ROOTCON

Microsoft Defender Will Be Defended - MemoryRanger Prevents Blinding Windows AV

Denis Pogonin

Igor Korkin

2022

WHO WE ARE

Denis Pogonin

- Bachelor of Information Security
- National Research Nuclear University MEPhI
- Cryptology and Cybersecurity Department

Igor Korkin, PhD

- Independent Security Researcher
- Speaker at CDFSL, BlackHat, HITB, SADFE
- sites.google.com/site/igorkorkin

AGENDA

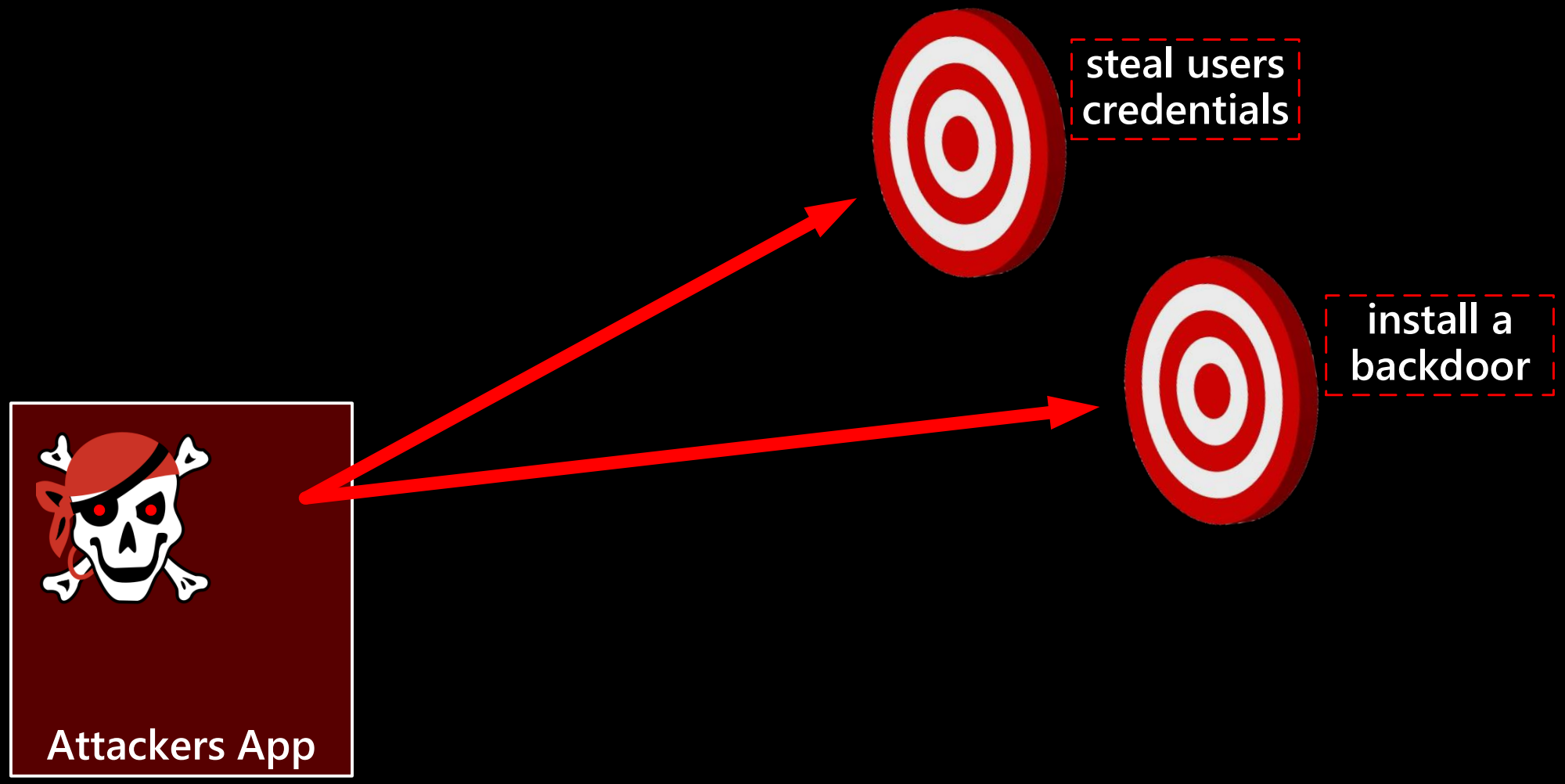
- Bypassing security products is a notorious malware trend
- Microsoft Defender is the key target of cyber criminals
- Kernel-mode threats are still the most risky

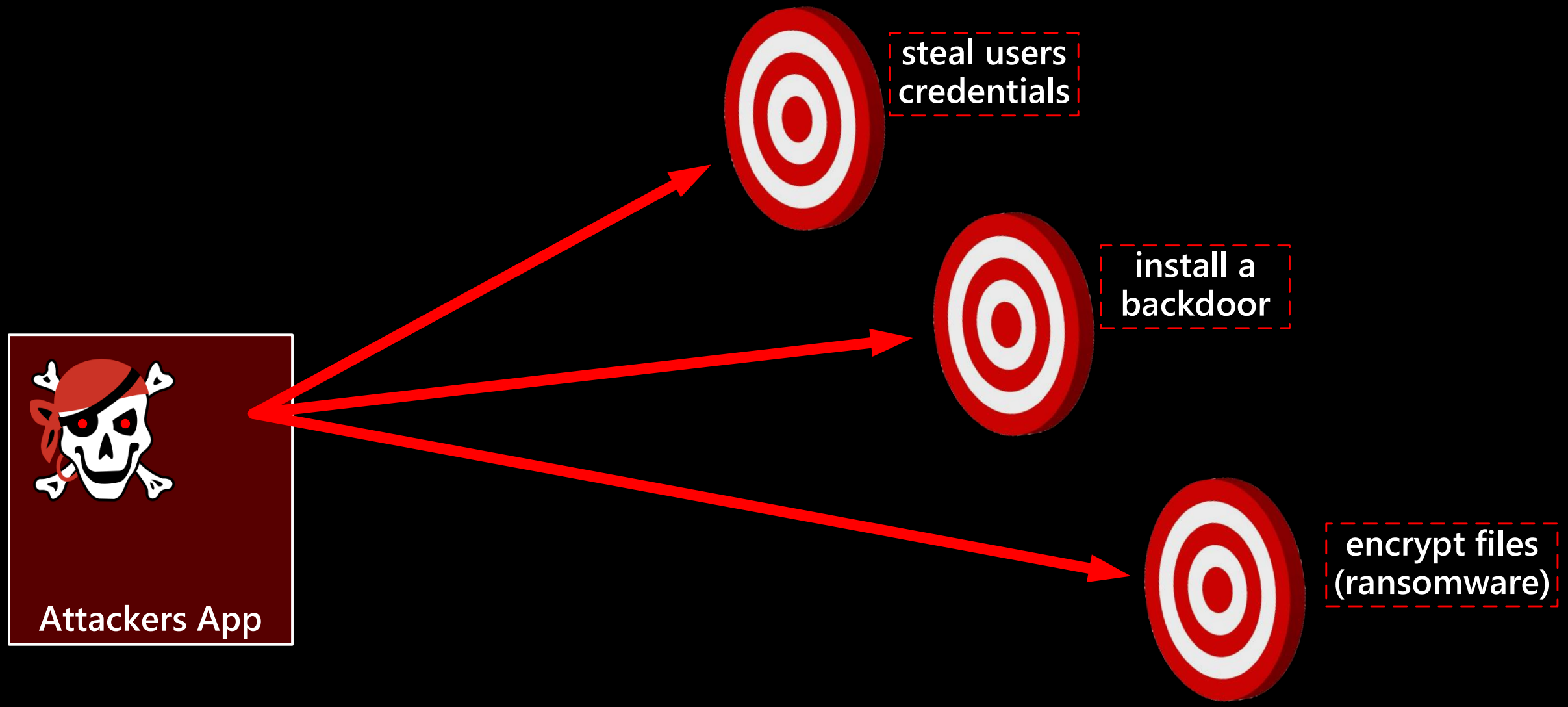
- Microsoft Defender Internals: Signature Detection
- Windows OS Internals: Mandatory Integrity Control

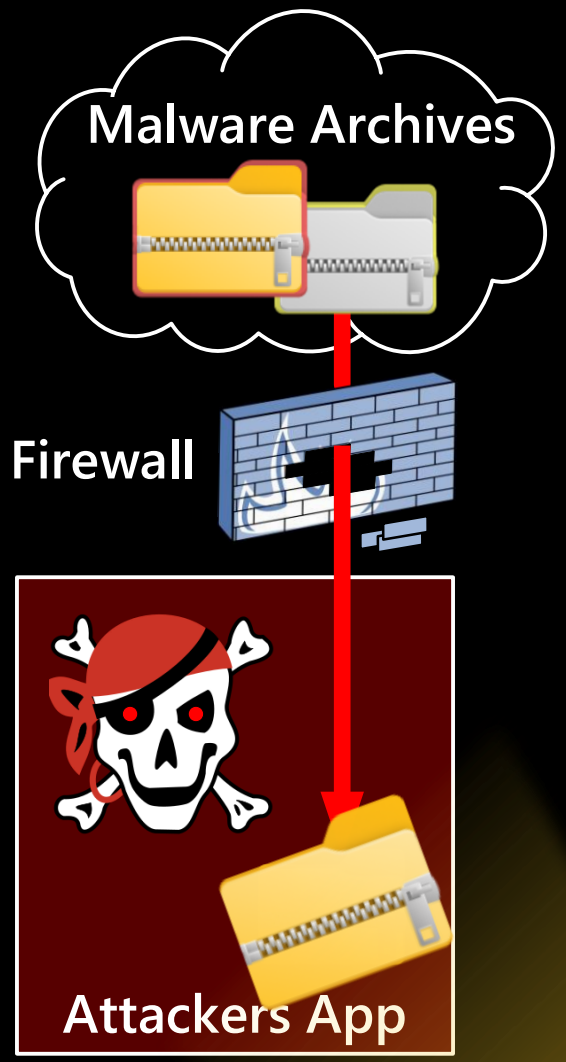
- New kernel attack disables Microsoft Defender
- MemoryRanger defends Microsoft Defender

Attackers App

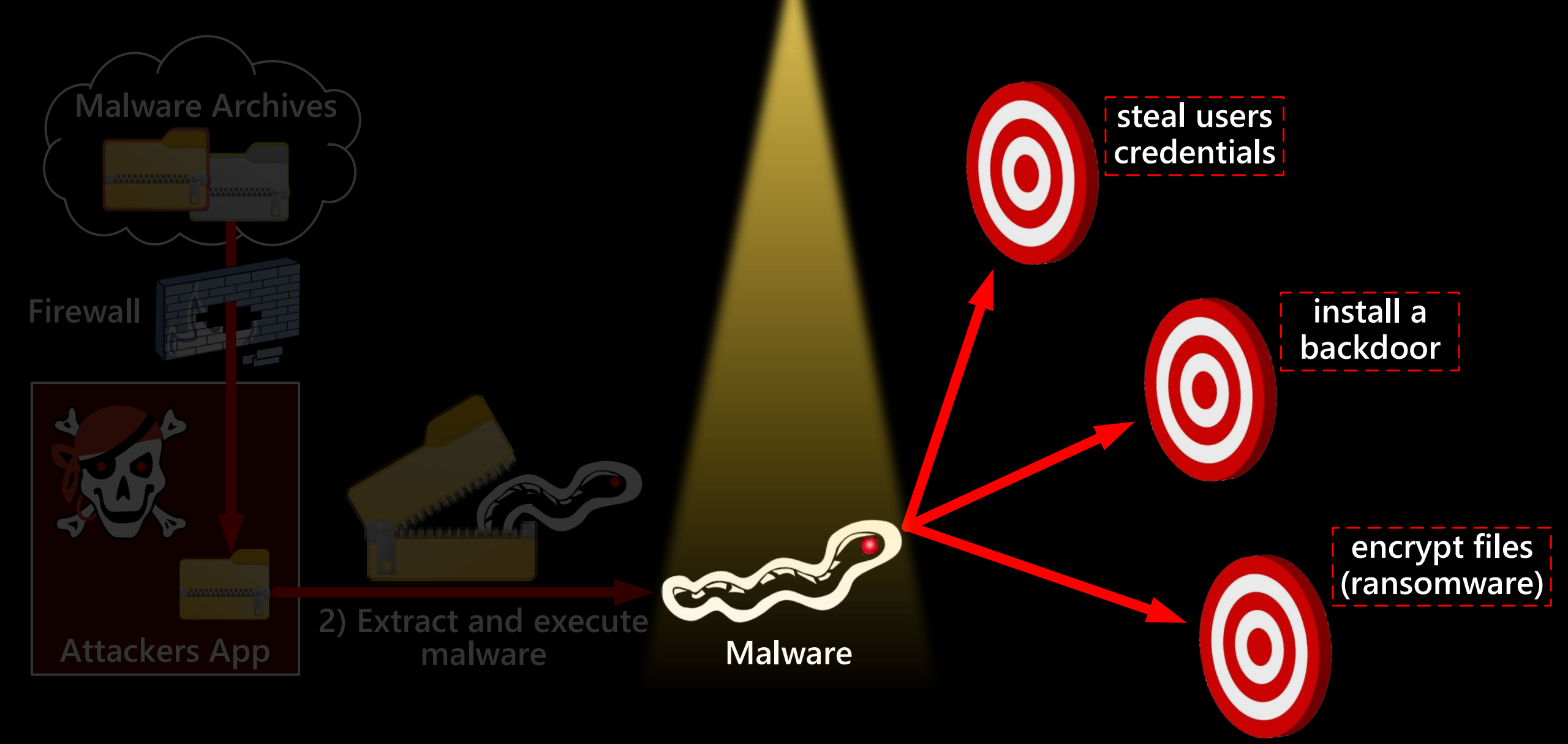
steal users credentials


steal users credentials
install a backdoor
Attackers App

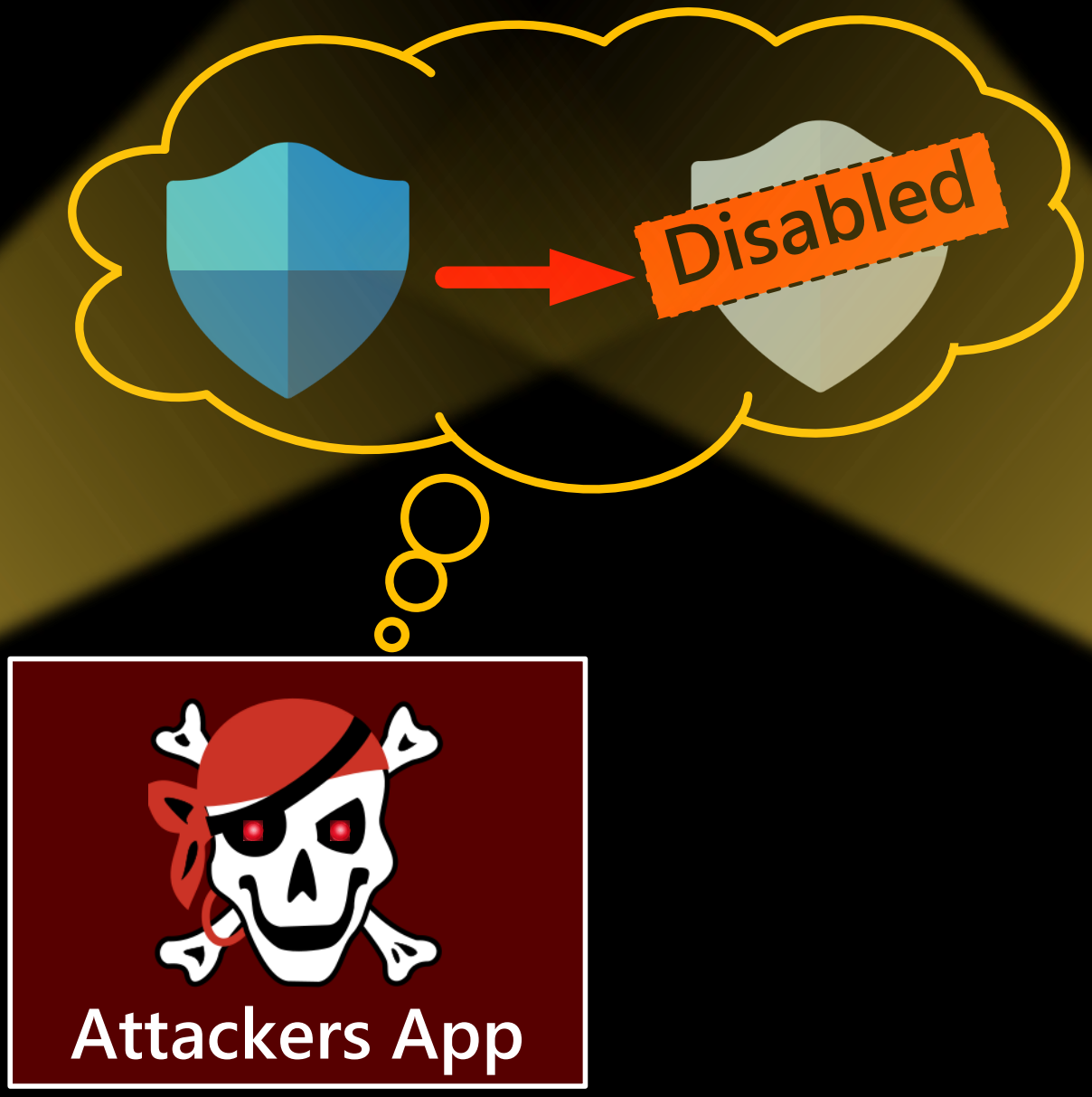

steal users credentials
install a backdoor
encrypt files (ransomware)
Attackers App


Malware Archives
Firewall
Attackers App

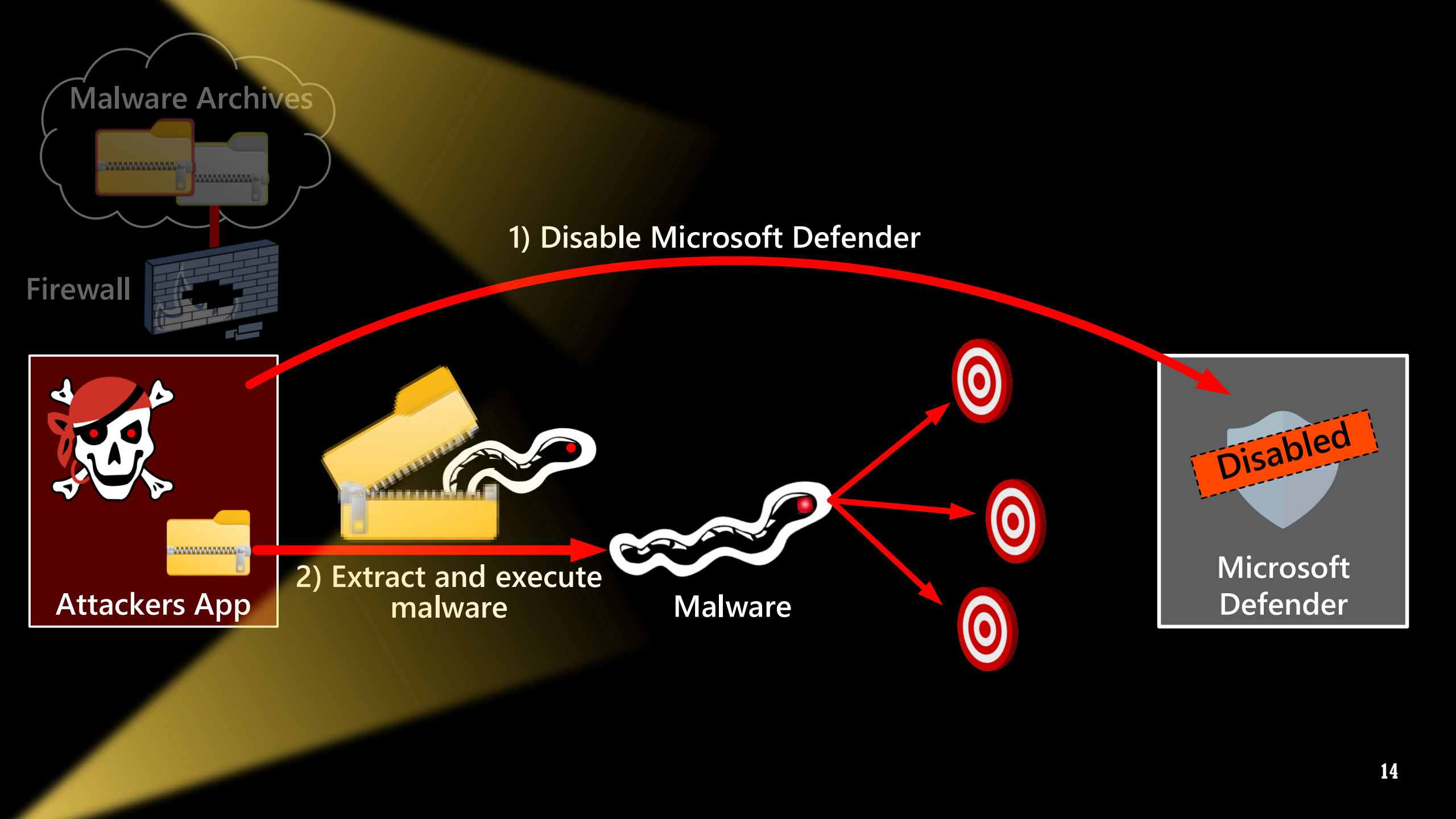

Malware Archives
Firewall
Attackers App
2) Extract and execute malware


Malware Archives
Firewall
Attackers App
2) Extract and execute malware
Malware
steal users credentials
install a backdoor
encrypt files (ransomware)


Malware Archives
Firewall
Attackers App
2) Extract and execute malware
Malware
Detect and remove malware
Microsoft Defender

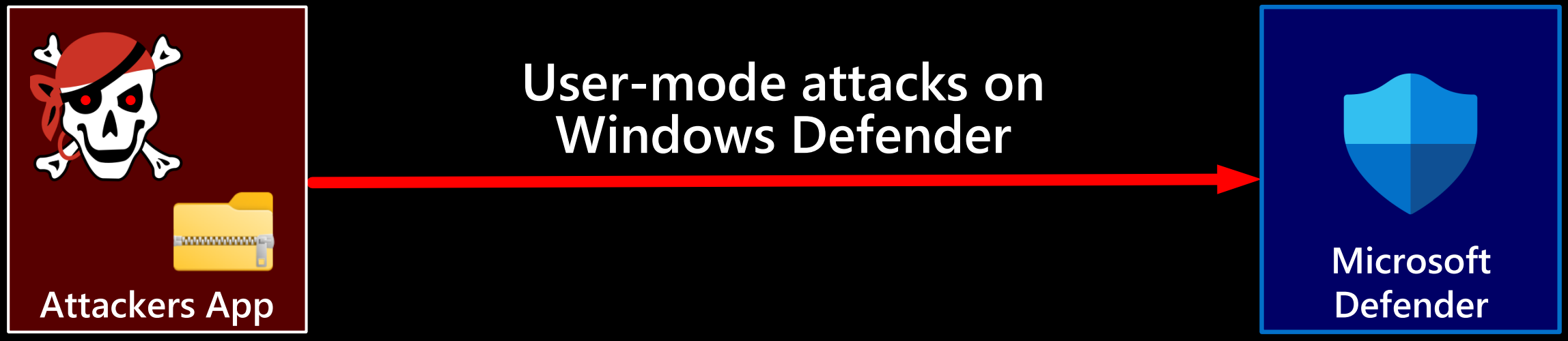

Disabled
Attackers App

1) Disable Microsoft Defender

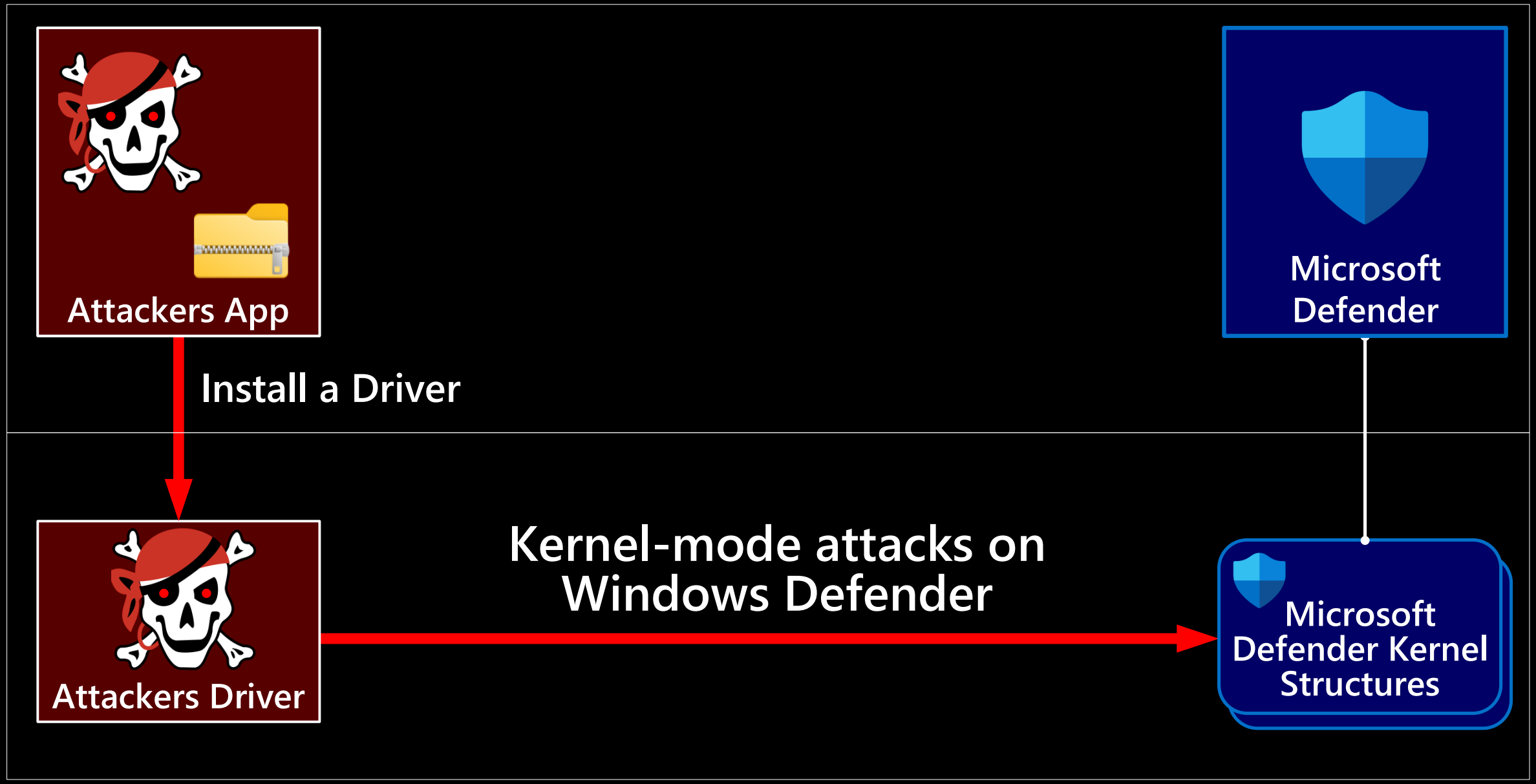

Malware Archives
Firewall
1) Disable Microsoft Defender
Attackers App
2) Extract and execute malware
Malware
Disabled
Microsoft Defender

Microsoft Defender is under attacks

Microsoft Defender is under attacks



Driver-based attacks can disable Microsoft Defender



MICROSOFT DEFENDER IS UNDER ATTACKS

Microsoft Defender is running on over 500 000 000 PCs

“

Windows Defender is protecting more than 50% of the Windows ecosystem, so we’re a big target, and everyone wants to evade us to get the maximum number of victims

Tanmay Ganacharya

Partner Director for Security Research

@ Microsoft Defender for Endpoint

* Top Microsoft Defender expert: These are the threats security hasn't yet solved, ZDNet, 2019
https://www.zdnet.com/article/top-windows-defender-expert-these-are-the-threats-security-hasnt-yet-solved

ATTACKS ON DEFENDER FROM

TWEETS ABOUT DISABLING MICROSOFT DEFENDER

TWEETS ABOUT DISABLING MICROSOFT DEFENDER

Joe Helle, Mayor of Hacktown, First of His Name
@joehelle

Let's bypass Windows Defender using reflection in Powershell. themayor.notion.site/53512dc072c241...

Qutaiba | قُتَيْبَة
@QutaibaM0

A simple python packer to easily bypass Windows Defender

Unknow101/
FuckThatPacker

TWEETS ABOUT DISABLING MICROSOFT DEFENDER

Joe Helle, Mayor of Hacktown, First of His Name
@joehelle

Let's bypass Windows Defender using reflection in Powershell. themayor.notion.site/53512dc072c241...

Qutaiba | قُتَيْبَة
@QutaibaMO

A simple python packer to easily bypass Windows Defender

Unknow101/
FuckThatPacker

Benjamin Delpy
@gentilkiwi

#trollday : epic Windows Defender bypass... before running #mimikatz : $mimikatz = 'C:\Users\Gentil Kiwi\Desktop\mimikatz.exe' ; Add-MpPreference -ExclusionPath $mimikatz -AttackSurfaceReductionOnlyExclusions $mimikatz

TWEETS ABOUT DISABLING MICROSOFT DEFENDER

Joe Helle, Mayor of Hacktown, First of His Name
@joehelle

Let's bypass Windows Defender using reflection in Powershell. themayor.notion.site/53512dc072c241...

Qutaiba | قُتَيْبَة
@QutaibaM0

A simple python packer to easily bypass Windows Defender

Unknow101/
FuckThatPacker

Benjamin Delpy
@gentilkiwi

#trollday : epic Windows Defender bypass... before running #mimikatz : $mimikatz = 'C:\Users\Gentil Kiwi\Desktop\mimikatz.exe' ; Add-MpPreference -ExclusionPath $mimikatz -AttackSurfaceReductionOnlyExclusions $mimikatz

last
@last0x00

I've published on @APTortellini's Github page a little project of mine called DefenderSwitch. It's a C++ program that can be used to disable/enable Windows Defender without interacting with the GUI by abusing TrustedInstaller. Admin privs needed.

APTortellini/
DefenderSwitch

Stop Windows Defender using the Win32 API

TWEETS ABOUT DISABLING MICROSOFT DEFENDER

Joe Helle, Mayor of Hacktown, First of His Name
@joehelle

Let's bypass Windows Defender using reflection in Powershell. themayor.notion.site/53512dc072c241...

Qutaiba | قُتَيْبَة
@QutaibaM0

A simple python packer to easily bypass Windows Defender

Unknow101/
FuckThatPacker

Benjamin Delpy
@gentilkiwi

#trollday : epic Windows Defender bypass... before running #mimikatz : $mimikatz = 'C:\Users\Gentil Kiwi\Desktop\mimikatz.exe' ; Add-MpPreference -ExclusionPath $mimikatz -AttackSurfaceReductionOnlyExclusions $mimikatz

last
@last0x00

I've published on @APTortellini's Github page a little project of mine called DefenderSwitch. It's a C++ program that can be used to disable/enable Windows Defender without interacting with the GUI by abusing TrustedInstaller. Admin privs needed.

APTortellini/
DefenderSwitch

Stop Windows Defender using the Win32 API

MALWARE ATTACKS MICROSOFT DEFENDER

2020

Ragnarok Ransomware

2021

Zloader Banking Trojan

2022

Kraken Botnet

MALWARE ATTACKS MICROSOFT DEFENDER

2020

Ragnarok Ransomware
disables the Microsoft Defender via a registry entry

2021

Zloader Banking Trojan

2022

Kraken Botnet

MALWARE ATTACKS MICROSOFT DEFENDER

2020

Ragnarok Ransomware
disables the Microsoft Defender via a registry entry

2021

Zloader Banking Trojan
disables Microsoft Defender via reconfiguring "Set-MpPreference"

2022

Kraken Botnet

MALWARE ATTACKS MICROSOFT DEFENDER

2020

Ragnarok Ransomware
disables the Microsoft Defender via a registry entry

2021

Zloader Banking Trojan
disables Microsoft Defender via reconfiguring "Set-MpPreference"

2022

Kraken Botnet
bypasses Microsoft Defender via adding exclusions permission

MALWARE ATTACKS MICROSOFT DEFENDER

2020

Ragnarok Ransomware
disables the Microsoft Defender via a registry entry

2021

Zloader Banking Trojan
disables Microsoft Defender via reconfiguring "Set-MpPreference"

2022

Kraken Botnet
bypasses Microsoft Defender via adding exclusions permission

Denis Wilson
@dwpia

Microsoft's Windows Defender has become a solid antivirus program and we are finding that malware programs are attempting to disable or bypass it. We have seen GootKit, TrickBot, and the Novter infections all utilizing some sort of Windows Defender bypass. buff.ly/38L3bTZ

ACADEMIC PAPERS AND BLOGS ABOUT ATTACKS ON MICROSOFT DEFENDER

Using Mimikatz' driver, Mimidrv, to disable Windows Defender in Windows

Bram Blaauwendraad
University of Amsterdam
Amsterdam, The Netherlands
bram.blaauwendraad@os3.nl

Thomas Ouddeken
University of Amsterdam
Amsterdam, The Netherlands
thomas.ouddeken@os3.nl

Supervisor
Cedric van Bockhaven
Deloitte
Amsterdam, The Netherlands

Journal of Cybersecurity and Privacy
MDPI

Article

An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors

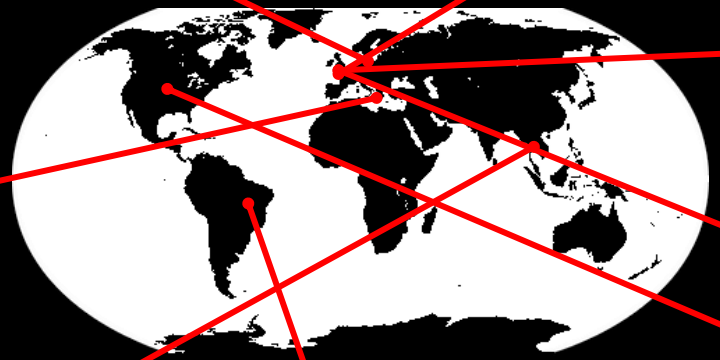
George Karantzas [1] and Constantinos Patsakis [1,2,*]

Evading Security Products for Credential Dumping Through Exploiting Vulnerable Driver in Windows Operating Systems

Huu-Danh Pham[1], Vu Thanh Nguyen[2](✉), Mai Viet Tiep[3]
Phu Phuoc Huy[5], and Pham Thi Vuon

AntiViruses under the Microscope: A Hands-On Perspective

Marcus Botacin[1] Felipe Duarte Domingues[2] Fabrício Ceschin[1] Raphael Machnicki[1]
Marco Antonio Zanata Alves[1] Paulo Lício de Geus[2] André Grégio[1]



PROCESS HERPADERPING – WINDOWS DEFENDER EVASION

Posted on January 18, 2021 by Administrator

Evading Windows Defender with 1 Byte Change

BYPASSING WINDOWS DEFENDER RUNTIME SCANNING

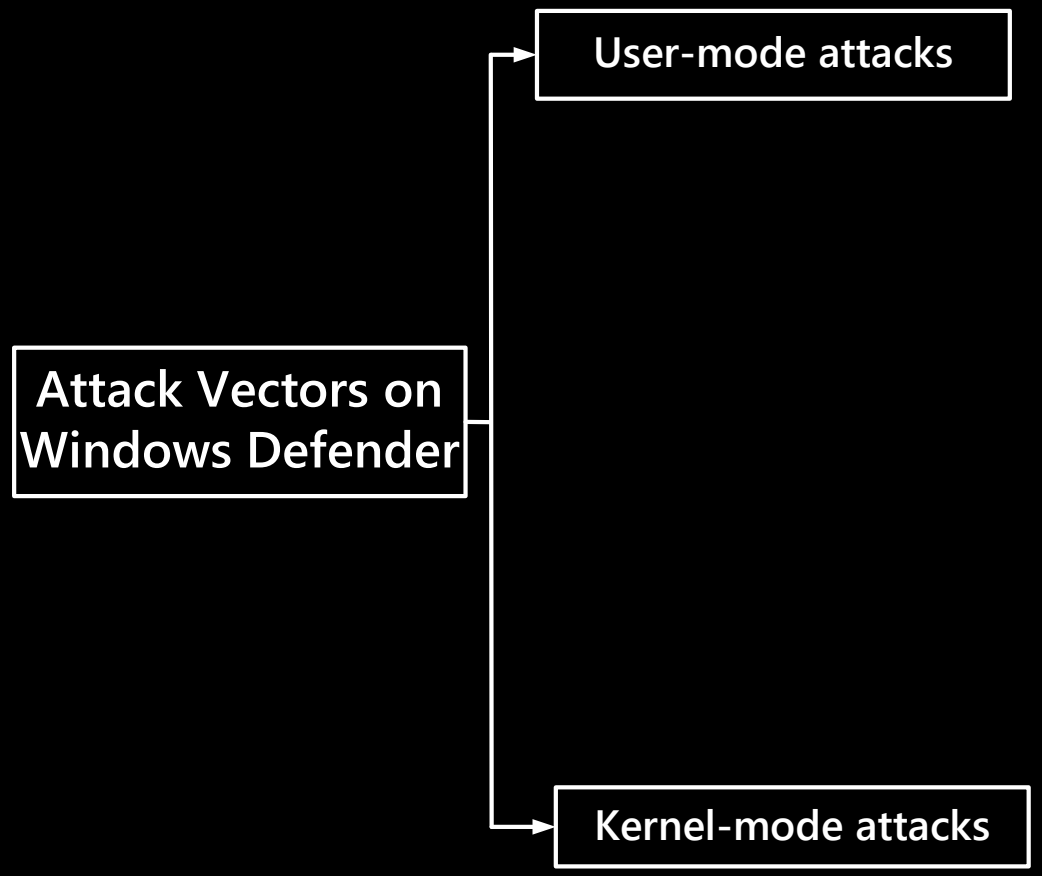
Charalampos Billinis, 1 May 2020

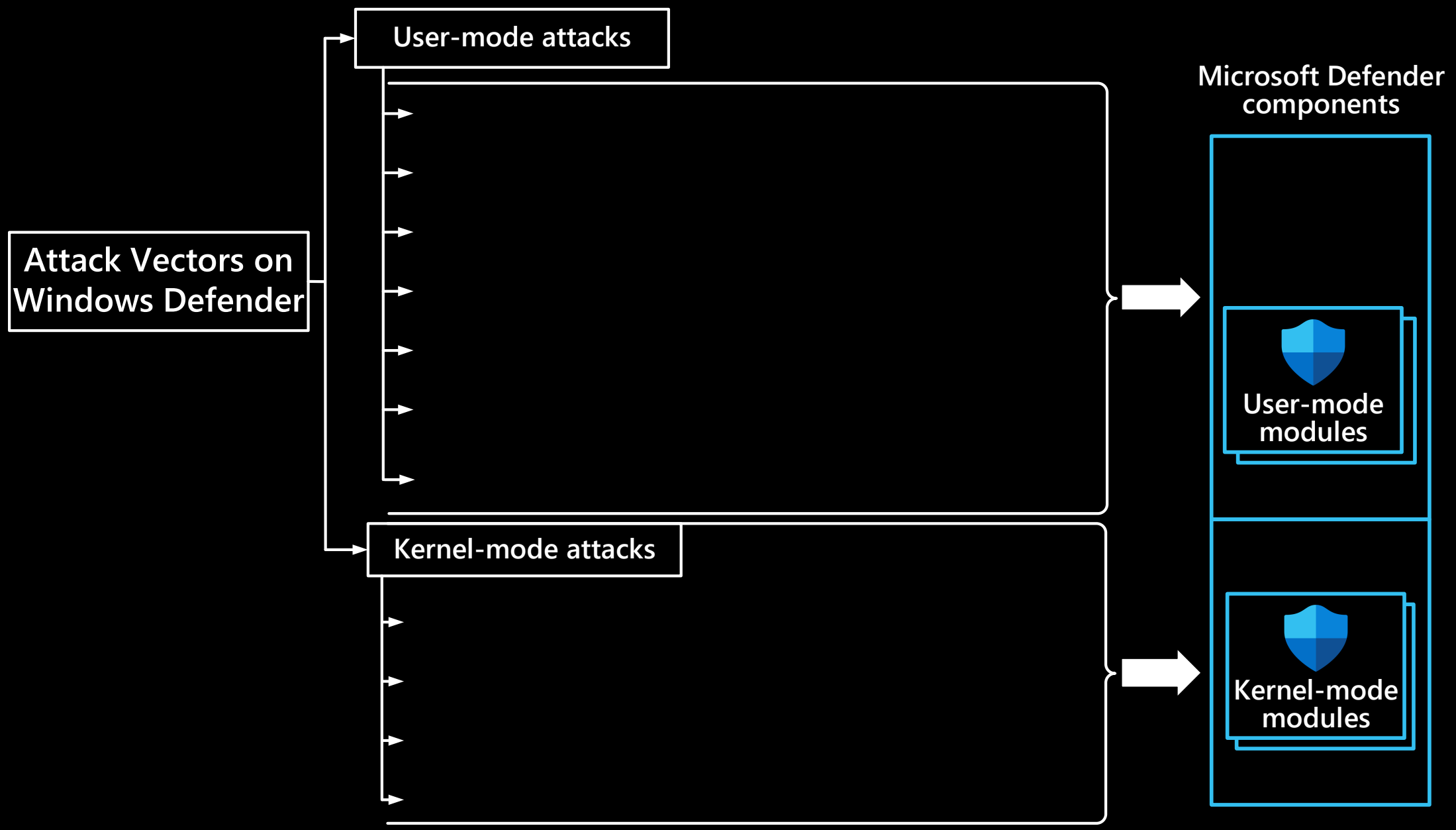
Windows Offender: Reverse Engineering Windows Defender's Antivirus Emulator

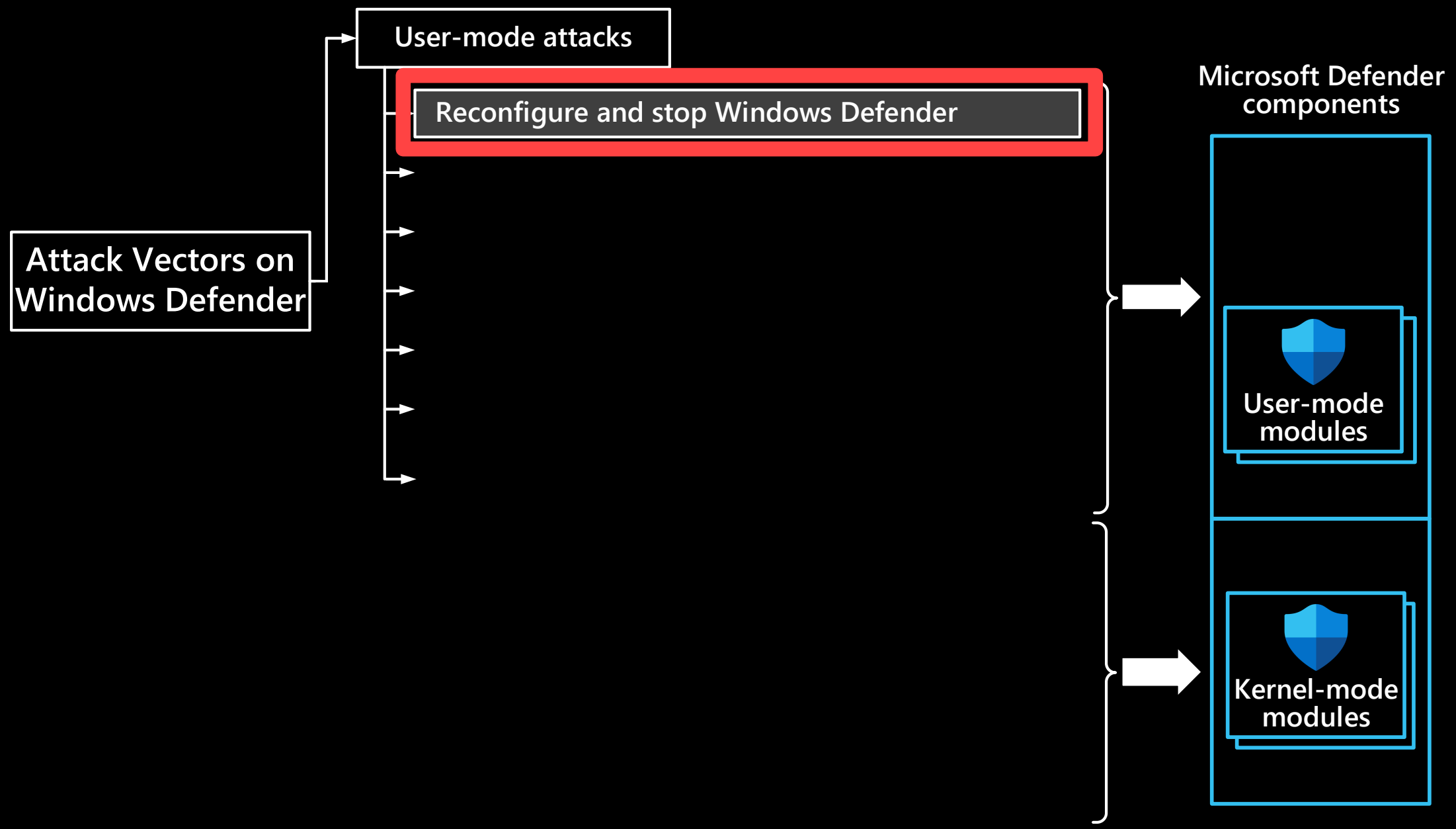
Alexei Bulazel
@0xAlexei

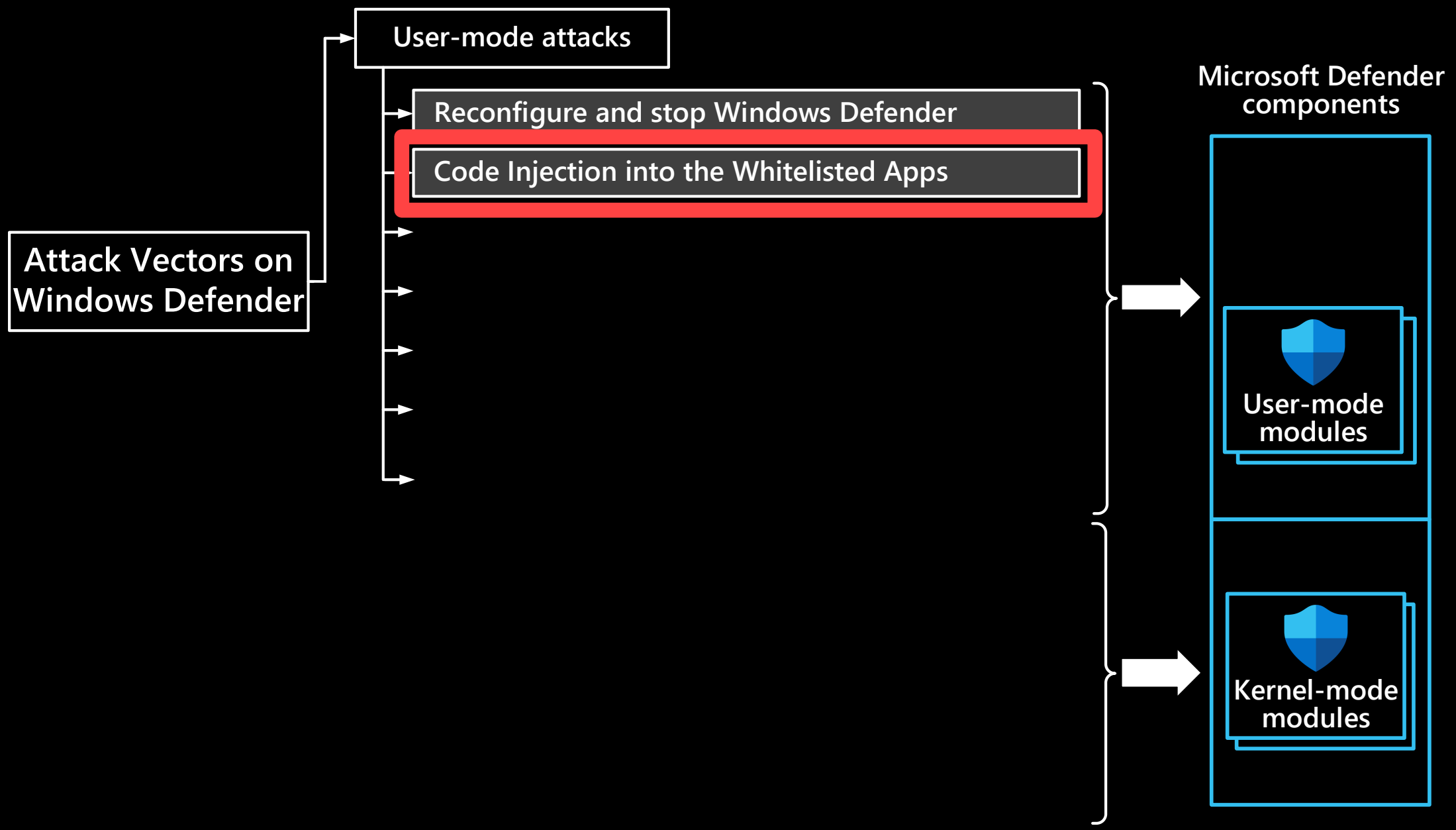
Black Hat 2018

ATTACK VECTORS ON MICROSOFT DEFENDER


Attack Vectors on Windows Defender
User-mode attacks
Kernel-mode attacks


Attack Vectors on Windows Defender
User-mode attacks
Kernel-mode attacks
Microsoft Defender components
User-mode modules
Kernel-mode modules


Attack Vectors on Windows Defender
User-mode attacks
Reconfigure and stop Windows Defender
Microsoft Defender components
User-mode modules
Kernel-mode modules

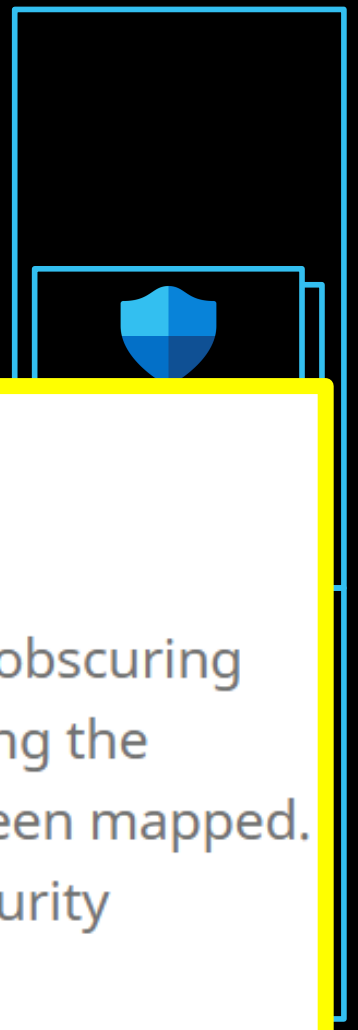

Attack Vectors on Windows Defender
User-mode attacks
Reconfigure and stop Windows Defender
Code Injection into the Whitelisted Apps
Microsoft Defender components
User-mode modules
Kernel-mode modules

Attack Vectors on Windows Defender

User-mode attacks

- Reconfigure and stop Windows Defender
- Code Injection into the Whitelisted Apps
- Process Herpaderping

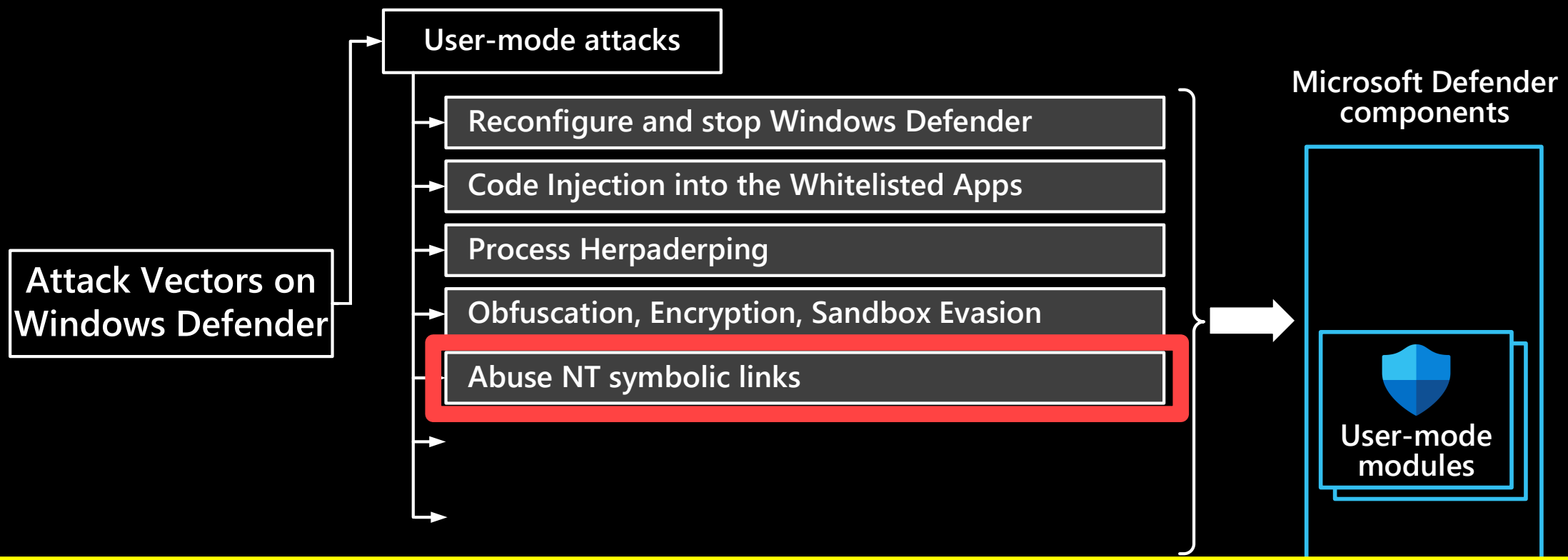
Microsoft Defender components



Process Herpaderping

Process Herpaderping is a method of obscuring the intentions of a process by modifying the content on disk after the image has been mapped. This results in curious behavior by security products and the OS itself.

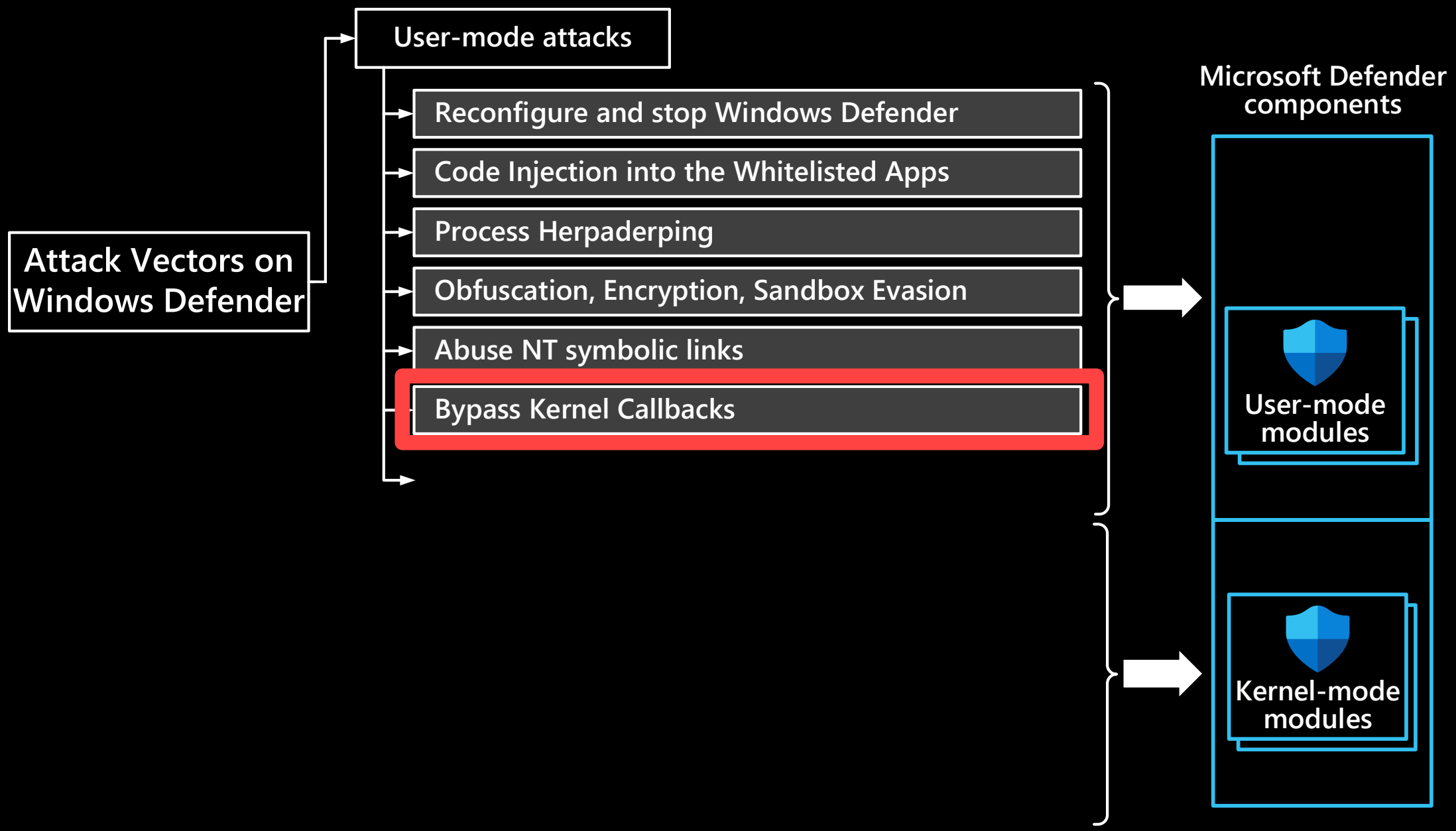

Attack Vectors on Windows Defender
User-mode attacks
Reconfigure and stop Windows Defender
Code Injection into the Whitelisted Apps
Process Herpaderping
Obfuscation, Encryption, Sandbox Evasion
Microsoft Defender components
User-mode modules
Kernel-mode modules



The dying knight in the shiny armour

Killing Defender through NT symbolic links redirection while keeping it unbothered

Aug 21, 2021 • last


Attack Vectors on Windows Defender
User-mode attacks
Reconfigure and stop Windows Defender
Code Injection into the Whitelisted Apps
Process Herpaderping
Obfuscation, Encryption, Sandbox Evasion
Abuse NT symbolic links
Bypass Kernel Callbacks
Microsoft Defender components
User-mode modules
Kernel-mode modules

Attack Vectors on Windows Defender

User-mode attacks

- Reconfigure and stop
- Code Injection into th
- Process Herpaderping
- Obfuscation, Encrypti
- Abuse NT symbolic lin
- Bypass Kernel Callbacks

Elastic Security Research

Sandboxing Antimalware Products for Fun

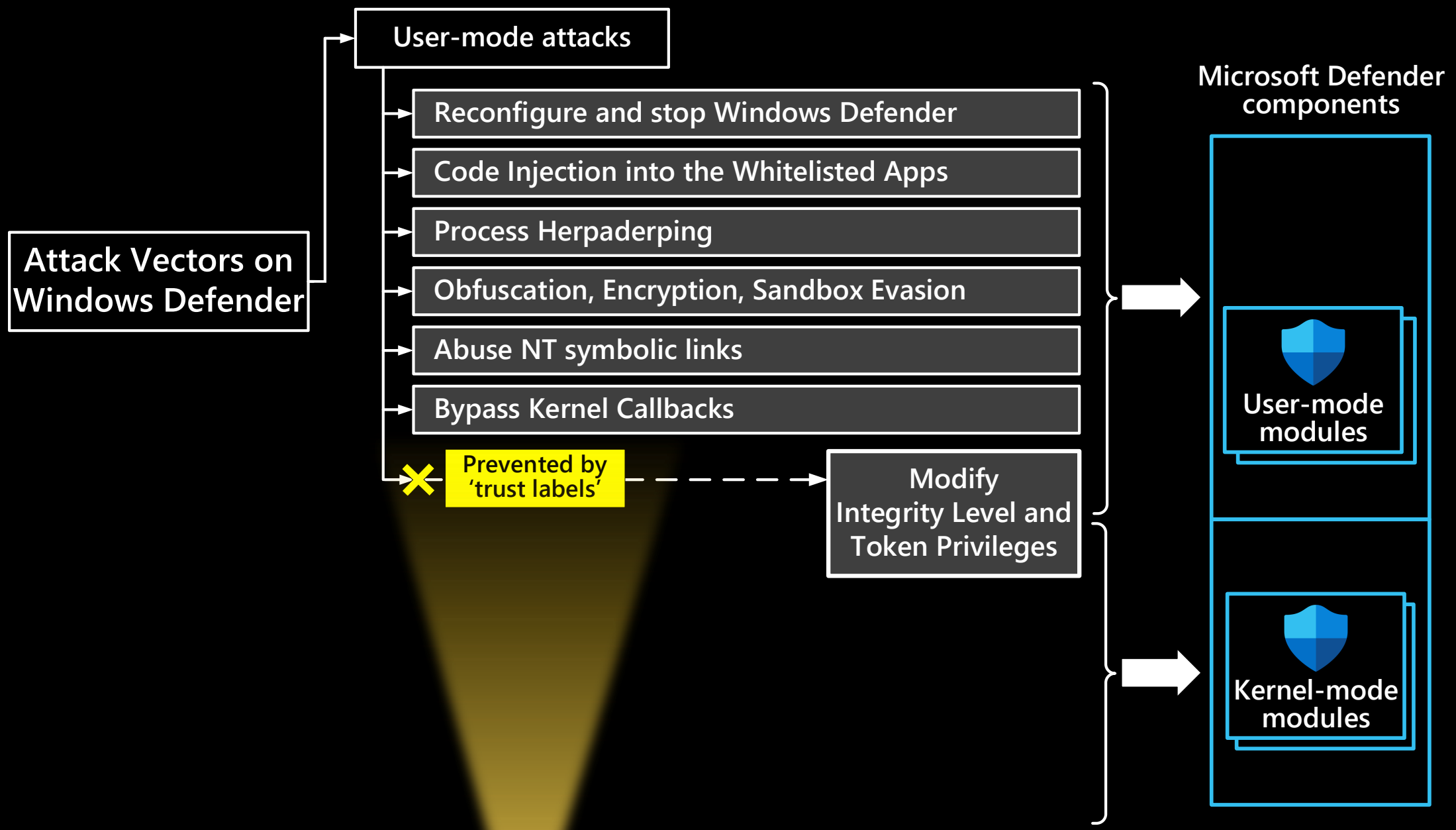
Elastic Security identifies Windows security feature bypass

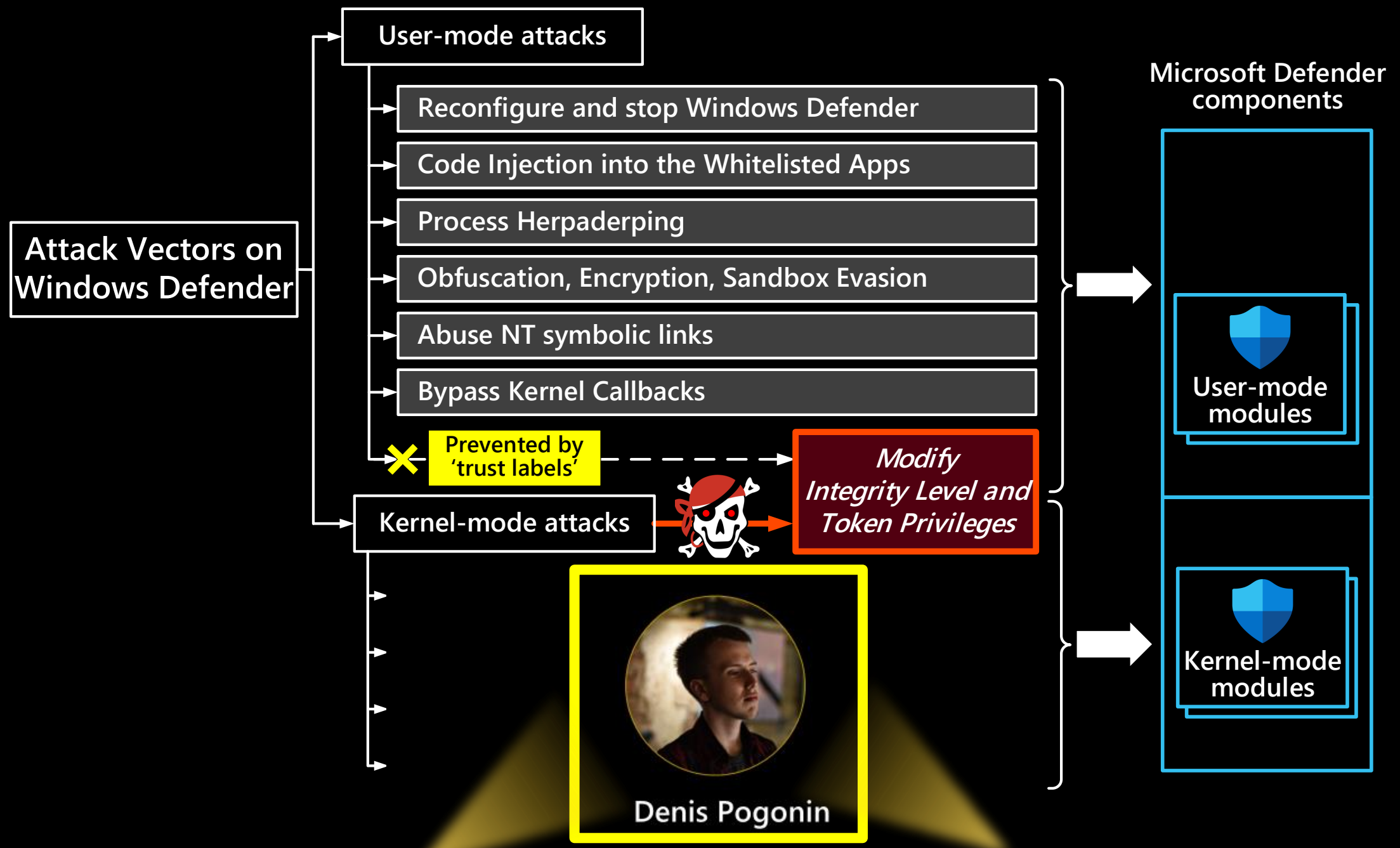
2022-02-02

Modify Integrity Level and Token Privileges

User-mode modules

Kernel-mode modules


Attack Vectors on Windows Defender
User-mode attacks
Reconfigure and stop Windows Defender
Code Injection into the Whitelisted Apps
Process Herpaderping
Obfuscation, Encryption, Sandbox Evasion
Abuse NT symbolic links
Bypass Kernel Callbacks
Prevented by 'trust labels'
Modify Integrity Level and Token Privileges
Microsoft Defender components
User-mode modules
Kernel-mode modules


Attack Vectors on Windows Defender
User-mode attacks
Reconfigure and stop Windows Defender
Code Injection into the Whitelisted Apps
Process Herpaderping
Obfuscation, Encryption, Sandbox Evasion
Abuse NT symbolic links
Bypass Kernel Callbacks
Prevented by 'trust labels'
Modify Integrity Level and Token Privileges
Kernel-mode attacks
Denis Pogonin
Microsoft Defender components
User-mode modules
Kernel-mode modules

Attack Vectors on Windows Defender

User-mode atta

Reconfigure

Code Injectio

Process Herp

Obfuscation,

Abuse NT sy

Bypass Kerne

Kernel-mode attacks

Token Privileges

Disabling ETW logger sessions

Kernel-mode modules

Attack Vectors on Windows Defender

User-mode attack

- Reconfigure ar
- Code Injection
- Process Herpac
- Obfuscation, E
- Abuse NT syml
- Bypass Kernel

Kernel-mode attacks

- Disabling ETW logger sessions
- Disabling PPL to stop Windows Defender

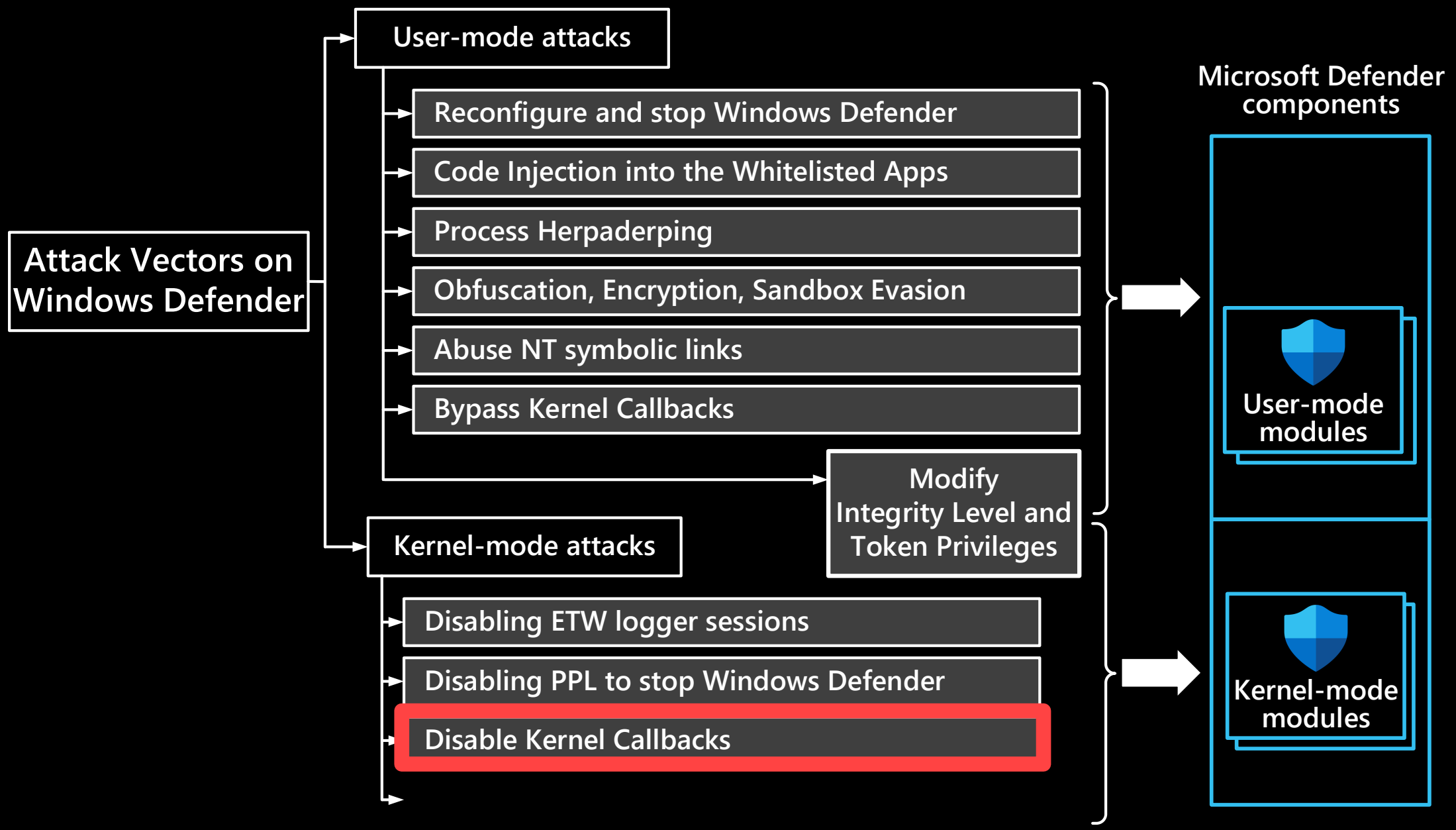
Token Privileges

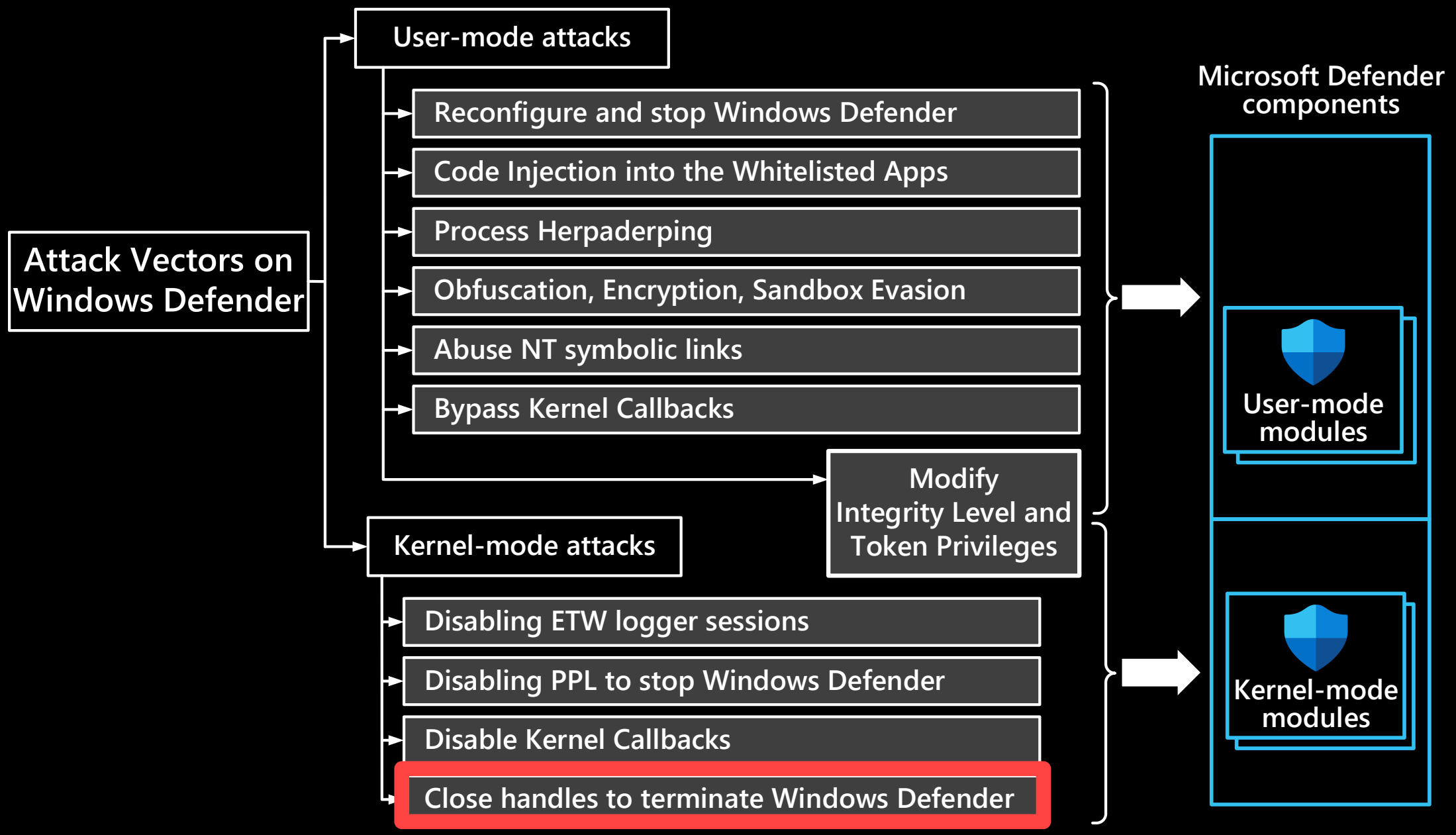
Kernel-mode modules

TEXAS CYBER SUMMIT
CYBER SECURITY CONFERENCE
2021
TEXASCYBER.COM

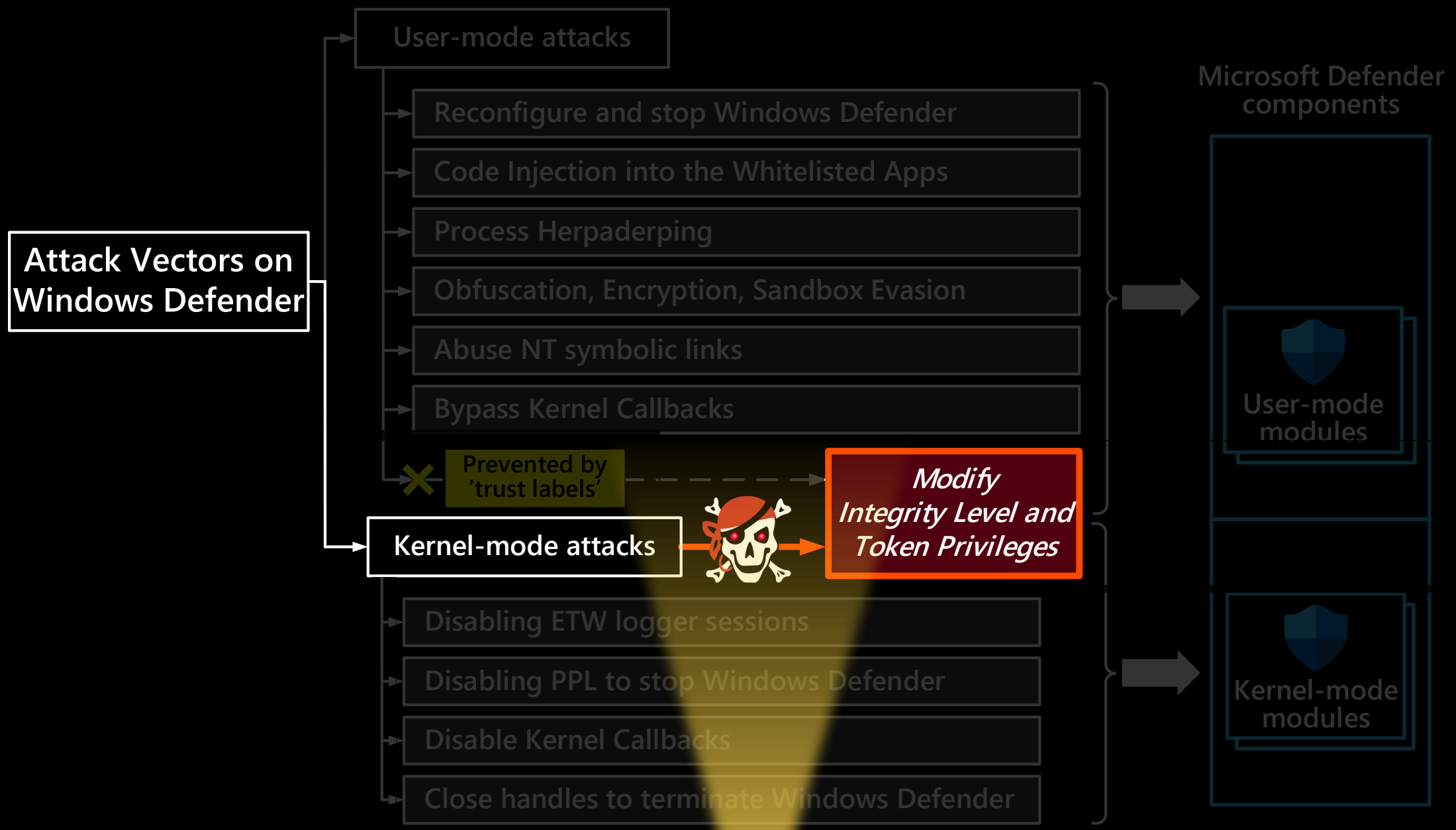
Protected Process Light will be Protected - MemoryRanger Fills the Gap Again

Igor Korkin
Independent Researcher
2021


Attack Vectors on Windows Defender
User-mode attacks
Reconfigure and stop Windows Defender
Code Injection into the Whitelisted Apps
Process Herpaderping
Obfuscation, Encryption, Sandbox Evasion
Abuse NT symbolic links
Bypass Kernel Callbacks
Modify Integrity Level and Token Privileges
Kernel-mode attacks
Disabling ETW logger sessions
Disabling PPL to stop Windows Defender
Disable Kernel Callbacks
Microsoft Defender components
User-mode modules
Kernel-mode modules



All the details of these attacks are in the research paper


Attack Vectors on Windows Defender
User-mode attacks
Reconfigure and stop Windows Defender
Code Injection into the Whitelisted Apps
Process Herpaderping
Obfuscation, Encryption, Sandbox Evasion
Abuse NT symbolic links
Bypass Kernel Callbacks
Prevented by 'trust labels'
Kernel-mode attacks
Modify Integrity Level and Token Privileges
Disabling ETW logger sessions
Disabling PPL to stop Windows Defender
Disable Kernel Callbacks
Close handles to terminate Windows Defender
Microsoft Defender components
User-mode modules
Kernel-mode modules

TRENDS OF KERNEL ATTACKS IN 2021-2022

Driver-Based Attacks* in 2021-2022

- **Bring Your Own Vulnerable Driver (BYOVD)**
  - HermeticWiper abuses EaseUS driver (2022)
  - Rapid7 experts gave 30 malware examples that use buggy signed drivers
- Malware Drivers signed with leaked certificates + WHQL Scandal
  - Stolen Nvidia certificates used to sign malware (2022)
  - Microsoft admits to signing rootkit named Netfilter (2021)
- UEFI Security Threats
  - UEFI rootkit named MoonBounce can install a malicious driver (2022)
  - Binarly experts found 20 UEFI bugs that impacted millions of devices (2022)

*More Examples are in the conference paper

Driver-Based Attacks* in 2021-2022

Bring Your Own Vulnerable Driver (BYOVD)

- HermeticWiper abuses EaseUS driver (2022)
- Rapid7 experts gave 30 malware examples that use buggy signed drivers

Year	Malware	3rd party driver
2022	HermeticWiper	EaseUS
2021	Iron Tiger	CPUID CPU-Z
	GhostEmperor	CheatEngine
	ZINC	eXplorer
	TunnelSnake	VirtualBox
2020	RobbinHood	Gigabyte
	Trickbot	RWEverything
	...	

More than **30** malware examples that abuse vulnerable signed drivers

Driver-Based Attacks* in 2021-2022

- Bring Your Own Vulnerable Driver (BYOVD)
  - HermeticWiper abuses EaseUS driver (2022)
  - Rapid7 experts gave 30 malware examples that use buggy signed drivers
- **Malware Drivers signed with leaked certificates + WHQL Scandal**
  - Stolen Nvidia certificates used to sign malware (2022)
  - Microsoft admits to signing rootkit named Netfilter (2021)
- UEFI Security Threats
  - UEFI rootkit named MoonBounce can install a malicious driver (2022)
  - Binarly experts found 20 UEFI bugs that impacted millions of devices (2022)

*More Examples are in the conference paper

Driver-Based Attacks* in 2021-2022

- Bring Your Own Vulnerable Driver (BYOVD)
  - ProHarmaticWiper abuses EaseUS driver (2022)
  - Rapid7 experts gave 30 malware examples that use dummy signed drivers
- Malware Drivers signed with leaked certificates + WHQL Scandal
  - ed to sign malware (2022)
  - rootkit named Netfilter (2021)
  - ounce can install a malicious driver (2022)
  - Binarly experts found 20 UEFI bugs that impacted millions of devices (2022)

*Mo[illegible]ples are in the conference paper

Lapsus$ hack leaves NVIDIA in a tight spot

The hackers have leaked NVIDIA's official code signing certificates.

BY AKASHDEEP ARUL

March 1

2022

Driver-Based Attacks* in 2021-2022

Bring Your Own Vulnerable Driver (BYOVD)

Malware

dal

ITPro.

Nvidia confirms data breach as hackers make additional demands

Nvidia has confirmed a rumoured hack on its systems for the first time as the first part of the alleged 1TB of company secrets is made available to download

by: Connor Jones 2 Mar 2022

Lapsus$ hacl in a tight spo

The hackers have leaked NVIDI code signing certificates.

BY AKASHDEEP ARUL

ounce can install a malicious driver (2022)

•Binarly experts found 20 UEFI bugs that impacted millions of devices (2022)

2022

March 1

March 2

*Mo ples are in the conference pa

Driver-Based Attacks* in 2021-2022

Bring Your Own Vulnera

Malware

Lapsus$ hacl
in a tight spo

The hackers have leaked NVIDIA
code signing certificates.

BY AKASHDEEP ARUL

Nvidia confir
make additio

Nvidia has confirm
the first time as th
secrets is made available to download

by: Connor Jones 2 Mar 2022

NVIDIA's Stolen Code-Signing Certs Used to Sign Malware

Author:
Lisa Vaas
March 7, 2022 / 12:46 pm

NVIDIA certificates are being used to sign malware, enabling malicious programs to pose as legitimate and slide past security safeguards on Windows machines.

bounce can install a malicious driver (2022)

•Binarly experts found 20 UEFI bugs that impacted millions of devices (2022)

*Mo ples are in the conference pa

2022

March 1

March 2

March 7

Driver-Based Attacks* in 2021-2022

Dark Web Research: Illicit Code Signing Certificates More Valuable Than Passports and Handguns

The certificates, available for prices ranging from $299 to $1,599, are being issued by reputable companies such as Symantec, Comodo, and Thawte, and are proving very effective at malware obfuscation, Recorded Future said in a report this week.

Driver-Based Attacks* in 2021-2022

- Bring Your Own Vulnerable Driver (BYOVD)
  - HermeticWiper abuses EaseUS driver (2022)
  - Rapid7 experts gave 30 malware examples that use buggy signed drivers
- Malware Drivers signed with leaked certificates
  - St
  - M 21)
- UEFI S
  - UE driver (2022)
  - Bi ns of devices (2022)

*More Ex

WHQL

Windows Hardware Quality Labs

WHQL Scandal

Driver-Based Attacks* in 2021-2022

- Bring Your Own Vulnerable Driver (BYOVD)
  - HermeticWiper abuses EaseUS driver (2022)
  - Rapid7 experts gave 30 malware examples that use buggy signed drivers
- Malware Drivers signed with leaked certificates — WHQL Scandal
  - Stolen Nvidia certificates used to sign malware (2022)
  - Microsoft admits to signing rootkit named Netfilter (2021)
  - Binarly experts found 20 UEFI bugs that impacted millions of devices (2022)

> Microsoft creates Windows Hardware Quality Labs (WHQL) to test drivers and award a digital signature when all requirements are fulfilled.

*More Examples are in the conference paper

Driver-Based Attacks* in 2021-2022

Windows 10 Compatible

Windows 11 Compatible

Driver (BYOVD)

leaked certificates + WHQL Scandal

used to sign malware (2022)

ng rootkit named Netfilter (2021)

- UEFI rootkit named MoonBounce can install a malicious driver (2022)
- Binarly experts found 20 UEFI bugs that impacted millions of devices (2022)

2021

June

*More examples are in the conference paper

Driver-Based Attacks* in 2021-2022

Windows 10 Compatible

Windows 11 Compatible

PC

Find products, advice, tech news

Microsoft Confirms it Signed Malicious 'Netfilter' Drivers

Microsoft says the Netfilter drivers used to distribute rootkit malware were signed as part of the Windows Hardware Compatibility Program.

By Nathaniel Mott

27 Jun 2021, 3:07 p.m.

Neowin

Microsoft WHQL-signed FiveSys driver was actually malware in disguise

Sayan Sen · Oct 22, 2021 02:12 EDT · HOT! 13

- UEFI rootkit named MoonBounce can install a malicious driver (2022)
- Binarly experts found 20 UEFI bugs that impacted millions of devices (2022)

2021

June

October

*More examples are in the conference paper

Driver-Based Attacks* in 2021-2022

- Bring Your Own Vulnerable Driver (BYOVD)
  - HermeticWiper abuses EaseUS driver (2022)
  - Rapid7 experts gave 30 malware examples that use buggy signed drivers
- Malware Drivers signed with leaked certificates + WHQL Scandal
  - Stolen Nvidia certificates used to sign malware (2022)
  - Microsoft admits to signing rootkit named Netfilter (2021)
- UEFI Security Threats
  - UEFI rootkit named MoonBounce can install a malicious driver (2022)
  - Binarly experts found 20 UEFI bugs that impacted millions of devices (2022)

*More Examples are in the conference paper

Driver-

BLEEPINGCOMPUTER

HP patches 16 UEFI firmware bugs allowing stealthy malware infections

By Bill Toulas

March 8, 2022 01:00 PM 0

•Stolen Nvidia certificate

•Microsoft admits to sig

OFFENSIVECON BY Blue Frost Security

ALEX ERMOLOV, ALEX MATROSOV AND YEGOR VASILENKO

UEFI FIRMWARE VULNERABILITIES: PAST, PRESENT AND FUTURE

UEFI Security Threats

- UEFI rootkit named MoonBounce can install a malicious driver (2022)
- Binarly experts found 20 UEFI bugs that impacted millions of devices (2022)

*More Examples are in the conference paper

Driver-Based Attacks* in 2021-2022

Bring Your Own Vulnerable Driver (BYOVD)

- HermeticWiper abuses EaseUS driver (2022)
- Rapid7 experts gave 30 malware examples that use buggy signed drivers

Malware Drivers signed with leaked certificates + WHQL Scandal

- Stolen Nvidia certificates used to sign malware (2022)
- Microsoft admits to signing rootkit named Netfilter (2021)

UEFI Security Threats

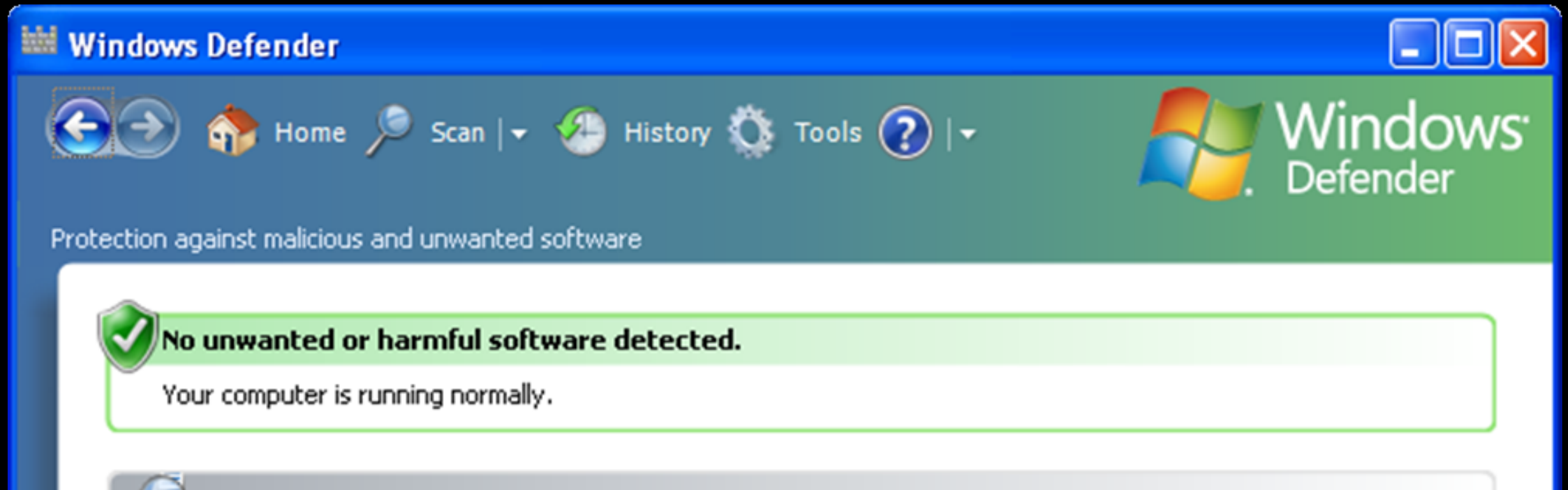
- UEFI rootkit named MoonBounce can install a malicious driver (2022)
- Binarly experts found 20 UEFI bugs that impacted millions of devices (2022)

*More Examples are in the conference paper

MICROSOFT DEFENDER: INTRO

MICROSOFT DEFENDER: INTRO

- 2005 – the first release as a free anti-spyware program

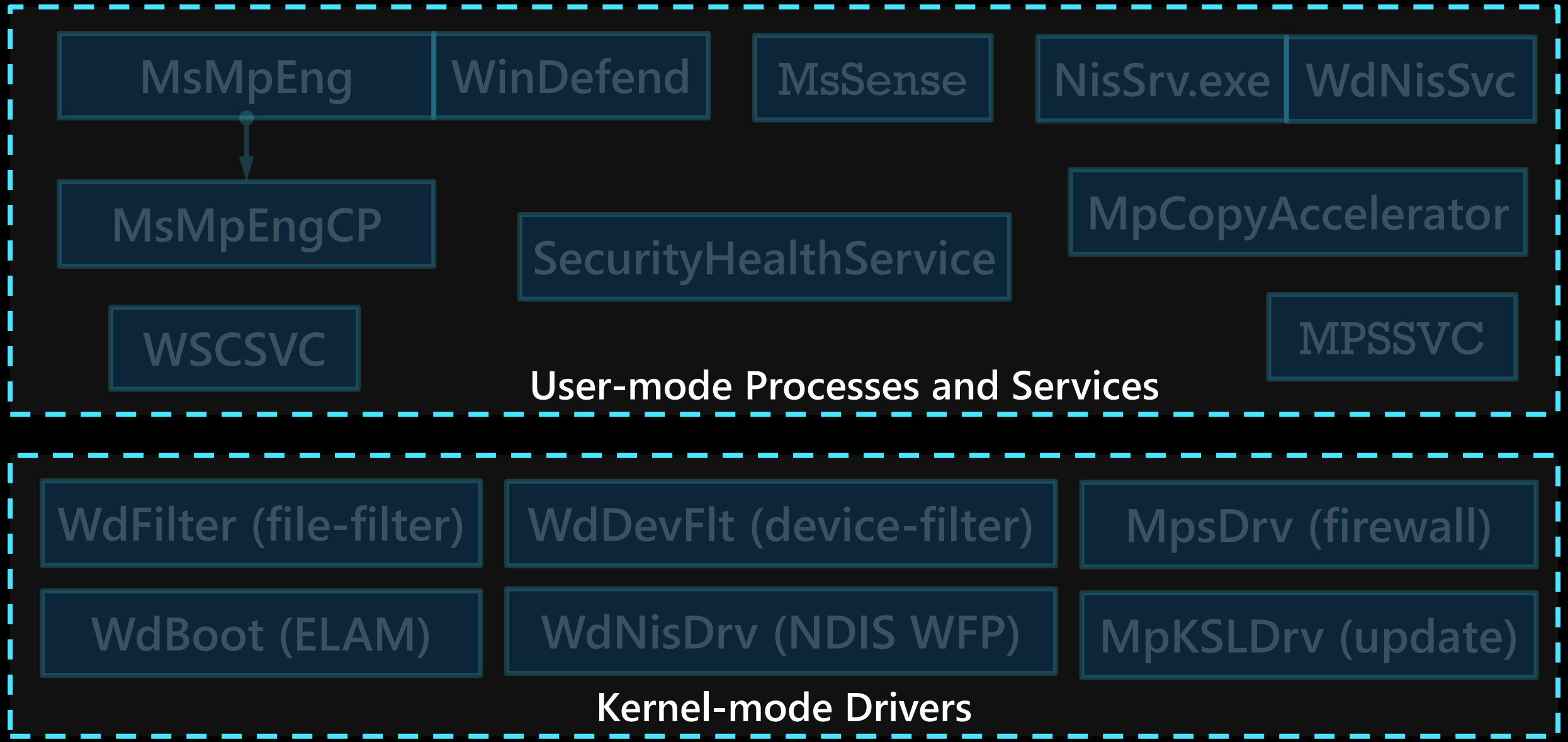


MICROSOFT DEFENDER: INTRO

- 2005 – the first release as a free anti-spyware program
- 2019 – Gartner: Microsoft Defender is the Leader in the Endpoint Protection Platforms (EPP) Magic Quadrant.

MICROSOFT DEFENDER: COMPONENTS

MICROSOFT DEFENDER: ABOUT 10 APPS + 6 DRIVERS



MICROSOFT DEFENDER: ABOUT 10 APPS + 6 DRIVERS

MsMpEng

WinDefend

MsSense

NisSrv.exe

WdNisSvc

MsMpEngCP

SecurityHealthService

MpCopyAccelerator

WSCSVC

MPSSVC

User-mode Processes and Services

WdFilter (file-filter)

WdDevFlt (device-filter)

MpsDrv (firewall)

WdBoot (ELAM)

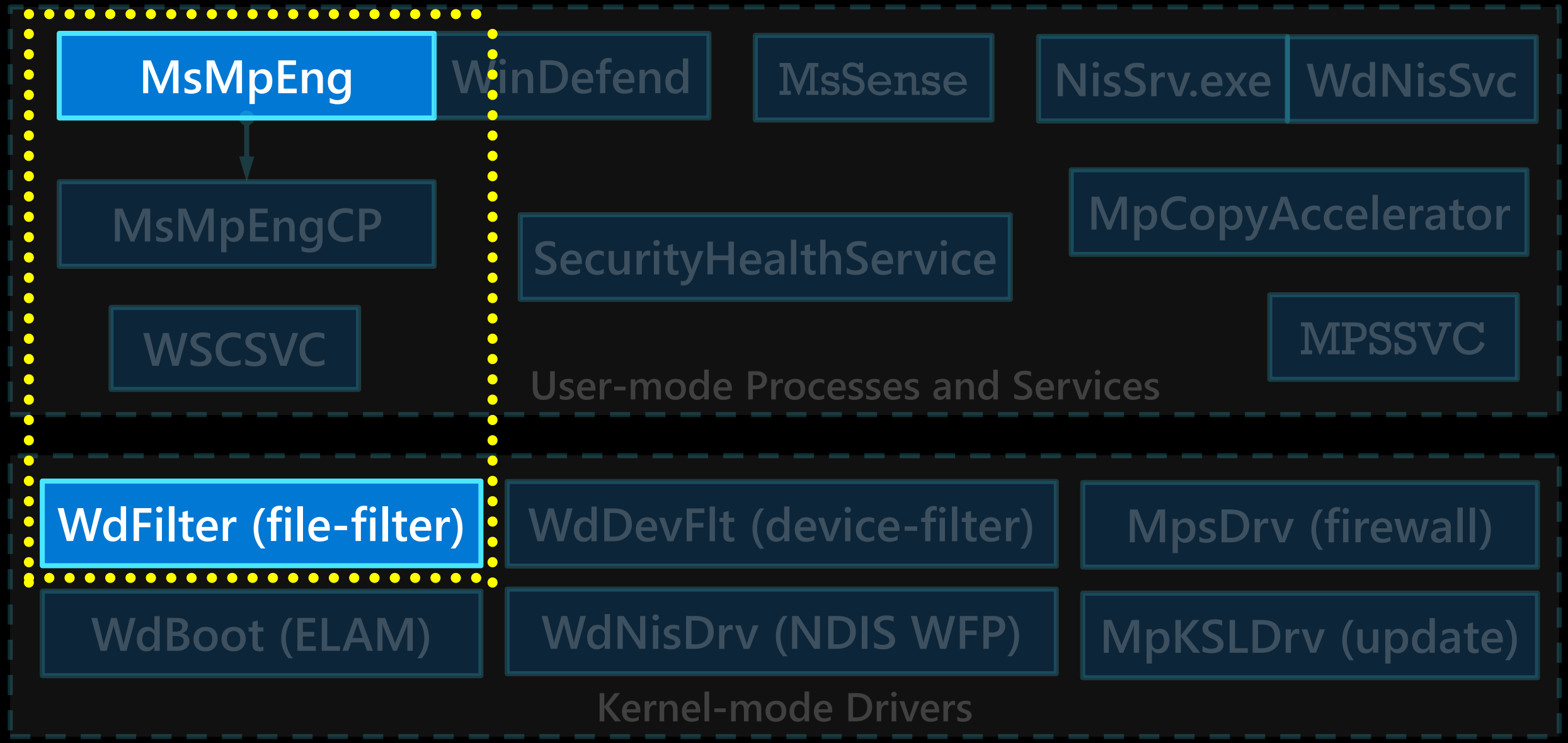
WdNisDrv (NDIS WFP)

MpKSLDrv (update)

Kernel-mode Drivers

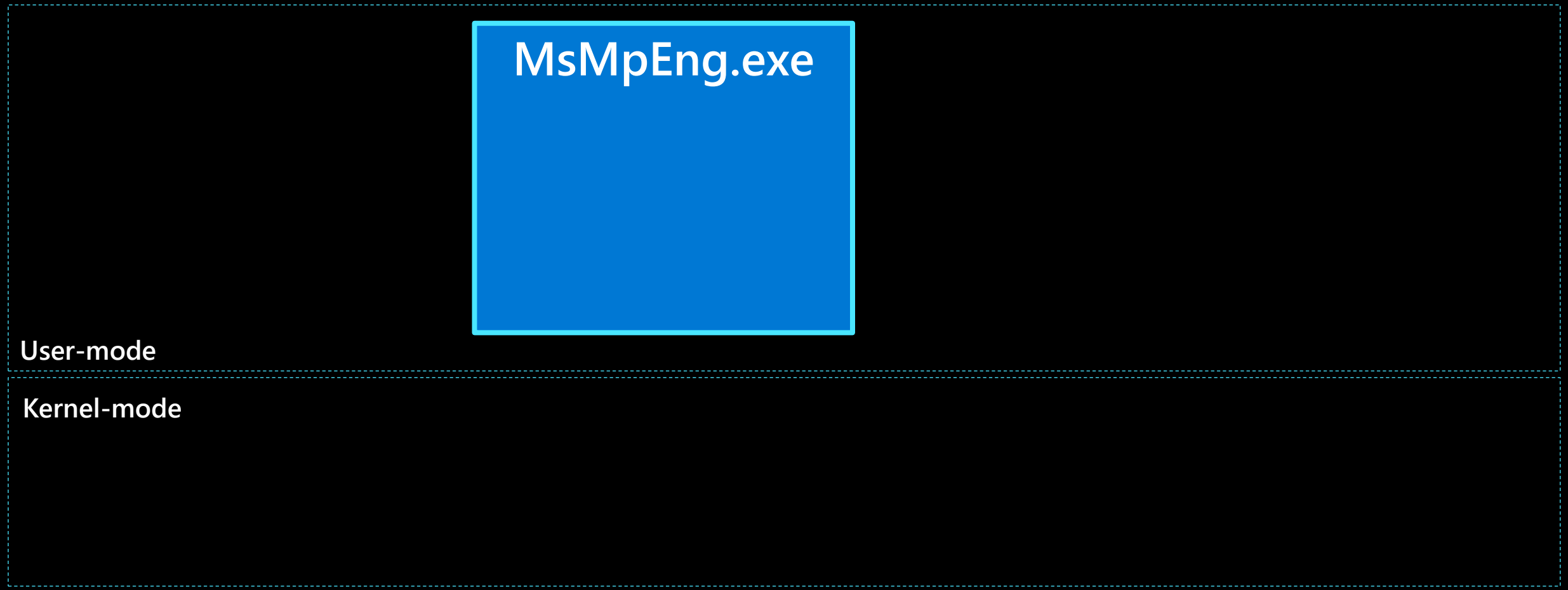
- %ProgramData%\Microsoft\Microsoft Defender\Platform
- %Windir%\System32\drivers\wd

MICROSOFT DEFENDER: ABOUT 10 APPS + 6 DRIVERS

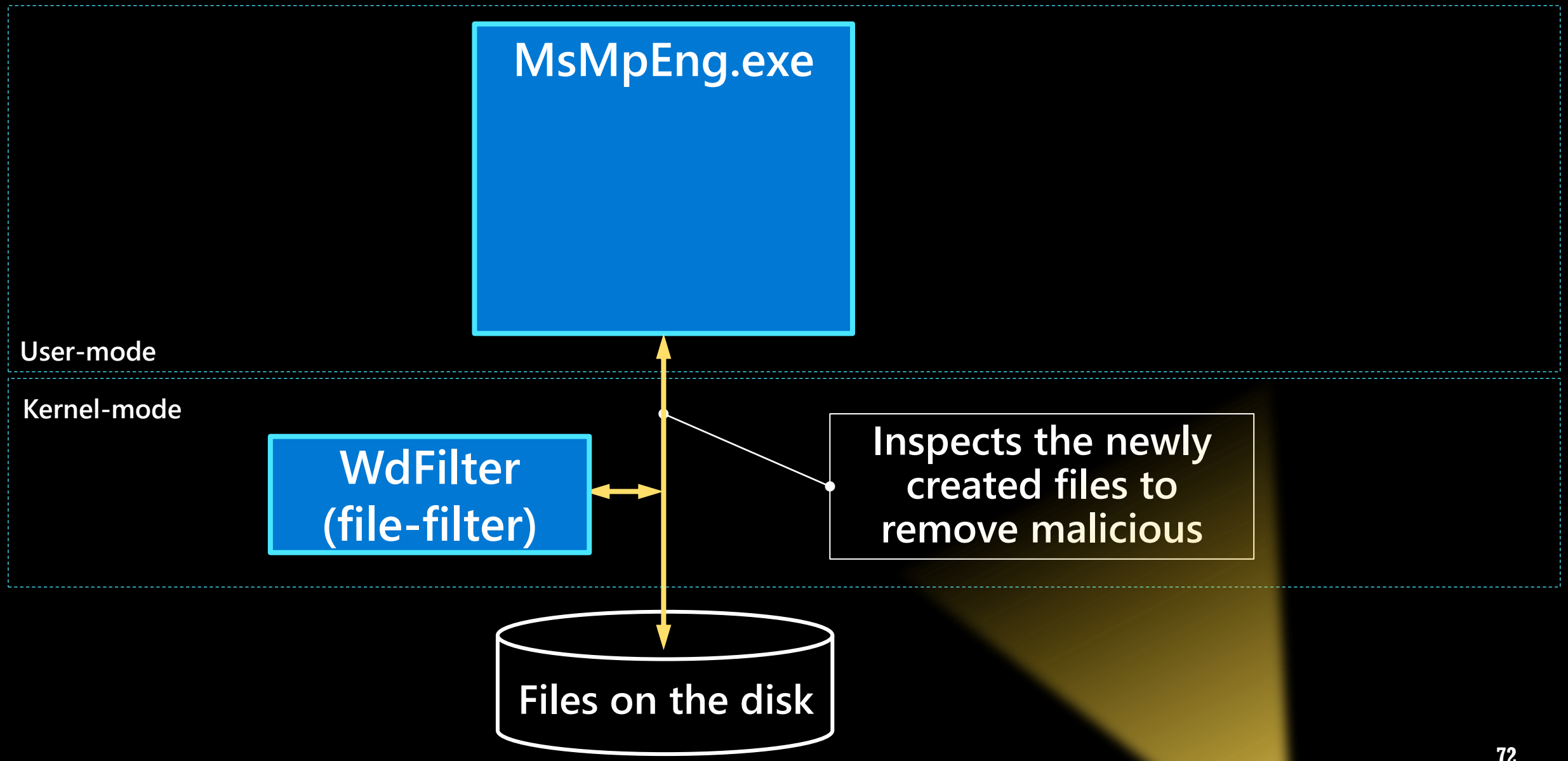


- %ProgramData%\Microsoft\Microsoft Defender\Platform
- %Windir%\System32\drivers\wd

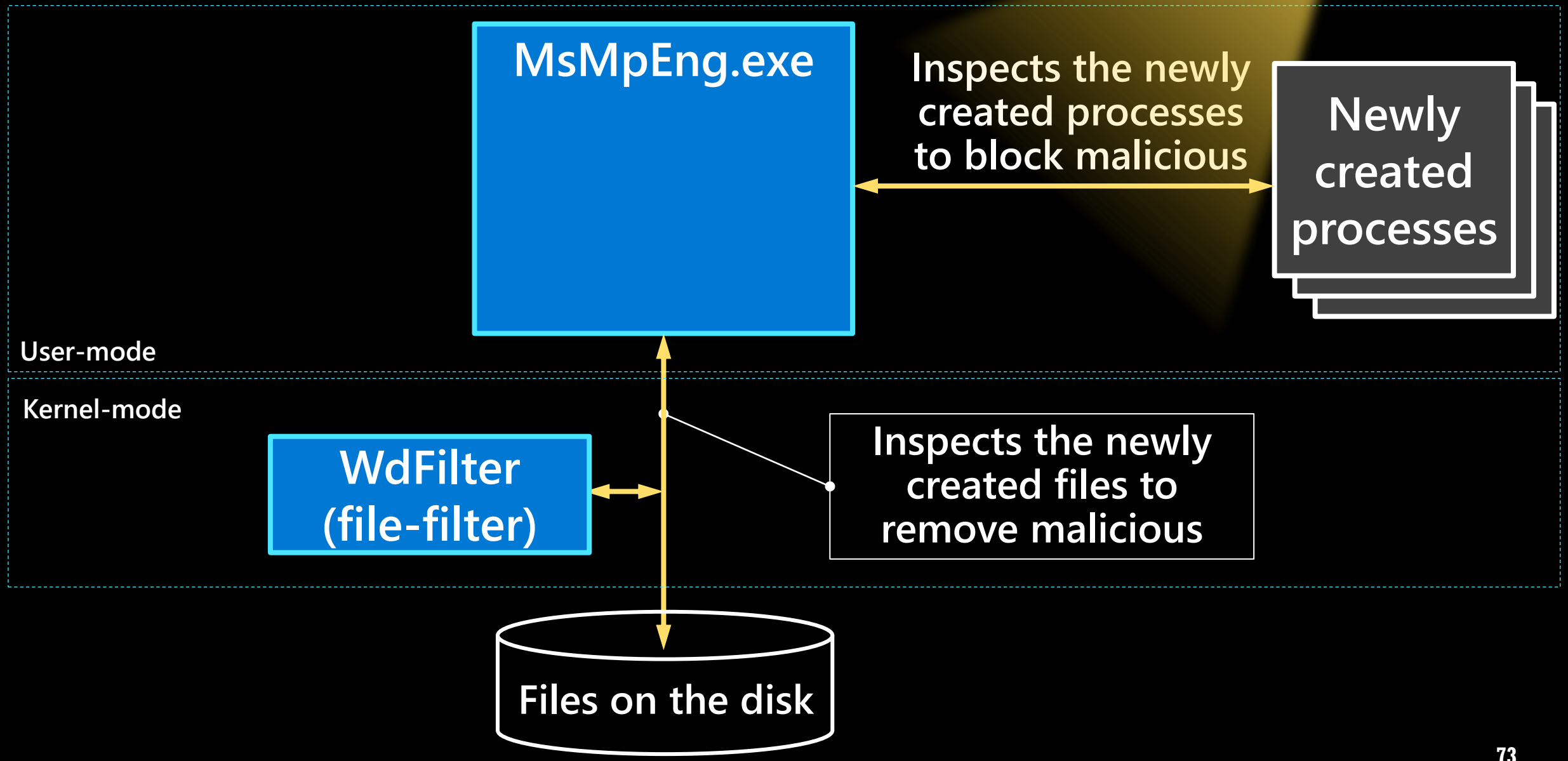
MICROSOFT DEFENDER: INTERNALS



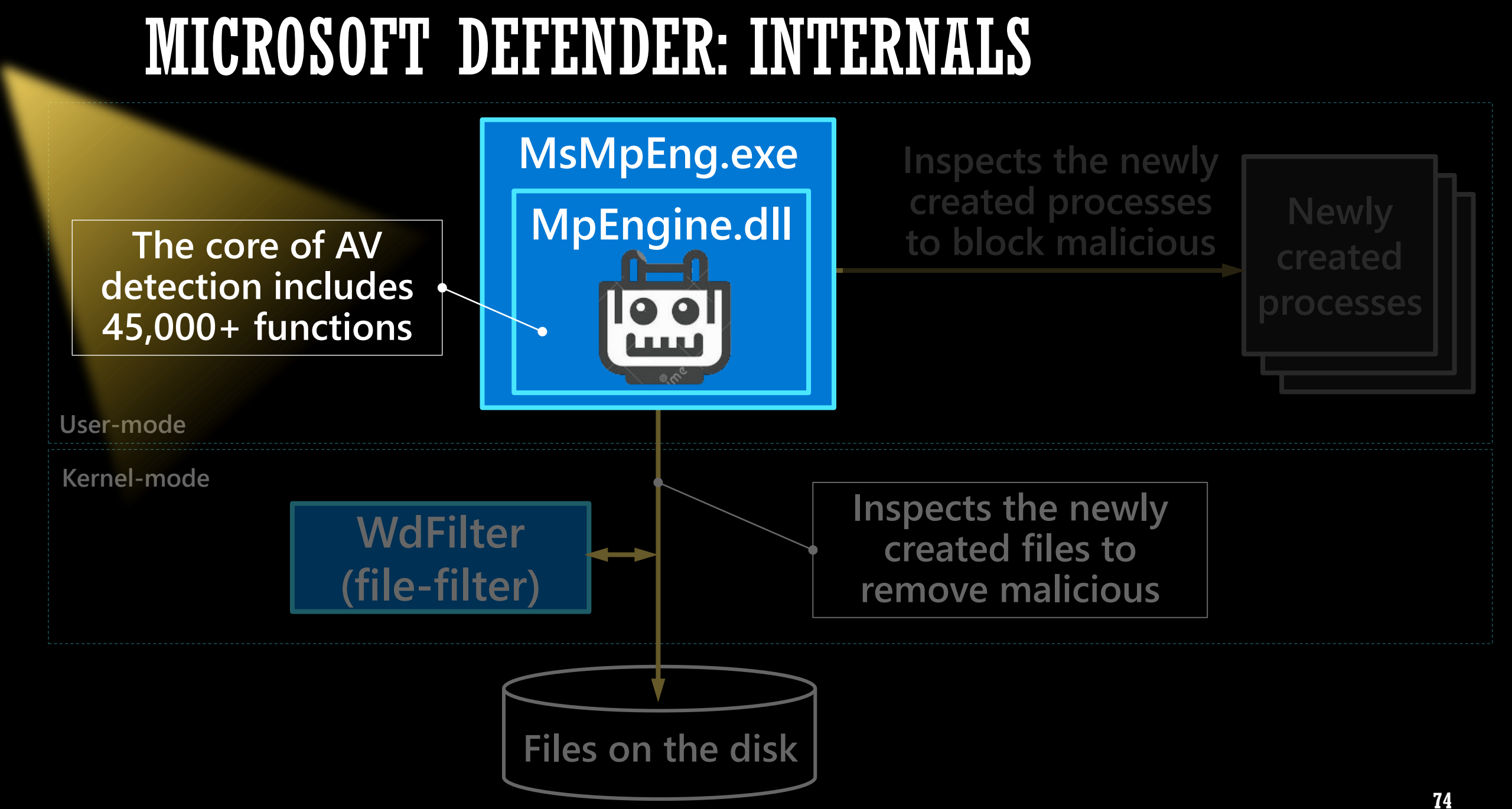
MICROSOFT DEFENDER: INTERNALS



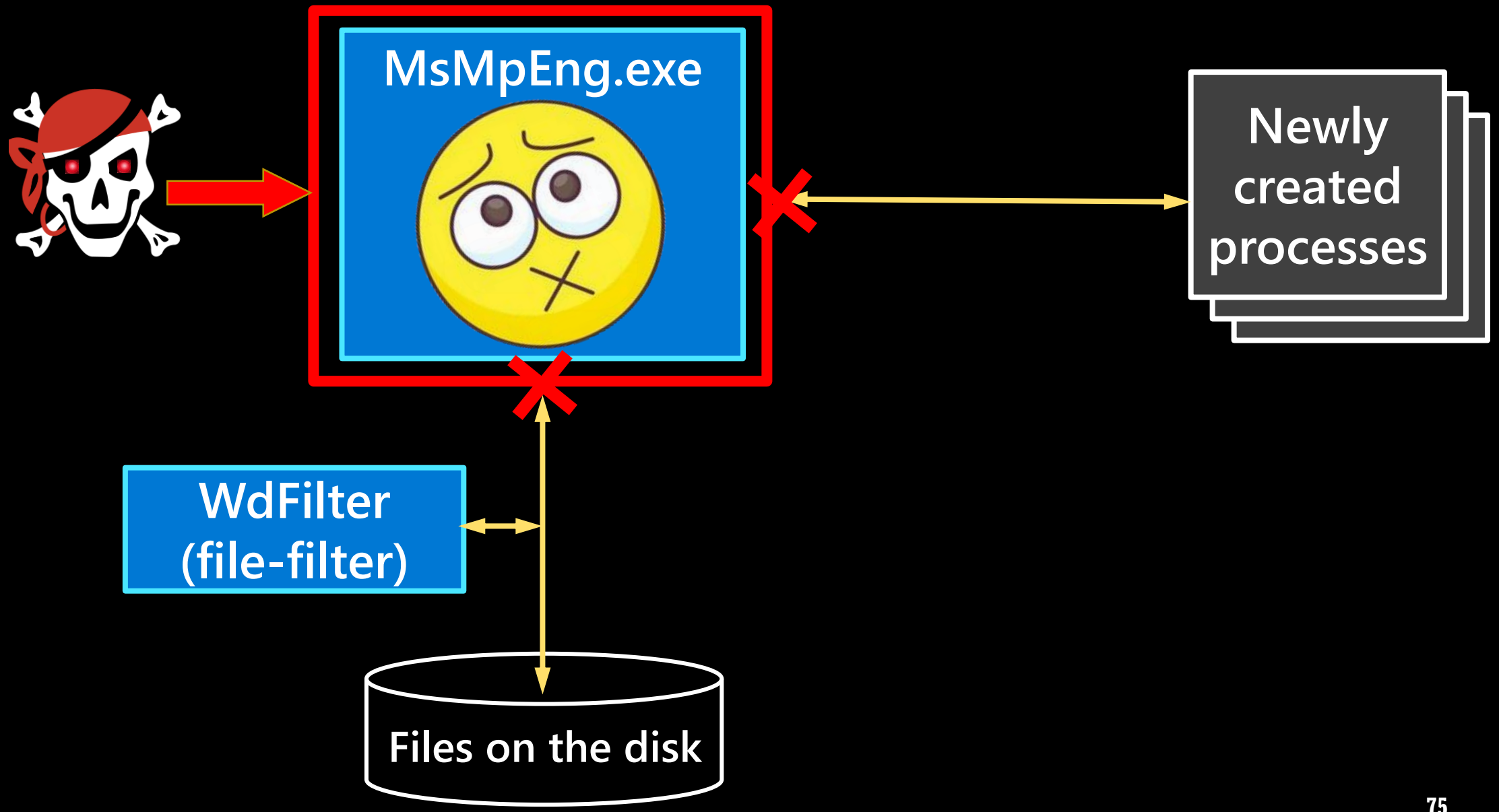
MICROSOFT DEFENDER: INTERNALS



MICROSOFT DEFENDER: INTERNALS

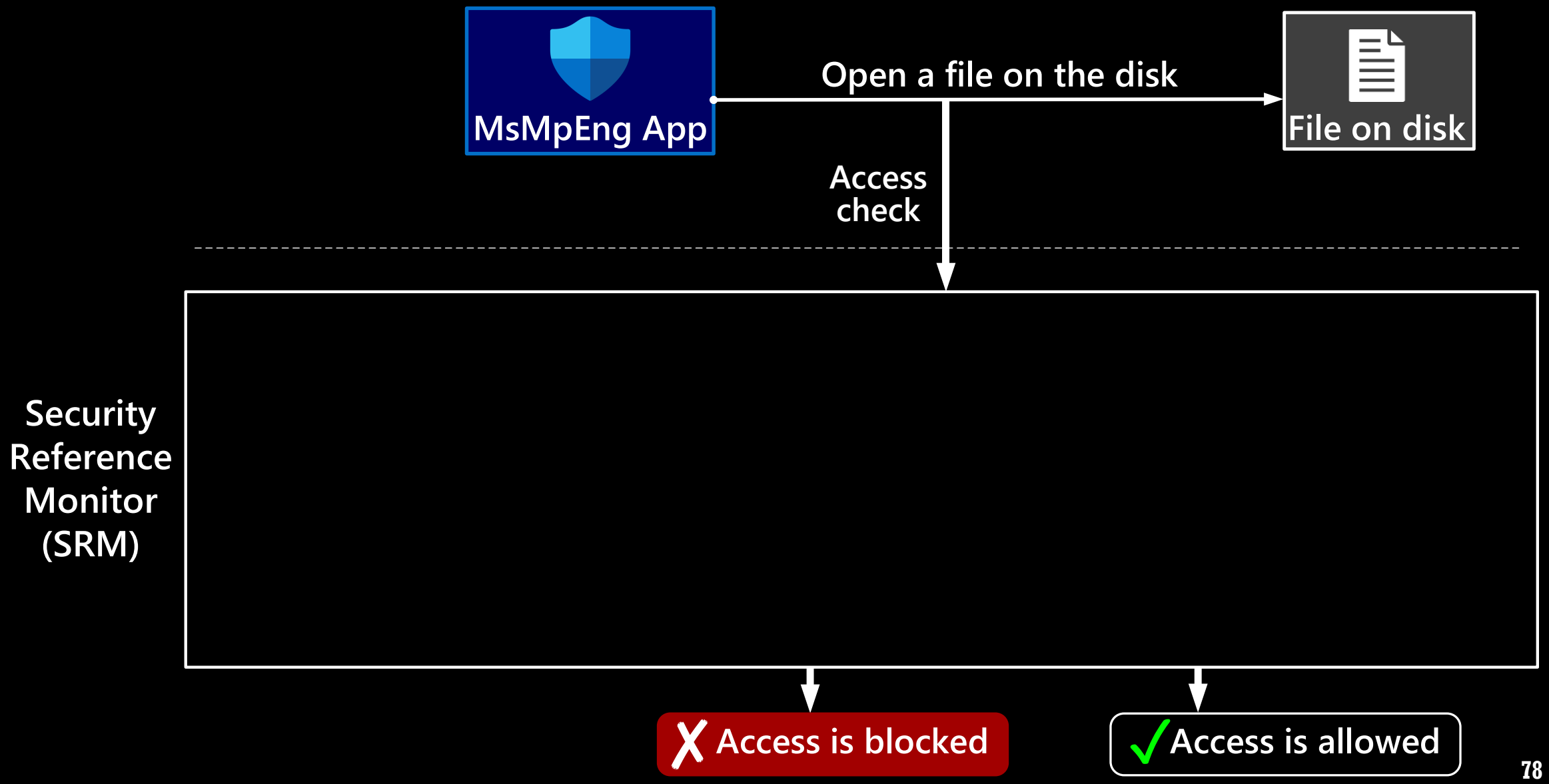


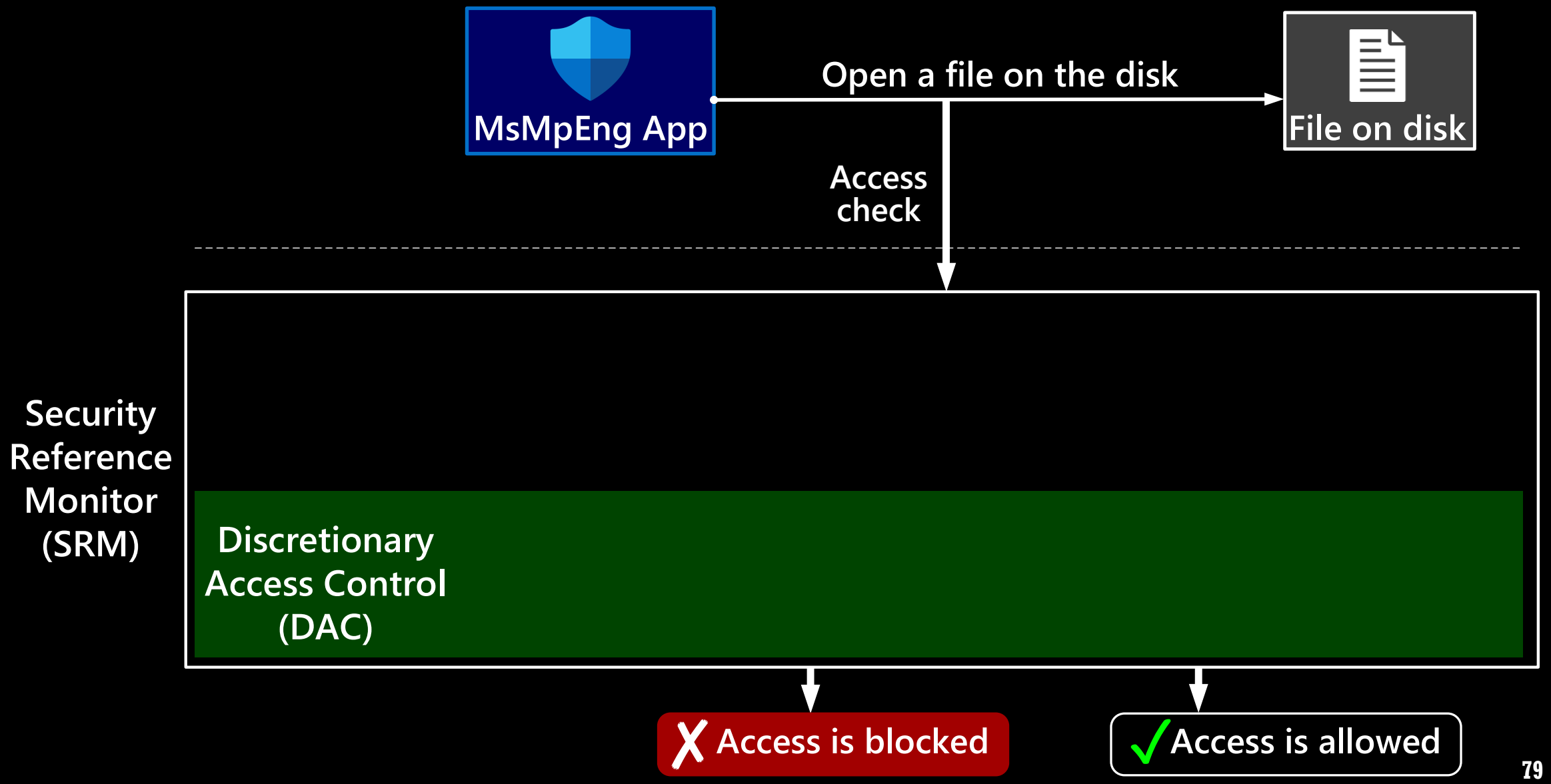
MICROSOFT DEFENDER: INTERNALS

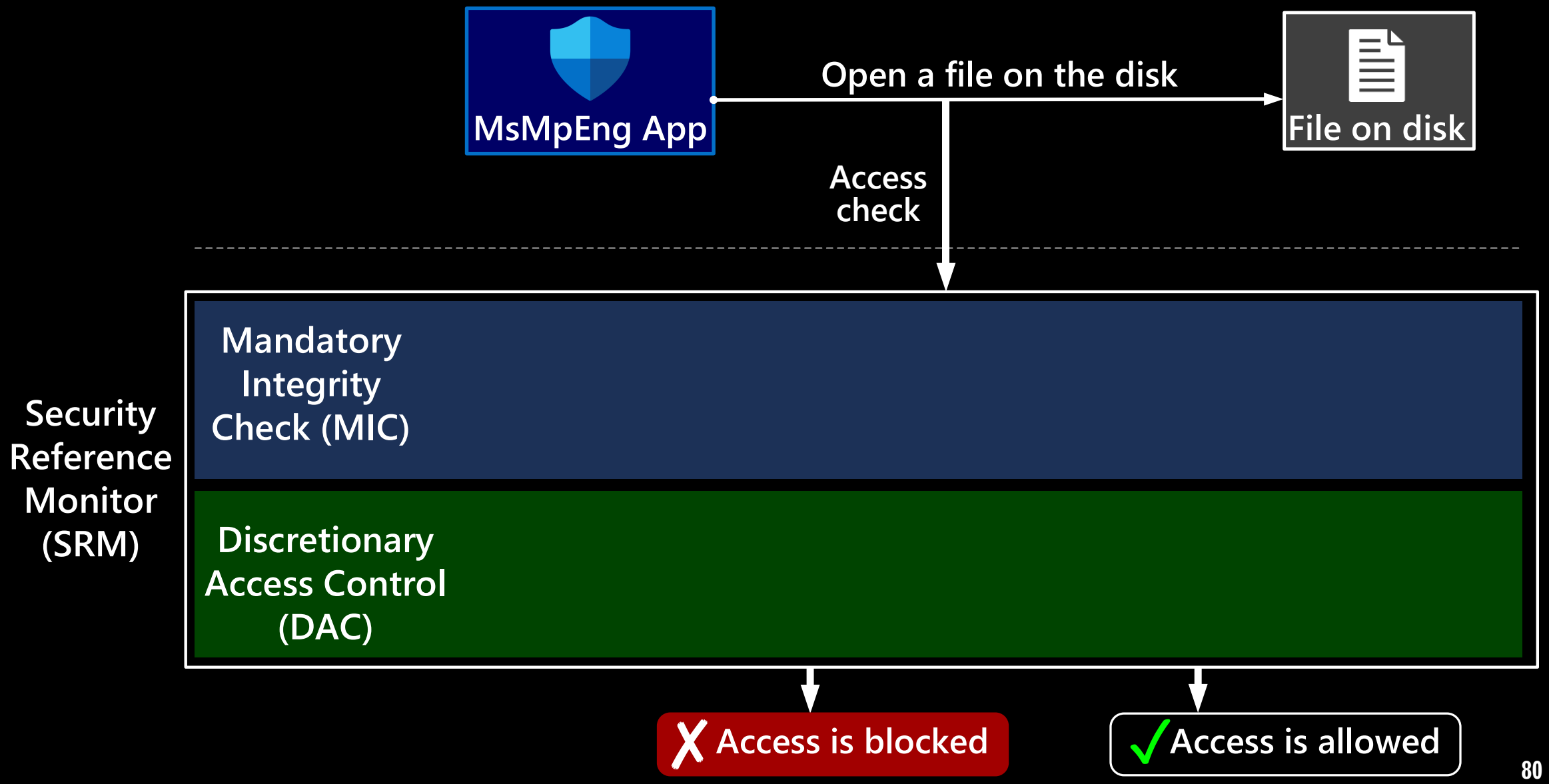


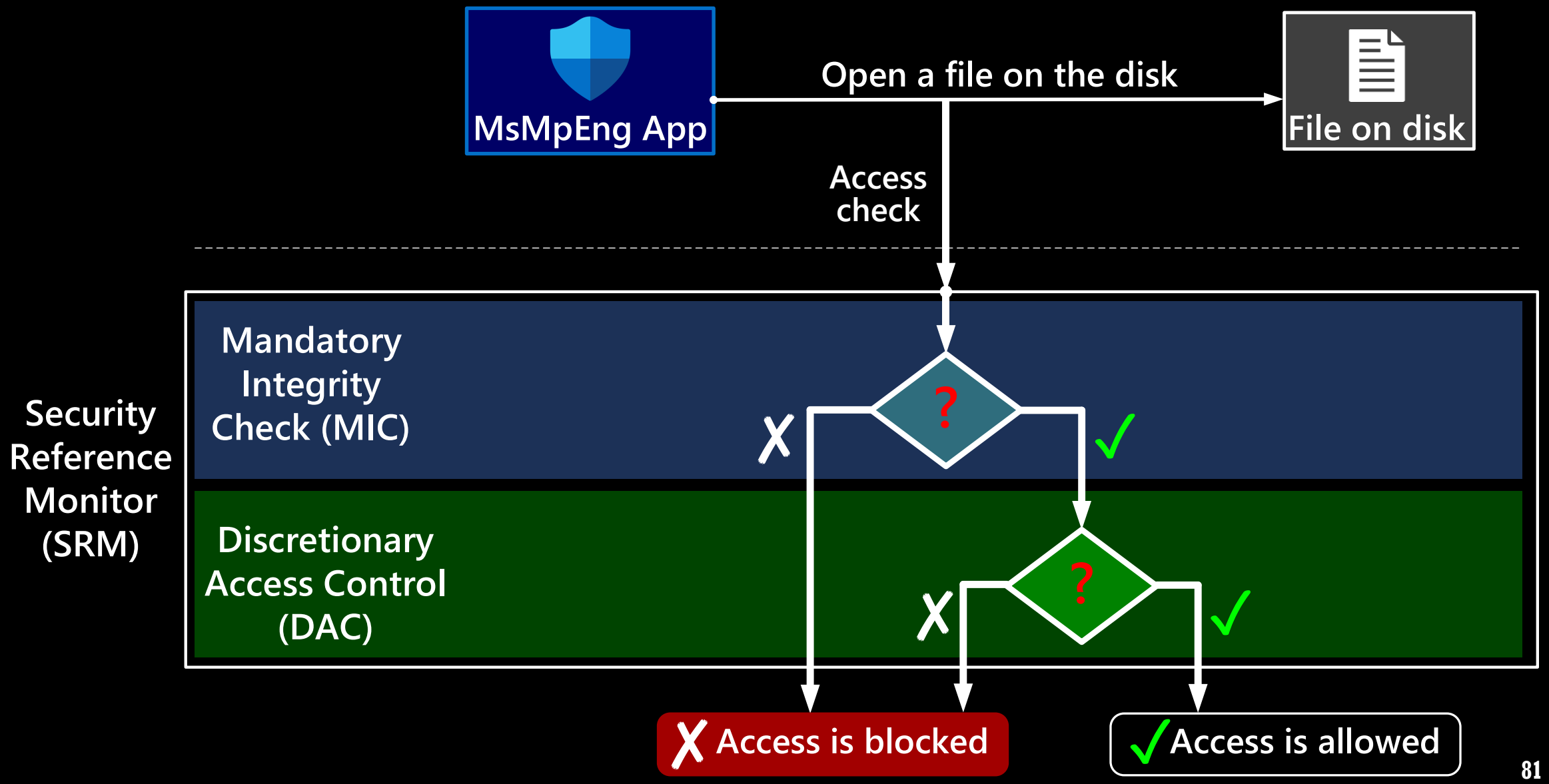
MANDATORY INTEGRITY CONTROL: INTRO

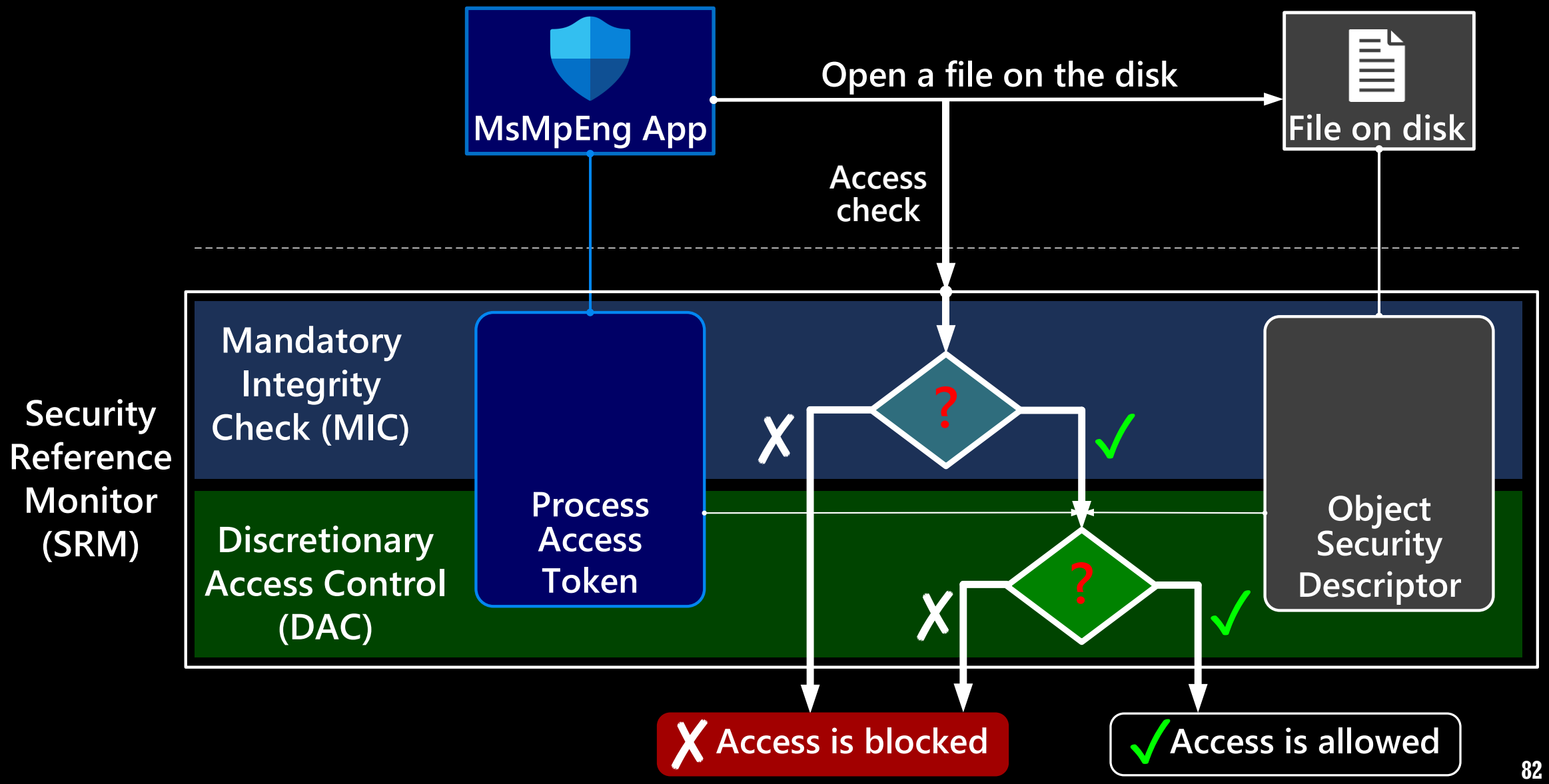

MsMpEng App
Open a file on the disk
File on disk

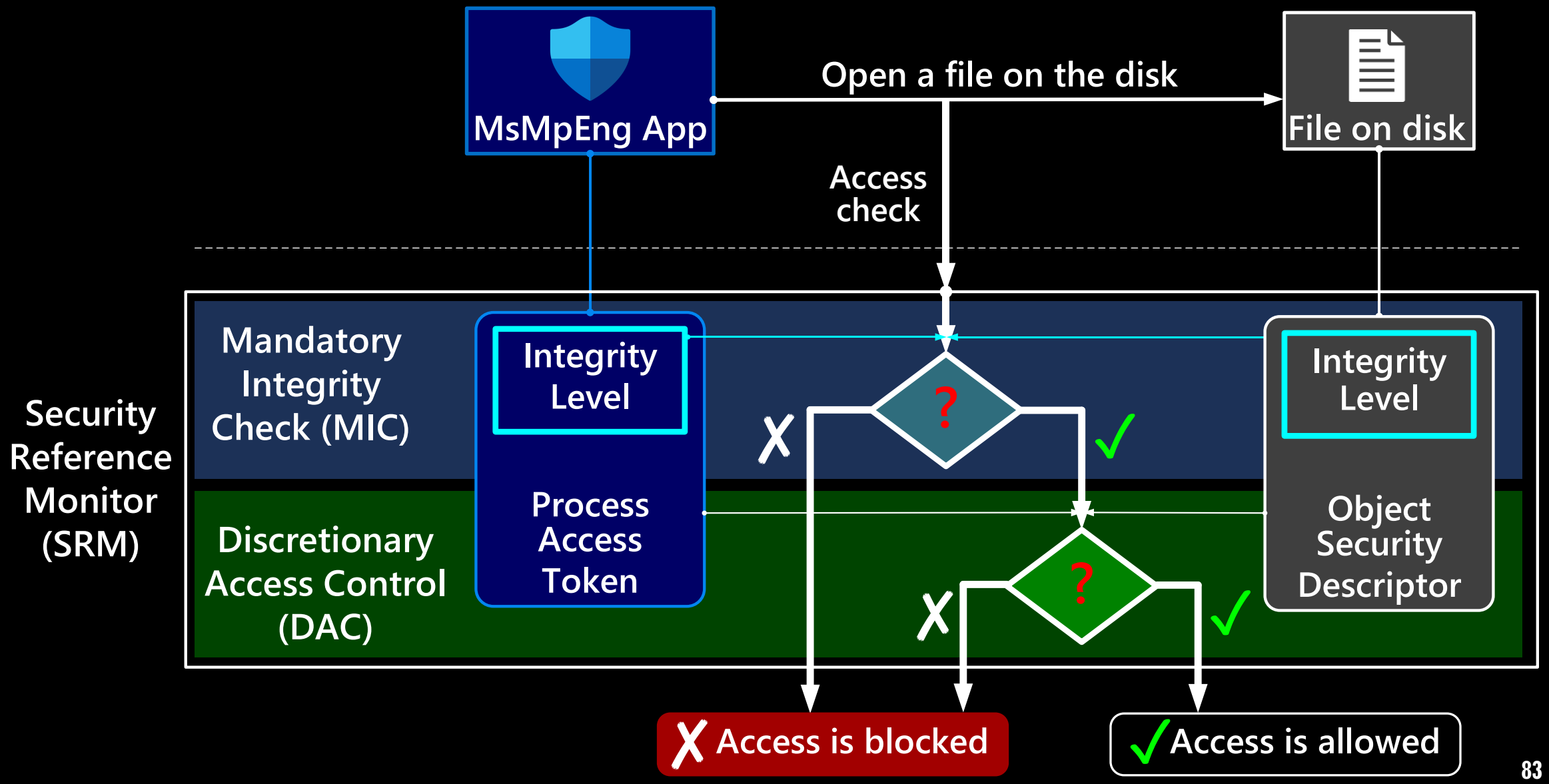

MsMpEng App
Open a file on the disk
File on disk
Access check
Security Reference Monitor (SRM)
Access is blocked
Access is allowed


MsMpEng App
Open a file on the disk
File on disk
Access check
Security Reference Monitor (SRM)
Discretionary Access Control (DAC)
Access is blocked
Access is allowed

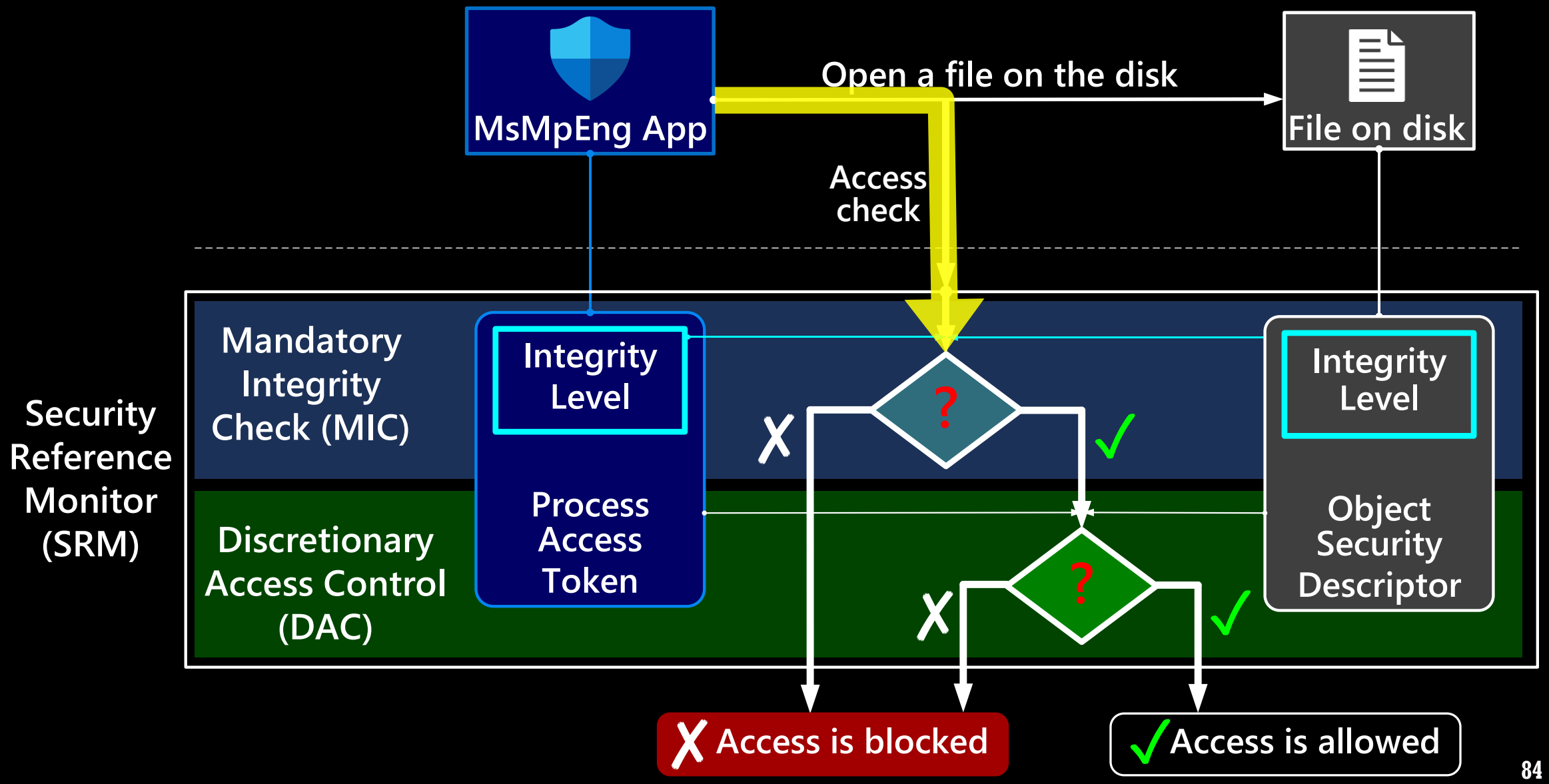

MsMpEng App
Open a file on the disk
File on disk
Access check
Security Reference Monitor (SRM)
Mandatory Integrity Check (MIC)
Discretionary Access Control (DAC)
Access is blocked
Access is allowed


MsMpEng App
Open a file on the disk
File on disk
Access check
Security Reference Monitor (SRM)
Mandatory Integrity Check (MIC)
Discretionary Access Control (DAC)
Access is blocked
Access is allowed

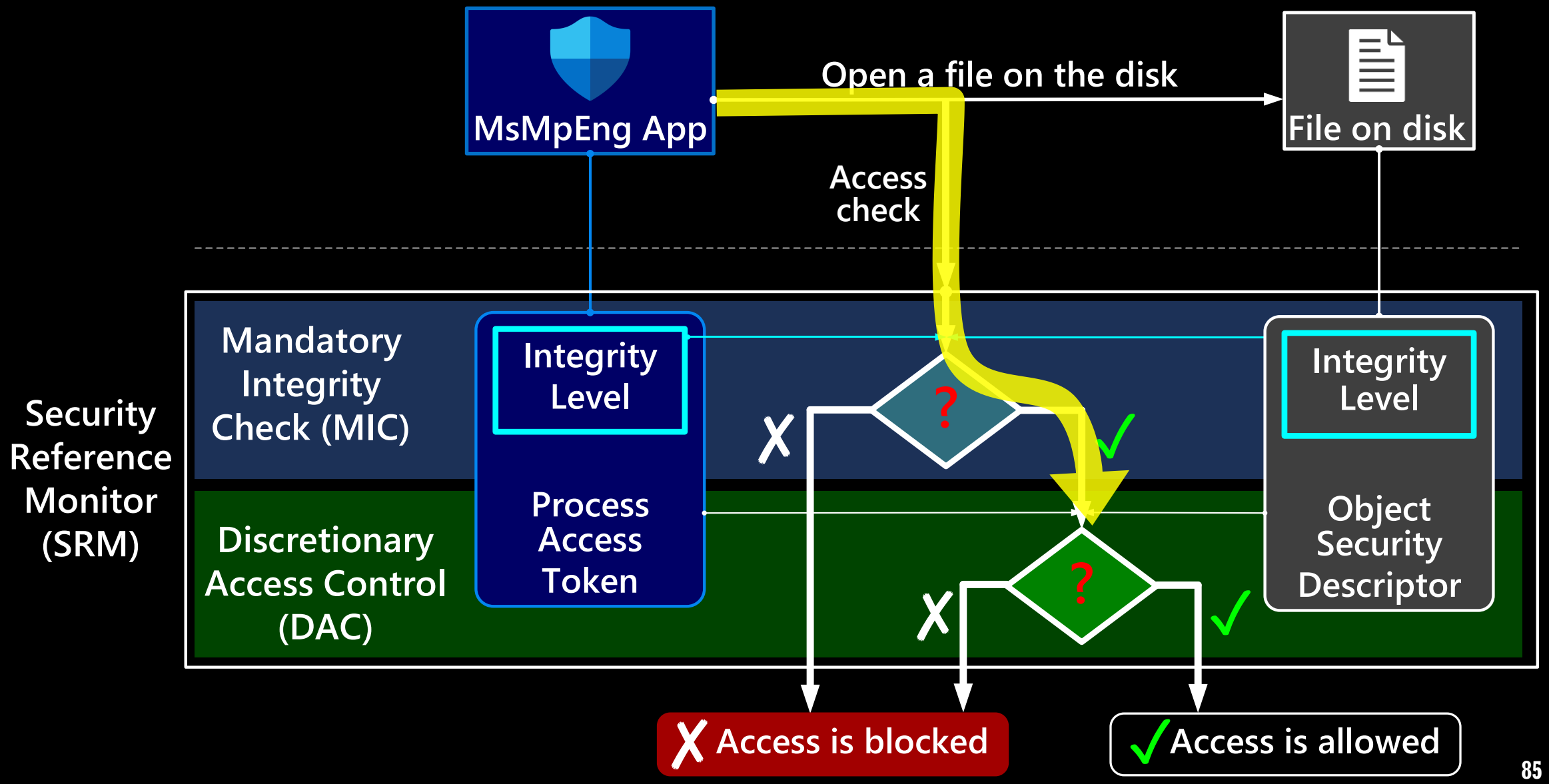

MsMpEng App
Open a file on the disk
File on disk
Access check
Security Reference Monitor (SRM)
Mandatory Integrity Check (MIC)
Discretionary Access Control (DAC)
Process Access Token
Object Security Descriptor
Access is blocked
Access is allowed


MsMpEng App
Open a file on the disk
File on disk
Access check
Security Reference Monitor (SRM)
Mandatory Integrity Check (MIC)
Integrity Level
Process Access Token
Integrity Level
Object Security Descriptor
Discretionary Access Control (DAC)
?
?
Access is blocked
Access is allowed

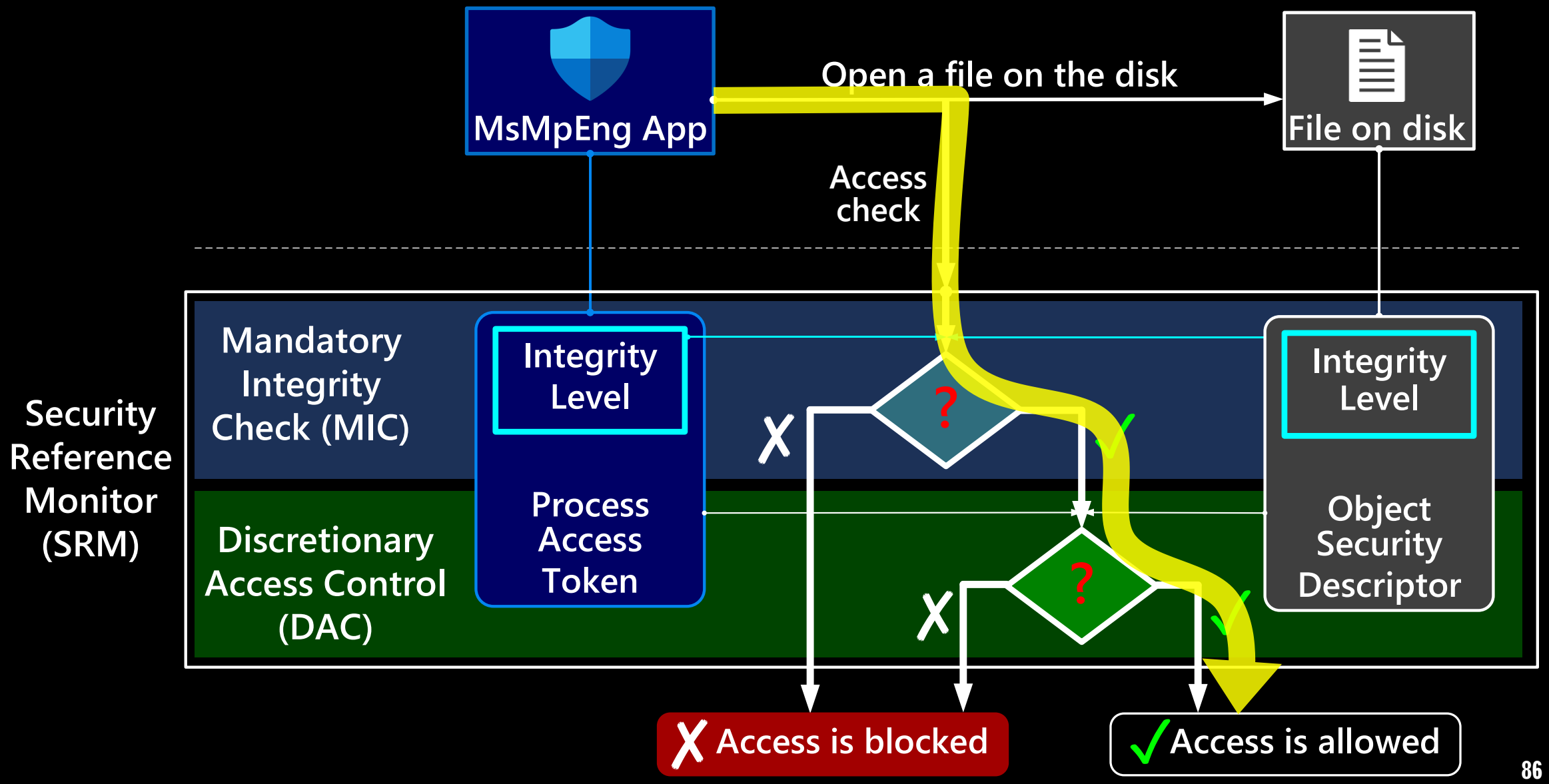
DEFENDER TRIES TO OPEN A FILE



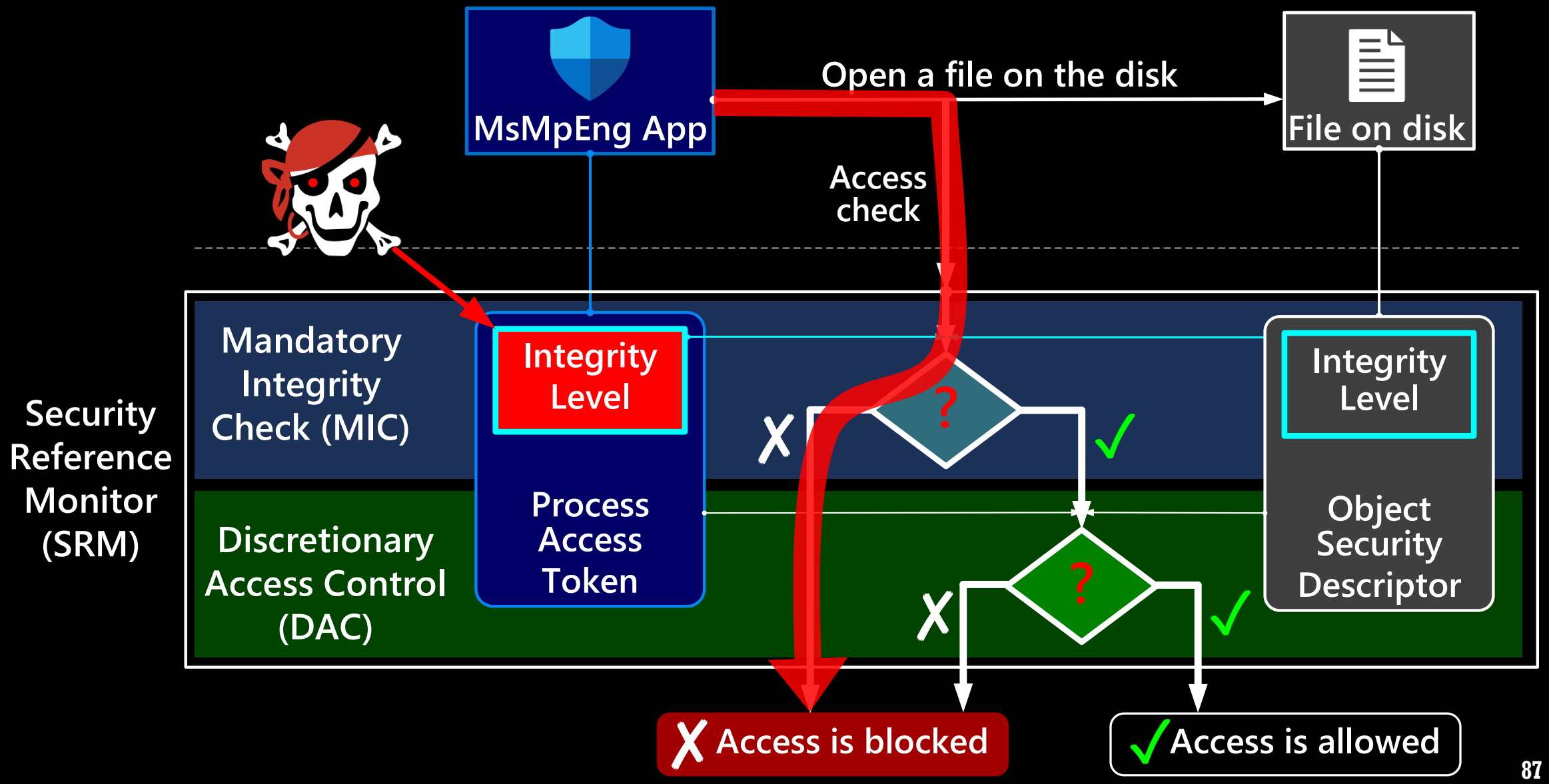
DEFENDER TRIES TO OPEN A FILE



DEFENDER TRIES TO OPEN A FILE



DEFENDER FAILS TO OPEN A FILE



MIC: INTEGRITY LEVELS

MIC: Integrity Levels

Integrity Levels	Examples
Low	
Untrusted	
Medium	
High	
System	

MIC: Integrity Levels

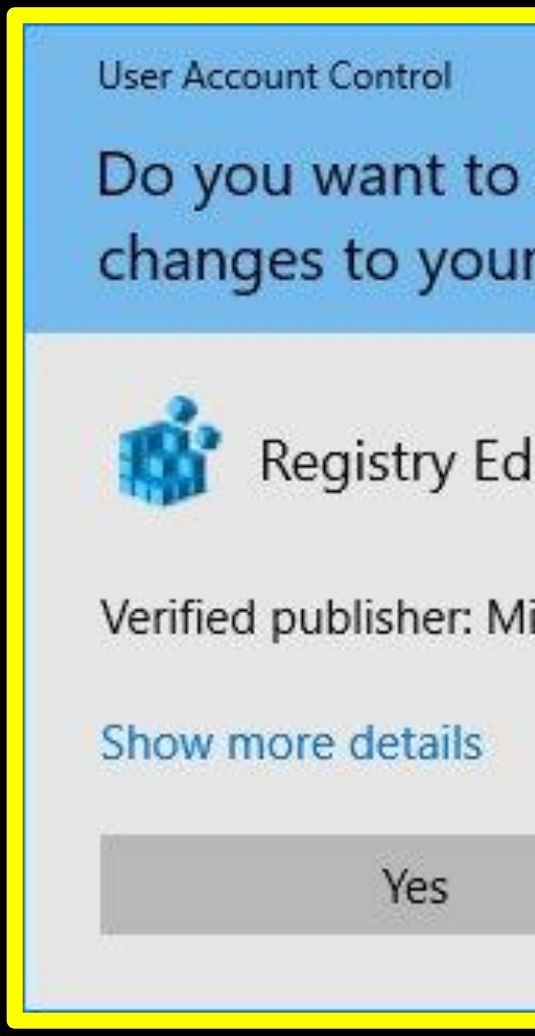
Integrity Levels	Examples
Low	
Untrusted	
Medium	
High	
System	

MIC: Integrity Levels

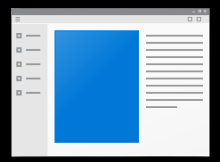
Integrity Levels	Examples
Low	
Untrusted	
Medium	
High	
System	

MIC: Integrity Levels

Integrity Levels	Examples
Low	
Untrusted	
Medium	
High	
System	



MIC: Integrity Levels

Integrity Levels	Examples
Low	  
Untrusted	
Medium	  
High	
System	 

MIC: Integrity Levels of files and folders

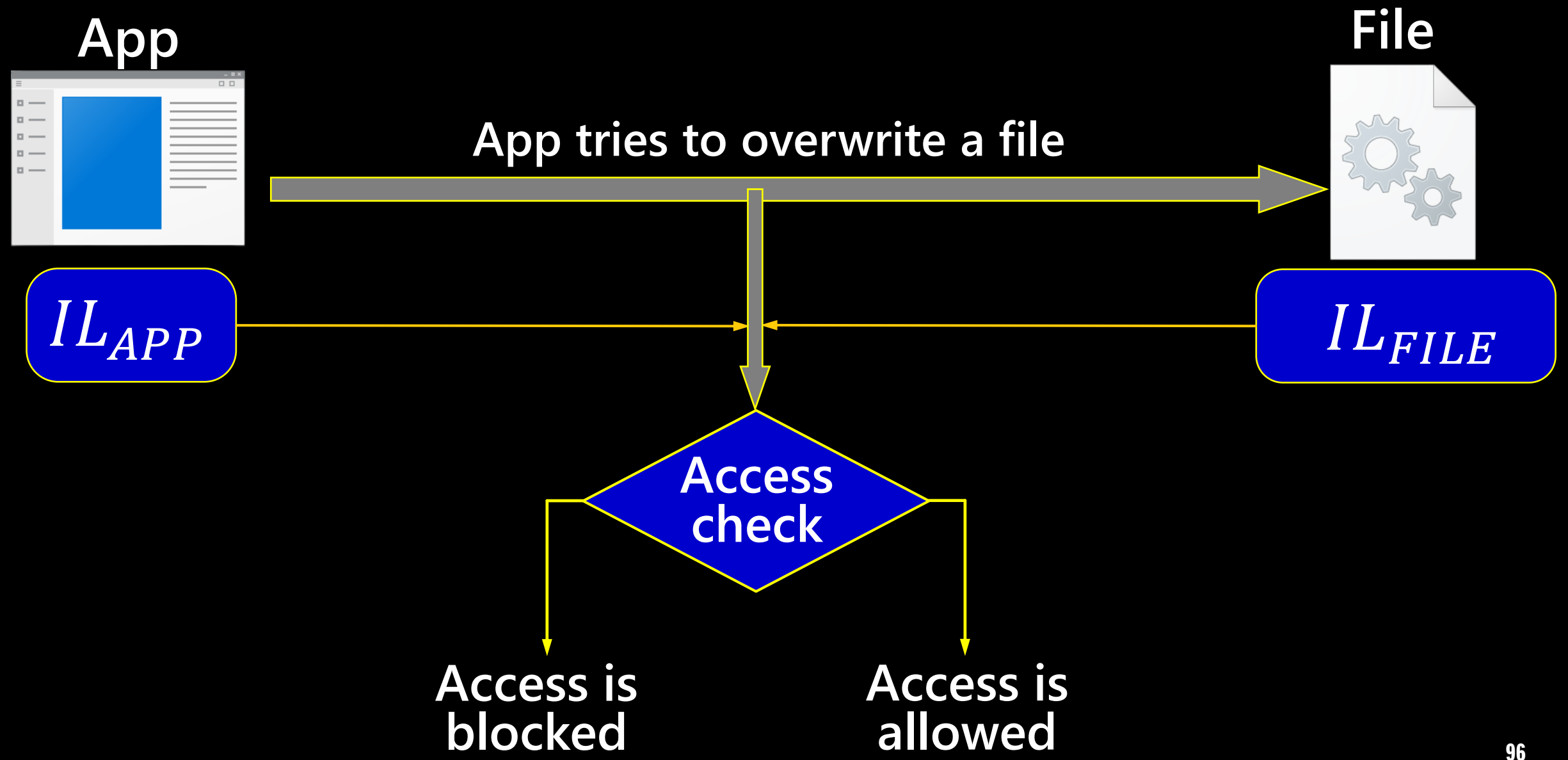
Process	Integrity
explorer.exe	Medium
SecurityHealthSystray.exe	Medium
msedge.exe	Medium
msedge.exe	Medium
msedge.exe	Low
msedge.exe	Medium
msedge.exe	Untrusted
procexp.exe	High
procexp64.exe	High
Notepad.exe	Medium

Folder	Integrity level
C:\	High
$Recycle.Bin	Low
$WinREAgent	Medium
adfsl2022	Medium
7-Zip	Medium
mimikatz	Medium
mimikatz.zip	Medium
mimikatz_extract_and_check.bat	Medium
Procmon.exe	Medium
Documents and Settings	Medium

* MicEnum – www.elevenpaths.com/innovation-labs/technologies/micenum

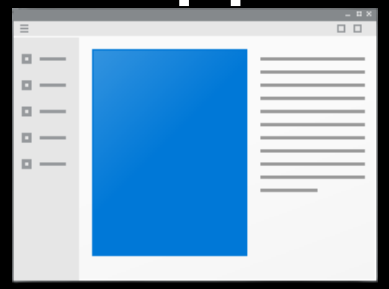
MIC is based on Bell-LaPadula Model (BLP)

MIC is based on Bell-LaPadula Model (BLP)



MIC is based on Bell-LaPadula Model (BLP)

App



File

App tries to overwrite a file

IL_{APP}

IL_{FILE}

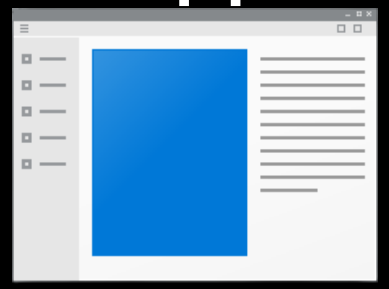
$$if\ (IL_{APP} \geq IL_{FILE}) \rightarrow access\ is\ allowed$$
$$else\ \rightarrow access\ is\ blocked$$

Access is blocked

Access is allowed

MIC is based on Bell-LaPadula Model (BLP)

App



File

App tries to overwrite a file

$Low\ IL$

IL_{FILE}

$$if\ (IL_{APP} \geq IL_{FILE}) \rightarrow access\ is\ allowed$$
$$else\ \rightarrow access\ is\ blocked$$

Apps with Low IL cannot get write access to the most OS objects

HOW INTEGRITY LEVEL ARE STORED IN WINDOWS?

MIC INTERNALS: TOKEN STRUCTURE

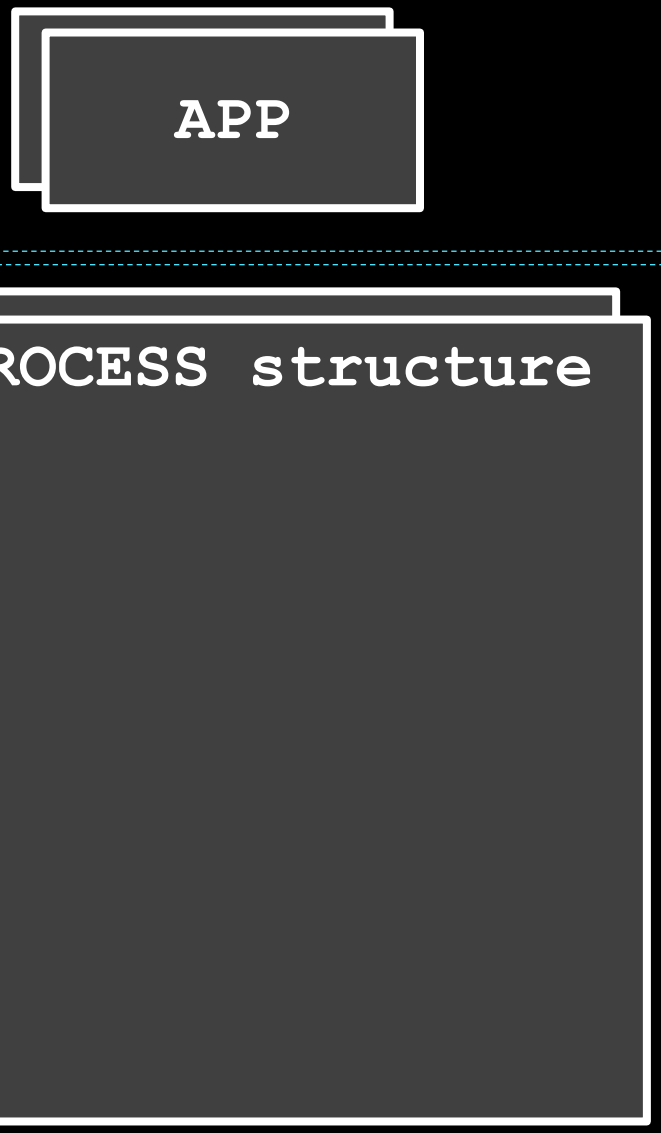
APP

User-mode

Kernel-mode

EPROCESS structure

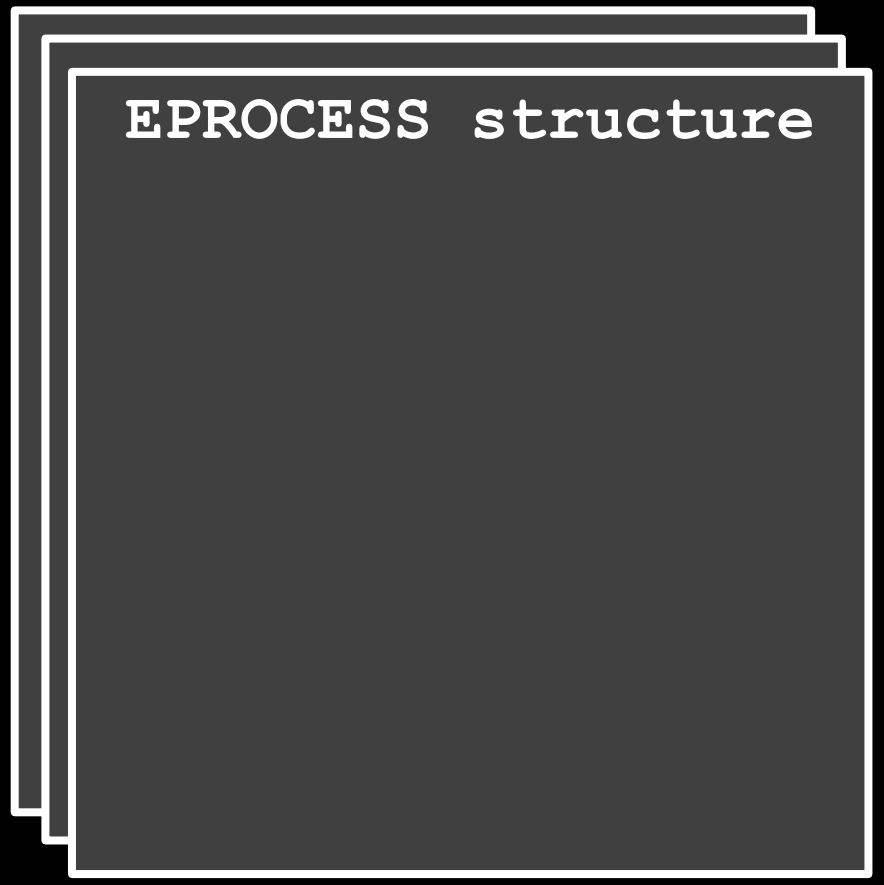
MIC INTERNALS: TOKEN STRUCTURE



MIC INTERNALS: TOKEN STRUCTURE

User-mode

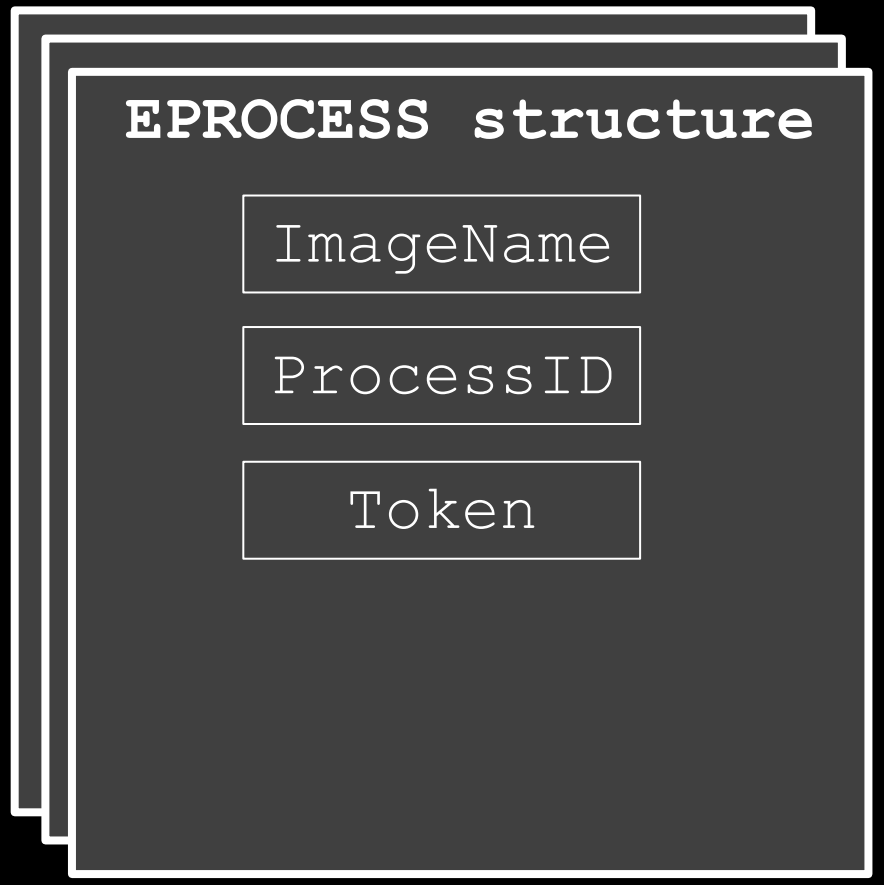
Kernel-mode



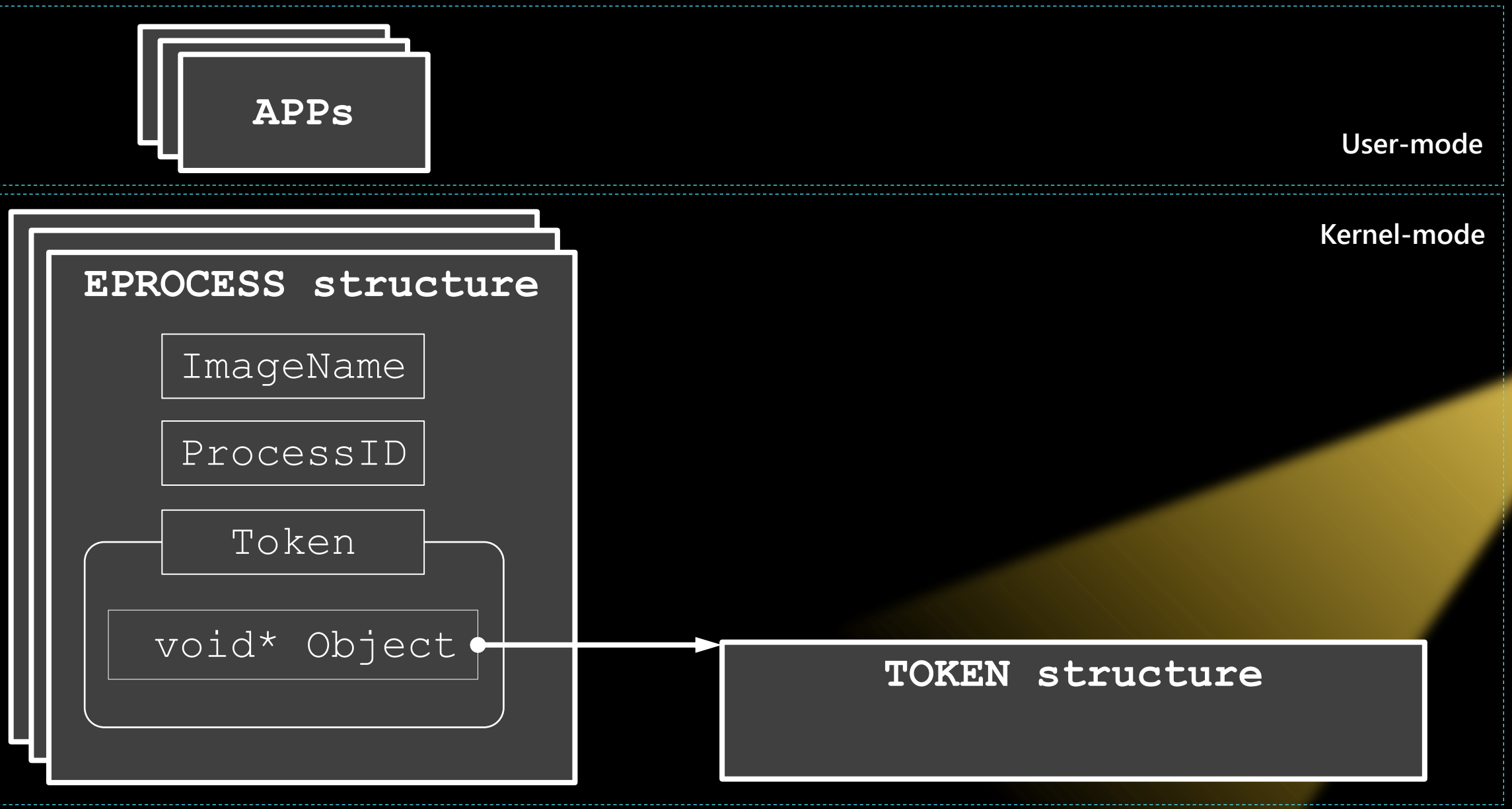
MIC INTERNALS: TOKEN STRUCTURE

User-mode

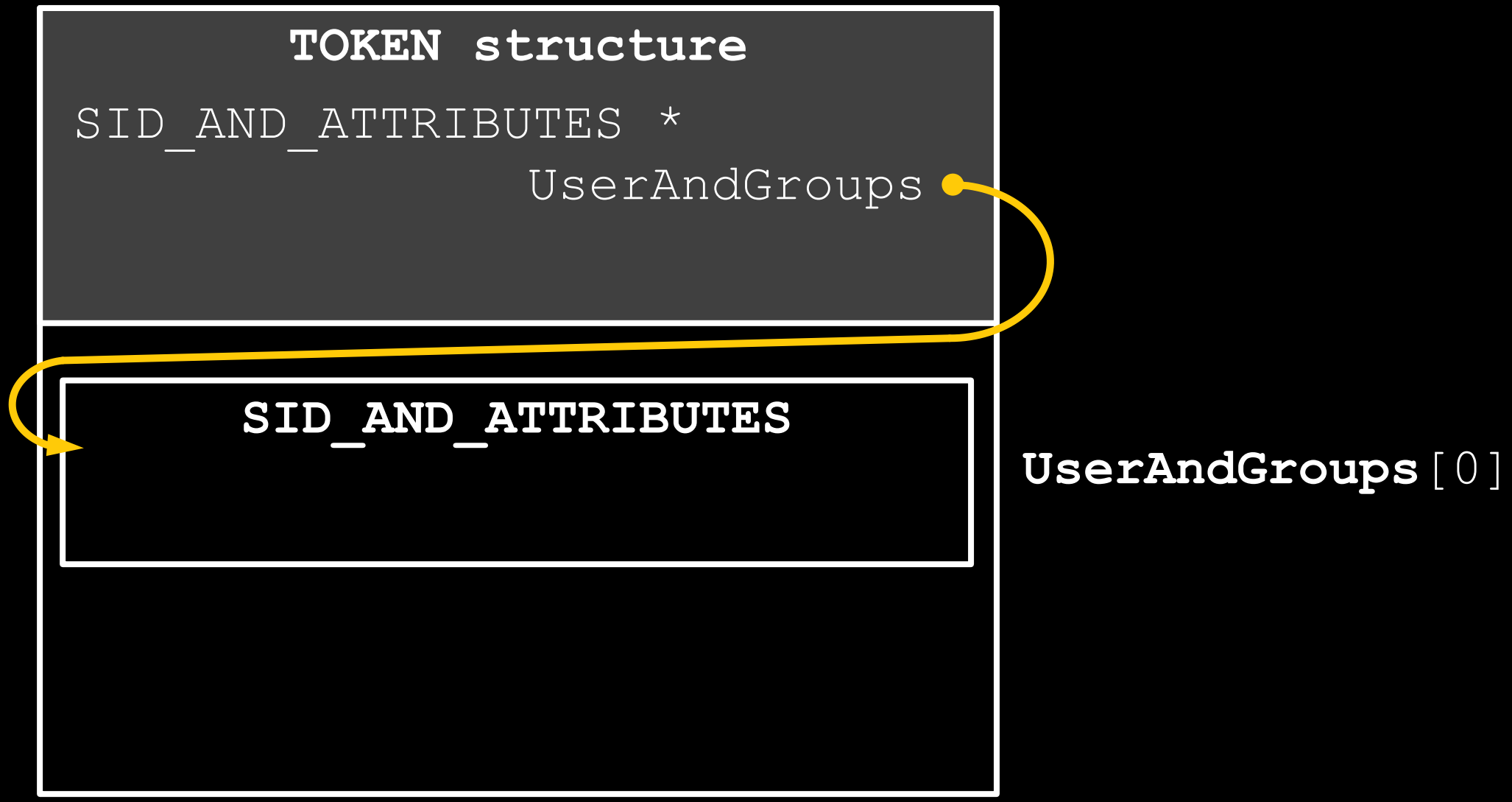
Kernel-mode



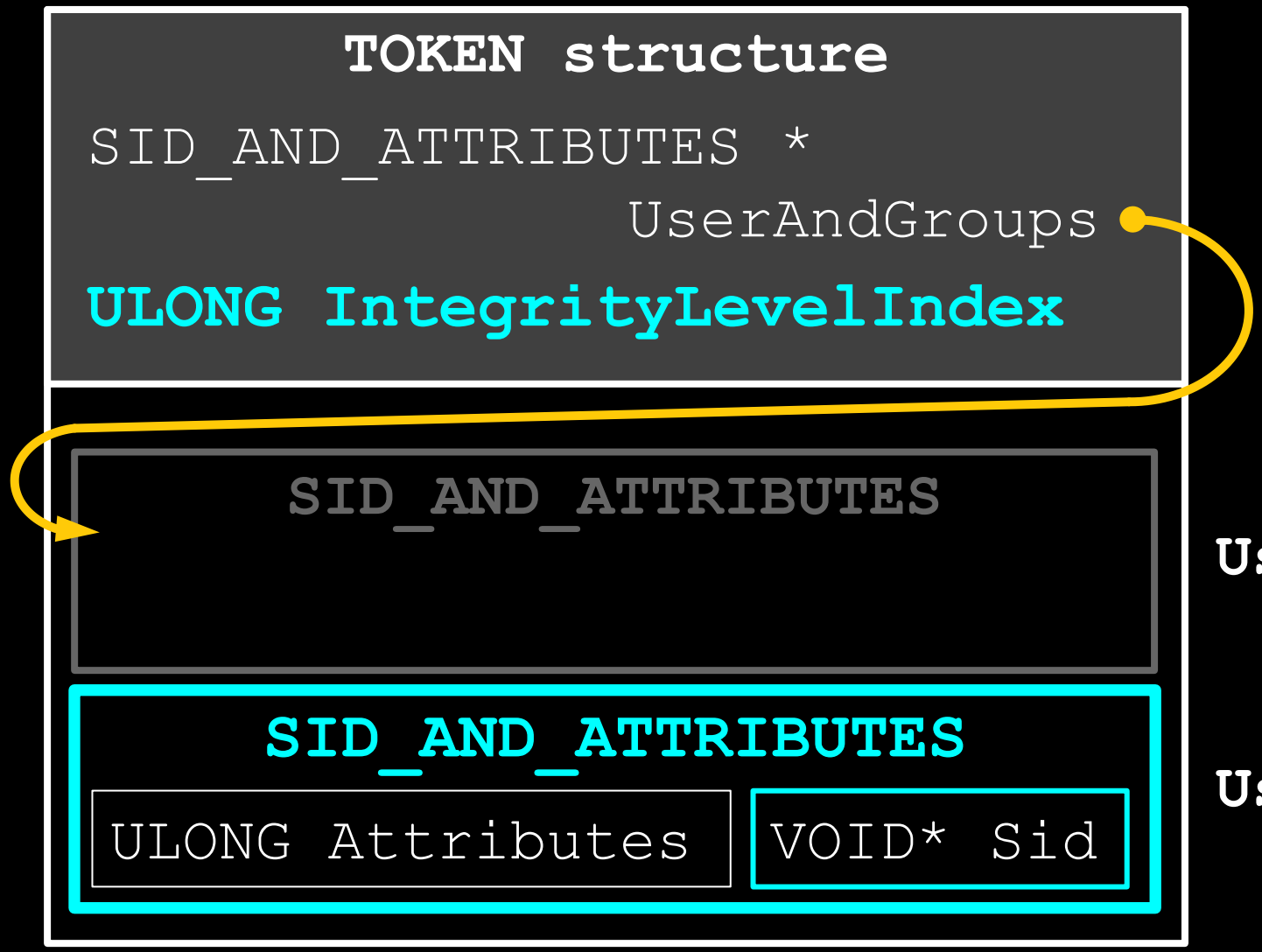
MIC INTERNALS: TOKEN STRUCTURE



MIC INTERNALS: TOKEN AND INDEX



MIC INTERNALS: TOKEN AND INDEX



UserAndGroups[0]

UserAndGroups
[**IntegrityLevelIndex**]

MIC INTERNALS: TOKEN AND INDEX

TOKEN structure

SID_AND_ATTRIBUTES *
UserAndGroups

ULONG IntegrityLevelIndex

SID_AND_ATTRIBUTES

SID_AND_ATTRIBUTES

ULONG Attributes | VOID* Sid

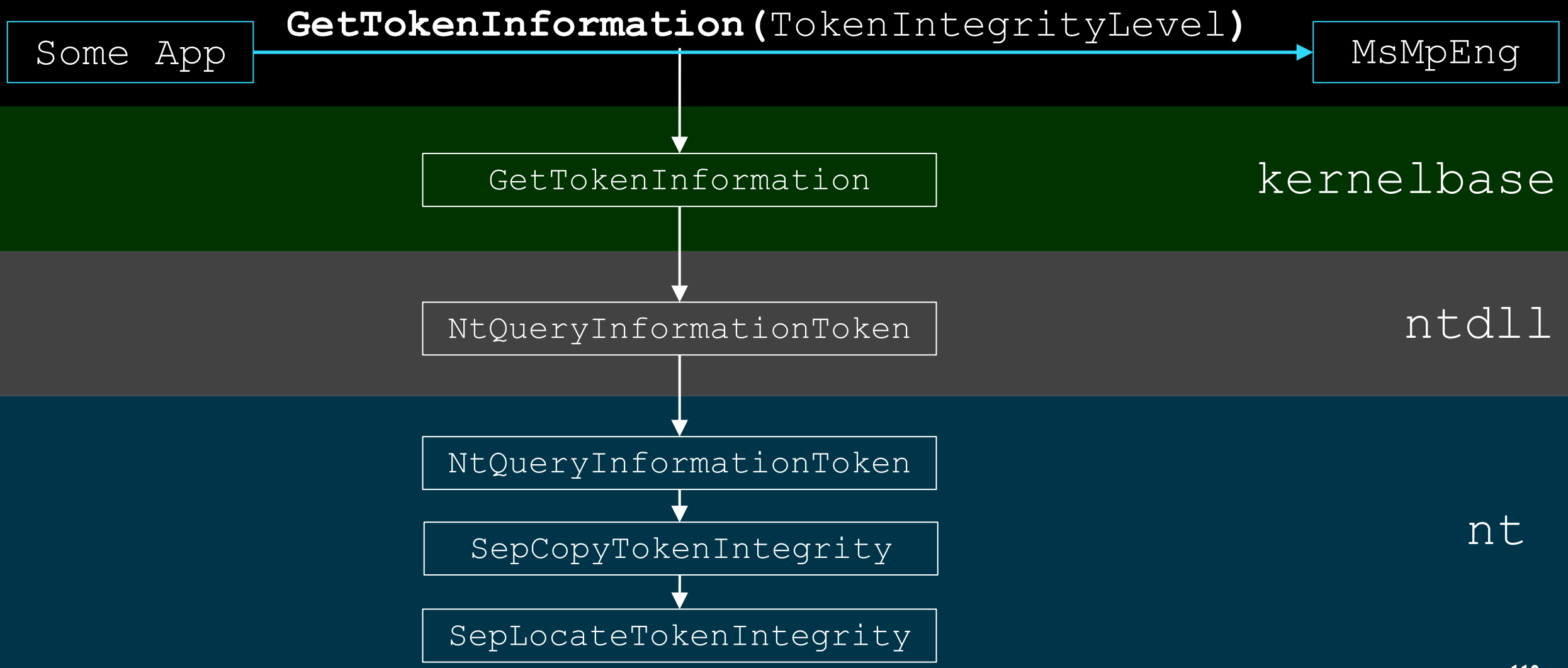
Integrity level SID

SID value	Integrity Level
S-1-16-8192	Medium
S-1-16-12288	High
S-1-16-16384	System

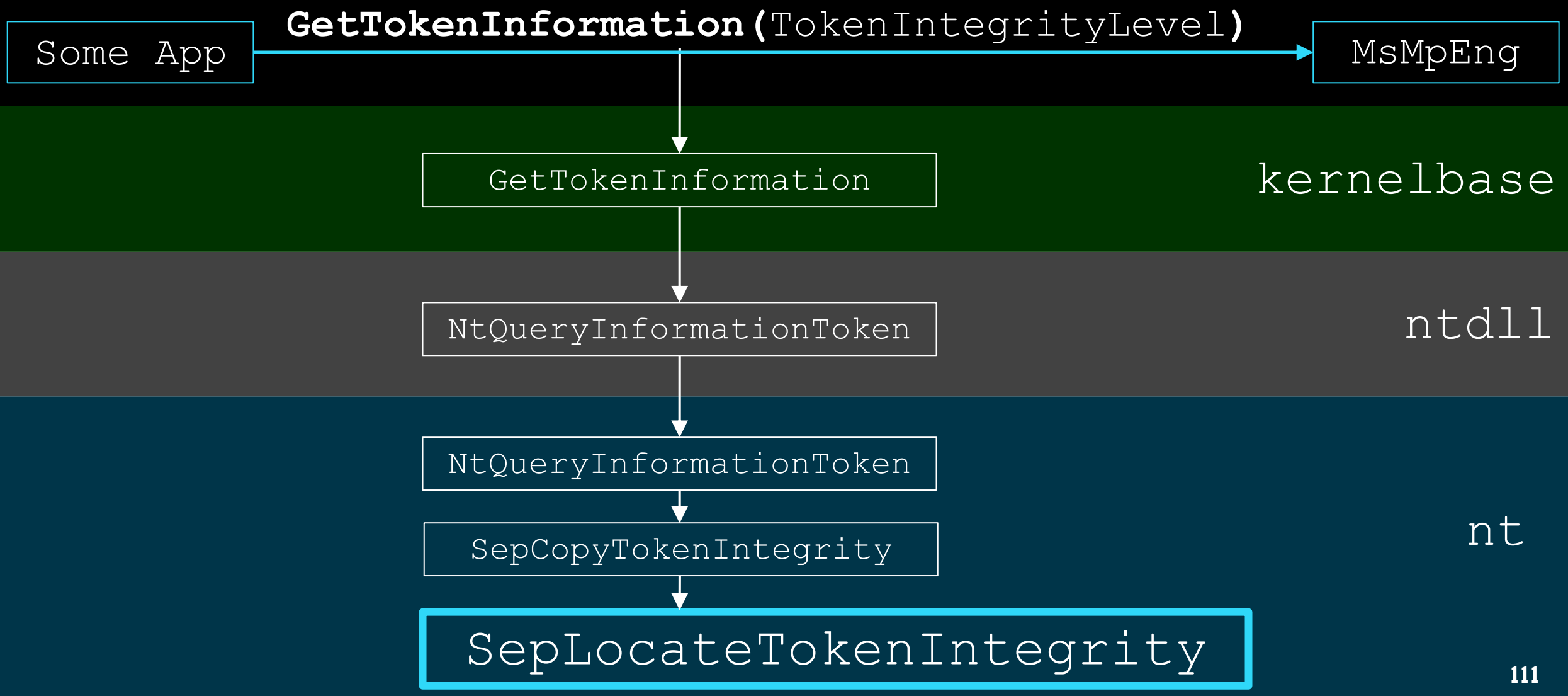
How Windows OS gets Integrity Levels?

MIC: Get Integrity Level

MIC: Get Integrity Level



MIC: Get Integrity Level



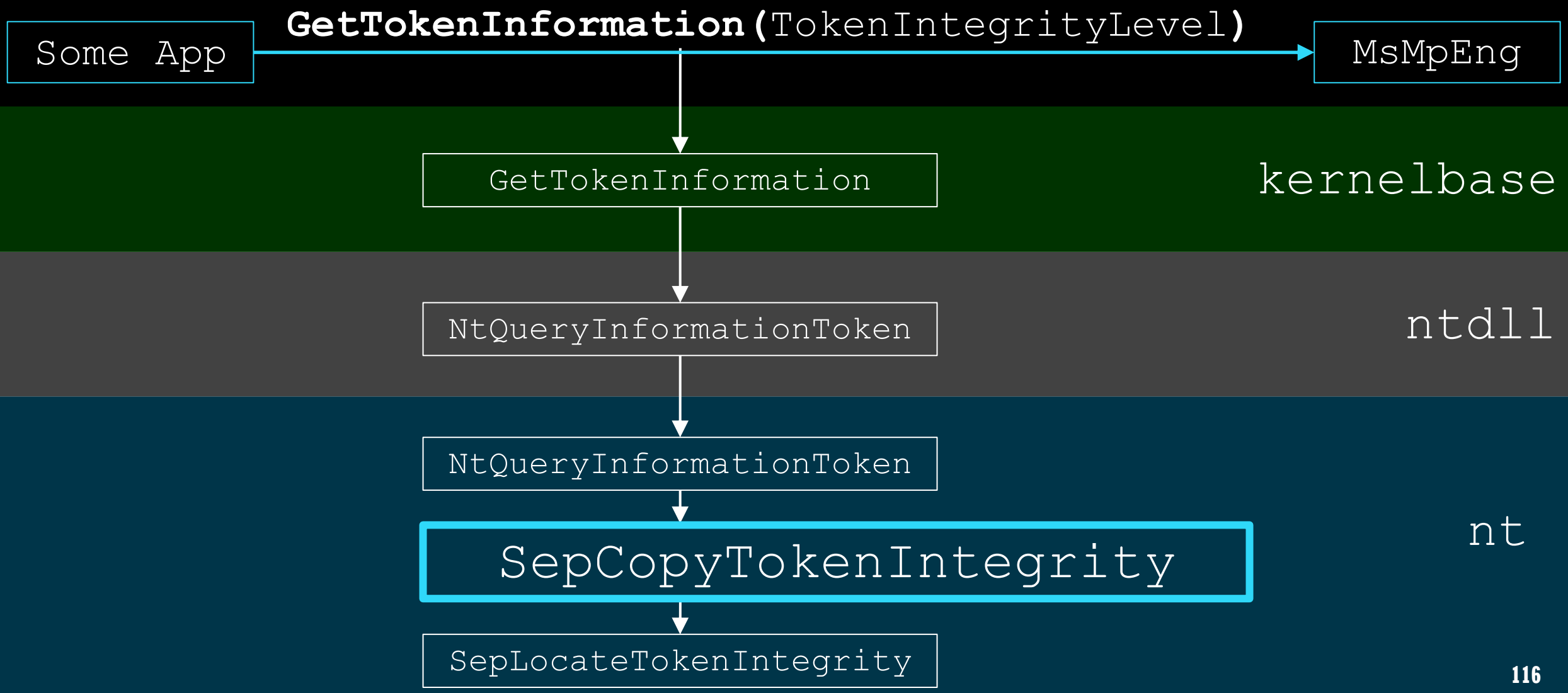
```
PSID_AND_ATTRIBUTES SepLocateTokenIntegrity(IN PTOKEN Token)
{
    PSID_AND_ATTRIBUTES TokenIntegrity = 0;
    ULONG64 index = Token->IntegrityLevelIndex;
    if (index == -1)
    {
        TokenIntegrity = 0;
    }
    else
    {
        TokenIntegrity = Token->UserAndGroups[index];
    }
    return TokenIntegrity;
}
```

```
PSID_AND_ATTRIBUTES SepLocateTokenIntegrity(IN PTOKEN Token)
{
    PSID_AND_ATTRIBUTES TokenIntegrity = 0;
    ULONG64 index = Token->IntegrityLevelIndex;
    if (index == -1)
    {
        TokenIntegrity = 0;
    }
    else
    {
        TokenIntegrity = Token->UserAndGroups[index];
    }
    return TokenIntegrity;
}
```

```
PSID_AND_ATTRIBUTES SepLocateTokenIntegrity(IN PTOKEN Token)
{
    PSID_AND_ATTRIBUTES TokenIntegrity = 0;
    ULONG64 index = Token->IntegrityLevelIndex;
    if (index == -1)
    {
        TokenIntegrity = 0;
    }
    else
    {
        TokenIntegrity = Token->UserAndGroups[index];
    }
    return TokenIntegrity;
}
```

```
PSID_AND_ATTRIBUTES SepLocateTokenIntegrity(IN PTOKEN Token)
{
    PSID_AND_ATTRIBUTES TokenIntegrity = 0;
    ULONG64 index = Token->IntegrityLevelIndex;
    if (index == -1)
    {
        TokenIntegrity = 0;
    }
    else
    {
        TokenIntegrity = Token->UserAndGroups[index];
    }
    return TokenIntegrity;
}
```

MIC: Get Integrity Level



```
ULONG SepCopyTokenIntegrity(
    IN  PTOKEN Token,
    OUT PSID_AND_ATTRIBUTES Output)
{
    PSID_AND_ATTRIBUTES TokenIntegrity = 0;
    TokenIntegrity = SepLocateTokenIntegrity(Token);
    if (TokenIntegrity)
    {
        Output->Sid = TokenIntegrity->Sid;
        Output->Attributes = TokenIntegrity->Attributes;
    }
    else
    {
        Output->Sid = SeUntrustedMandatorySid;
        Output->Attributes = 0x60;
    }
    return Output->Attributes;
}
```

```
ULONG SepCopyTokenIntegrity(
    IN  PTOKEN Token,
    OUT PSID_AND_ATTRIBUTES Output)
{
    PSID_AND_ATTRIBUTES TokenIntegrity = 0;
    TokenIntegrity = SepLocateTokenIntegrity(Token);
    if (TokenIntegrity)
    {
        Output->Sid = TokenIntegrity->Sid;
        Output->Attributes = TokenIntegrity->Attributes;
    }
    else
    {
        Output->Sid = SeUntrustedMandatorySid;
        Output->Attributes = 0x60;
    }
    return Output->Attributes;
}
```

```
ULONG SepCopyTokenIntegrity(
    IN  PTOKEN Token,
    OUT PSID_AND_ATTRIBUTES Output)
{
    PSID_AND_ATTRIBUTES TokenIntegrity = 0;
    TokenIntegrity = SepLocateTokenIntegrity(Token);
    if (TokenIntegrity)
    {
        Output->Sid = TokenIntegrity->Sid;
        Output->Attributes = TokenIntegrity->Attributes;
    }
    else
    {
        Output->Sid = SeUntrustedMandatorySid;
        Output->Attributes = 0x60;
    }
    return Output->Attributes;
}
```

```
ULONG SepCopyTokenIntegrity(
    IN  PTOKEN Token,
    OUT PSID_AND_ATTRIBUTES Output)
{
    PSID_AND_ATTRIBUTES TokenIntegrity = 0;
    TokenIntegrity = SepLocateTokenIntegrity(Token);
    if (TokenIntegrity)
    {
        Output->Sid = TokenIntegrity->Sid;
        Output->Attributes = TokenIntegrity->Attributes;
    }
    else
    {
        Output->Sid = SeUntrustedMandatorySid;
        Output->Attributes = 0x60;
    }
    return Output->Attributes;
}
```

```
ULONG SepCopyTokenIntegrity(
    IN  PTOKEN Token,
    OUT PSID_AND_ATTRIBUTES Output
{
    PSID_AND_ATTRIBUTES TokenIntegrity = 0;
    TokenIntegrity = SepLocateTokenIntegrity(Token);
    if (TokenIntegrity)
    {
        Output->Sid = TokenIntegrity->Sid;
        Output->Attributes = TokenIntegrity->Attributes;
    }
    else
    {
        Output->Sid = SeUntrustedMandatorySid;
        Output->Attributes = 0x60;
    }
    return Output->Attributes;
}
```

```
ULONG64 index = Token->IntegrityLevelIndex;
if (index == -1)
{
    TokenIntegrity = 0;
}
```

Attack on MIC

ATTACK ON MIC: SCHEME

ATTACK ON MIC: SCHEME

1) Use a kernel driver to attack Microsoft Defender

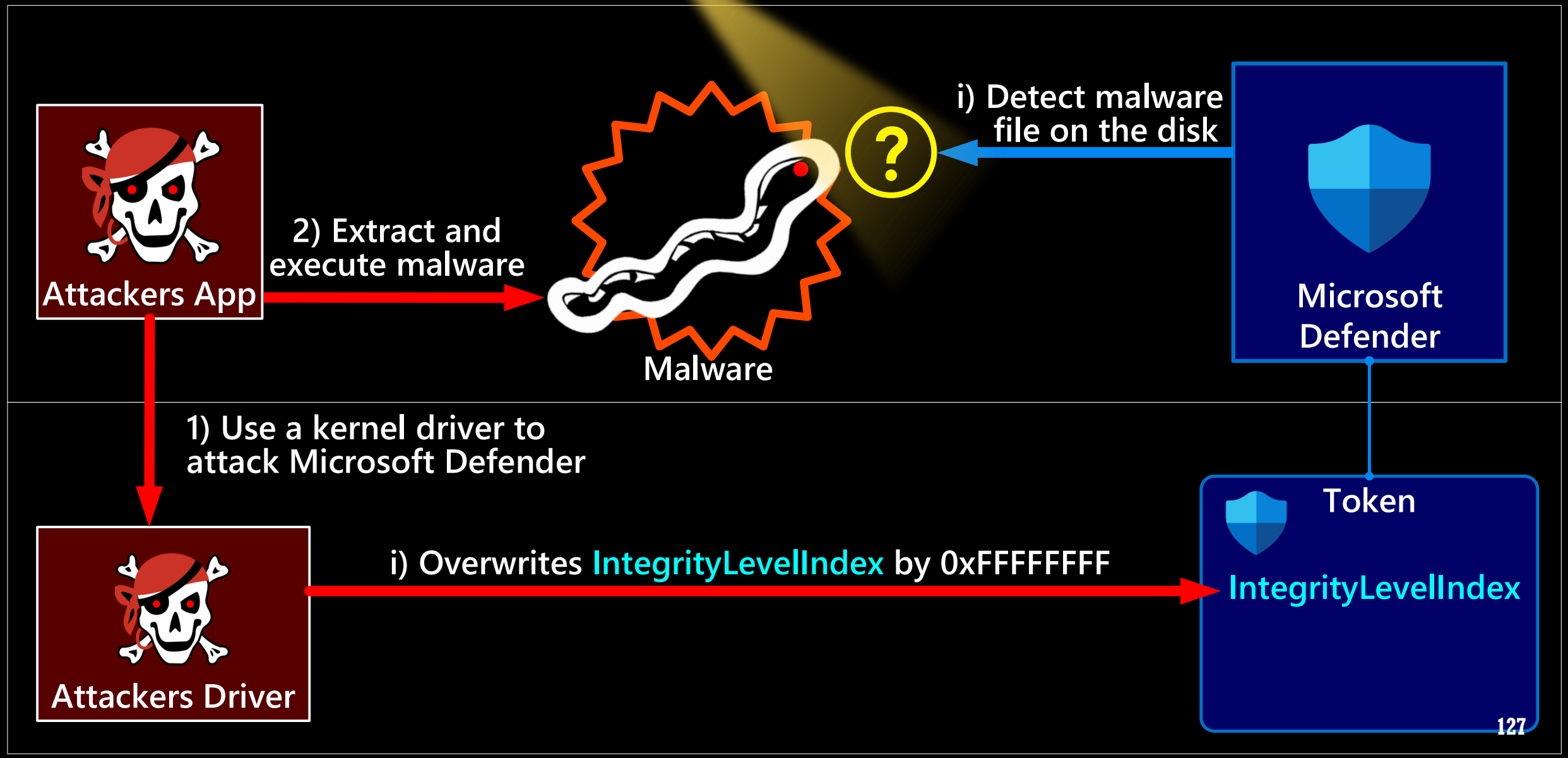
ATTACK ON MIC: SCHEME

1) Use a kernel driver to attack Microsoft Defender

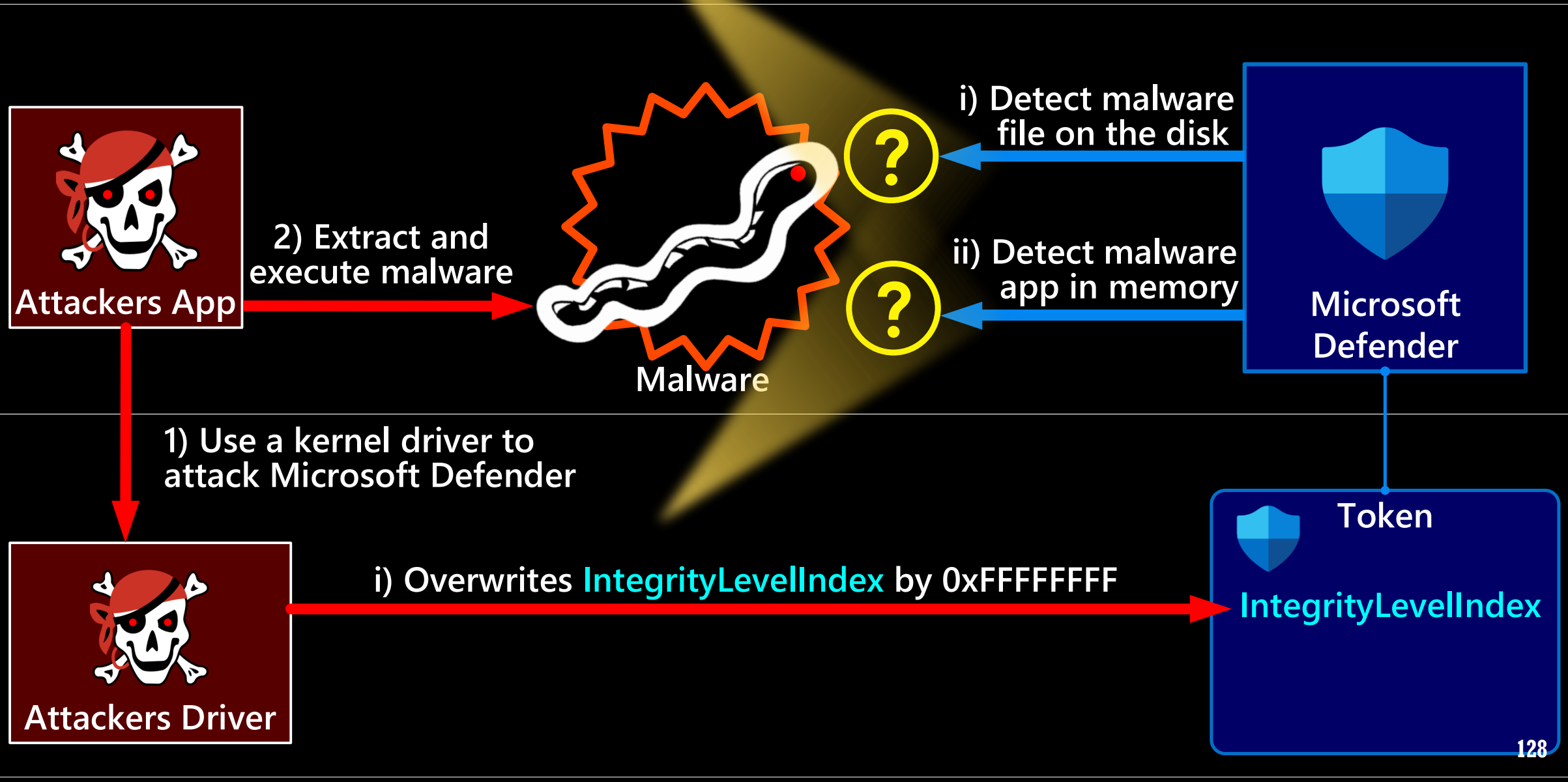
i) Overwrites IntegrityLevelIndex by 0xFFFFFFFF

ATTACK ON MIC: SCHEME

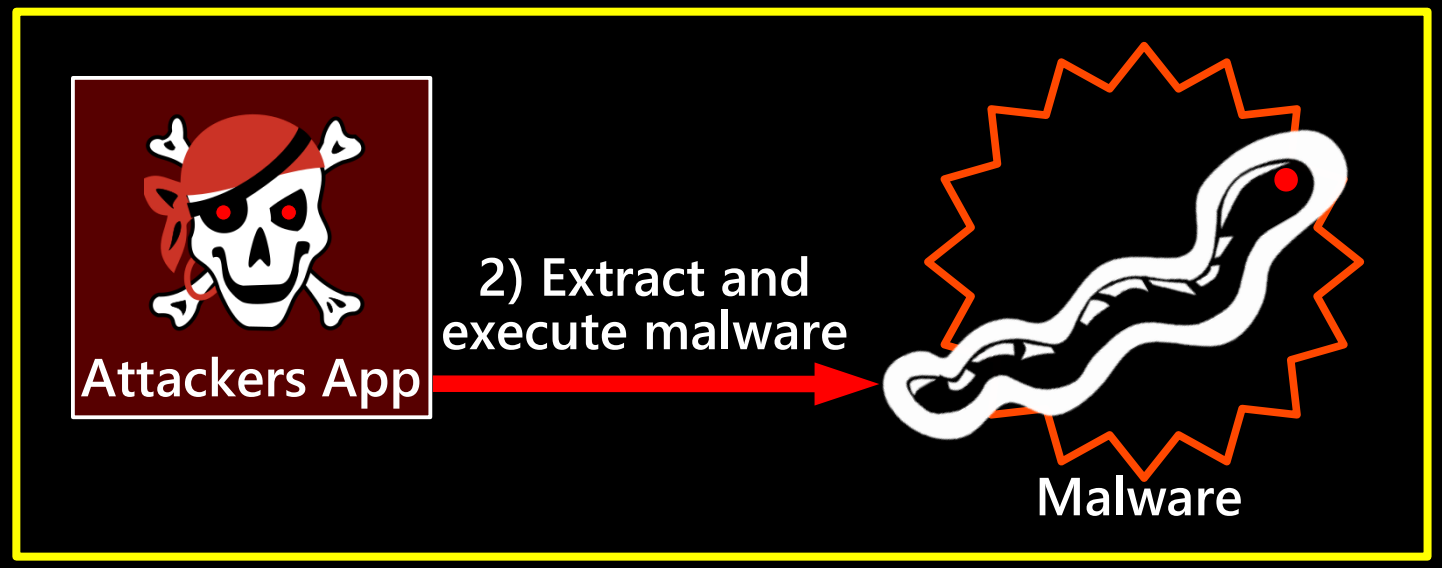
ATTACK ON MIC: SCHEME



ATTACK ON MIC: SCHEME



ATTACK ON MIC: SCHEME




>_
CMD.exe
a zip password-
protected archive
Mimikatz App

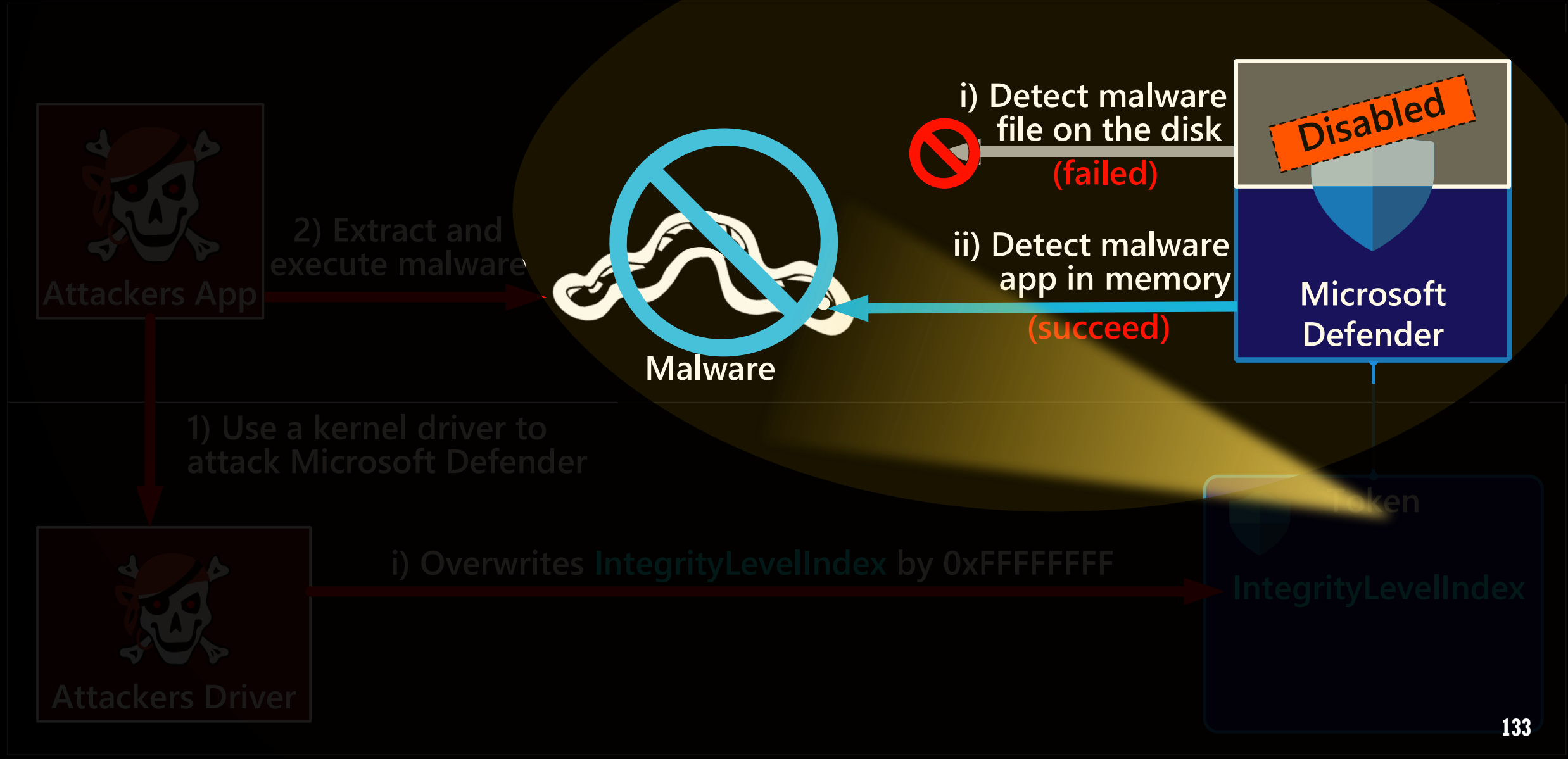
clear_extract_and_check.bat:

```
rmdir mimikatz /S/Q

7z.exe x "mimikatz.zip" -aos -o"mimikatz" -pinfected
dir    "mimikatz\mimikatz_trunk\x64"
start "mimikatz\mimikatz_trunk\x64\mimikatz.exe"
```

ATTACK ON MIC: DEMO

The online version is here –
https://www.youtube.com/embed/AJV4UVaw8kg?vq=hd1440


Attackers App
2) Extract and execute malware
Malware
i) Detect malware file on the disk
(failed)
ii) Detect malware app in memory
(succeed)
Disabled
Microsoft Defender
1) Use a kernel driver to attack Microsoft Defender
Attackers Driver
i) Overwrites IntegrityLevelIndex by 0xFFFFFFFF
Token
IntegrityLevelIndex

SUMMARY

- Microsoft Defender app removes malware files via call:

```
FILE_DISPOSITION_INFORMATION file_info;
file_info.DeleteFile = TRUE;
NtSetInformationFile(mlwr_handle, &file_info);
```

- CMD fails to launch mimikatz with

  STATUS_VIRUS_INFECTED (0xC0000906)

  that is returned by AV to block running malware app

SUMMARY

- Microsoft Defender app removes malware files via call:

```
FILE_DISPOSITION_INFORMATION file_info;
file_info.DeleteFile = TRUE;
NtSetInformationFile(mlwr_handle, &file_info);
```

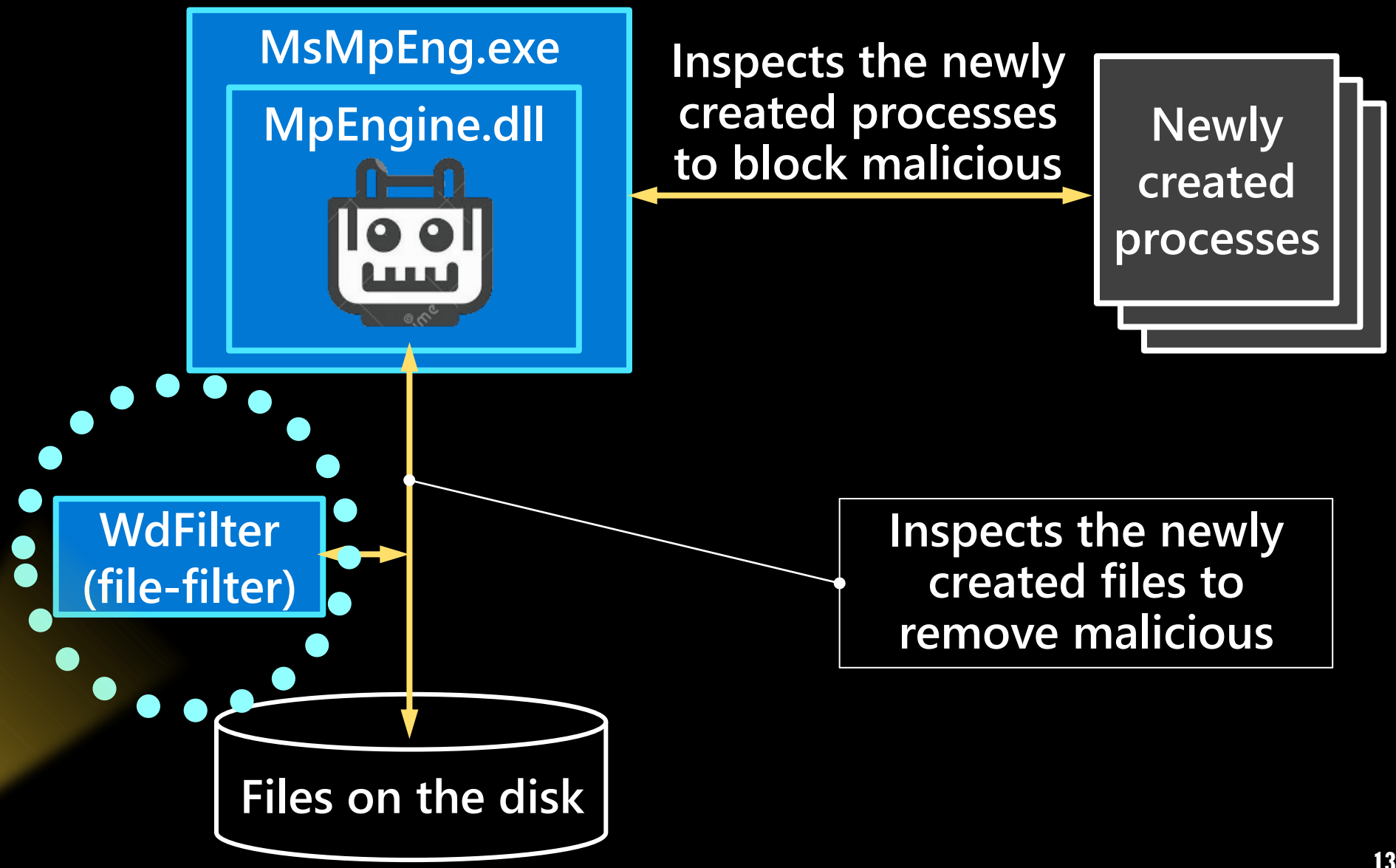
- CMD fails to launch mimikatz with

  STATUS_VIRUS_INFECTED (0xC0000906)

  that is returned by AV to block running malware app

Which driver returns this status?

MICROSOFT DEFENDER: INTERNALS



WDFilter

- It register a mini-filter via FltRegisterFilter()
- It prevents launching a malware via post-create callback

```
FLT_POSTOP_CALLBACK_STATUS WdFilterPostCreate(...)
{
    if (infected) {
        FltCancelFileOpen(Instance, FileObject);
        IoStatus.Status = STATUS_VIRUS_INFECTED;
    }
}
```

WDFilter

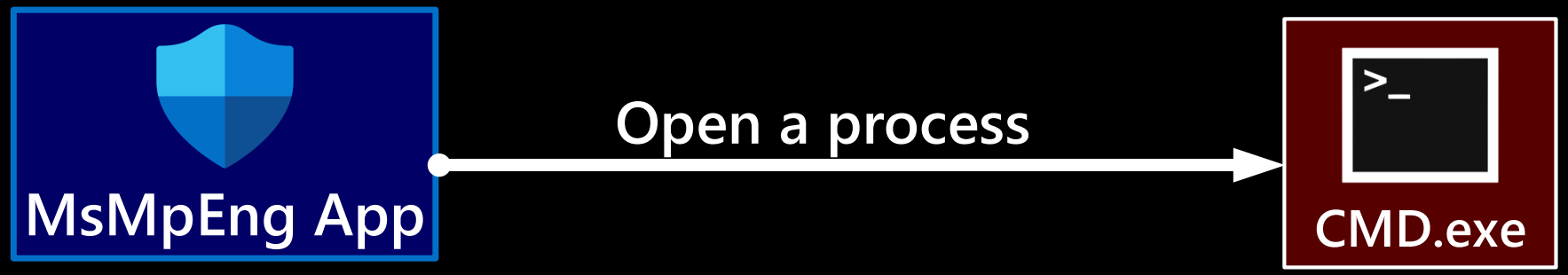
- It register a mini-filter via FltRegisterFilter()
- It prevents launching a malware via post-create callback

```
FLT_POSTOP_CALLBACK_STATUS WdFilterPostCreate(...)
{
    if (infected) {
        FltCancelFileOpen(Instance, FileObject);
        IoStatus.Status = STATUS_VIRUS_INFECTED;
    }
}
```

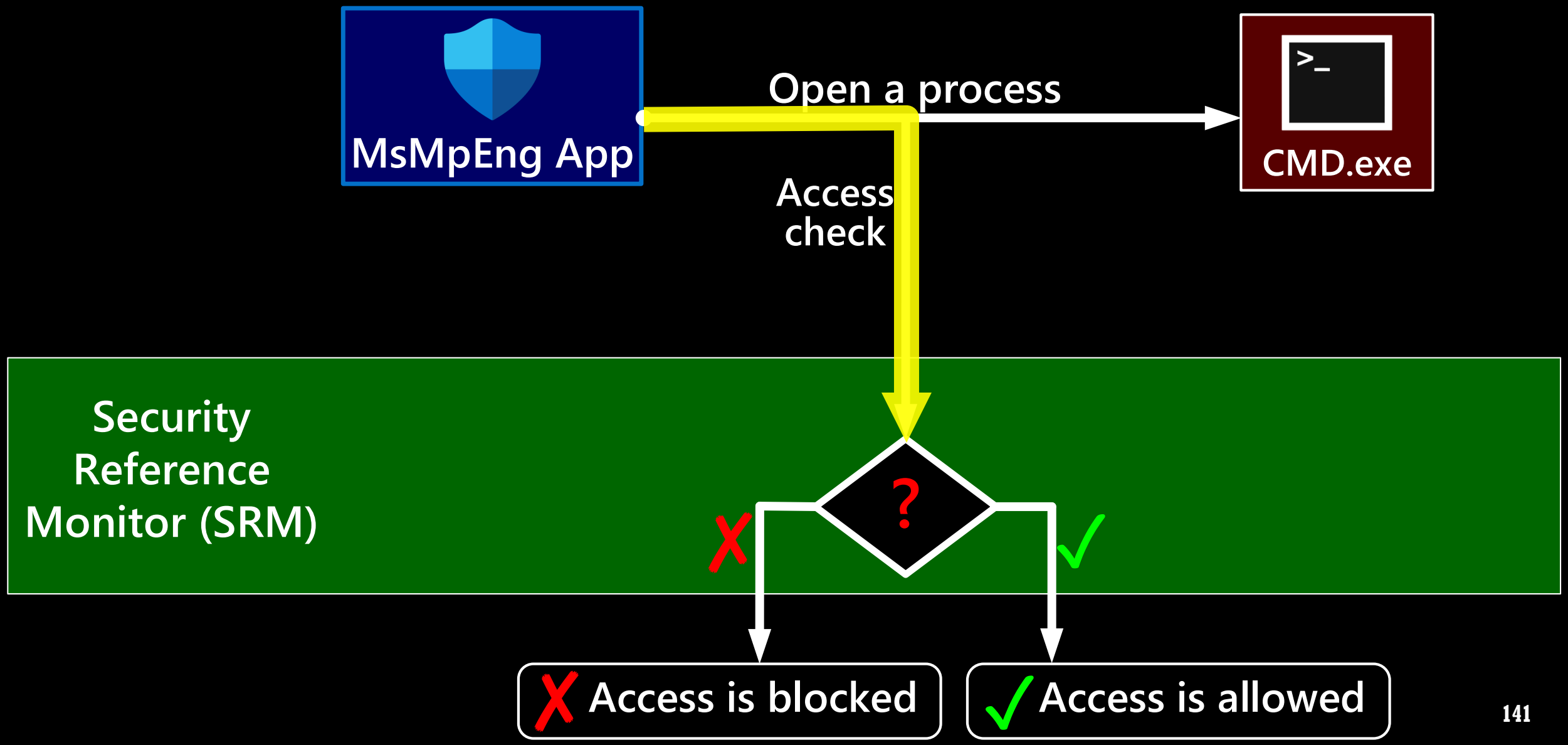
Defender is still able to access apps memory. But how?

How can Microsoft Defender get access to apps memory?

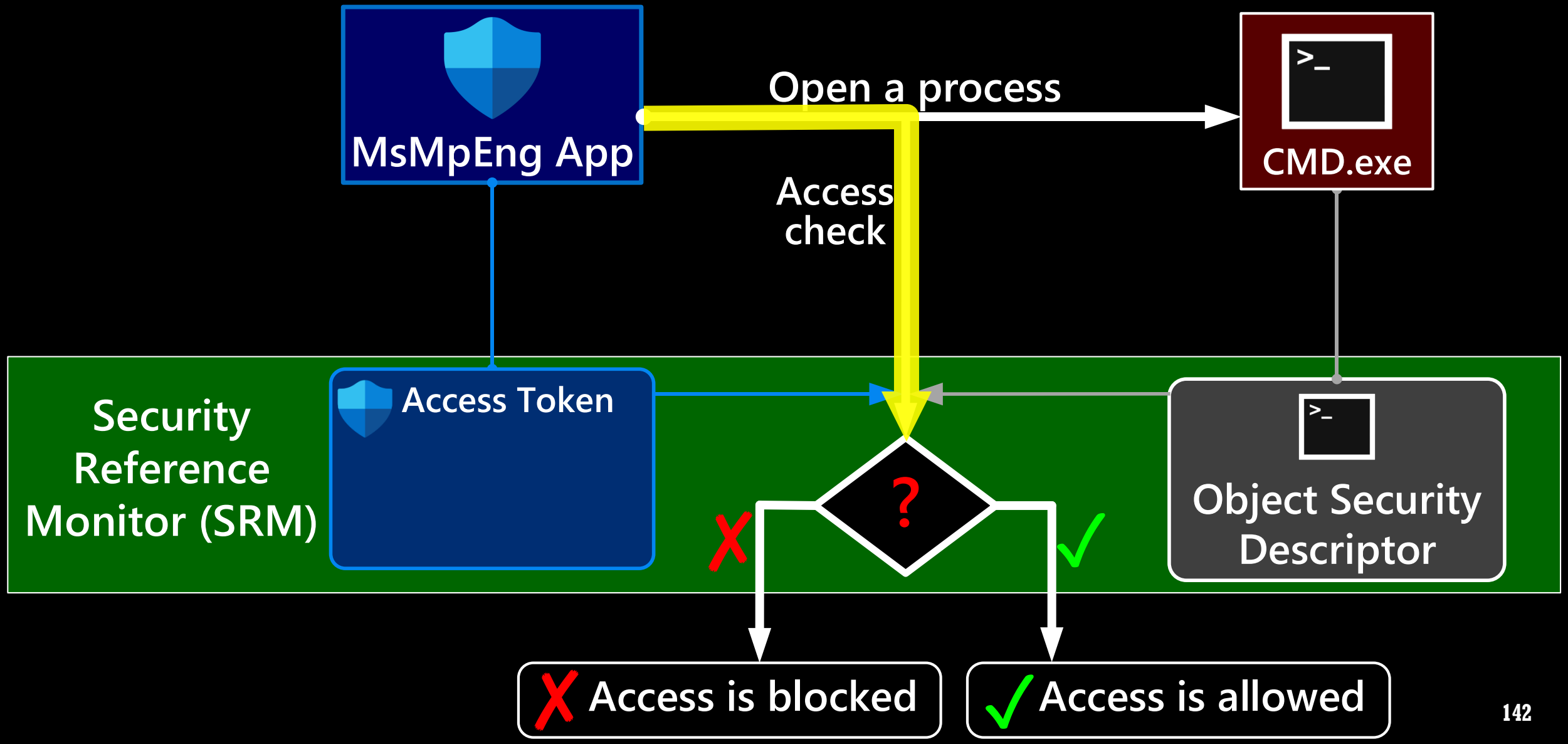
DEFENDER OPENS A PROCESS



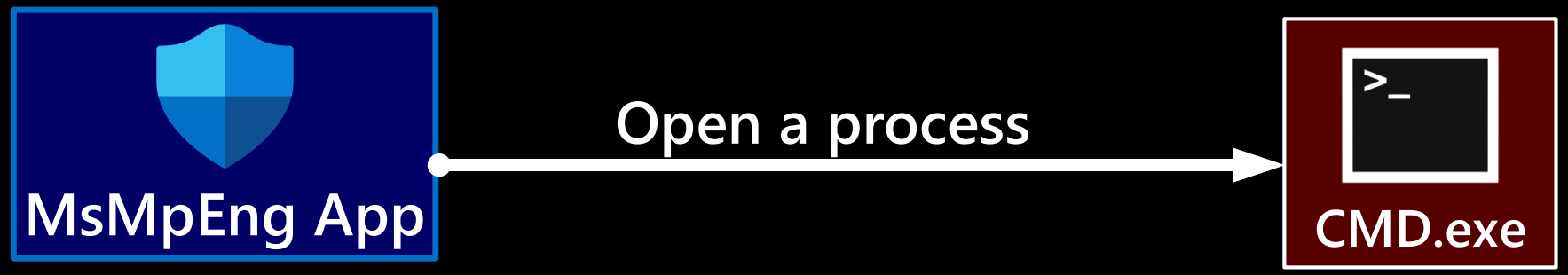
DEFENDER OPENS A PROCESS



DEFENDER OPENS A PROCESS



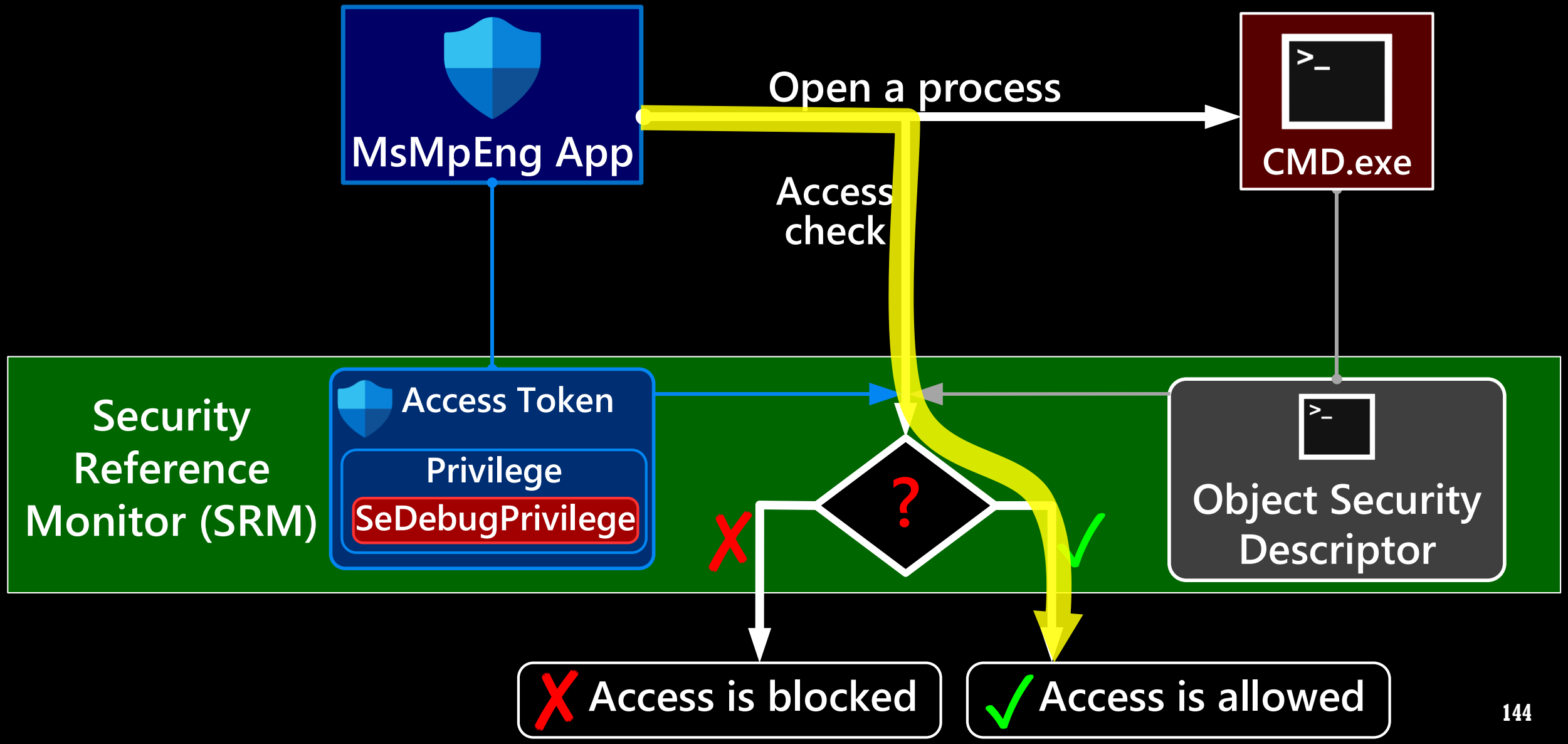
DEBUG PRIVILEGE ALLOWS TO GET ACCESS TO ALL APPS MEMORY



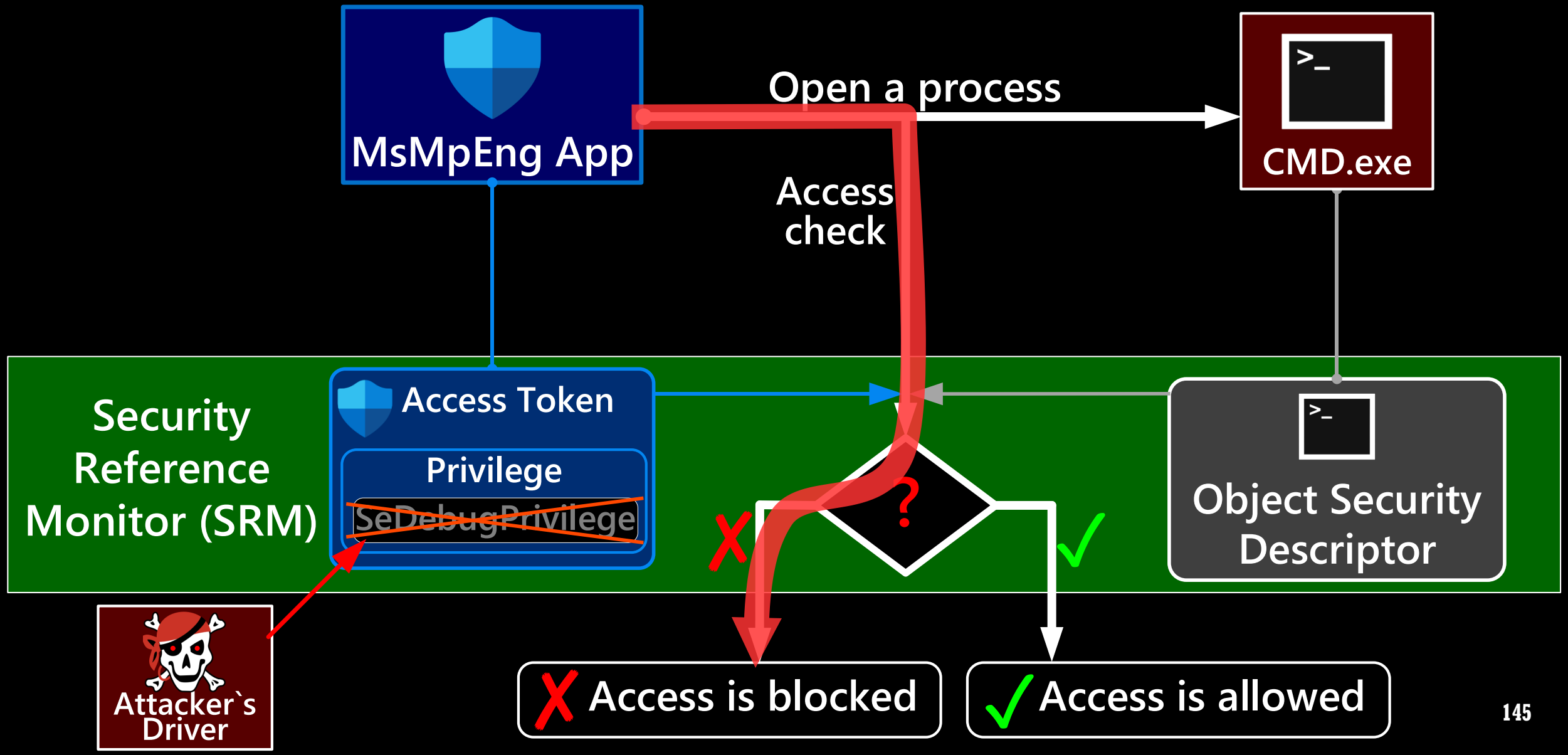
Name	User name
MsMpEng.exe	NT AUTHORITY\SYSTEM
cmd.exe	DESKTOP-2FNCGCH\igork

To open a process running on another user account MsMpEng has "SeDebugPrivilege" privilege

DEFENDER OPENS A PROCESS



DEFENDER OPENS A PROCESS



TOKEN PRIVILEGES

```
typedef struct _SEP_TOKEN_PRIVILEGES
{
    UINT64 Present;
    UINT64 Enabled;
    UINT64 EnabledByDefault;
} SEP_TOKEN_PRIVILEGES, *PSEP_TOKEN_PRIVILEGES;
```

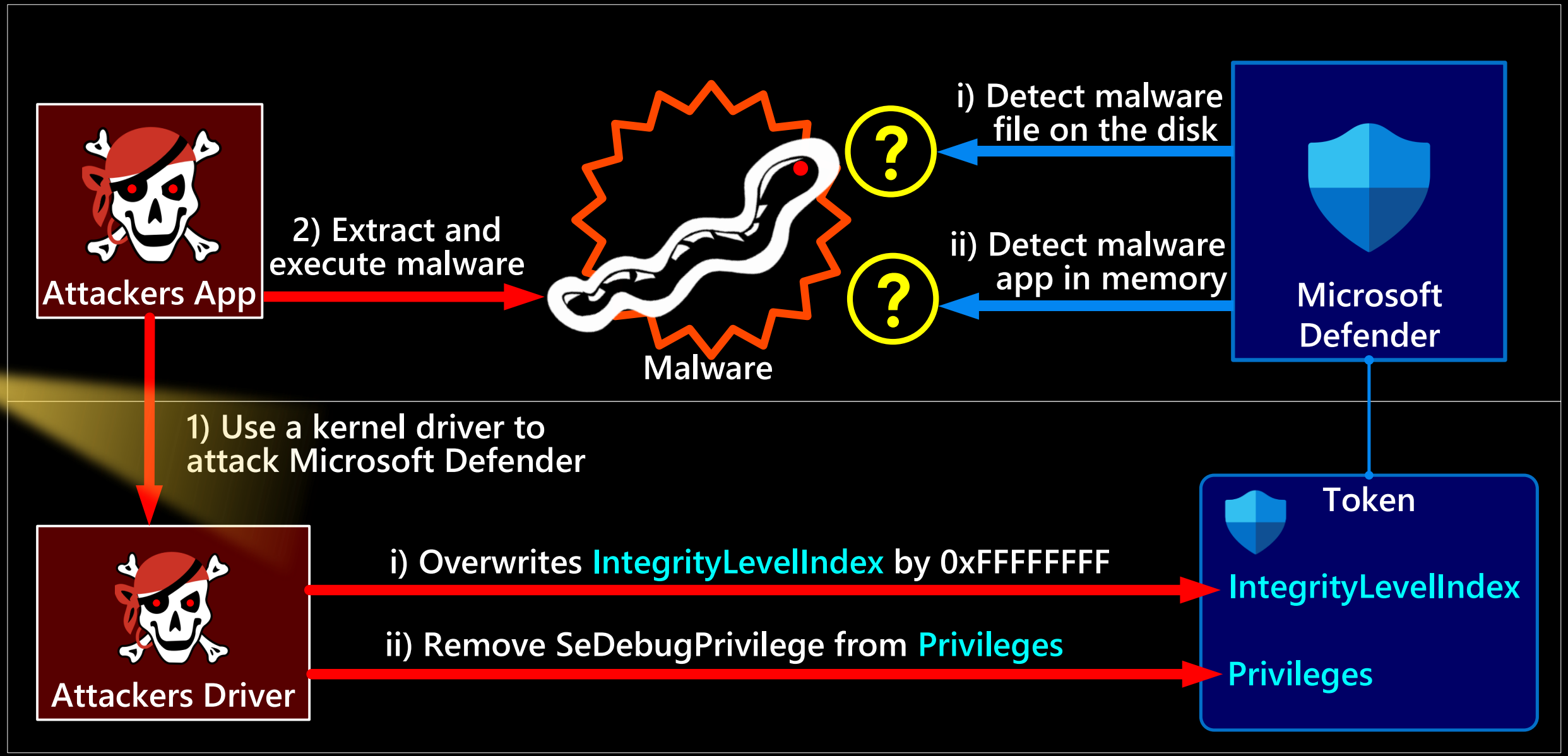
Research results:

revoking "SeDebugPrivilege" from "Enabled" is enough to prevent Defender from inspecting the apps memory.

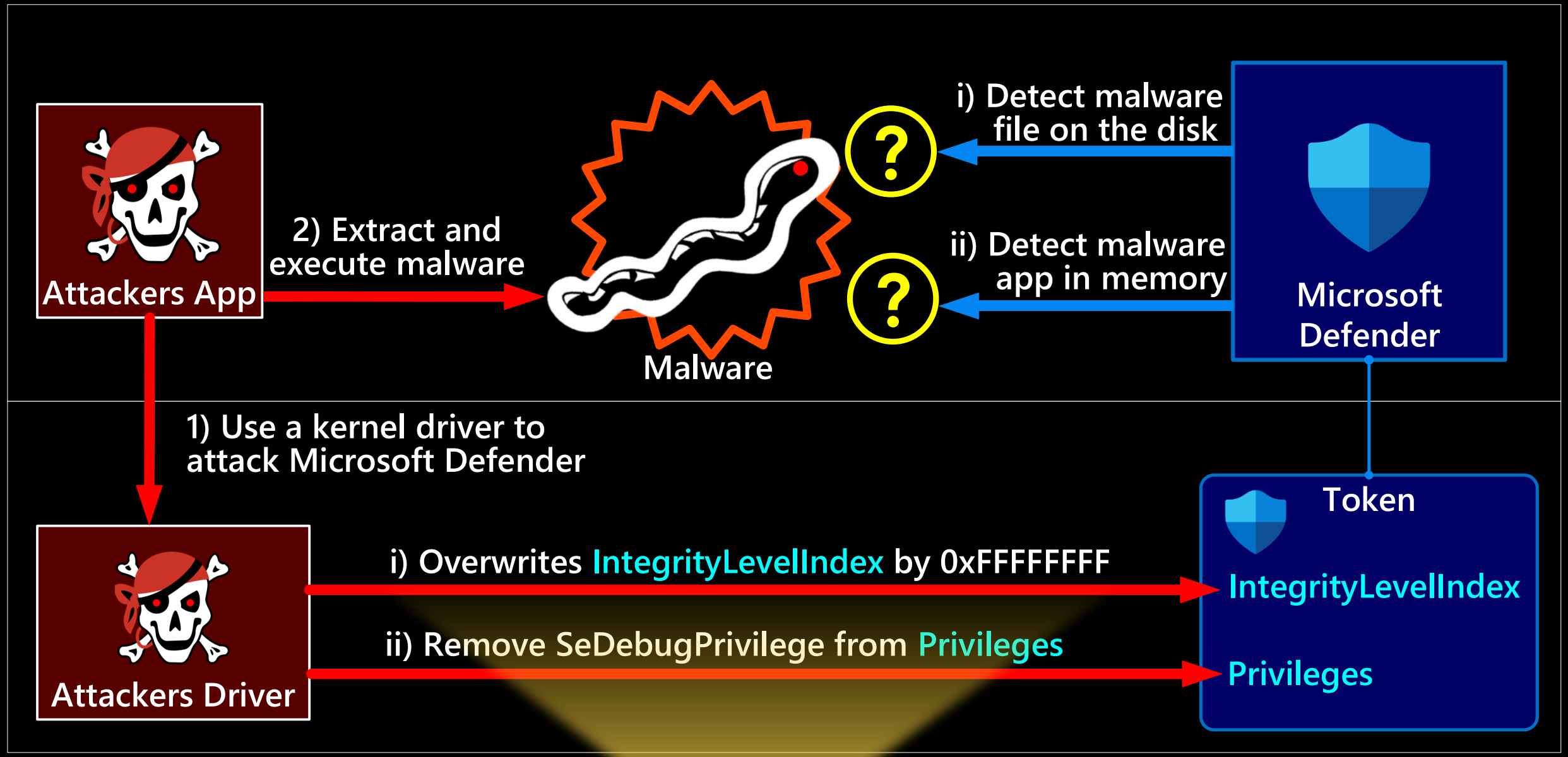
Attack on MIC and Token Privilege can disable Microsoft Defender without terminating its apps

ATTACK ON MIC + TOKEN PRIVILEGE: SCHEME

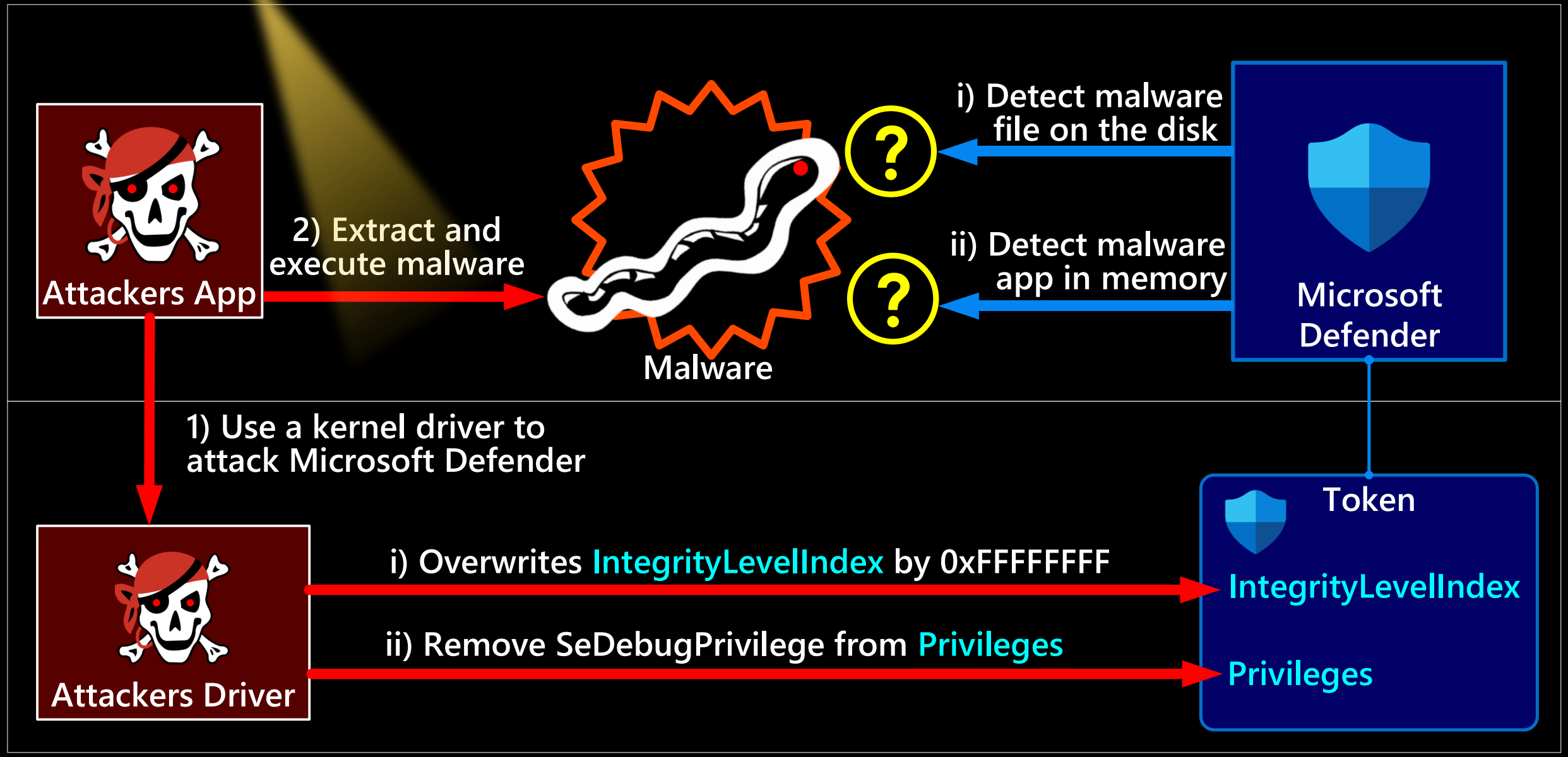
ATTACK ON MIC + TOKEN PRIVILEGE: SCHEME



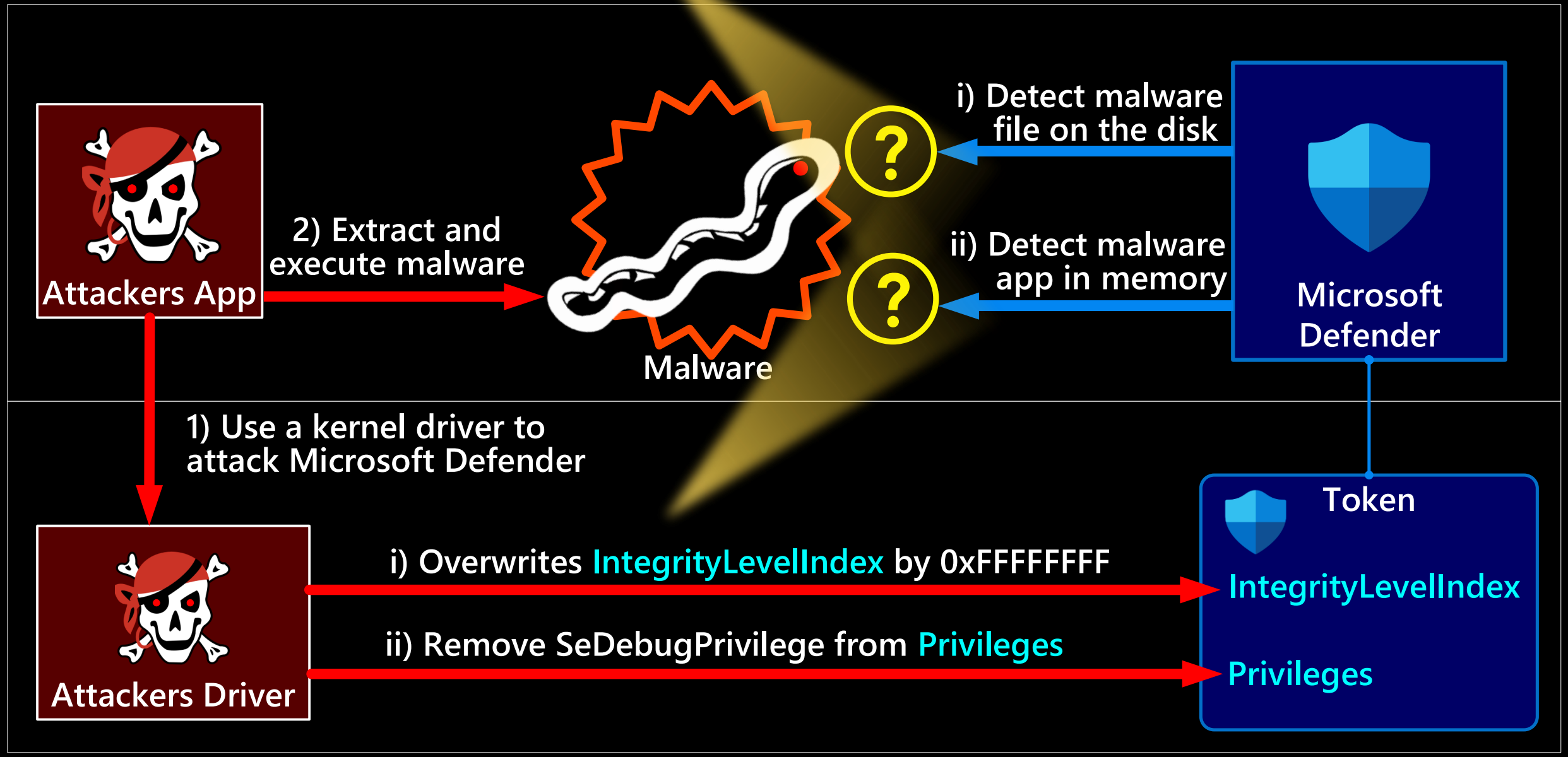
ATTACK ON MIC + TOKEN PRIVILEGE: SCHEME



ATTACK ON MIC + TOKEN PRIVILEGE: SCHEME



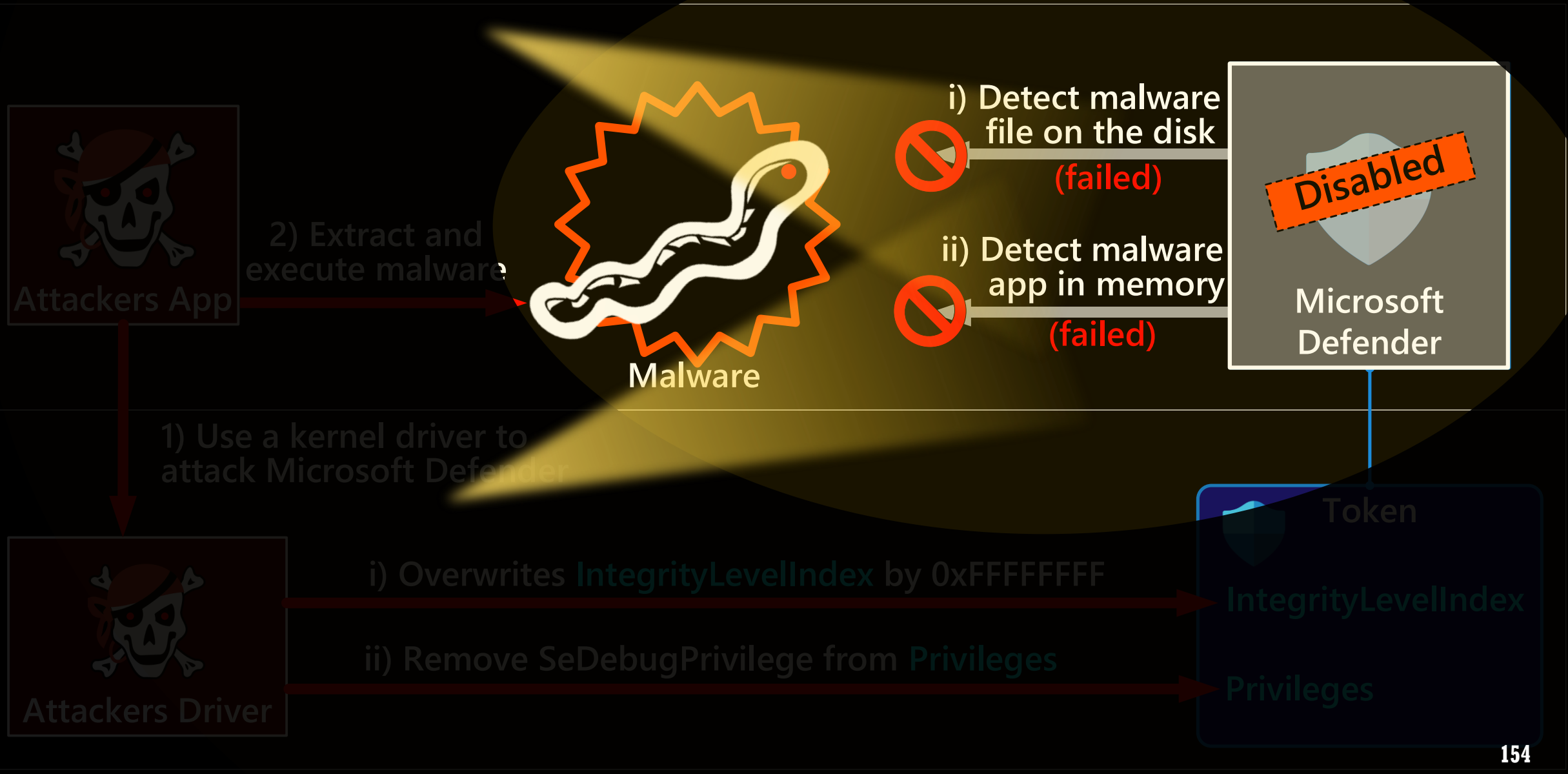
ATTACK ON MIC + TOKEN PRIVILEGE: SCHEME

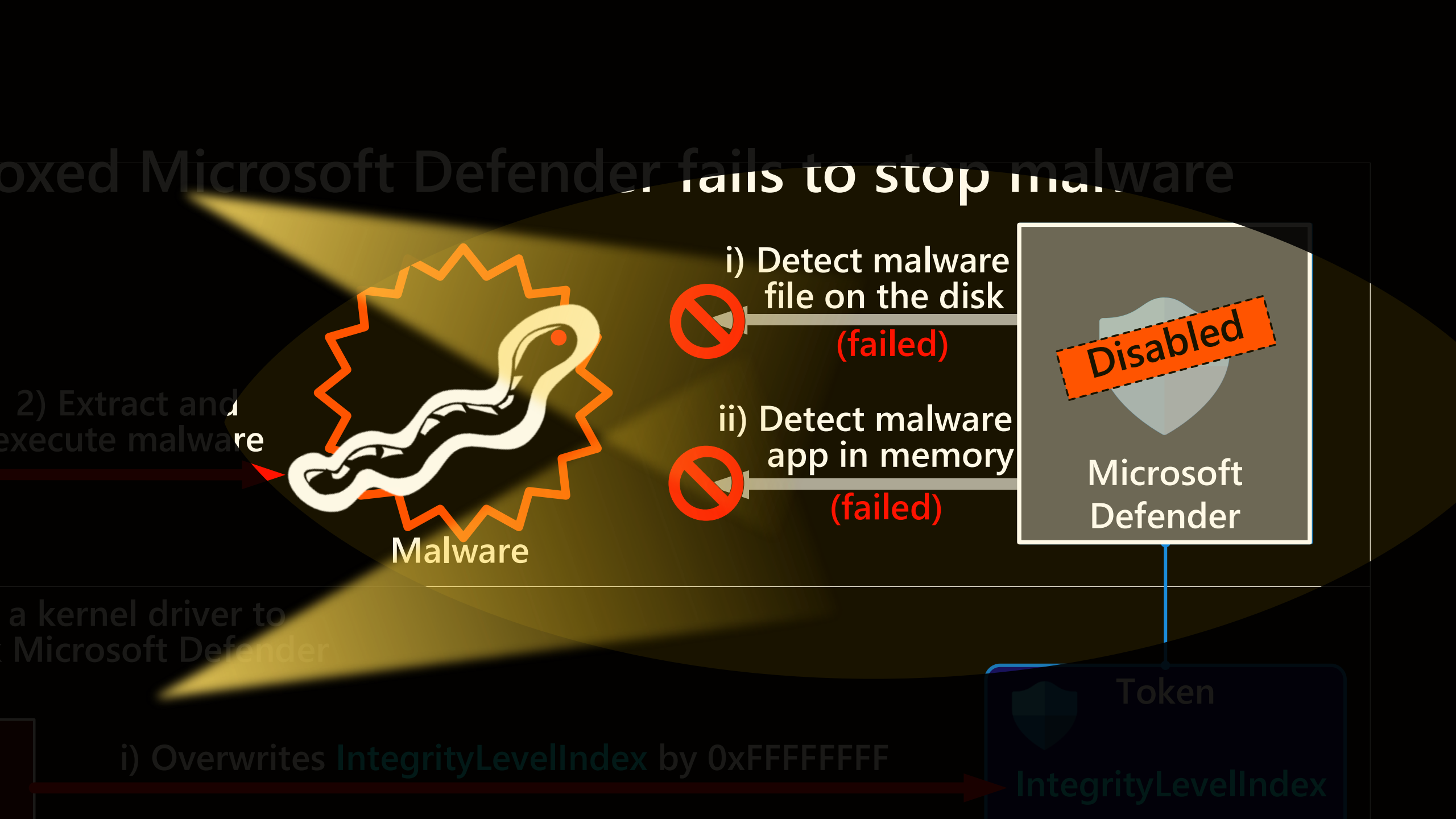


ATTACK ON MIC + TOKEN PRIVILEGE: DEMO

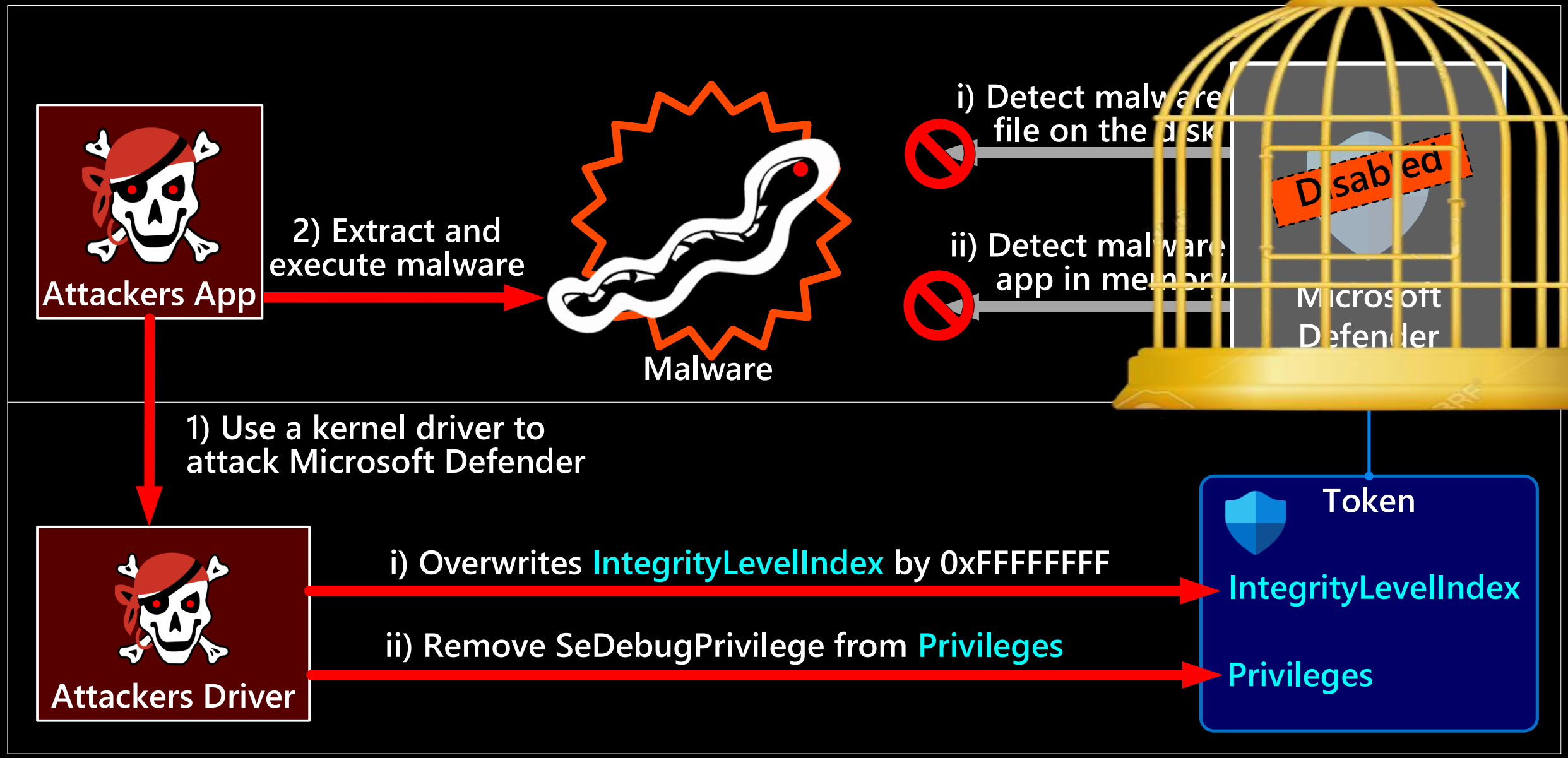
The online version is here –
https://www.youtube.com/embed/ihhUUd9qJTY?vq=hd1440

Sandboxed Microsoft Defender fails to stop malware




oxed Microsoft Defender fails to stop malw
2) Extract and
execute malwa
re
Malware
i) Detect malware
file on the disk
(failed)
ii) Detect malware
app in memory
(failed)
Disabled
Microsoft
Defender
a kernel driver to
Microsoft Defender
Token
i) Overwrites IntegrityLevelIndex by 0xFFFFFFFF
IntegrityLevelIndex

Sandboxed Microsoft Defender fails to stop malware



This attack can blind Microsoft Defender.
What about other AVs?

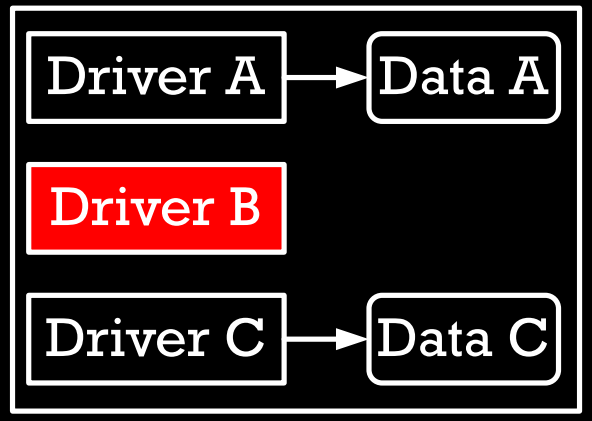
MIC-BASED ATTACK BLINDS TOP AV SOLUTIONS

AV Name	AV ability to detect malicious files	AV ability to detect malicious processes
Microsoft Defender	Disabled	Disabled
McAfee	Disabled	Disabled
Malwarebytes	Disabled	Disabled
avast	Disabled	Disabled
AVG	Disabled	Disabled
kaspersky	Disabled	Enabled
TREND MICRO	Enabled, but AV cannot remove malware files	Disabled

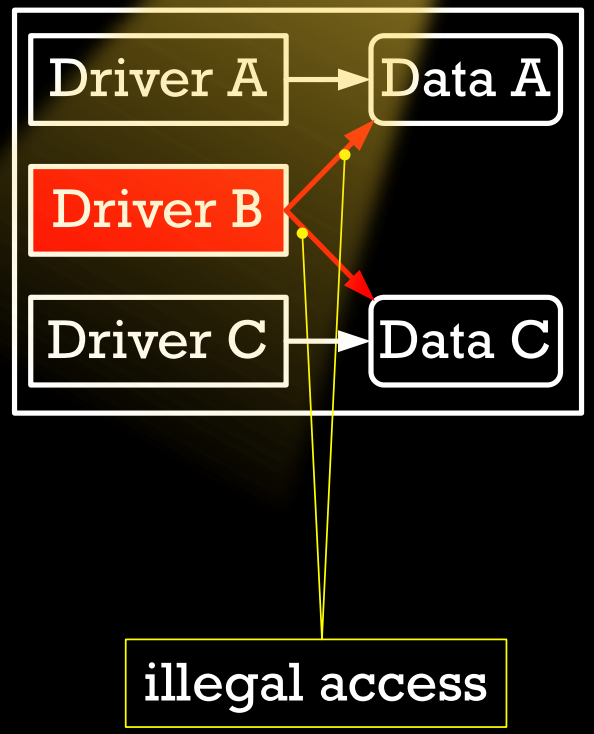
Disclaimer: The purpose is to provide technical review only. This analysis is not designed to promote any solutions. We do respect all antiviruses and endpoint security solutions.

MemoryRanger
Defends
Microsoft Defender

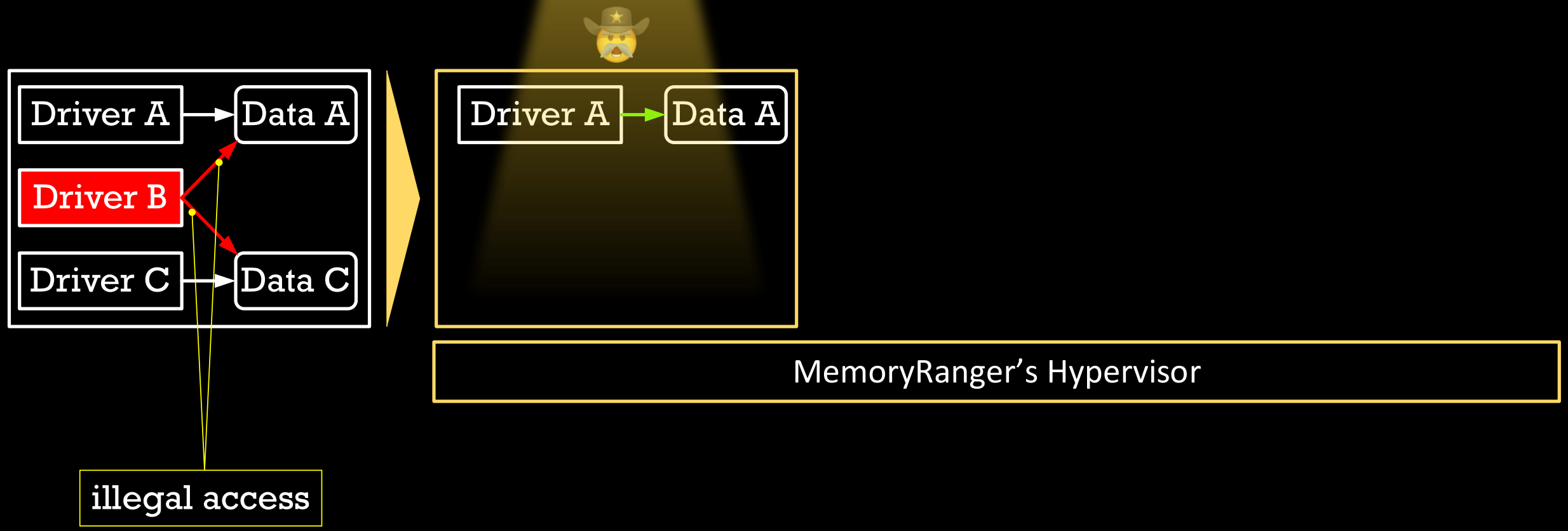
MemoryRanger: Intro



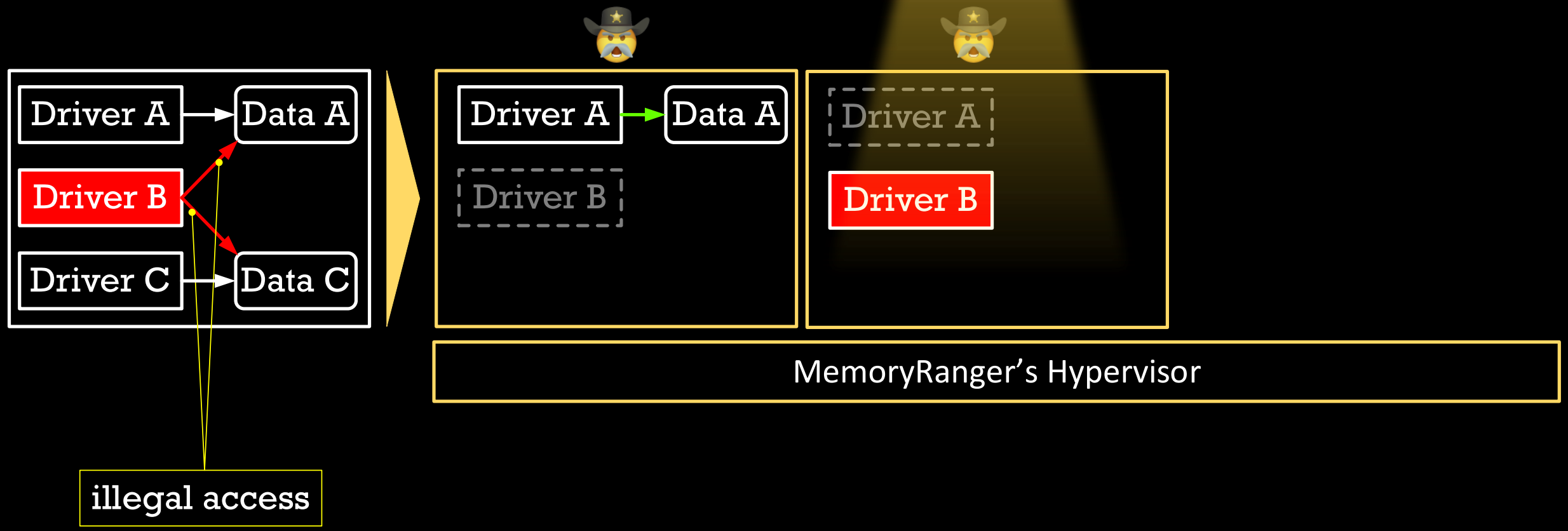
MemoryRanger: Intro



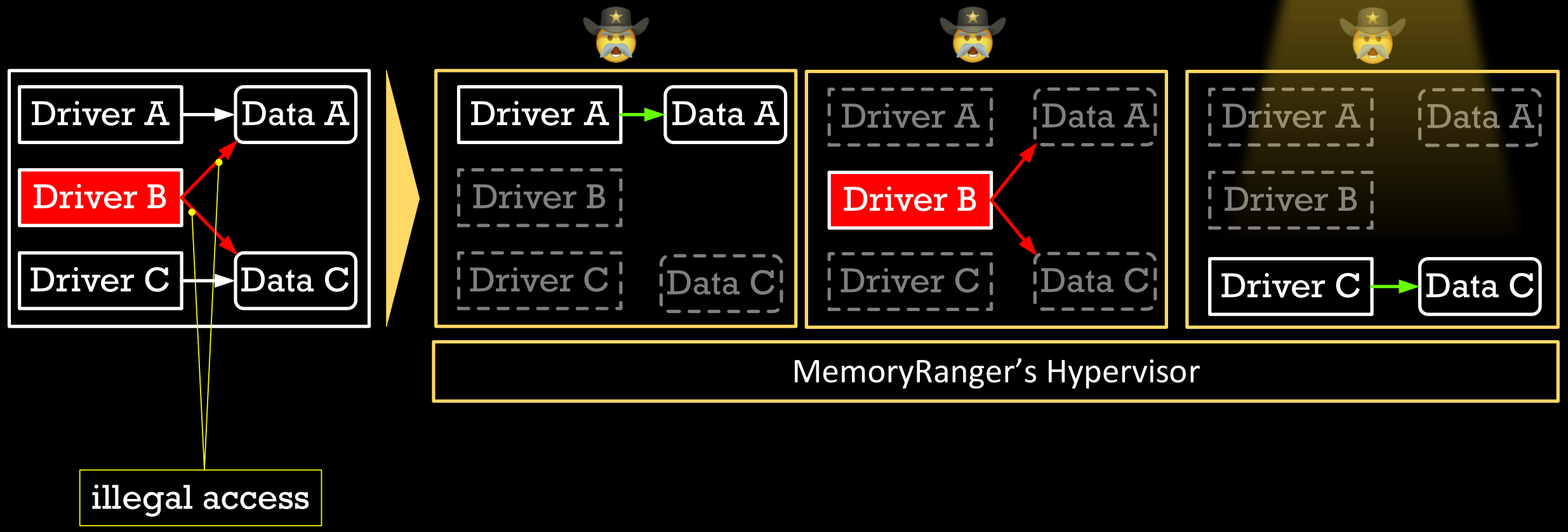
MemoryRanger: Intro



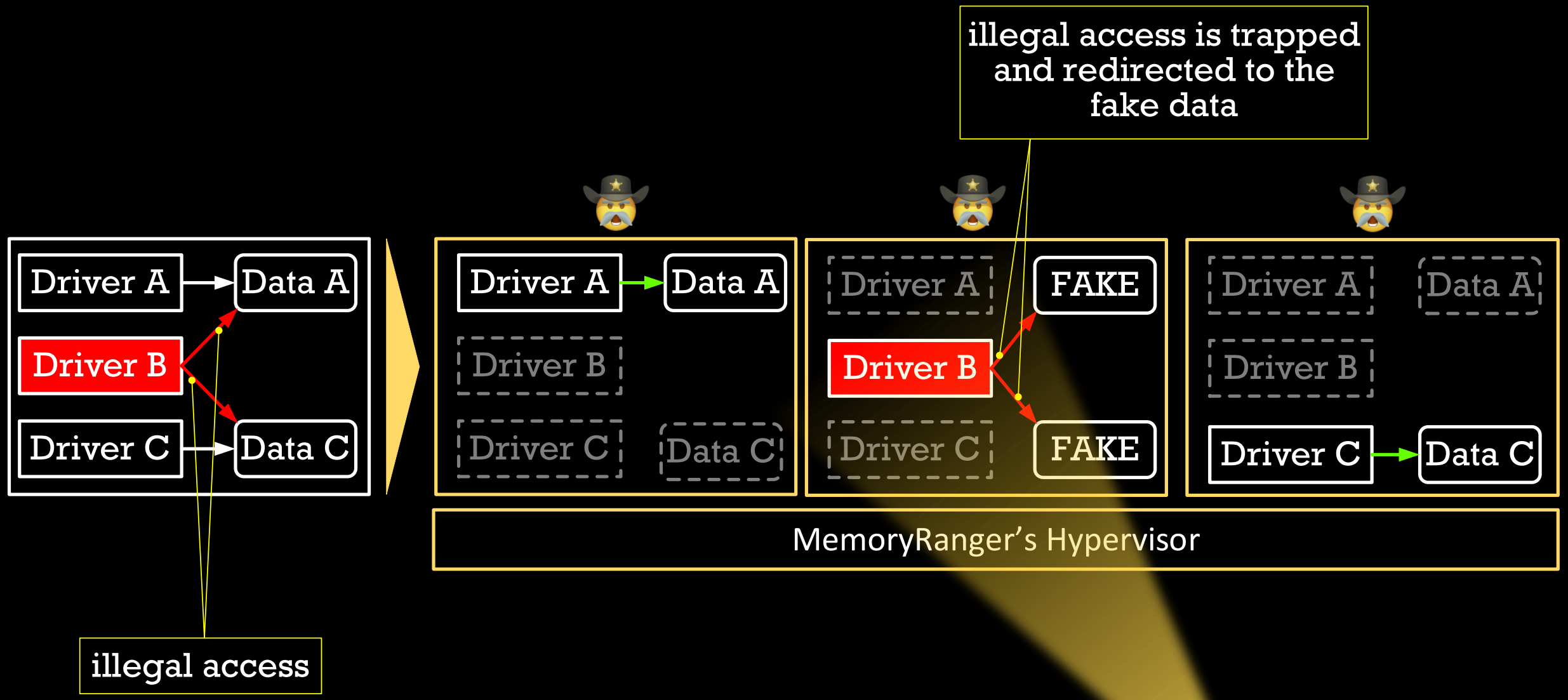
MemoryRanger: Intro



MemoryRanger: Intro



MemoryRanger: Intro



MemoryRanger: Features

- Components:
  - user-mode control app
  - kernel-mode driver to register OS callbacks
  - hypervisor based dispatcher based on Intel VT-x and EPT technologies

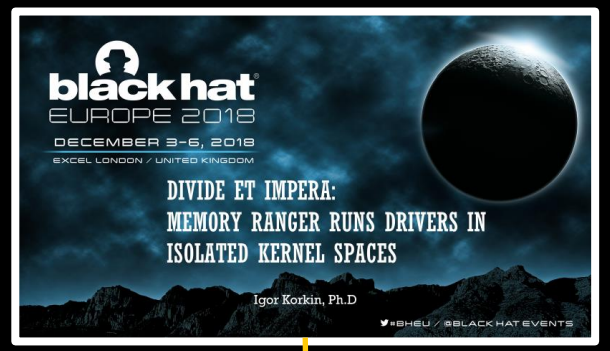
- The key features:
  - Runs kernel-mode drivers into isolated memory enclaves
  - Allows different memory access configuration for each memory enclave
  - Number of enclaves can be increased in runtime (while VBS has fixed 2 enclaves)

- Technical features:
  - Hooks kernel API routines
  - Redirects illegal access to the sensitive data to the fake content
  - Supports newest Windows 11 x64 and it is open-source

github.com/IgorKorkin/MemoryRanger

MemoryRanger was in US, UK, and Asia and twice at BlackHat

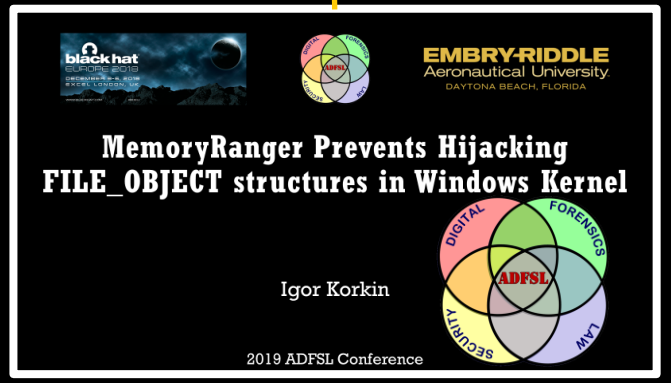
black hat EUROPE 2018



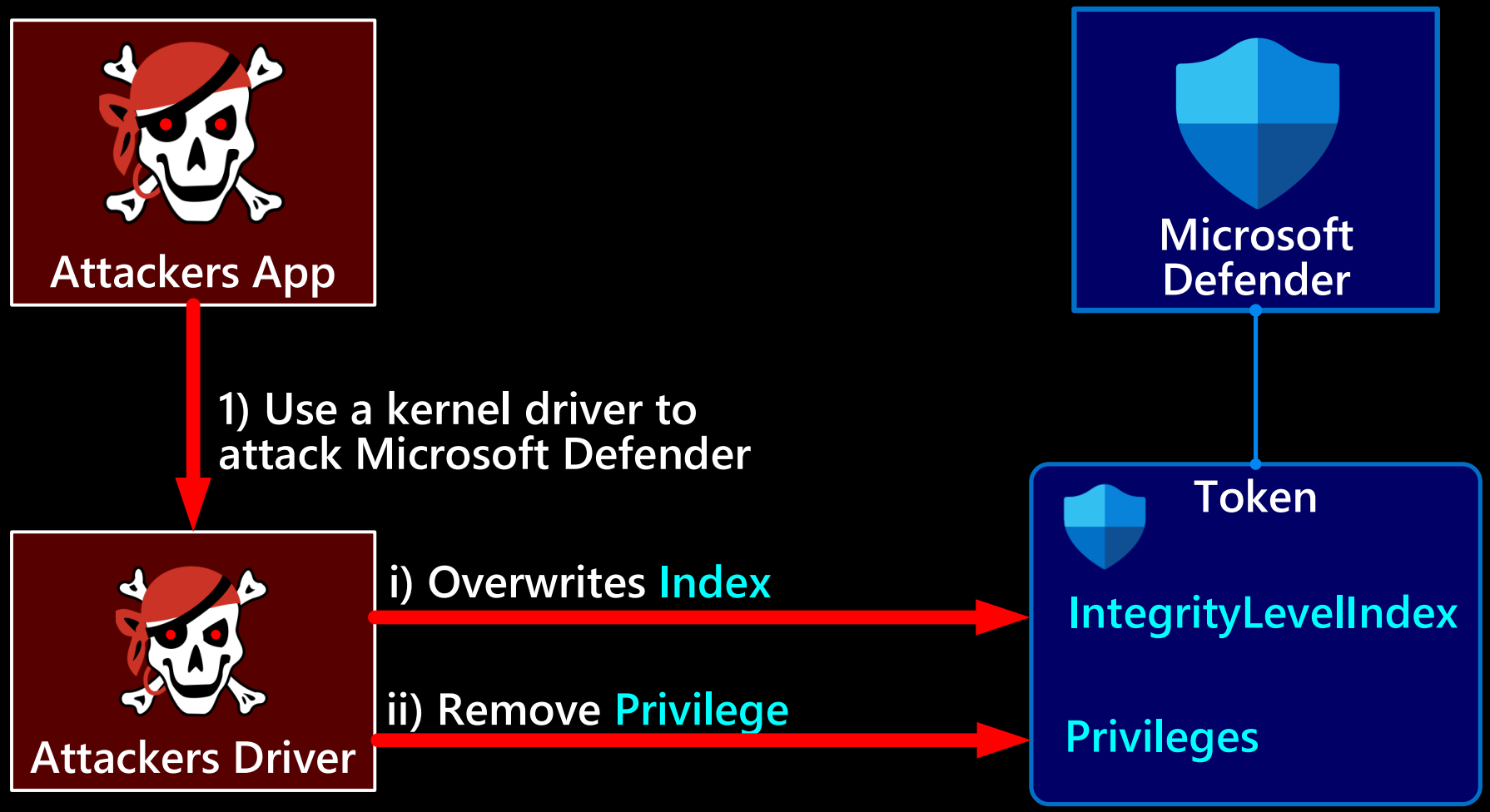
HITBSecConf

black hat EUROPE 2021

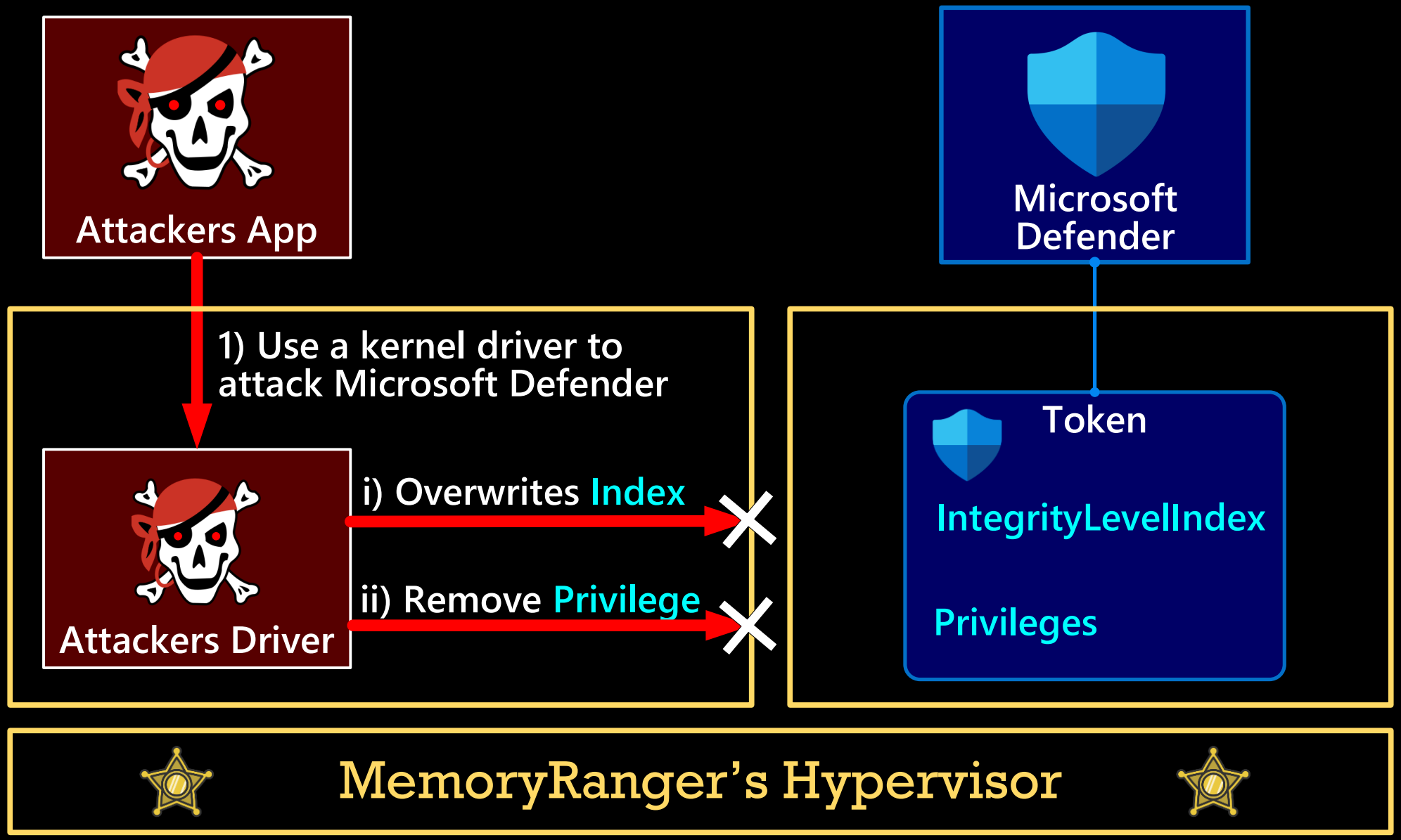
2018 → 2019 → 2020 → 2021 → 2022



MemoryRanger Customization protects Microsoft Defender

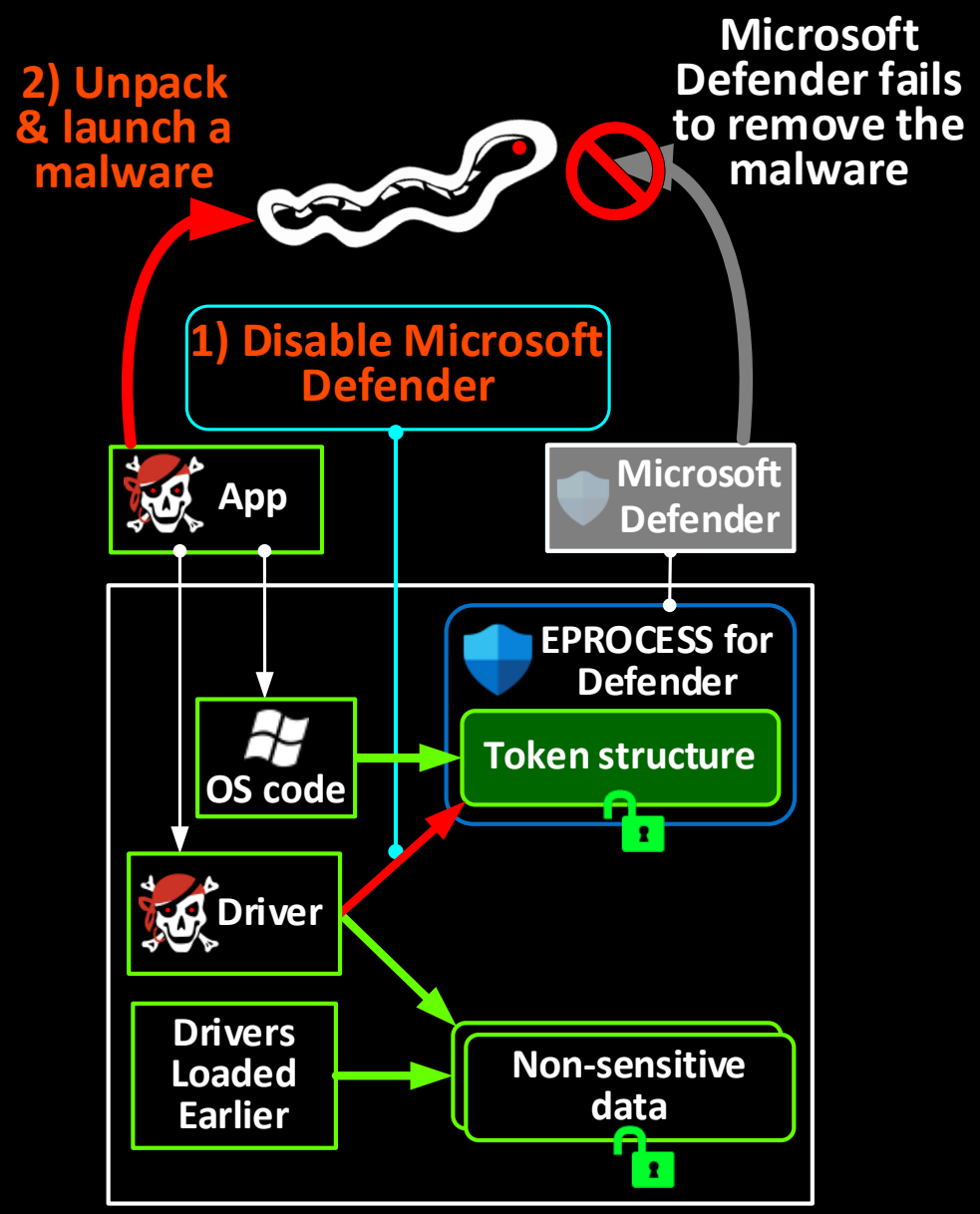


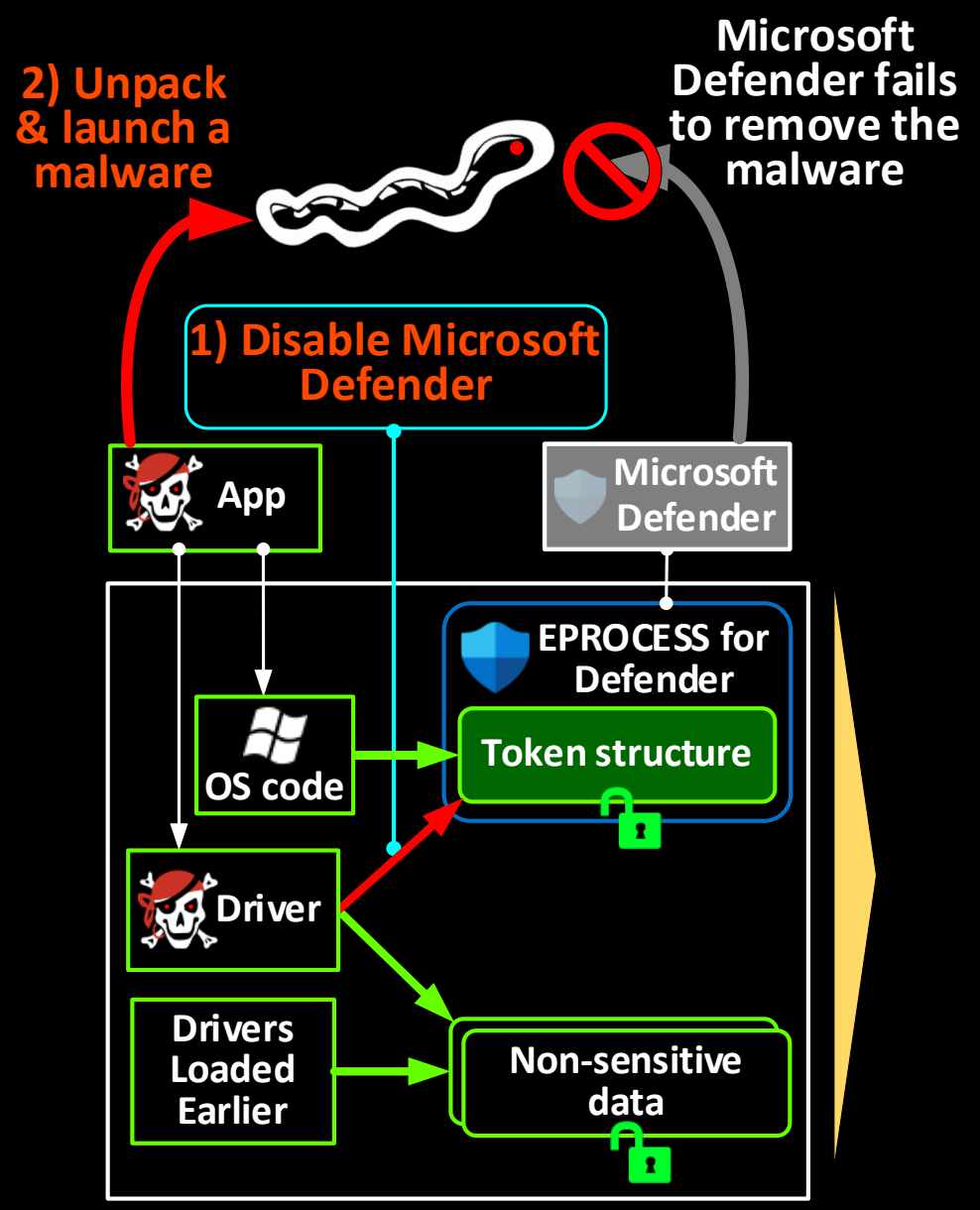
MemoryRanger Customization protects Microsoft Defender



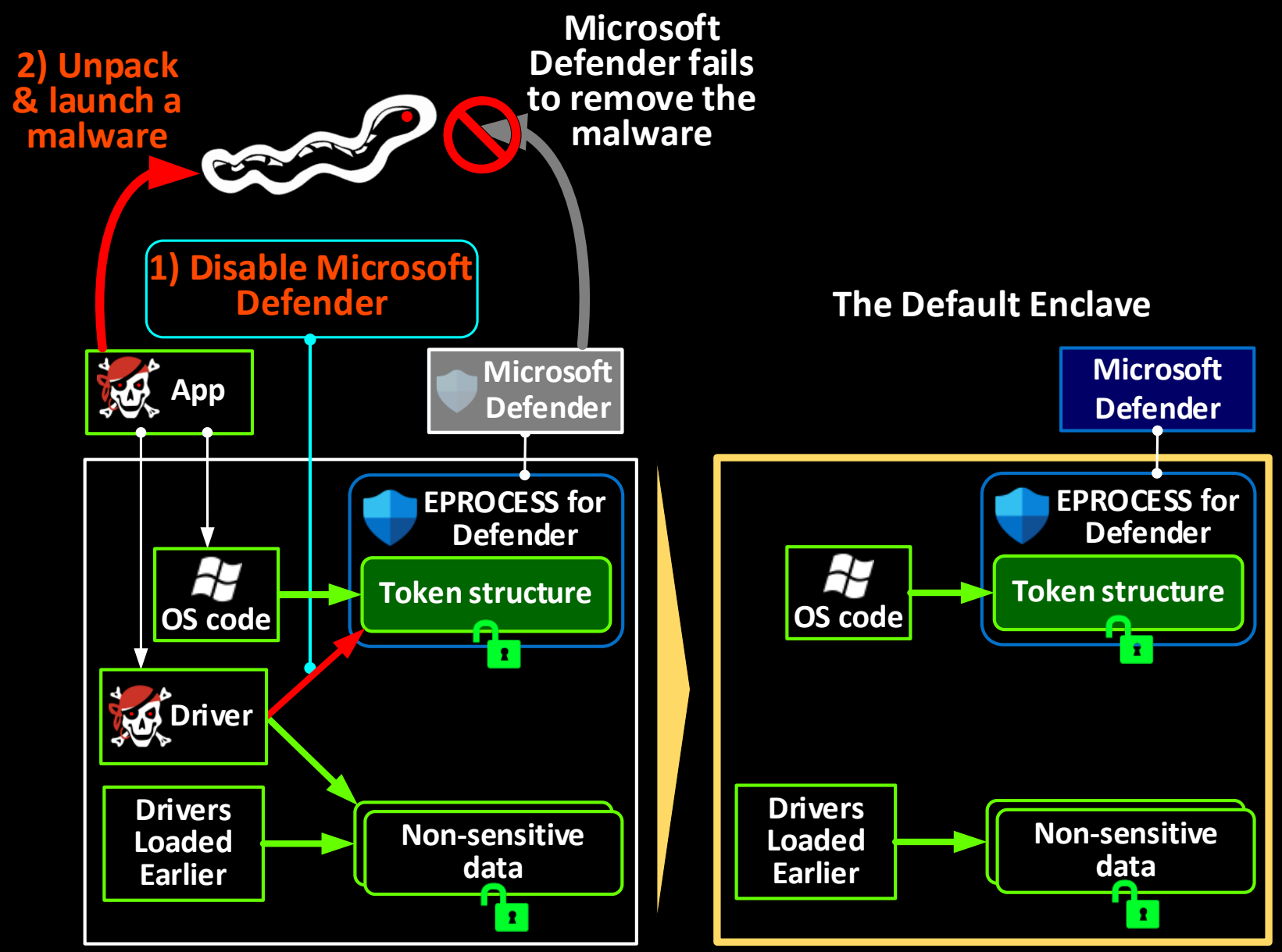
MemoryRanger Defends Microsoft Defender: Demo

The online version is here –
https://www.youtube.com/embed/Ohqhq50wVjI?vq=hd1440

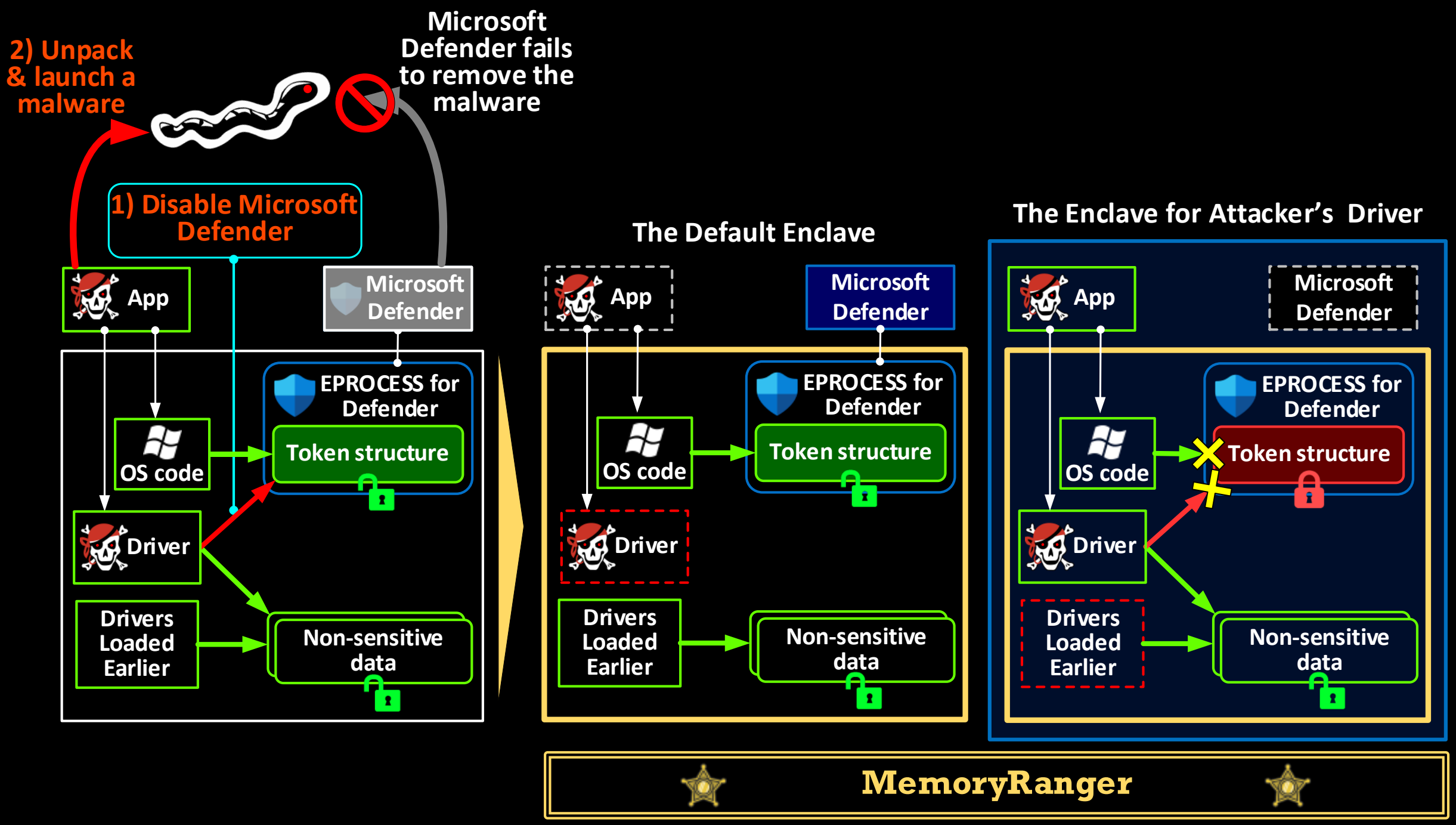

2) Unpack & launch a malware
Microsoft Defender fails to remove the malware
1) Disable Microsoft Defender
App
Microsoft Defender
EPROCESS for Defender
Token structure
OS code
Driver
Drivers Loaded Earlier
Non-sensitive data

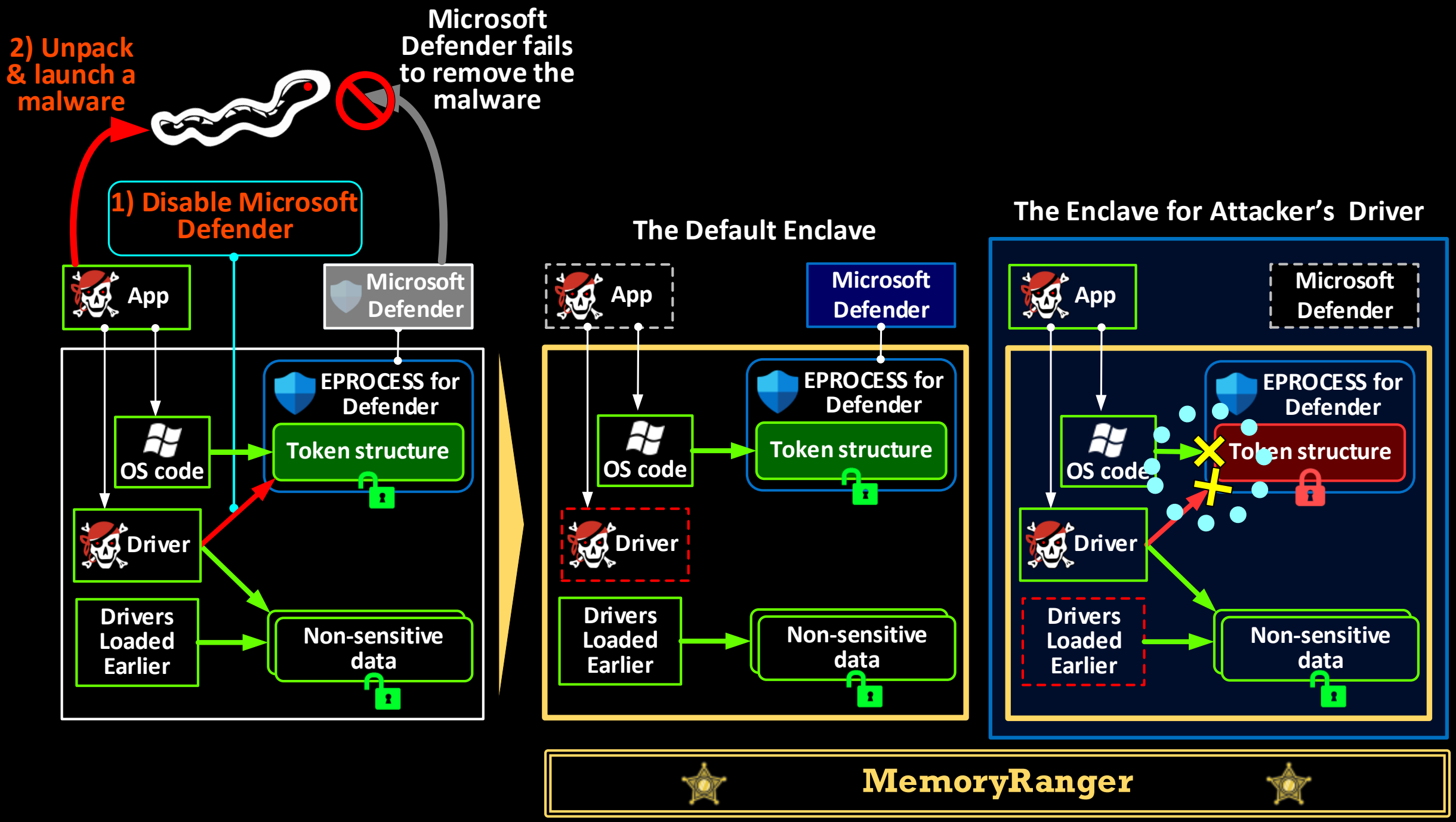


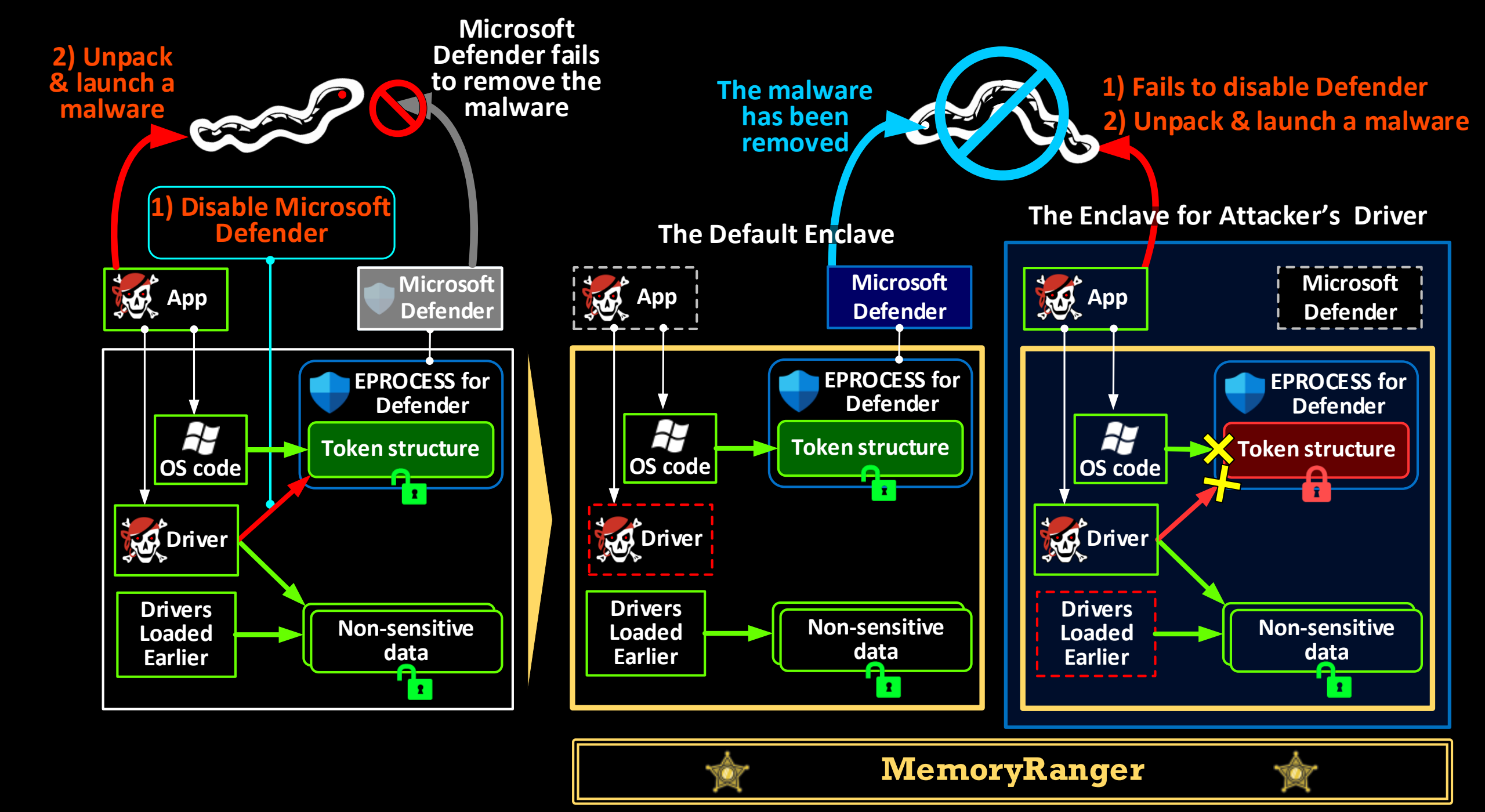
MemoryRanger



MemoryRanger


2) Unpack & launch a malware
Microsoft Defender fails to remove the malware
1) Disable Microsoft Defender
App
Microsoft Defender
EPROCESS for Defender
OS code
Token structure
Driver
Drivers Loaded Earlier
Non-sensitive data
The Default Enclave
App
Microsoft Defender
EPROCESS for Defender
OS code
Token structure
Driver
Drivers Loaded Earlier
Non-sensitive data
The Enclave for Attacker's Driver
App
Microsoft Defender
EPROCESS for Defender
OS code
Token structure
Driver
Drivers Loaded Earlier
Non-sensitive data
MemoryRanger


2) Unpack & launch a malware
Microsoft Defender fails to remove the malware
1) Disable Microsoft Defender
App
Microsoft Defender
EPROCESS for Defender
Token structure
OS code
Driver
Drivers Loaded Earlier
Non-sensitive data
The Default Enclave
App
Microsoft Defender
EPROCESS for Defender
Token structure
OS code
Driver
Drivers Loaded Earlier
Non-sensitive data
The Enclave for Attacker's Driver
App
Microsoft Defender
EPROCESS for Defender
Token structure
OS code
Driver
Drivers Loaded Earlier
Non-sensitive data
MemoryRanger


2) Unpack & launch a malware
Microsoft Defender fails to remove the malware
1) Disable Microsoft Defender
App
Microsoft Defender
EPROCESS for Defender
Token structure
OS code
Driver
Drivers Loaded Earlier
Non-sensitive data
The Default Enclave
App
Microsoft Defender
EPROCESS for Defender
Token structure
OS code
Driver
Drivers Loaded Earlier
Non-sensitive data
The malware has been removed
1) Fails to disable Defender
2) Unpack & launch a malware
The Enclave for Attacker's Driver
App
Microsoft Defender
EPROCESS for Defender
Token structure
OS code
Driver
Drivers Loaded Earlier
Non-sensitive data
MemoryRanger

CONCLUSION

1. Kernel-mode threats are very dangerous even for Windows 11 x64
2. The global malware trend is to bypass or disable security products without terminating the AV/EDR apps
3. Microsoft Defender is the most desired goal for attackers
4. Mandatory Integrity Control (MIC) is designed to sandbox untrusted apps, but attackers can abuse MIC to sandbox Microsoft Defender and other AVs.
5. MemoryRanger blocks attacks on kernel data including attacks on MIC

Thank you!

Denis Pogonin denpog00@gmail.com
Igor Korkin igor.korkin@gmail.com

All the details are here igorkorkin.blogspot.com