Orange
Cyberdefense

Aveugler les EDR avec le WFP

Florian Audon

Pentester

Barbhack - 31.08.2024

Whoami

Florian Audon

Pentester @ Orange Cyberdefense Switzerland

Organisation Insomni’hack

Intéressé par

- Windows
- AV / EDR

Sommaire

1. Le Windows Filtering Plateform (WFP)
2. Deux types d'EDR
3. Isolé, vraiment ?
4. Détections

Le Windows Filtering Plateform (WFP)

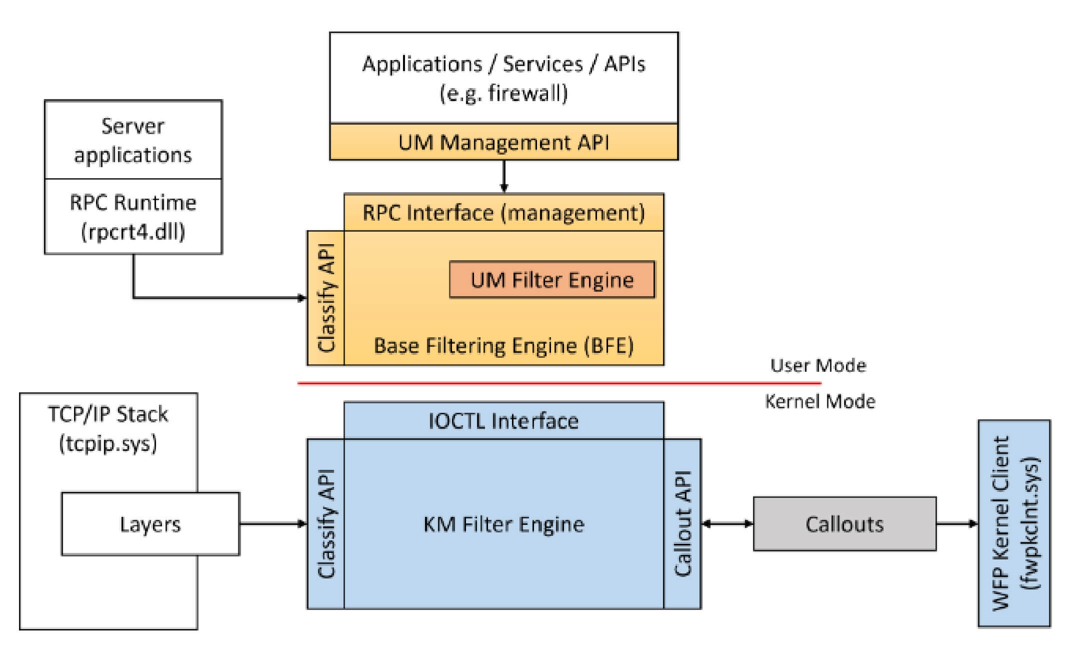
- Aucun firewall avant XP SP2
  - Hooking NDIS (Network Driver Interface Specification) driver (kernel)
  - Hook Winsock SPI (userland)

- Introduit avec Vista

Le Windows Filtering Plateform (WFP)

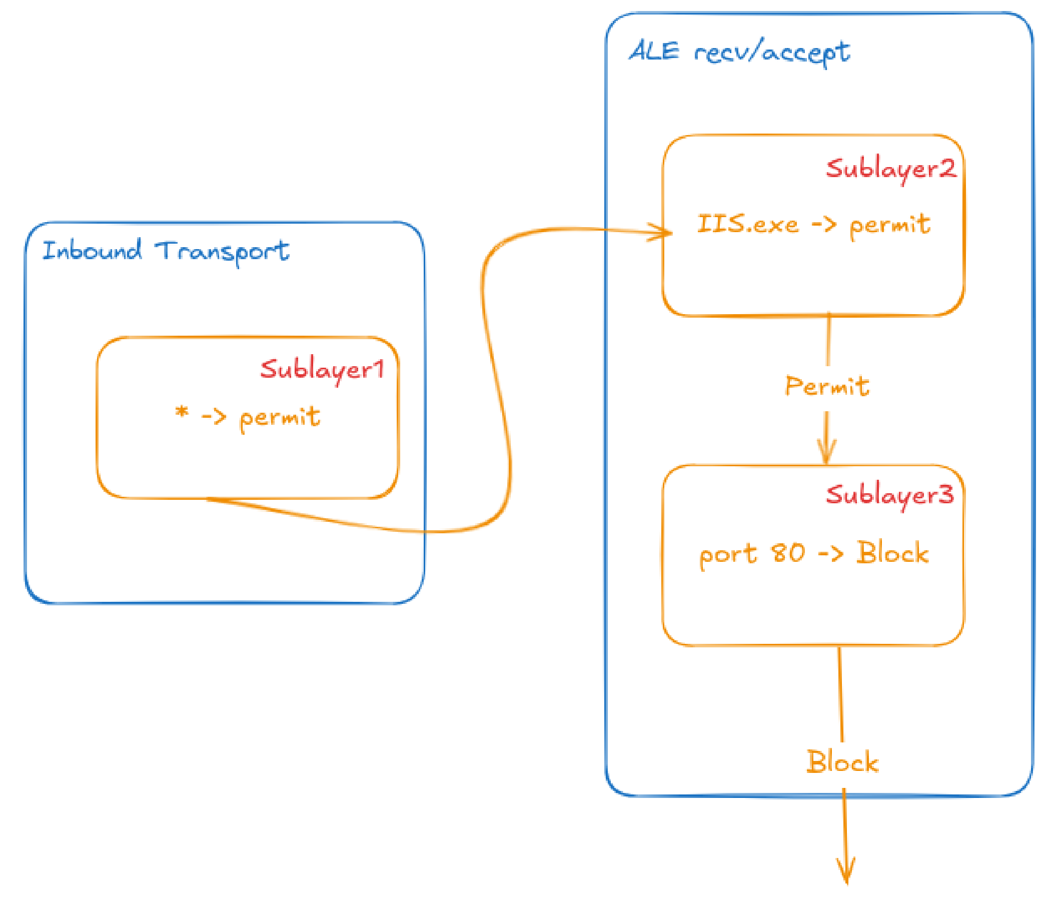
- Ensemble d’API pour contrôler le firewall

- Utilisé par:
  - IPS
  - AV
  - EDRs
  - Outils de monitoring
  - Contrôle parental



Le Windows Filtering Plateform (WFP)

- Les “filters”: Règle
- Les “layers”: Point d’inspection
- Les “sublayers”: Container
- Block > permit

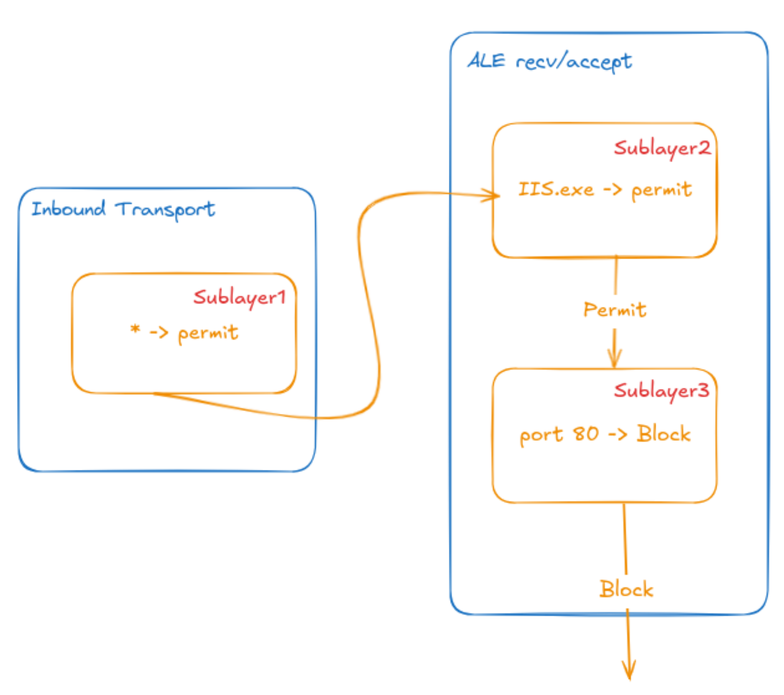


Le Windows Filtering Plateform (WFP)

- Block > permit
- FWPM_FILTER_FLAG_CLEAR_ACTION_RIGHT
  - Les décisions peuvent être “hard” ou “soft”
- Callout
  - Terminating (veto)
  - Unkown
  - Inspection

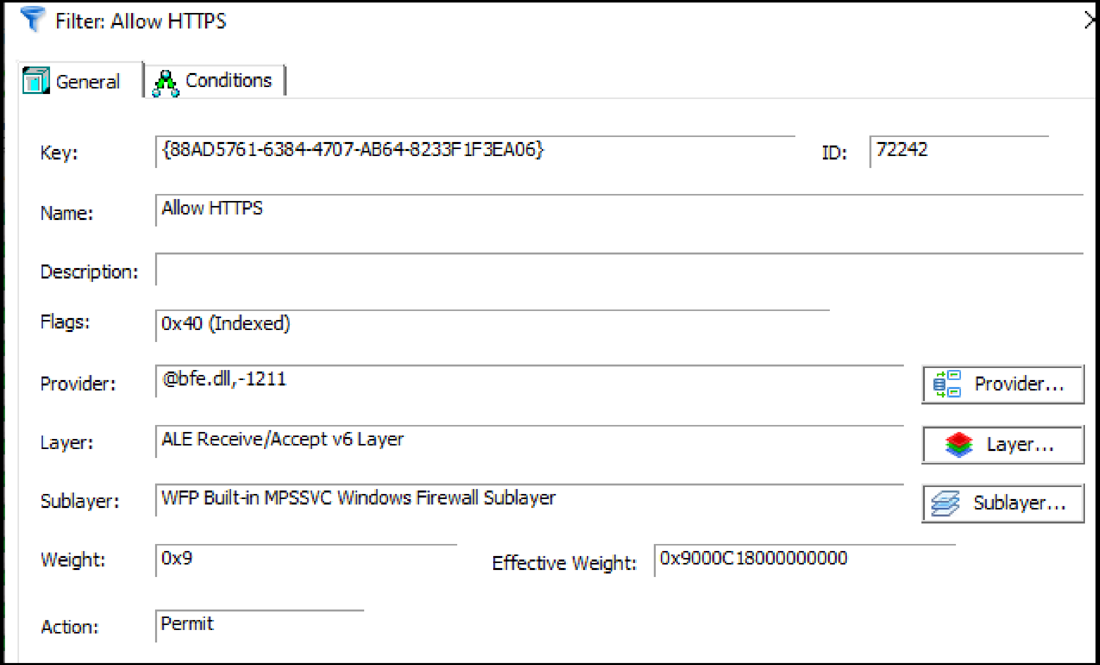
Le Windows Filtering Plateform (WFP)

- Points clés:
  - Sublayer avec une seul régle
  - FWPM_FILTER_FLAG_CLEAR_ACTION_RIGHT
  - Veto



Le Windows Filtering Plateform (WFP)

- Example avec une règle du firewall Windows



Key: {88AD5761-6384-4707-AB64-8233F1F3EA06}
ID: 72242

Name: Allow HTTPS

Description:

Flags: 0x40 (Indexed)

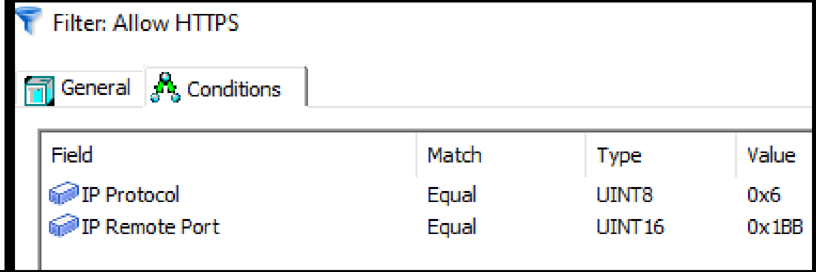
Provider: @bfe.dll,-1211

Layer: ALE Receive/Accept v6 Layer

Sublayer: WFP Built-in MPSSVC Windows Firewall Sublayer

Weight: 0x9
Effective Weight: 0x9000C18000000000

Action: Permit



Field	Match	Type	Value
IP Protocol	Equal	UINT8	0x6
IP Remote Port	Equal	UINT16	0x1BB

Le Windows Filtering Plateform (WFP)

- 05/21: Premier outil: shutter
- 09/23: Fireblock de Nighthawk
- 12/23: Outils publique reprenant la description de Fireblock

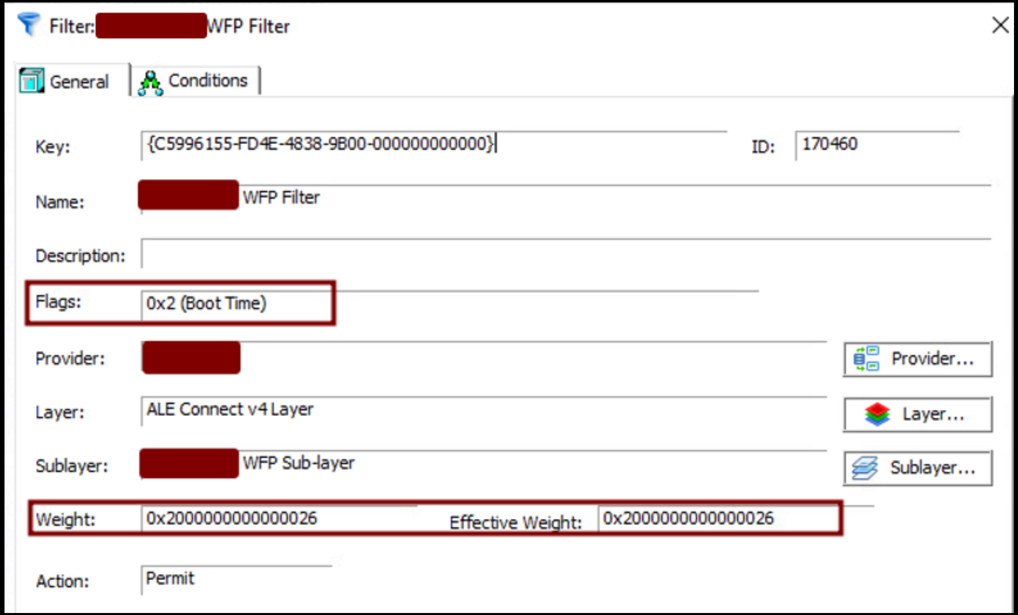
Deux types d’EDR

- Intelligence en local
  - ⊕ Fiable si isolé d’Internet
  - ⊖ Vulnérable au reverse

- Intelligence dans le cloud
  - ⊕ Résistant au reverse
  - ⊖ Efficacité réduite si coupé d’Internet

Deux types d’EDR

- Flag Clear Action Right
- Poids maximum pas utilisé



Filter: [redacted] WFP Filter

Key: {C5996155-FD4E-4838-9B00-000000000000}
ID: 170460

Name: [redacted] WFP Filter

Description:

Flags: 0x2 (Boot Time)

Provider: [redacted]

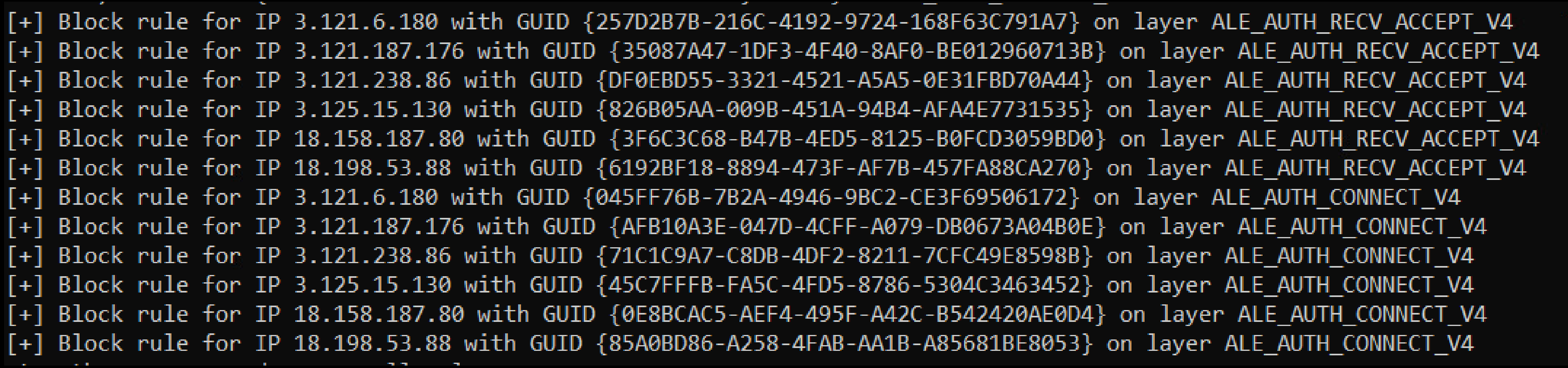
Layer: ALE Connect v4 Layer

Sublayer: [redacted] WFP Sub-layer

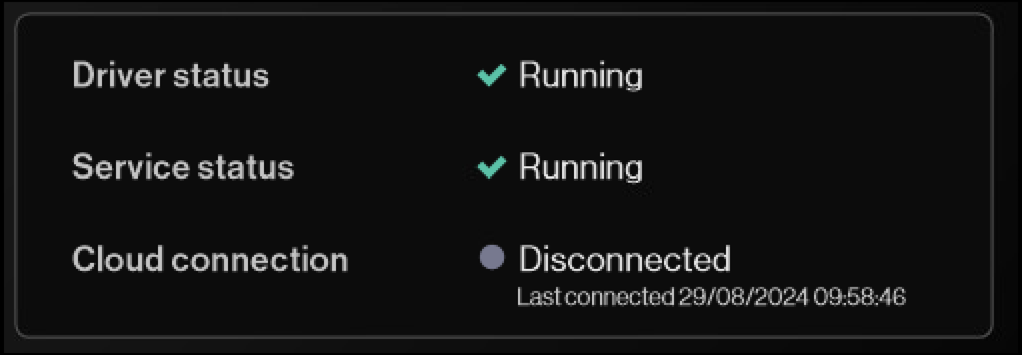
Weight: 0x2000000000000026
Effective Weight: 0x2000000000000026

Action: Permit

Deux types d’EDR



```
[+] Block rule for IP 3.121.6.180 with GUID {257D2B7B-216C-4192-9724-168F63C791A7} on layer ALE_AUTH_RECV_ACCEPT_V4
[+] Block rule for IP 3.121.187.176 with GUID {35087A47-1DF3-4F40-8AF0-BE012960713B} on layer ALE_AUTH_RECV_ACCEPT_V4
[+] Block rule for IP 3.121.238.86 with GUID {DF0EBD55-3321-4521-A5A5-0E31FBD70A44} on layer ALE_AUTH_RECV_ACCEPT_V4
[+] Block rule for IP 3.125.15.130 with GUID {826B05AA-009B-451A-94B4-AFA4E7731535} on layer ALE_AUTH_RECV_ACCEPT_V4
[+] Block rule for IP 18.158.187.80 with GUID {3F6C3C68-B47B-4ED5-8125-B0FCD3059BD0} on layer ALE_AUTH_RECV_ACCEPT_V4
[+] Block rule for IP 18.198.53.88 with GUID {6192BF18-8894-473F-AF7B-457FA88CA270} on layer ALE_AUTH_RECV_ACCEPT_V4
[+] Block rule for IP 3.121.6.180 with GUID {045FF76B-7B2A-4946-9BC2-CE3F69506172} on layer ALE_AUTH_CONNECT_V4
[+] Block rule for IP 3.121.187.176 with GUID {AFB10A3E-047D-4CFF-A079-DB0673A04B0E} on layer ALE_AUTH_CONNECT_V4
[+] Block rule for IP 3.121.238.86 with GUID {71C1C9A7-C8DB-4DF2-8211-7CFC49E8598B} on layer ALE_AUTH_CONNECT_V4
[+] Block rule for IP 3.125.15.130 with GUID {45C7FFFB-FA5C-4FD5-8786-5304C3463452} on layer ALE_AUTH_CONNECT_V4
[+] Block rule for IP 18.158.187.80 with GUID {0E8BCAC5-AEF4-495F-A42C-B542420AE0D4} on layer ALE_AUTH_CONNECT_V4
[+] Block rule for IP 18.198.53.88 with GUID {85A0BD86-A258-4FAB-AA1B-A85681BE8053} on layer ALE_AUTH_CONNECT_V4
```



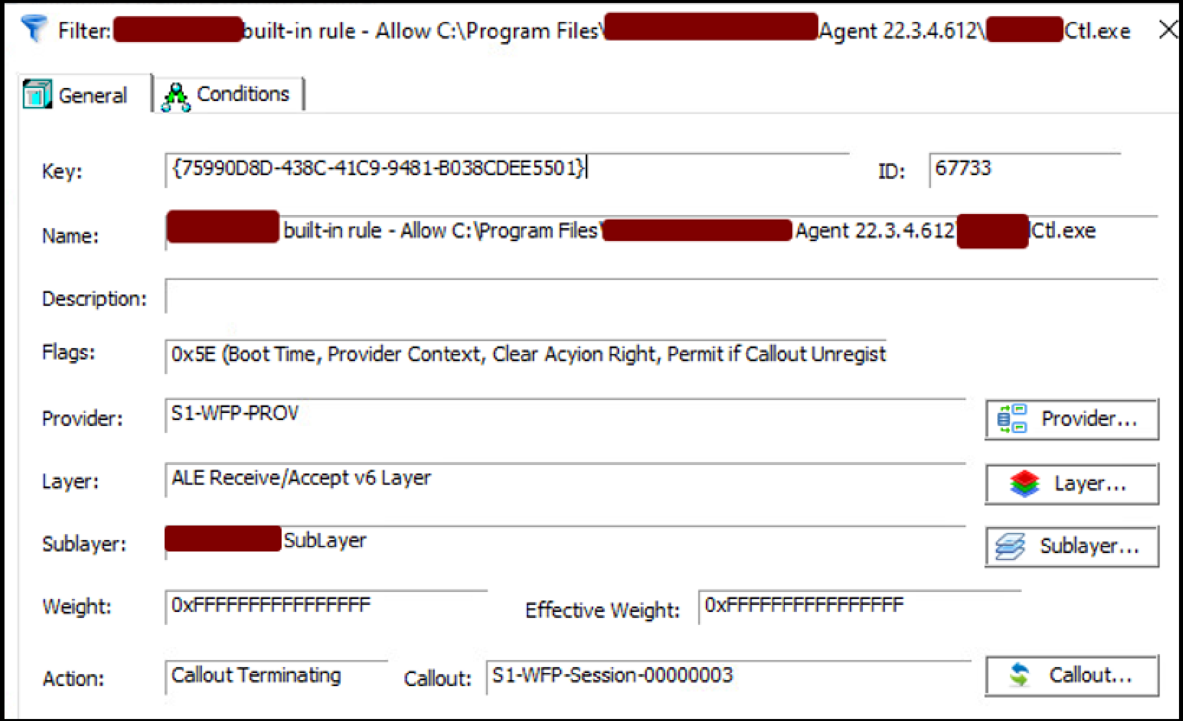
Driver status ✓ Running

Service status ✓ Running

Cloud connection ● Disconnected
Last connected 29/08/2024 09:58:46

Deux types d’EDR

- Callout



Filter: [redacted]built-in rule - Allow C:\Program Files\[redacted]Agent 22.3.4.612\[redacted]Ctl.exe

Key: {75990D8D-438C-41C9-9481-B038CDEE5501}

ID: 67733

Name: [redacted]built-in rule - Allow C:\Program Files\[redacted]Agent 22.3.4.612[redacted]Ctl.exe

Description:

Flags: 0x5E (Boot Time, Provider Context, Clear Acyion Right, Permit if Callout Unregist

Provider: S1-WFP-PROV

Layer: ALE Receive/Accept v6 Layer

Sublayer: [redacted]SubLayer

Weight: 0xFFFFFFFFFFFFFFFF

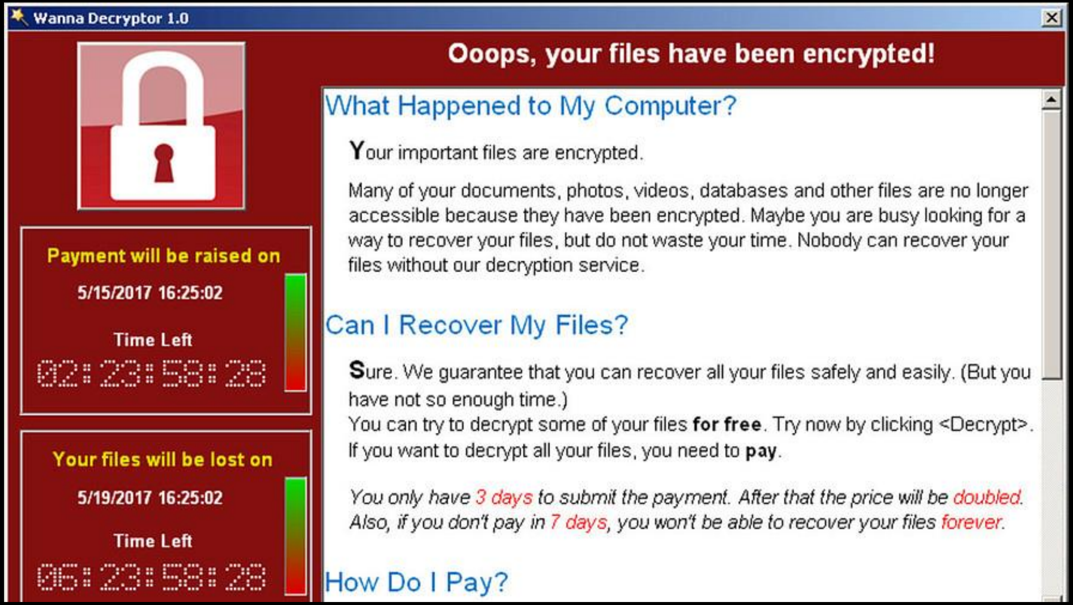
Effective Weight: 0xFFFFFFFFFFFFFFFF

Action: Callout Terminating

Callout: S1-WFP-Session-00000003

Isolé, vraiment ?

- Isolation lors d’un incident



Ooops, your files have been encrypted!

Payment will be raised on

5/15/2017 16:25:02

Time Left

02:23:58:28

Your files will be lost on

5/19/2017 16:25:02

Time Left

06:23:58:28

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

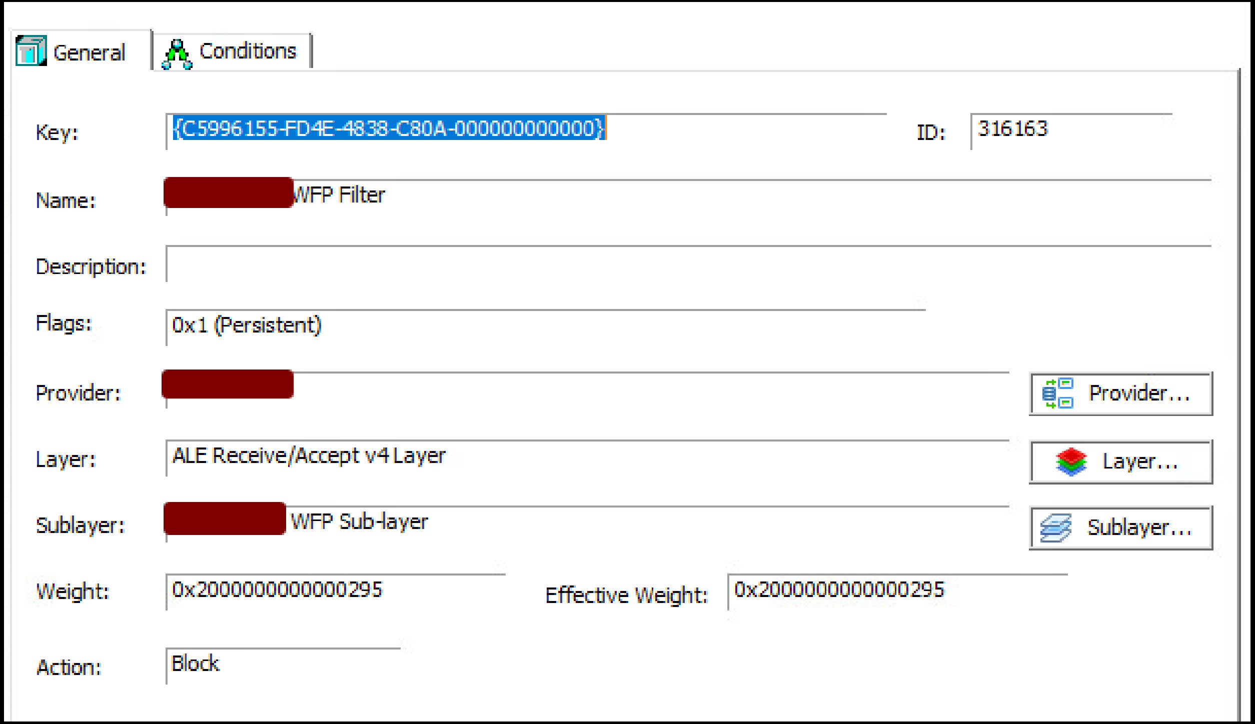
Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

*You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.*

How Do I Pay?

Isolé, vraiment ?

- Flag Clear Action Right
- Poids maximum pas utilisé



Key: {C5996155-FD4E-4838-C80A-000000000000} ID: 316163

Name: [redacted]WFP Filter

Description:

Flags: 0x1 (Persistent)

Provider: [redacted]

Layer: ALE Receive/Accept v4 Layer

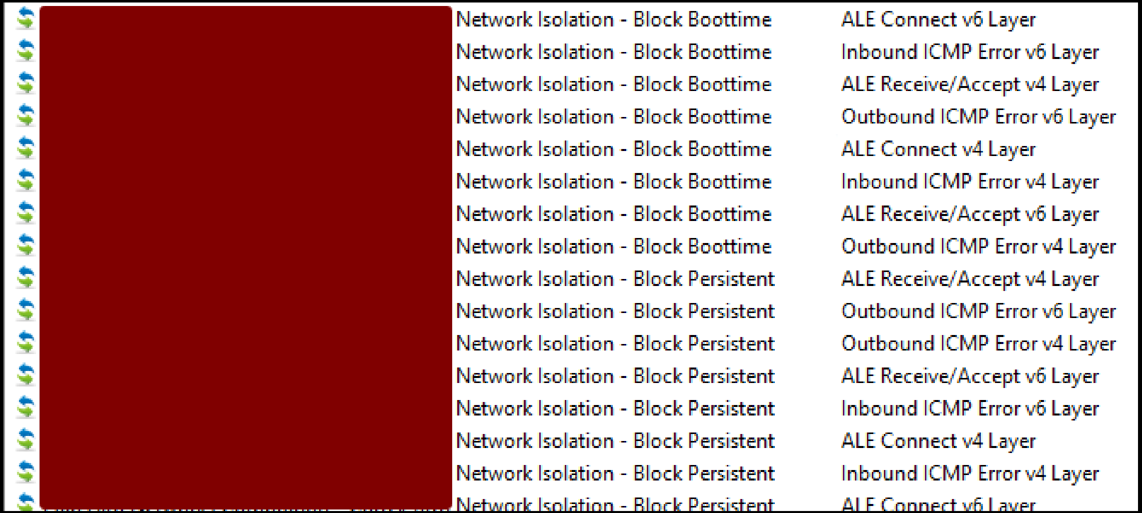
Sublayer: [redacted] WFP Sub-layer

Weight: 0x2000000000000295 Effective Weight: 0x2000000000000295

Action: Block

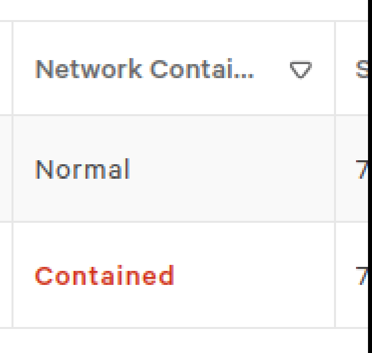
Isolé, vraiment ?

- Callout

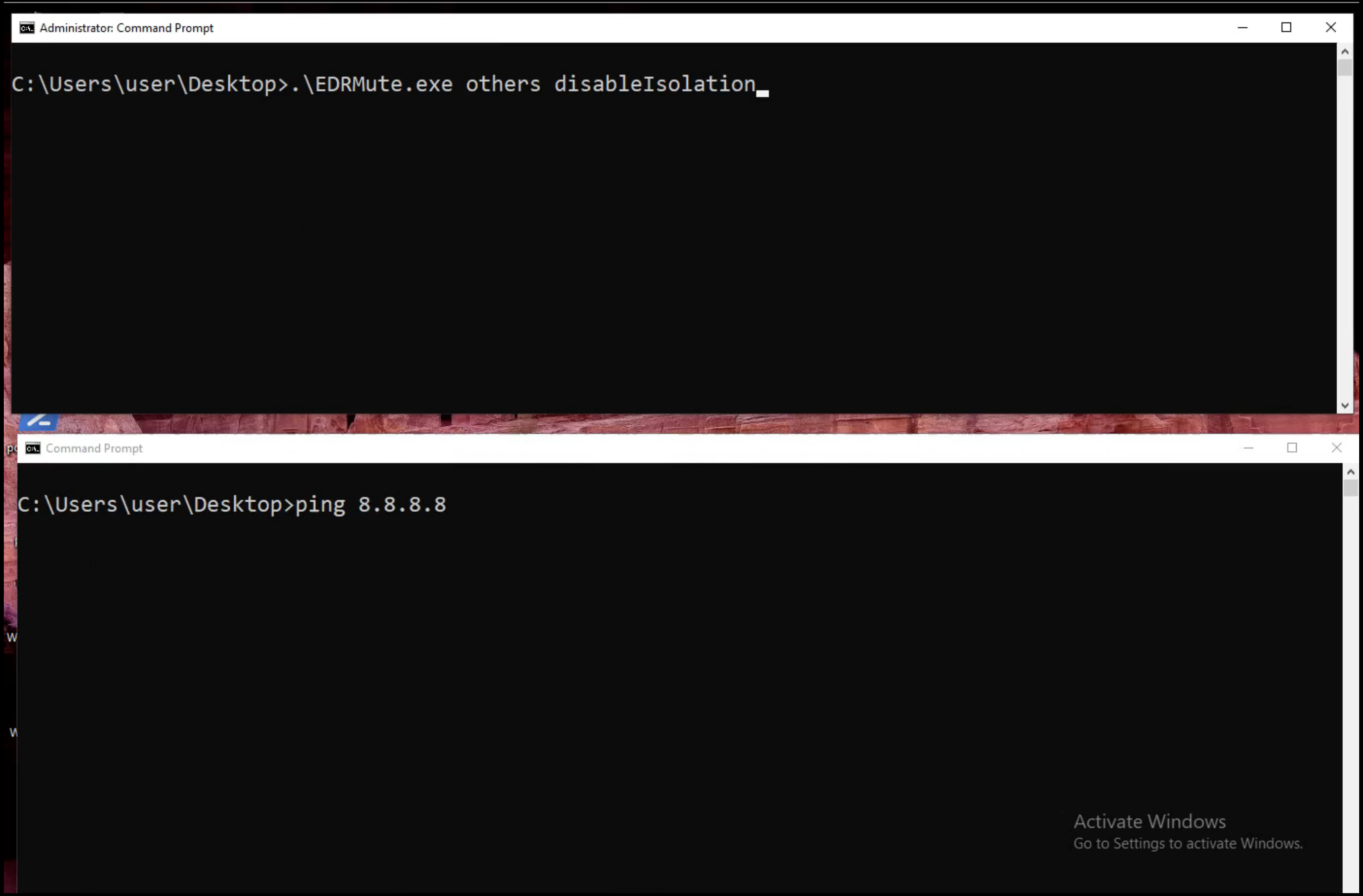


⇄	[redacted]	Network Isolation - Block Boottime	ALE Connect v6 Layer
⇄	[redacted]	Network Isolation - Block Boottime	Inbound ICMP Error v6 Layer
⇄	[redacted]	Network Isolation - Block Boottime	ALE Receive/Accept v4 Layer
⇄	[redacted]	Network Isolation - Block Boottime	Outbound ICMP Error v6 Layer
⇄	[redacted]	Network Isolation - Block Boottime	ALE Connect v4 Layer
⇄	[redacted]	Network Isolation - Block Boottime	Inbound ICMP Error v4 Layer
⇄	[redacted]	Network Isolation - Block Boottime	ALE Receive/Accept v6 Layer
⇄	[redacted]	Network Isolation - Block Boottime	Outbound ICMP Error v4 Layer
⇄	[redacted]	Network Isolation - Block Persistent	ALE Receive/Accept v4 Layer
⇄	[redacted]	Network Isolation - Block Persistent	Outbound ICMP Error v6 Layer
⇄	[redacted]	Network Isolation - Block Persistent	Outbound ICMP Error v4 Layer
⇄	[redacted]	Network Isolation - Block Persistent	ALE Receive/Accept v6 Layer
⇄	[redacted]	Network Isolation - Block Persistent	Inbound ICMP Error v6 Layer
⇄	[redacted]	Network Isolation - Block Persistent	ALE Connect v4 Layer
⇄	[redacted]	Network Isolation - Block Persistent	Inbound ICMP Error v4 Layer
⇄	[redacted]	Network Isolation - Block Persistent	ALE Connect v6 Layer

Isolé, vraiment ?



Network Contai... ▽	S
Normal	7
Contained	7



Administrator: Command Prompt

```
C:\Users\user\Desktop>.\EDRMute.exe others disableIsolation_
```

```
C:\Users\user\Desktop>ping 8.8.8.8
```

Activate Windows
Go to Settings to activate Windows.

Détections

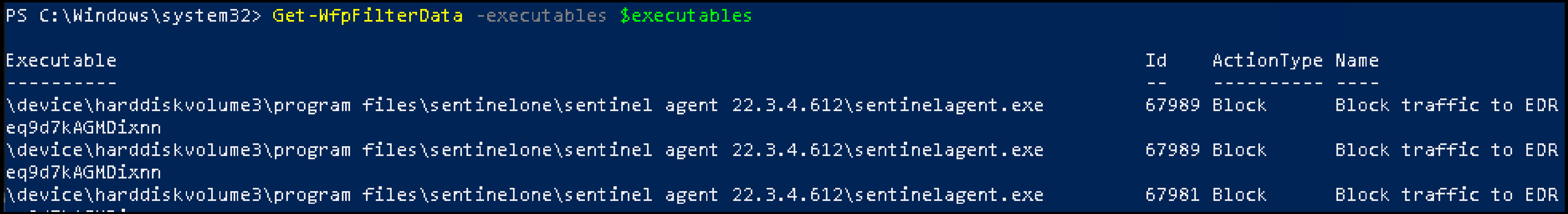
- Event ID

```
5446 : A Windows Filtering Platform callout has been changed.
5447 : A Windows Filtering Platform filter has been changed.
5448 : A Windows Filtering Platform provider has been changed.
5449 : A Windows Filtering Platform provider context has been changed.
5450 : A Windows Filtering Platform sub-layer has been changed.
```

- Hook
- Callout
- Verification d’intégrité

Détections

- https://github.com/amjcyber/EDRNoiseMaker



```
PS C:\Windows\system32> Get-WfpFilterData -executables $executables

Executable                                                                                            Id    ActionType Name
----------                                                                                            --    ---------- ----
\device\harddiskvolume3\program files\sentinelone\sentinel agent 22.3.4.612\sentinelagent.exe         67989 Block      Block traffic to EDR
eq9d7kAGMDixnn
\device\harddiskvolume3\program files\sentinelone\sentinel agent 22.3.4.612\sentinelagent.exe         67989 Block      Block traffic to EDR
eq9d7kAGMDixnn
\device\harddiskvolume3\program files\sentinelone\sentinel agent 22.3.4.612\sentinelagent.exe         67981 Block      Block traffic to EDR
```

Conclusion

- https://github.com/netero1010/EDRSilencer
- https://github.com/dsnezhkov/shutter
- Vulnérabilité dans des drivers WFP: https://github.com/senzee1984/EDRPrison

Orange
Cyberdefense

Merci !

Questions ?

orangecyberdefense.com

orange™