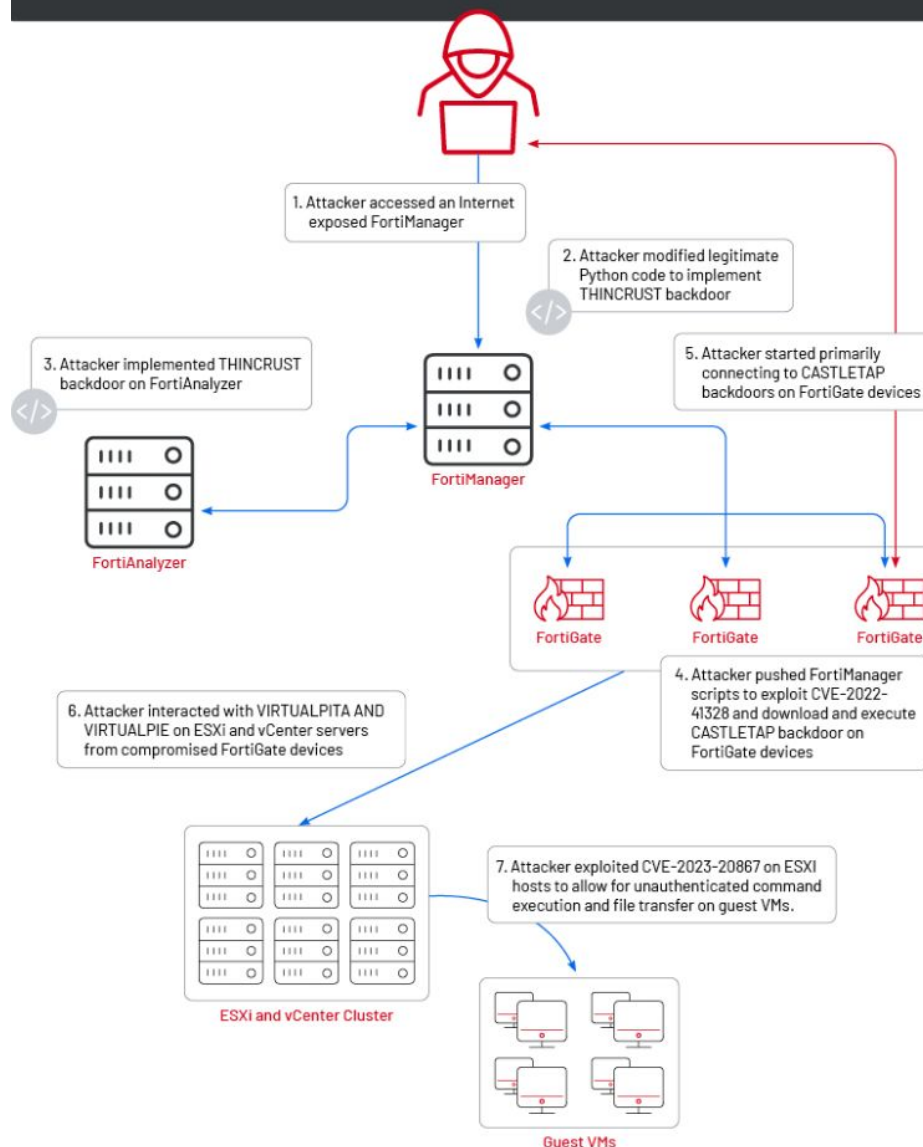


2023-07: UNC3886 targeted **FORTINET** VMware devices to remain undetected

2022-10: UNC4841 exploited a 0-day (CVE-2023-2868) in Barracuda Email Security Gateway to establish a reverse shell

UNC3886 EXPLOITED TWO ZERO-DAYS IN COMPLEX OPERATIONS

7



— Attacker had direct access to the devices after the CASTLETAP backdoor was installed.
— Attacker accessed ESXi and vCenter servers from various compromised FortiGate devices

EDR evasion operations

8

Avoiding
the EDR

EDR
tampering



EDR tampering

★ BYOVD

Vulnerable drivers

Forged timestamps

ETW bypass

AMSI bypass

DLL side loading

Blinding
sensors

Blocking communications

DLL unhooking

Kernel callbacks

File/driver deletion

Process injection

Direct Kernel Object
Manipulation

Bring Your Own [Vulnerable] Driver

2024
Lazarus group

- `appid.sys`: native driver for AppLocker exploited ([Avast](#)). Reported in July 2023 to Microsoft

2024
Kasseika ransomware

- `Martini.sys` / `viragt64.sys` (part of VirIT Agent System developed by TG Soft) ([TrendMicro](#))

2022
Sunlogin driver

- Sunlogin remote control utility (from Oray company) - CNVD-2022-10270 / CNVD-2022-03672 ([ASEC](#))

2022
AMD driver

- AMD's Ryzen master driver v17 ([GitHub](#))
- CPU overclocking control

2022
Scattered Spider

- Intel Ethernet diagnostic drivers `iqvw64.sys` - CVE-2015-2291 ([CrowdStrike](#))

2022
BurntCigar malware

- Signed with a legitimate WHCP certificate ([Sophos](#))

2021
Lazarus group

- Dell DBUtil drivers - CVE-2021-21551 ([ESET](#))

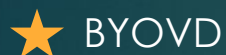
2021
Cuba ransomware

- Avast driver `aswArPot.sys` ([AON](#))

2019
BlackByte ransomware

- Micro-Star's MSI AfterBurner
- Graphics card overclocking utility `RTCore[32/64].sys` ([Sophos](#))

EDR tampering



BYOVD

Vulnerable drivers

Forged timestamps

ETW bypass

AMSI bypass

DLL side loading

Blinding
sensors

Blocking communications

DLL unhooking

Kernel callbacks

File/driver deletion

Process injection

Direct Kernel Object
Manipulation

MITRE

ATT&CK™

T1068-Priv. escalation

10



Bring Your Own [Vulnerable] Driver

1845 lines (1845 sloc) | 117 KB

```
1 title: Vulnerable Driver Load
2 id: 7aaaf4b8-e47c-4295-92ee-6ed40a6f60c8
3 status: experimental
4 description: Detects the load of known vulnerable drivers by hash value
5 references:
6   - https://lolldrivers.io/
7 author: Nasreddine Bencherchali (Nextron Systems)
8 date: 2022/08/18
9 modified: 2023/04/10
10 tags:
11   - attack.privilege_escalation
12   - attack.t1543.003
13   - attack.t1068
14 logsource:
15   product: windows
16   category: driver_load
17 detection:
18   selection_sysmon:
19     hashes|contains:
20       - 'MD5=64efbffa153b0d53dc1bccda4279299'
21       - 'MD5=d3e40644a91327da2b1a7241606fe559'
22       - 'MD5=1ed043249c21ab201edccb37f1d40af9'
23       - 'MD5=6126065af2fc2639473d12ee3c0c198e'
24       - 'MD5=63e333d64a8716e1ae59f914cb686ae8'
```

Provided with an
API feed
(JSON & CSV)

Name

gameink.sys

krprocesshacker.sys

Learn / Windows / Security /

Microsoft recommended driver block rules

Article • 01/25/2024 • 5 contributors •

Applies to: ☒ Windows 11, ☒ Windows 10, ☒ Windows Server 2022, ☒ Windows Server 2019, ☒ Windows Server 2016

Feedback

EDR tampering

BYOVD

Vulnerable drivers

Forged timestamps

★ ETW bypass

AMSI bypass

DLL side loading

Blinding
sensors

Blocking communications

DLL unhooking

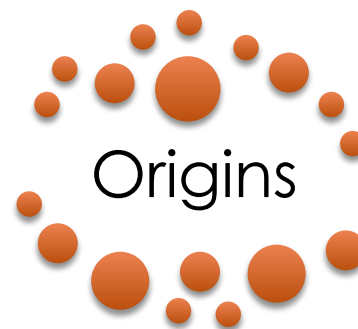
Kernel callbacks

File/driver deletion

Process injection

Direct Kernel Object
Manipulation

Event Tracing for Windows (ETW)



- Introduced in Windows XP
- Built-in logging mechanism
- Allow to observe and troubleshoot system



Windows 11 can produce more than 50K events with 1000 different providers

ETW abuses

- Blind security applications and ETW telemetry
- Used as a sniffer without kernel drivers or callback
- Can help to detect some sandbox detonations

EDR tampering

BYOVD

Vulnerable drivers

Forged timestamps

★ ETW bypass

AMSI bypass

DLL side loading

Blinding
sensors

Blocking communications

DLL unhooking

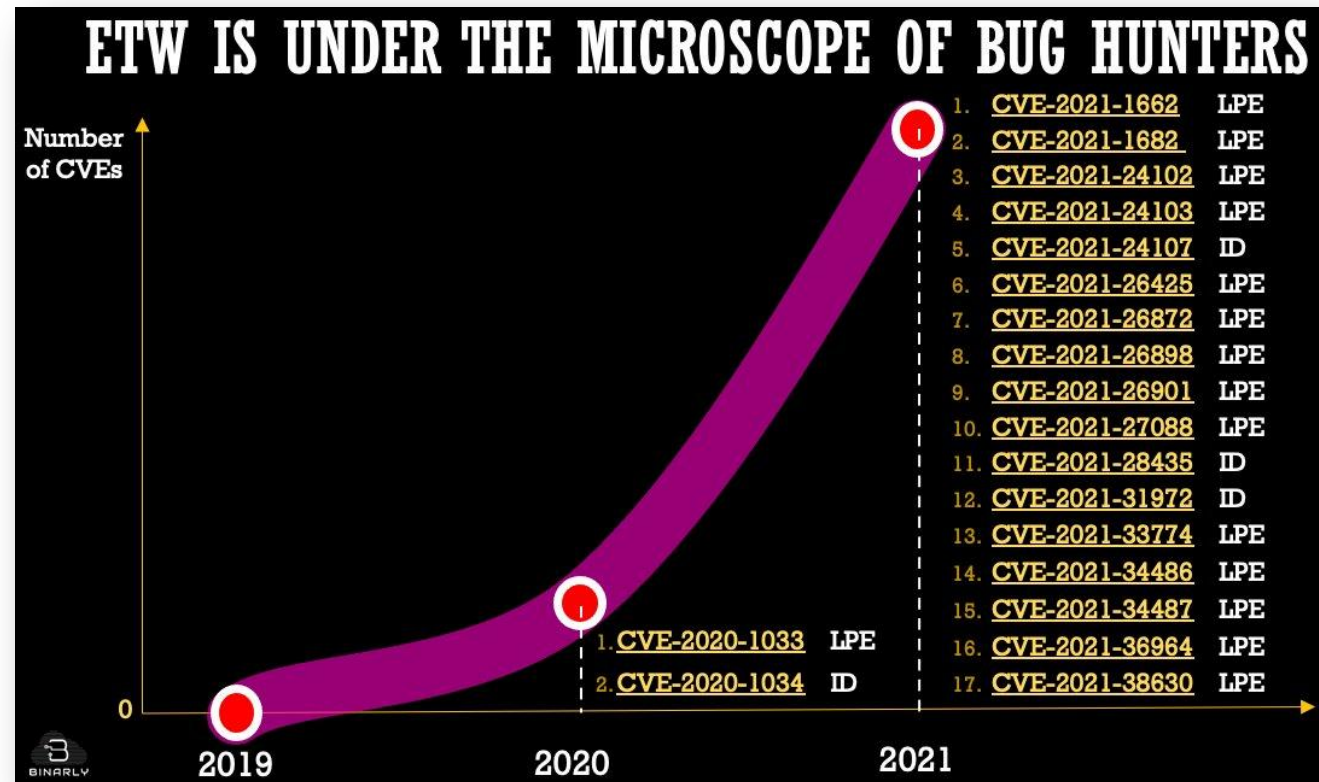
Kernel callbacks

File/driver deletion

Process injection

Direct Kernel Object
Manipulation

ETW vulnerabilities evolution



Source: Design issues of modern EDRs: bypassing ETW-based solutions – Binarly.io - November 2021

EDR tampering

BYOVD

Vulnerable drivers

Forged timestamps

★ ETW bypass

AMSI bypass

DLL side loading

Blinding
sensors

Blocking communications

DLL unhooking

Kernel callbacks

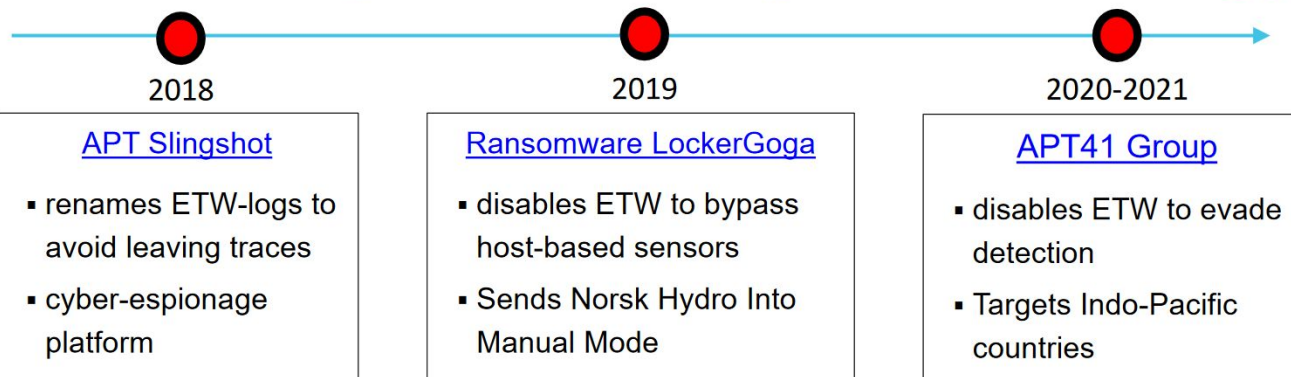
File/driver deletion

Process injection

Direct Kernel Object
Manipulation

ETW malware examples

Malware Examples of evading ETW-based logging



Defense Evasion (post-exploitation) Frameworks:

- [SharpSploit](#) disable ETW monitoring for current process
- [ScareCrow](#) – payload creation framework bypasses EDR
- [EDR Evasion](#) – about 10 examples of blocking ETW logging

[MITRE ATT&CK – Impair Defenses](#)

- Indicator Blocking
- Disable Cloud Logs

#BHEU @BlackHatEvents

Source: Attacks on ETW Blind EDR Sensors – Blackhat Nov. 2021

EDR tampering

BYOVD

Vulnerable drivers

Forged timestamps

★ ETW bypass

AMSI bypass

DLL side loading

Blinding sensors

Blocking communications

DLL unhooking

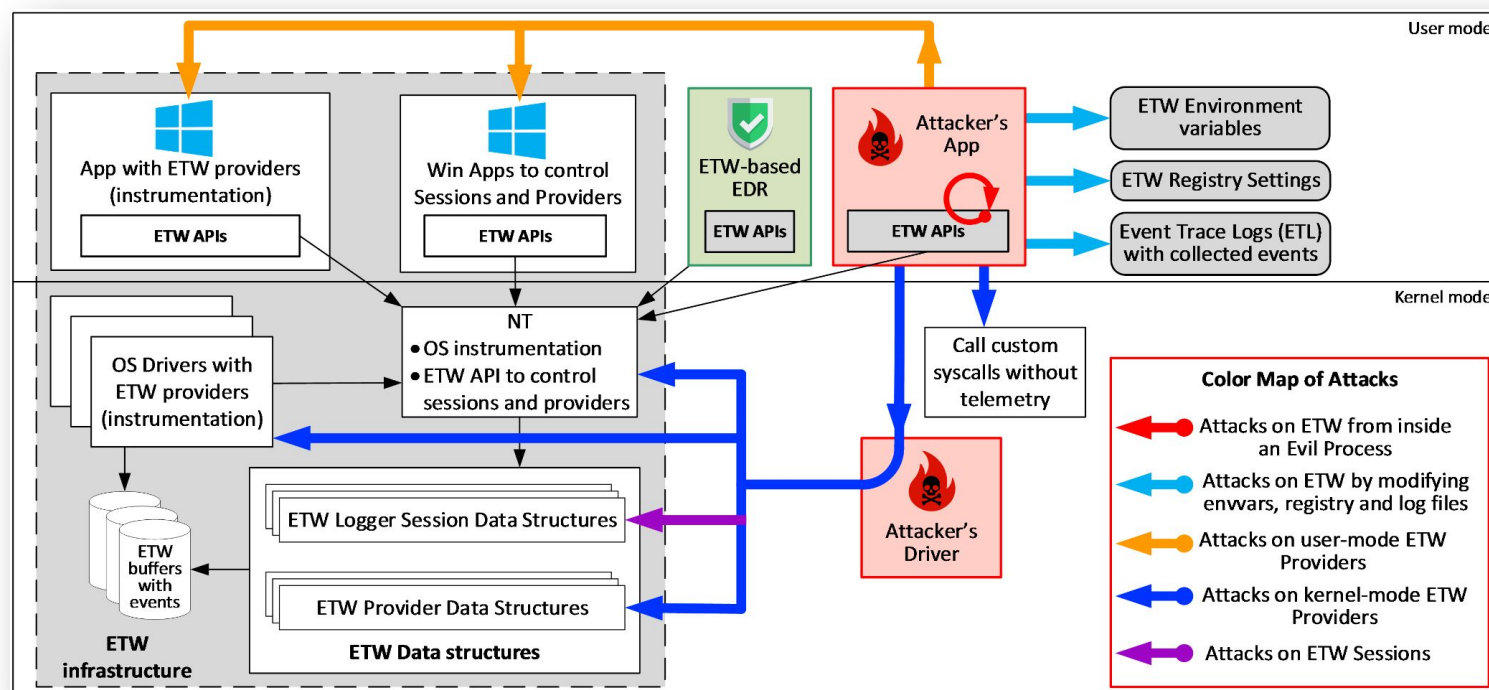
Kernel callbacks

File/driver deletion

Process injection

Direct Kernel Object Manipulation

ETW attack surface



Source: Attacks on ETW Blind EDR Sensors – Blackhat Nov. 2021

EDR tampering

BYOVD

Vulnerable drivers

Forged timestamps

ETW bypass

★ AMSI bypass

DLL side loading

Blinding
sensors

Blocking communications

DLL unhooking

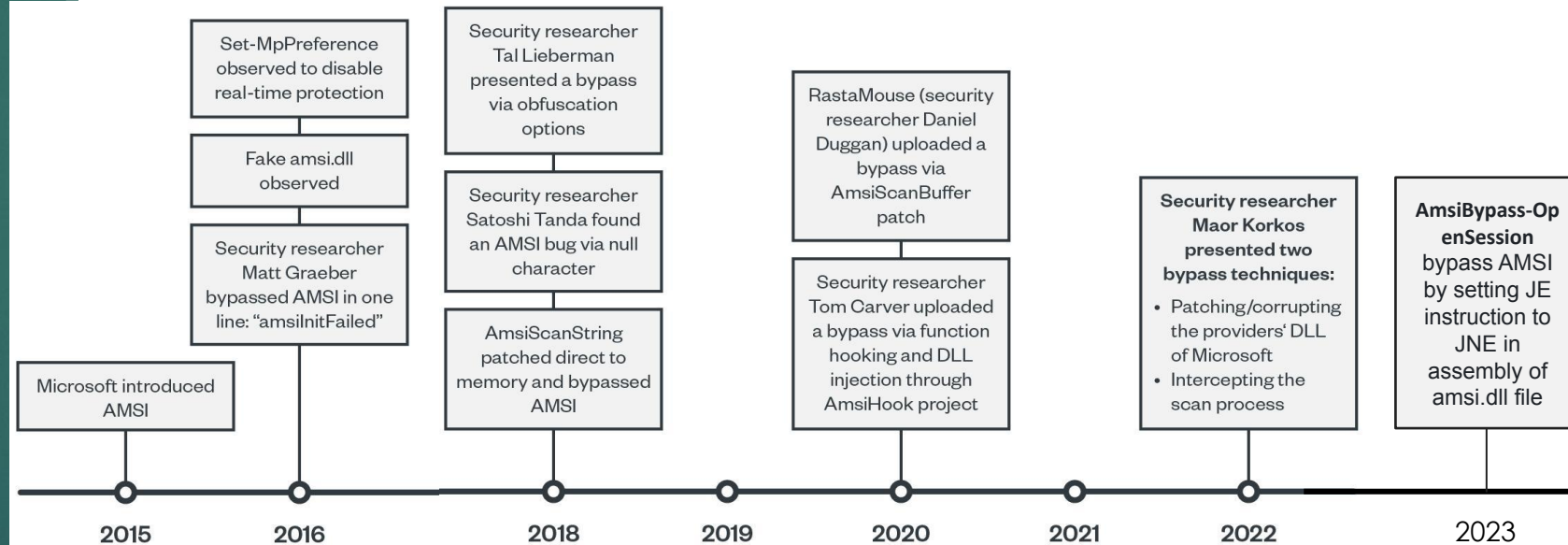
Kernel callbacks

File/driver deletion

Process injection

Direct Kernel Object
Manipulation

Antimalware Scan Interface (AMSI) bypass evasion techniques evolution



Source: Detecting Windows AMSI bypass techniques
TrendMicro - December 2022

Source: AMSI bypass new way
2023

EDR tampering

BYOVD

Vulnerable drivers

Forged timestamps

ETW bypass

AMSI bypass

★ DLL side loading

Blinding
sensors

Blocking communications

DLL unhooking

Kernel callbacks

File/driver deletion

Process injection

Direct Kernel Object
Manipulation

DLL side loading

DLL Hijacking manipulates a trusted application into executing an unauthorized DLL.

HijackLibs

☒ Sideloadng ☒ Environment Variable ☒ Phantom ☒ Search Order

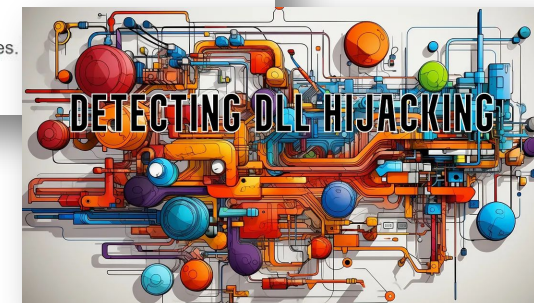
Latest entries:

[nvsmartmax.dll](#) [safestore32.dll](#) [formdll.dll](#) [opera_elf.dll](#) [rijvplatform.dll](#)
[shellchromeapi.dll](#) [sensapi.dll](#) [acrodstdll.dll](#) [classicexplorer32.dll](#)
[dbgmodel.dll](#)

By vendor:

Microsoft 422 McAfee 4 Symantec 3 Trend Micro 3 HP 2 VMWare 2 Adobe 1 Asus 1 Avast 1
Baidu 1 BitDefender 1 Cisco 1 Classic Shell 1 CyberArk 1 F-Secure 1 Google 1 Lenovo 1
LogMeIn 1 Luxand 1 Mozilla 1 npm 1 Nvidia 1 Opera 1 Palo Alto 1 Python 1 Razer 1 Smadav 1
Sophos 1 Toshiba 1 Unity 1 VentaFax 1 Vivaldi 1 VLC 1 x64dbg 1

The database contains 386 Sideloadng, 89 Environment Variable, 12 Phantom and 9 Search Order entries. hijacking entries, click [here](#).



Source: Detect DLL Hijacking techniques from HijackLibs with Splunk – DetectFYI – Oct. 2023

EDR tampering

BYOVD

Vulnerable drivers

Forged timestamps

ETW bypass

AMSI bypass

DLL side loading

★ Blinding
sensors

Blocking communications

DLL unhooking

Kernel callbacks

File/driver deletion

Process injection

Direct Kernel Object
Manipulation

Blinding EDR sensors

Event Trace (ETW) patch

Removing the DLL hooks

Removing kernel callbacks

Block EDR outbound traffic (EDR
silencer)

Set MaxConnections to 0 for internal
communication between process and
driver

EDR evasion operations

18

Avoiding
the EDR

EDR
tampering

Blending
into the
environment



EDR blending

★ LOLBINS

WSL (Subsystem for Linux)

Remote services or software

Living of the land binaries (LOLBINS)



[Research](#) [Threat intelligence](#) [Microsoft Defender](#) [Threat actors](#)

10 min read

Volt Typhoon targets US critical infrastructure with living-off-the-land techniques

By [Microsoft Threat Intelligence](#)

Source: Volt Typhoon - Microsoft May 2023

Binary	Function					
	Compile	Decode	Download	Execute	Modify System Settings	Reconnaissance
Rundll32				■		
Regsvr32				■		
Msixexec				■		
Mshra				■		
Certutil		■	■		■	
MSBuild	■			■		
WMIC				■	■	■
WmiPrvSe				■		

Source: 8 LOLBINS every threat hunter should know – CrowdStrike – March 2023

EDR blending

★ LOLBINS

WSL (Subsystem
for Linux)

Remote services
or software

Living of the land binaries (LOLBINS)

LOLBAS

☆ Star 5,323



Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our [contribution guide](#). Our [criteria list](#) sets out what we define as a LOLBin/Script/Lib. More information on programmatically accessing this project can be found on the [API page](#).

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation. You can see the current ATT&CK® mapping of this project on the [ATT&CK® Navigator](#).

If you are looking for UNIX binaries, please visit [gtfobins.github.io](#).

Search among 178 binaries by name (e.g. 'MSBuild'), function (e.g. '/execute'), type (e.g. '#Script') or ATT&CK info (e.g. 'T1218')

Binary	Functions	Type	ATT&CK® Techniques
AppInstaller.exe	Download	Binaries	T1105: Ingress Tool Transfer
AspNet_Compiler.exe	AWL bypass	Binaries	T1127: Trusted Developer Utilities Proxy Execution
At.exe	Execute	Binaries	T1053.002: At
Atbroker.exe	Execute	Binaries	T1218: System Binary Proxy Execution













Living off the living off the land

Living Off the Living Off the Land



21

A great collection of resources to thrive off the land

logo	link	description
	https://br0k3nlab/LoFP/	Living off the False Positive is an autogenerated collection of false positives sourced from some of the most popular rule sets. The information is categorized along with ATT&CK techniques, rule source, and data source.
	https://loldrivers.io	Living Off The Land Drivers is a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks
	https://gtfobins.github.io	GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems
	https://lolbas-project.github.io	The goal of the LOLBAS project is to document every binary, script, and library that can be used for Living Off The Land techniques
	https://lots-project.com	Attackers are using popular legitimate domains when conducting phishing, C&C, exfiltration and downloading tools to evade detection. The list of websites below allow attackers to use their domain or subdomain
	https://filesec.io	File extensions being used by attackers
	https://malapi.io	MalAPI.io maps Windows APIs to common techniques used by malware
	https://hijacklibs.net	This project provides an curated list of DLL Hijacking candidates
	https://wadcoms.github.io	WADComs is an interactive cheat sheet, containing a curated list of offensive security tools and their respective commands, to be used against Windows/AD environments
	https://www.loobins.io	Living Off the Orchard: macOS Binaries (LOOBins) is designed to provide detailed information on various built-in macOS binaries and how they can be used by threat actors for malicious purposes
	https://lolapps-project.github.io	This project was made because exploitation isn't limited to binaries using command line techniques. Both built-in and third-party applications have been used & abused for adversarial gain since the dawn of time, and knowing these methods can help when all else fail.
		Curated list of known malicious bootloaders for various operating systems. The project

EDR blending

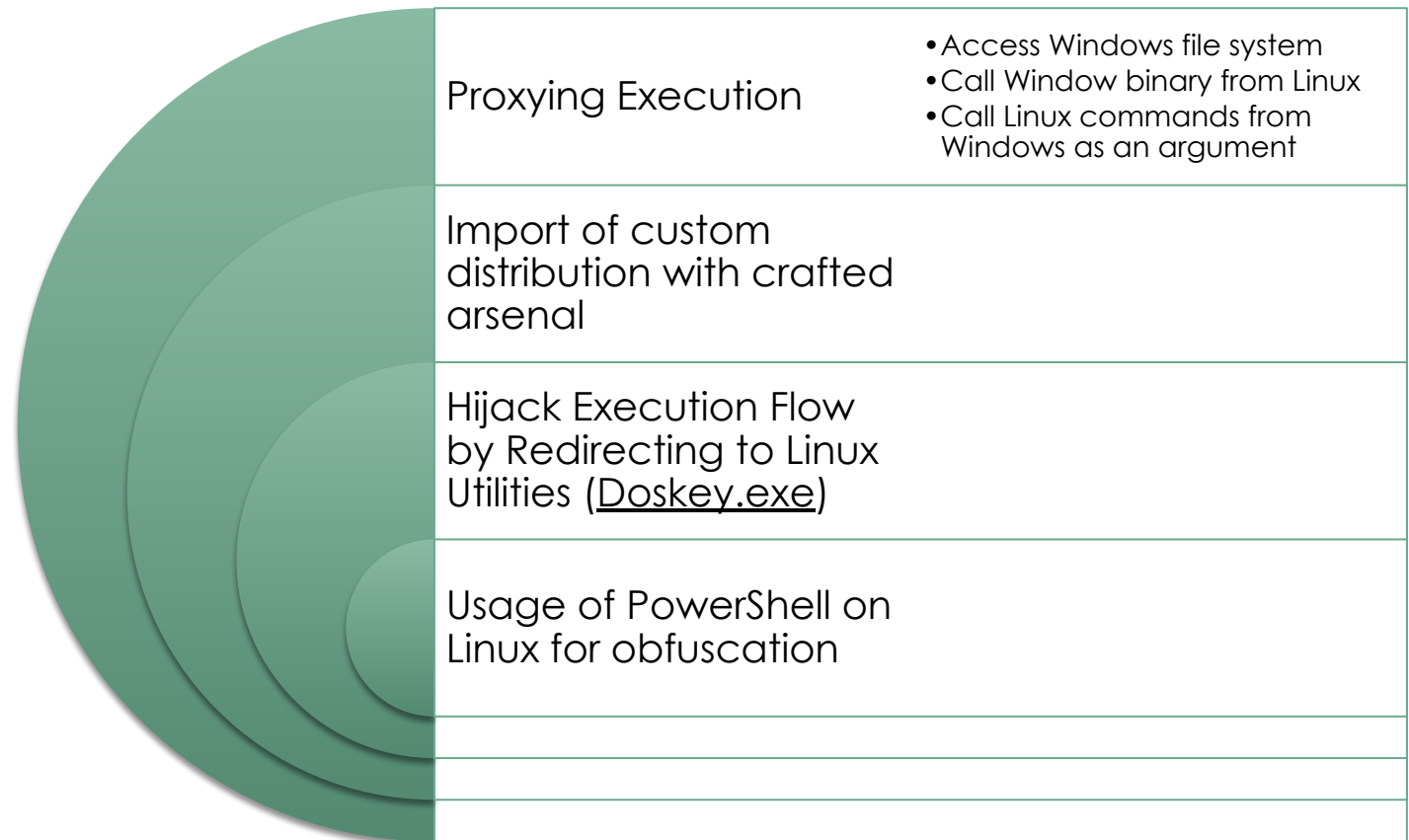
LOLBINS

★ WSL (Subsystem for Linux)

Remote services or software



Windows Subsystem for Linux (WSL)



Source: Attack Tactics, Techniques & Procedures using Windows Subsystem for Linux
Qualys – December 2022

EDR blending

LOLBINS

★ WSL (Subsystem for Linux)

Remote services or software

MITRE

ATT&CK™

T1564.006 - Hide Artifacts: Run Virtual Instance

23



Windows Subsystem for Linux (WSL)

```
SubjectUserSid S-1-5-21-2249913968-[REDACTED]
SubjectUserName D[REDACTED]
SubjectDomainName K[REDACTED]
SubjectLogonId 0x326810
NewProcessId 0x616c
NewProcessName C:\Users\D[REDACTED]\AppData\Local\Packages\KaliLinux.54290C8133FEE_ey8k8hqnwqnm\LocalState\rootfs\usr\bin\truncate
TokenElevationType %%1938
ProcessId 0x6edc
CommandLine truncate -s 0 dpkg.log
TargetUserSid S-1-0-0
TargetUserName -
TargetDomainName -
TargetLogonId 0x0
ParentProcessName C:\Users\D[REDACTED]\AppData\Local\Packages\KaliLinux.54290C8133FEE_ey8k8hqnwqnm\LocalState\rootfs\usr\bin\bash
MandatoryLabel S-1-16-8192
```

WSL commands re-transcription in process execution events logs



The Defender for Endpoint for **WSL2 plug-in** enables Defender for Endpoint to provide more visibility into all running WSL containers, by plugging into the isolated subsystem.
December 2023

EDR blending

LOLBINS

WSL (System for Linux)

★ Remote services or software



Remote services / Remote software

Category of legitimate tools

#	Category	Example	
1	MS Native Tools	PowerShell, PsExec, WMI, MSBuild, ...	Techniques are being well researched.
2	Pentest Tools	Cobalt Strike, Mimikatz, Bloodhound, ...	AV products are making effort to detect them.
3	Commercial Tools	AnyDesk, Splashtop, Rclone(MEGA), ...	Our focus on this presentation

Target RMM tools



Target SYNC tools



Source: Analysis on legit tools abused in human operated ransomware – Trend Micro – 2023

EDR evasion operations

25

Avoiding
the EDR

EDR
tampering

Blending
into the
environment

Operating in
blind spots



Attacker's pyramid of pain - Mapping risk levels to EDR evasion category



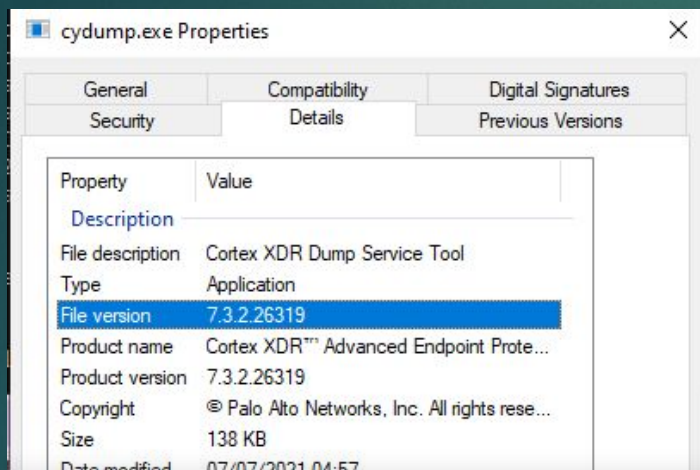
Source: Living-Off-the-Blindspot - Operating into EDRs' blindspot
September 2022

EDR



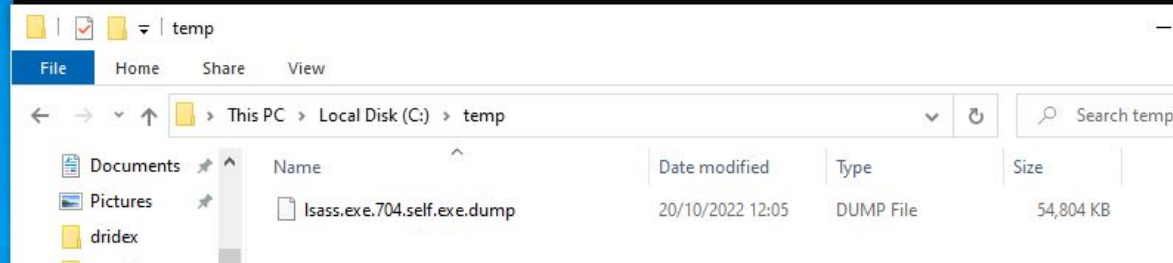
26

Dumping LSASS with **Palo Alto Cortex XDR**
“cydump.exe” tool (patched in July 2021)



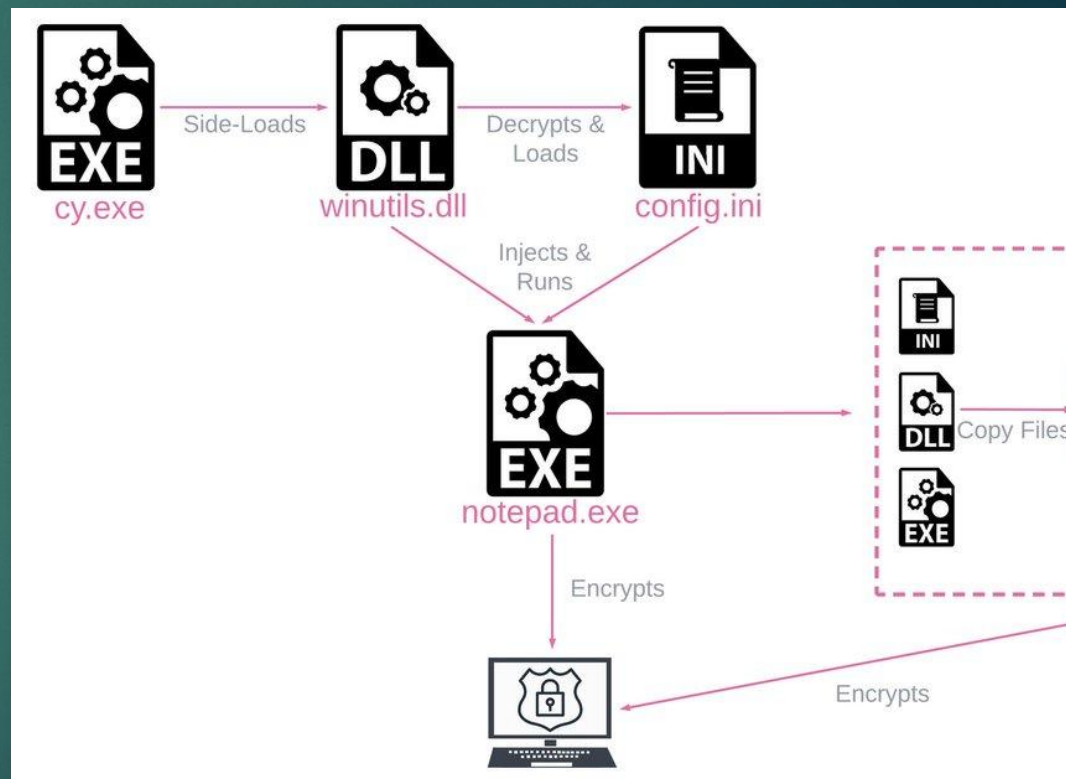
```
C:\Users\Milhouse\Desktop\cydump>
C:\Users\Milhouse\Desktop\cydump>cydump.exe dumpservice 2c0 C:\\temp\\
cydump.exe dumpservice 2c0 C:\\temp\\

C:\Users\Milhouse\Desktop\cydump>Dump file written
```

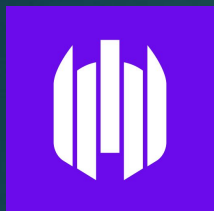


Source: Randsec – July 2022

DLL sideloading with **Palo Alto Cortex XDR** “cy.exe” tool



Source: “Rorschach: a new sophisticated ransomware” -
Checkpoint – April 2023



“Uses a CoSetProxyBlanket to call the dump function in SentinelAgent.exe to dump a PID to disk. Requires local admin.”

```
[11/18/2023 00:00:29] Trying to dump SentinelAgent to 'C:\Windows\temp\' ...  
[11/18/2023 00:00:29] Initializing SentinelHelper COM object...  
[11/18/2023 00:00:29] SentinelHelper COM object initialized successfully  
[11/18/2023 00:00:29] Fetching SentinelAgent ProcessId...  
[11/18/2023 00:00:29] SentinelAgent Found: 3420
```

Name	Date modified	Type	Size
_SentinelAgentKernel.dmp	11/18/2023 12:00 AM	Memory Dump File	1,024 KB
_SentinelAgentUser.dmp	11/18/2023 12:00 AM	Memory Dump File	381,045 KB
vdagent.log	11/17/2023 11:39 PM	Text Document	40 KB
vdservice.log	11/17/2023 8:54 PM	Text Document	4 KB

Source: Adam Svoboda – Nov. 2023

EDR



cross platform, LLVM base, bypass statis

28



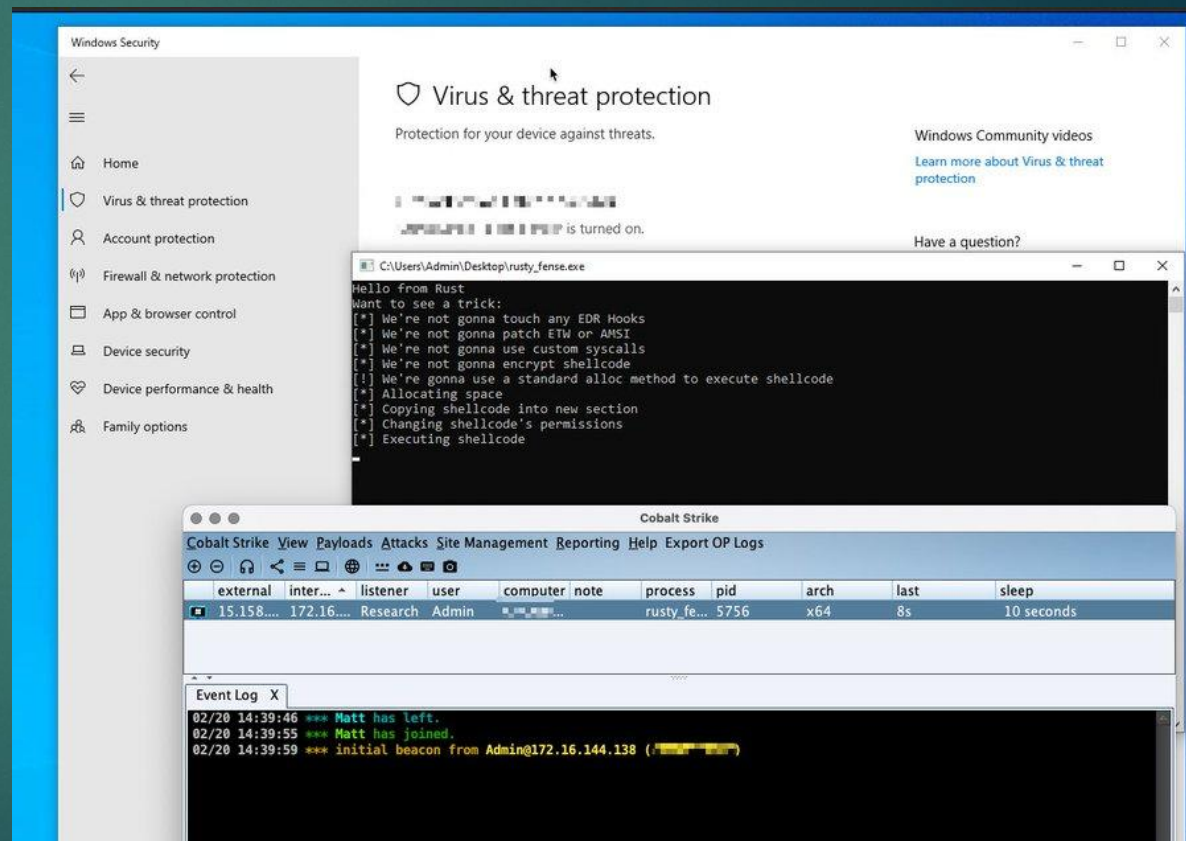
OKTA breach: LAPSUS downloaded “Process Hacker” and terminated the **FireEye HX** service agent.
(was tamper protection on ?)



Offensive Rust – More and more ransomware groups abused it since 2022
(cross platform, LLVM base, bypass static analysis...)

Date (UTC)	Event	Attack Phase
2022-01-16 00:33:23	First logon event from [SYSTEM NAME REDACTED]. Logon to [SYSTEM NAME REDACTED] from [SYSTEM NAME REDACTED] (10.112.137.64)	Initial Compromise
2022-01-19 19:19:47	RDP logon by [ACCOUNT NAME REDACTED] from LOCAL to [SYSTEM NAME REDACTED]	Initial Compromise
2022-01-19 19:45:39	Bing search for Privilege escalation tools on Github by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01 19:47:58	UserProfileSvcEop.exe downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:31:19	Account [ACCOUNT NAME REDACTED] created on [SYSTEM NAME REDACTED]	Maintain Presence
2022-01-20 18:32:32	RDP logon by [ACCOUNT NAME REDACTED] from LOCAL to [SYSTEM NAME REDACTED]	Move Laterally
2022-01-20 18:39:43	Bing search for Process Explorer by [ACCOUNT NAME REDACTED]	Internal Recon
2022-01-20 18:40:04	Process Explorer executed by [ACCOUNT NAME REDACTED]	Internal Recon
2022-01-20 18:43:51	Bing search for Process Hacker by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:44:01	Process Hacker downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:44:17	Process Hacker execution by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:46:22	FireEye Endpoint Agent service terminated on [SYSTEM NAME REDACTED]	Establish Foothold
2022-01-20 18:46:55	Bing search for Mimikatz by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:48:28	Mimikatz downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:50:10	Mimikatz executed by [ACCOUNT NAME REDACTED] on [SYSTEM NAME REDACTED]	Escalate Privileges

Source: @BillDemirkapi - January 2022



Source: A closer look at rust based malware -
February 2023

EDR configuration extraction

29

```
python XDRConfExtractor.py demo.ldb
```



LAOKOON SECURITY
[===] Homepage: <https://laokoon-security.com> [===]
[===] Follow us on Twitter: @LaokoonSecurITy [===]
[===] Created by: Luca Greeb (Yeeb) [===]

AGENT HASH AND SALT

Description:

The password has at least 9 or more characters and must contain letters, number
For more information see: <https://mrd0x.com/cortex-xdr-analysis-and-bypass/>

AGENT SALT: 79q3mds4r67261zfmnobpi
AGENT HASH: 5b12f604e592035f4a3e8b3da6ceff4d2afacd3c642981deba53d5e3ed6672a57bc0a00247c

MITRE

ATT&CK™

T1518.001 - Software Discovery: Security Software Discovery

Uninstall
Password Hash
& Salt

Excluded Signer
Names

DLL Security
Exclusions &
Settings

Office Files
Security
Exclusions &
Settings

Credential
Gathering
Module
Exclusions

Webshell
Protection
Module
Exclusions

Child process
Execution chain
Exclusions

Behavioral
Threat Module
Exclusions

Local Malware
Scan Module
Exclusions

Memory
Protection
Module Status

Global Hash
Exclusions

Ransomware
Protection
Module Modus
& Settings

EDR offensive / defensive tools

30

Terminator

- Relay on Zemana Anti-Malware driver ([GitHub](#))
- Used by Akira group

EDR Snowblat ([Sandblast](#) fork)

- Drivers & EDR process communication deactivation ([GitHub](#))

EDR silencer

- ([source](#)) vs EDR noise maker ([source](#))

Chimera

- DLL sideloading ([GitHub](#)) with encrypted shellcode

CrimsonEDR

- identify specific malware patterns and leverage diverse detection methods (unhook, ETW patch, AMSI patch...)





Who is monitoring the EDR ?

Identify EDR weak points

32

Process monitoring

EDR may be **tampered** or **disabled**

Not all devices can be enrolled

Ensure a **constant coverage** over time

Air gapped devices without internet access

EDR may have shorter **retention** time

EDR may implemented filters, or collect partial data

Telemetry Feature Category	Sub-Category	Carbon Black	CrowdStrike	Cybereason	ESET Inspect	Elastic	Harfanglab	LimaCharlie	MDE
Process Activity	Process Creation	■	■	■	■	■	■	■	■
	Process Termination	■	■	■	■	■	■	■	■
	Process Access	■	■	■	■	■	■	■	■
	Image/Library Loaded	■	■	■	■	■	■	■	■
	Remote Thread Creation	■	■	■	■	■	■	■	■
	Process Tampering Activity	■	■	?	■	■	■	■	■
File Manipulation	File Creation	■	■	■	■	■	■	■	■
	File Opened	■	■	■	■	■	■	■	■
	File Deletion	■	■	■	■	■	■	■	■
	File Modification	■	■	■	■	■	■	■	■
	File Renaming	■	■	■	■	■	■	■	■
User Account Activity	Local Account Creation	■	■	■	■	■	■	■	■
	Local Account Modification	■	■	■	■	■	■	■	■
	Local Account Deletion	■	■	■	■	■	■	■	■
	Account Login	■	■	■	■	■	■	■	■
Network Activity	Account Logoff	■	■	■	■	■	■	■	■
	TCP Connection	■	■	■	■	■	■	■	■
	UDP Connection	■	■	■	■	■	■	■	■
	URL	■	■	■	■	■	■	■	■
	DNS Query	■	■	■	■	■	■	■	■
Hash Algorithms	File Downloaded	■	■	■	■	■	■	■	■
	MD5	■	■	■	■	■	■	■	■
	SHA	■	■	■	■	■	■	■	■
	IMPHASH	■	■	■	■	■	■	■	■
	Key/Value Creation	■	■	■	■	■	■	■	■

Source: 4688-Sysmon ([Github project](#)) – reprise99

Source: EDR telemetry ([Github project](#)) - Tsale



SIEM at the rescue

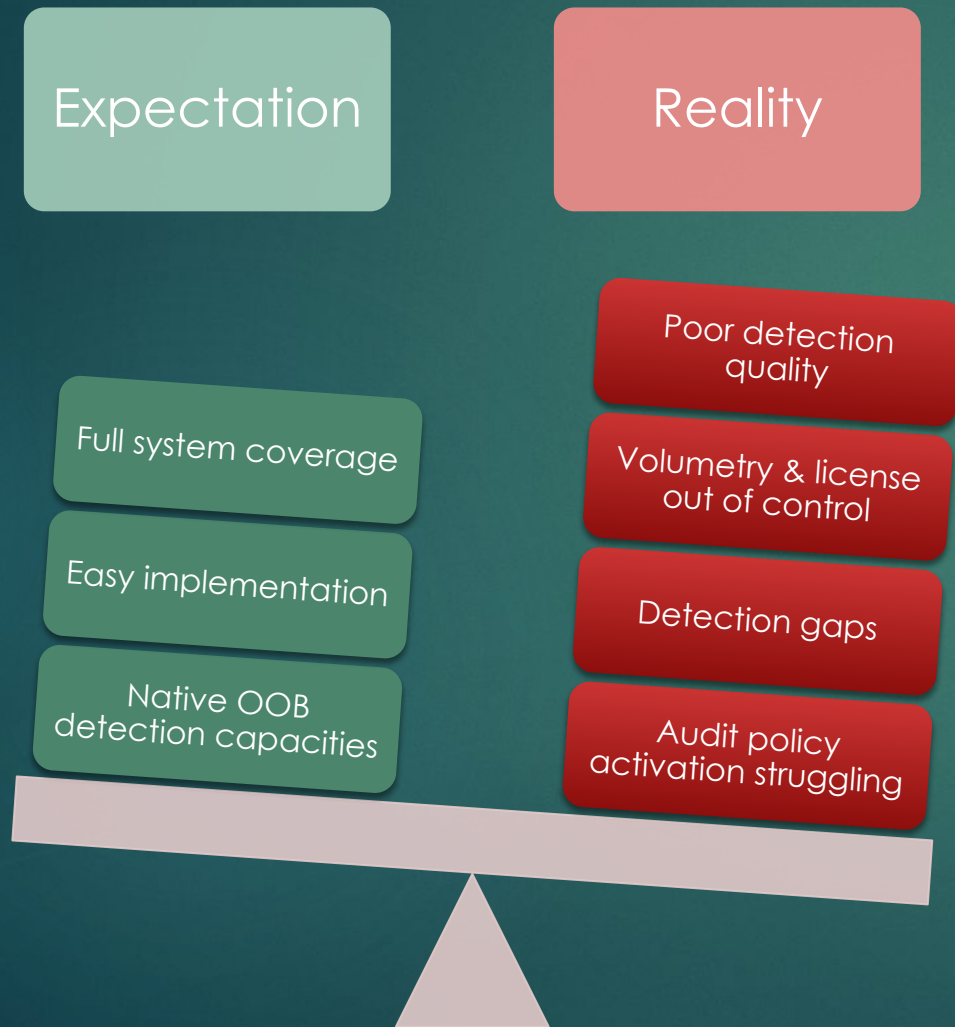
SIEM at a glance

34



SIEM implementation challenges

35



Buy a SIEM

Enable
OOB detections

Tune detections
down and keep engineers
busy normalizing data

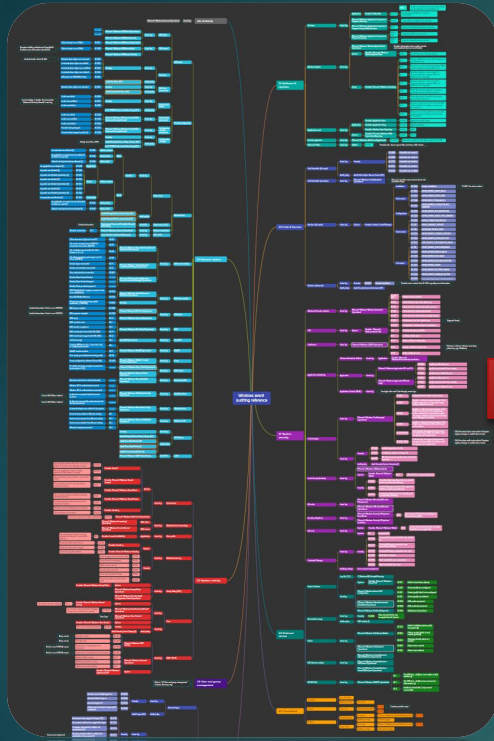
Add a MITRE stamp
to each detection and
deliver a kickass
presentation to the board



imgflip.com

Log collection toolkit (Windows)

36



Category	Subcategory	Outcom	To colla	Event ID	Event Description	TTP ID	TTP Name
None	None	Yes	None	1100	Event logging service has shut down	T1562.002	Disable Windows Event Logging
				1101	Audit events have been dropped by the transport.	T1070.001	Indicator Removal on Host
				1102	Event log cleared	T1562.002	Disable Windows Event Logging
				1104	Security log is now full	T1562.002	Disable Windows Event Logging
				1105	Event log automatic backup	T1562.002	Disable Windows Event Logging
				1108	The event logging service encountered an error	T1562.002	Disable Windows Event Logging
				4774	An account was mapped for logonSuccess		
				4776	The computer attempted to validate the credentials for an account		
				4775	An account could not be mapped for logon		
				4774	An account was mapped for logon		
Account Logon	Audit Credential Validation	Success	Yes/Noisy	4776	The computer attempted to validate the credentials for an1110	Bruteforce	
				4777	The domain controller failed to validate the credentials for1110	Bruteforce	
				4822	NTLM authentication failed because the account was a me11078.002	Valid Accounts: Domain Accounts	
				4823	NTLM authentication failed because access control restrict11078.002	Valid Accounts: Domain Accounts	
				4768	A Kerberos authentication ticket [TGT] was requested	T1558	Steal or Forge Kerberos Tickets
				4768	A Kerberos authentication ticket [TGT] was requested	T1110	Bruteforce
				4771	Kerberos preauthentication failed	T1110	Bruteforce
				4772	A Kerberos authentication ticket request failed	T1110	Bruteforce
				4820	A Kerberos Ticket granting ticket [TGT] was denied because11078.002	Valid Accounts: Domain Accounts	
				4824	Kerberos preauthentication by using DES or RC4 failed bec11078.002	Valid Accounts: Domain Accounts	
Kerberos Authentication Service	Failure	Yes/Noisy	Yes	4769	A Kerberos service ticket was requested	T1558	Steal or Forge Kerberos Tickets
				4770	A Kerberos service ticket was renewed	T1558	Steal or Forge Kerberos Tickets
				4769	A Kerberos service ticket was requested	T1558	Steal or Forge Kerberos Tickets
				4770	A Kerberos service ticket was renewed	T1558	Steal or Forge Kerberos Tickets
				4769	A Kerberos service ticket was requested	T1558	Steal or Forge Kerberos Tickets
				4770	A Kerberos service ticket was renewed	T1558	Steal or Forge Kerberos Tickets
				4769	A Kerberos service ticket was requested	T1558	Steal or Forge Kerberos Tickets
				4770	A Kerberos service ticket was renewed	T1558	Steal or Forge Kerberos Tickets
				4769	A Kerberos service ticket was requested	T1558	Steal or Forge Kerberos Tickets
				4770	A Kerberos service ticket was renewed	T1558	Steal or Forge Kerberos Tickets
Kerberos Service	Success	Yes	Yes	4769	A Kerberos service ticket was requested	T1558	Steal or Forge Kerberos Tickets
				4770	A Kerberos service ticket was renewed	T1558	Steal or Forge Kerberos Tickets
				4769	A Kerberos service ticket was requested	T1558	Steal or Forge Kerberos Tickets
				4770	A Kerberos service ticket was renewed	T1558	Steal or Forge Kerberos Tickets
				4769	A Kerberos service ticket was requested	T1558	Steal or Forge Kerberos Tickets
				4770	A Kerberos service ticket was renewed	T1558	Steal or Forge Kerberos Tickets
				4769	A Kerberos service ticket was requested	T1558	Steal or Forge Kerberos Tickets
				4770	A Kerberos service ticket was renewed	T1558	Steal or Forge Kerberos Tickets
				4769	A Kerberos service ticket was requested	T1558	Steal or Forge Kerberos Tickets
				4770	A Kerberos service ticket was renewed	T1558	Steal or Forge Kerberos Tickets

Preconfigured group policy objects

Enable auditing

Increase log size

Enable disabled event logs

```
WinEventLog://Microsoft-Windows-Authentication/ProtectedUser-Client]
disabled = 0
whitelist = 104,304
# !!! EVENT LOG FILE DISABLED PER DEFAULT !!!
# ID 104: The security package on the client does not contain the credentials
# ID 304: The security package does not store the Protected User's credentials

[WinEventLog://Microsoft-Windows-Authentication/ProtectedUserFailures-Domain]
disabled = 0
whitelist = 100,104
# !!! EVENT LOG FILE DISABLED PER DEFAULT !!!
# ID 100: An NTLM sign-in failure occurs for an account that is in the Protected
# ID 104: DES or RC4 encryption types are used for Kerberos authentication

[WinEventLog://Microsoft-Windows-Authentication/ProtectedUserSuccesses-Domain]
disabled = 0
whitelist = 303
# !!! EVENT LOG FILE DISABLED PER DEFAULT !!!
# ID 303: A Kerberos ticket-granting-ticket (TGT) was successfully issued for

[WinEventLog://Microsoft-Windows-NTLM/Operational]
disabled = 0
whitelist = 8004
# ID 8004: Domain Controller Blocked Audit: Audit NTLM authentication to the

# -----
# Specific channels - RDP
# -----

[WinEventLog://Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational]
disabled = 0
whitelist = 104,131,140,168,169
# ID 104: Client timezone is [1] hour from UTC / MITRE TTP T1021.001 - Remote
# ID 131: The server accepted a new UDP/TCP connection from client [IP]:Port
# ID 140: Connection failed; bad username or password / MITRE TTP T1021
# ID 168: Connection failed; bad username or password / MITRE TTP T1021
# ID 169: Connection failed; bad username or password / MITRE TTP T1021
# ID 104: Client timezone is [1] hour from UTC / MITRE TTP T1021.001 - Remote
# ID 131: The server accepted a new UDP/TCP connection from client [IP]:Port
# ID 140: Connection failed; bad username or password / MITRE TTP T1021
# ID 168: Connection failed; bad username or password / MITRE TTP T1021
# ID 169: Connection failed; bad username or password / MITRE TTP T1021
```

Source: Splunk Windows baseline
<https://github.com/mdcrevoisier/Splunk-input-windows-baseline>

Source: Microsoft eventlog mindmap
<https://github.com/mdcrevoisier/Microsoft-eventlog-mindmap>

Source: Microsoft auditing baseline
<https://github.com/mdcrevoisier/Windows-auditing-baseline>

ATT&CK®

Covers more than 70 different event logs with event ID description and MITRE ATT&CK mapping: Exchange, MS SQL, Bitlocker, DNS Server, IIS, RDP, WinRM, WMI, ADFS, Winsock, Office ...



Source: SIGMA detection rules
<https://github.com/mdcrevoisier/SIGMA-detection-rules>

Struggling with log volume/EPS?



37

Apply noise reduction

Use SYSMON

Use different collecting
baselines « full / light »

- Enable the « *triggering vs attesting approach* »

- Enable new type of detections
- Extend log collection perimeter (if restricted)
- Increase detection for offensive action against EDR



Collecting baseline strategy

38

Full collecting baseline

- ▶ Process execution
- ▶ Powershell (modern)
- ▶ Login (success and failures)
- ▶ Kerberos (success and failure)
- ▶ + *light baseline* (aka « triggering VS attesting events »)

Light collecting baseline

- ▶ RDP activity + denied access
- ▶ Failed logins, success login (interactive, RDP, Pass the hash)
- ▶ Service & task creation
- ▶ Local user & groups
- ▶ SSH/WinRM authentication
- ▶ Server roles: SQL Server, ADFS, ADCS/PKI, NPS, Exchange, IIS
- ▶ Misc: drivers, Bitlocker, Printer, Firewall configuration, BITS, WMI, Defender (threats), VHD/ISO, audit policy change, event log, password reset/lockout, AppLocker ...
- ▶ Process exec with focus on LOLBINS



DC: ~1-2GB
Server: ~300-700MB
(per day)

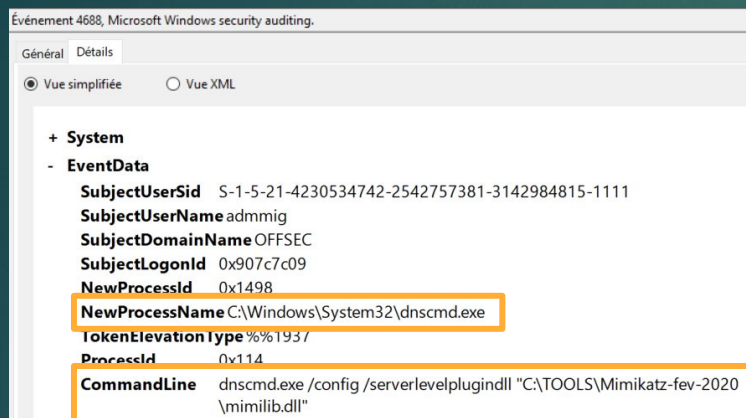
Server: <5MB
(per day)

Server: ~20-50MB
(per day)

Triggering vs attesting events

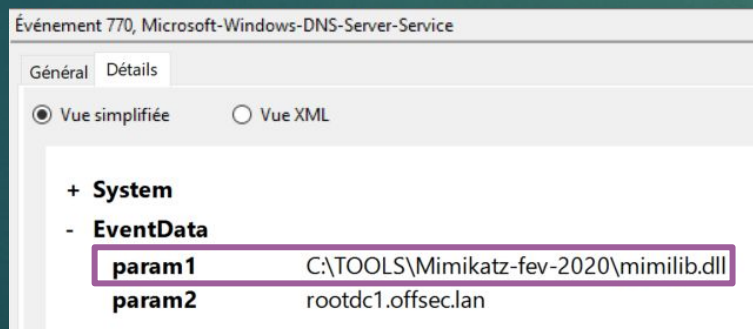


39



Event log: Security.evtx

T1574.002: Hijack Execution Flow: DLL Side-Loading



Event log: DNS Server.evtx

Triggering

Good security context and documentation

Provides a larger scope of TTP coverage

Risk of detection failure due to improper detection, auditing or obfuscation

Do not confirm triggering actions at 100%

Auditing configuration required

Attesting

Poor structure and lack of documentation

Some event log are disabled per default

Attest with high probability results from triggering actions

Nearly no auditing configuration required

Lighter detection queries (hardware)

Increasing visibility with hidden treasures

40



T1574.002 - Hijack Execution Flow:
DLL Side-Loading

PrintNightmare vulnerability

ID 321 | 354 | 808 (Printer)

T1048 - Exfiltration Over Alternative
Protocol

BITS client activity

ID 59-60 (BITS client)

T1574.002 - Hijack Execution Flow:
DLL Side-Loading

DNS DLL server plugin load

ID 150 | 770 (DNS Server)

T1505.004 - Server Software
Component: IIS Components

New IIS module loaded

ID 29 (IIS Operational)

T1505.002 - Server Software
Component: Transport Agent

New transport agent deployed

ID 1 | 6 (Exchange Mgmt)

T1562.004 - Impair Defenses:
Disable or Modify System Firewall

New "any/any" firewall rule

ID 2004 | 2005 (Advanced Firewall)

T1543.003 - Create or Modify
System Process: Windows Service

New service installed

ID 4697 (Security) / 7045 (System)

Increasing visibility for EDR tampering

41

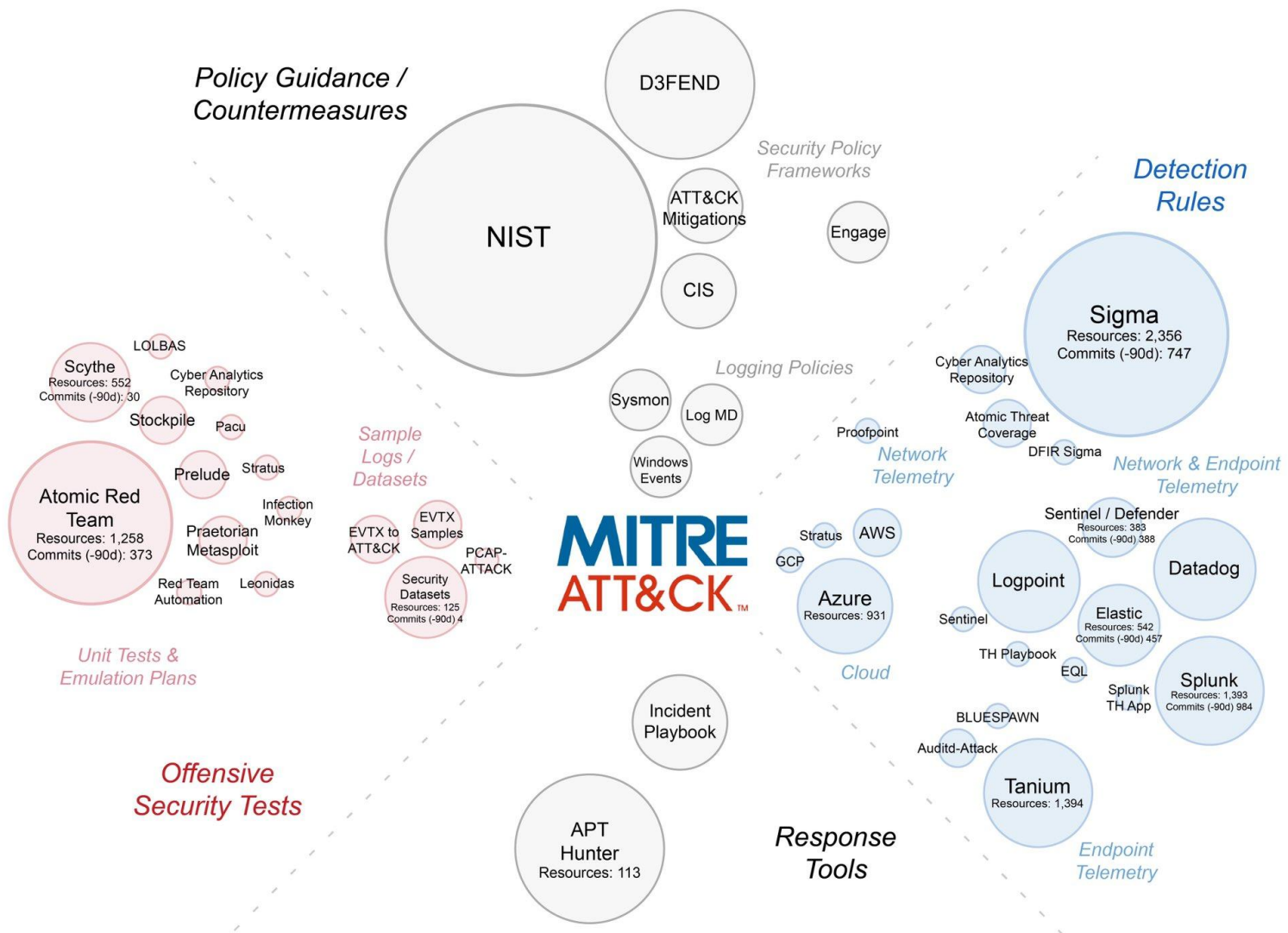
Approach	Threat	TTP ID	MITRE	ATT&CK™	Event log	Event ID	ID Desc
Avoiding EDR	Evasion	T1090	Proxy		WinINet-Config	5600	Proxy config. Changed
		T1572	Protocol Tunneling (eg: via RDP)		Terminal Services	1149	User authentication succeeded
Tampering EDR	BYOVD	T1068	Privilege escalation		SYSMON	6	Driver load
		T1543.00	Create or Modify a Windows Service		Security/System	4697/7045	Service creation
	DLL sideloading	T1574.002	Hijack Execution Flow: DLL Side-Loading		SYSMON	7	Image load
	AMSI	T1562.001	Impair Defenses: Disable or Modify Tools	SYSMON	7	Image load	
				SYSMON	13/14	Registry events	
	Defender			5007	Exclusion		
	SYSMON			13/14	Registry events		
	Defender			3002	Protection failure		
	Defender			5004	Configuration change		
	ETW bypass	T1562.006	Impair Defenses: Indicator Blocking		SYSMON	13/14	Registry events
	NG wiper/symlink	T1547.009	Boot or Logon Autostart : Shortcut modif.	SYSMON	11	File creation	
				SYSMON/Security	1/4688	Process execution	
				Security	4664	Hard link creation	
	LOLBINS	T1218	System Binary Proxy Execution		SYSMON/Security	1/4688	Process execution
T1127		Trusted dev Utilities Proxy exec.		Application:MsilInstaller	11707	Product installed	
WSL	T1564.006	Hide Artifacts: Run Virtual Instance		Setup:Windows-Servicing	9	New package turned on	
Blending EDR	Replicate company tools	T1021.001	Remote services: RDP	Terminal Services	131	Connection from <ip>	
				Terminal Services	1149	User authentication succeeded	
		T1021.004	Remote Services: SSH	OpenSSH	4	SSH server listening on	
Configuration	Config. extraction	T1518.001	Security Software Discovery		SYSMON/Security	1/4688	Process execution

Detection validation

ASSESSING YOUR DEFENSES

Control Validation Resource Ecosystem

Public resources aligned with common descriptions of adversary behavior (MITRE ATT&CK)



Control validation resource ecosystem

Source: Control Compass – May 2022

EDR assessment tools

44



Atomic Red team
(Red Canary)



Attack range
(Splunk)

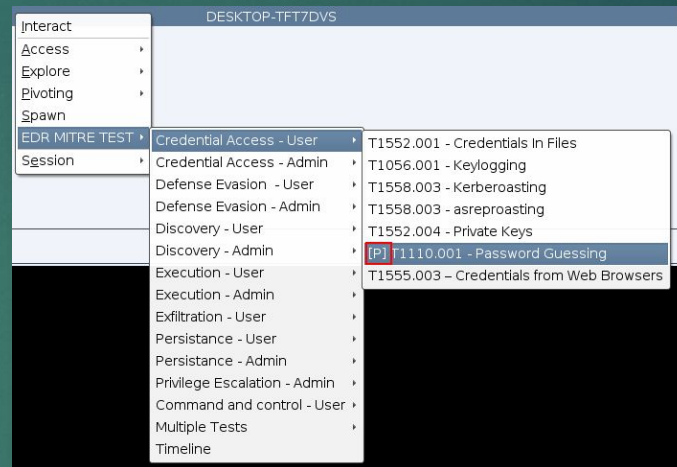


APT Simulator
(Nextron)

Caldera
(MITRE)



Threatest
(Datadog)

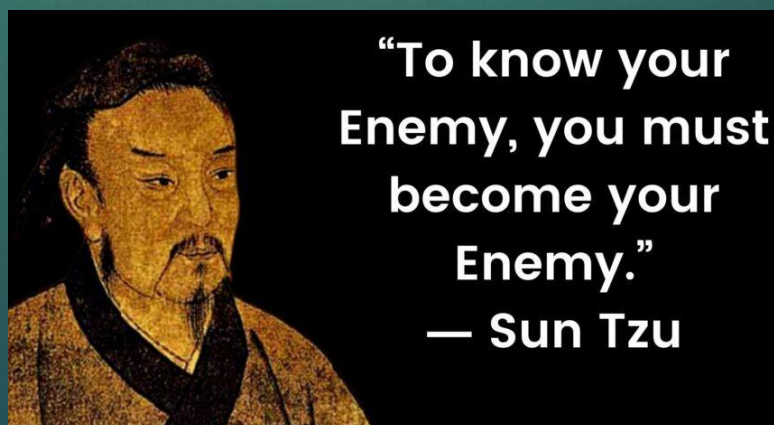


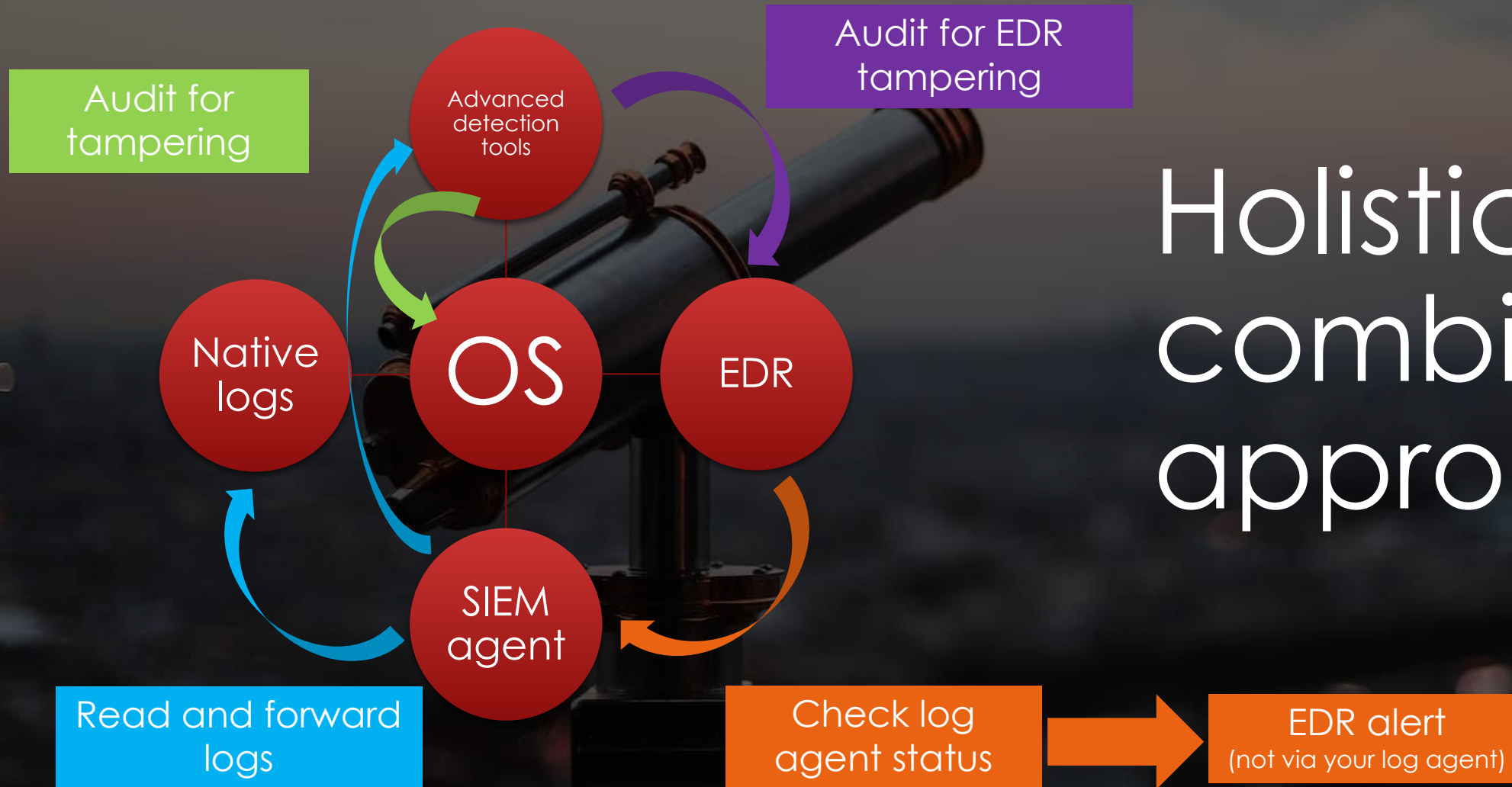
EDR-test

- A good alternative to Atomic Red Team not using PowerShell

Pyramid

- Perform offensive tasks by leveraging Python evasion techniques





Holistic and combined approach

BlackMamba: a polymorphic threat

46

“Exploits large language model to synthesize polymorphic keylogger functionality on-the-fly, dynamically modifying the benign code at runtime - all without any command-and-control infrastructure.”

**BACK
TO
THE FUTURE**

Source: Blackmamba, using AI to generic polymorphic malware - HYAS - Mars 2023

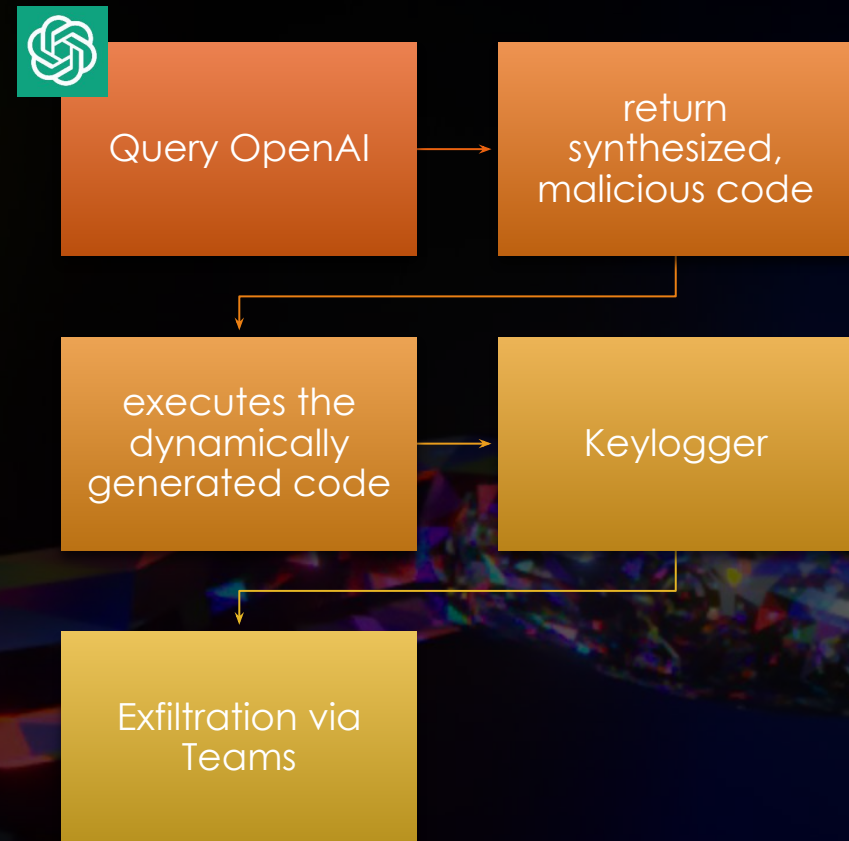
BlackMamba: a polymorphic threat 47

C2 removal

- intelligent automation and attacker-bound data through a benign communication channel

Leverage AI code

- synthesize new malware variants, by changing the code and evade detection algorithms.



**BACK
TO THE FUTURE**

Source: Blackmamba, using AI to generic polymorphic malware - HYAS - Mars 2023

Thank you!

