



# Dive Into WDAG

Yunhai Zhang



# ▶▶ Who am I

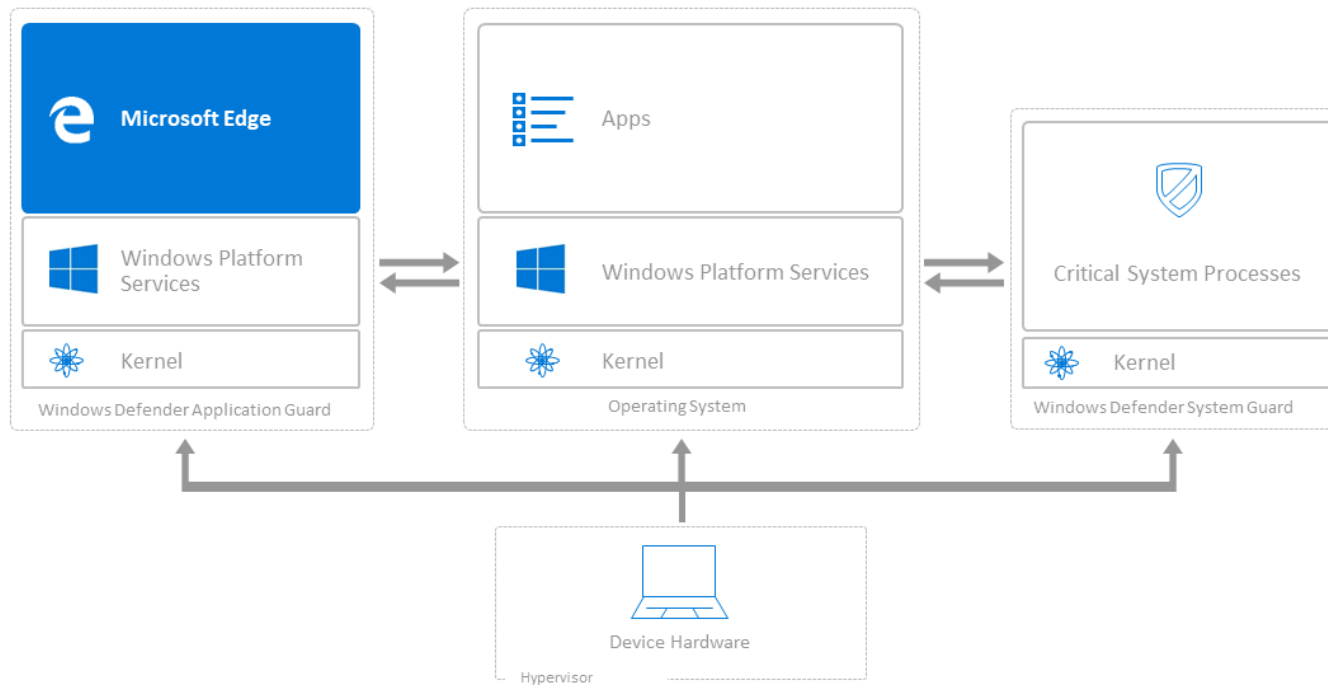
- ❑ Yunhai Zhang
- ❑ Twitter: @\_f0rgetting\_
- ❑ Researcher of NSFOCUS
- ❑ Winner of Mitigation Bypass Bounty: 2014 ~ 2018

# ▶▶ What is WDAG

- ❑ Windows Defender Application Guard
  - A security feature of Windows 10
  - Hardware isolation based on virtualization technology
  - Separate untrusted content from the host operating system
  - Keep the host safe and remove potential malware

# ▶▶ What is WDAG

## HARDWARE ISOLATION OF **MICROSOFT EDGE** WITH **WINDOWS DEFENDER APPLICATION GUARD**

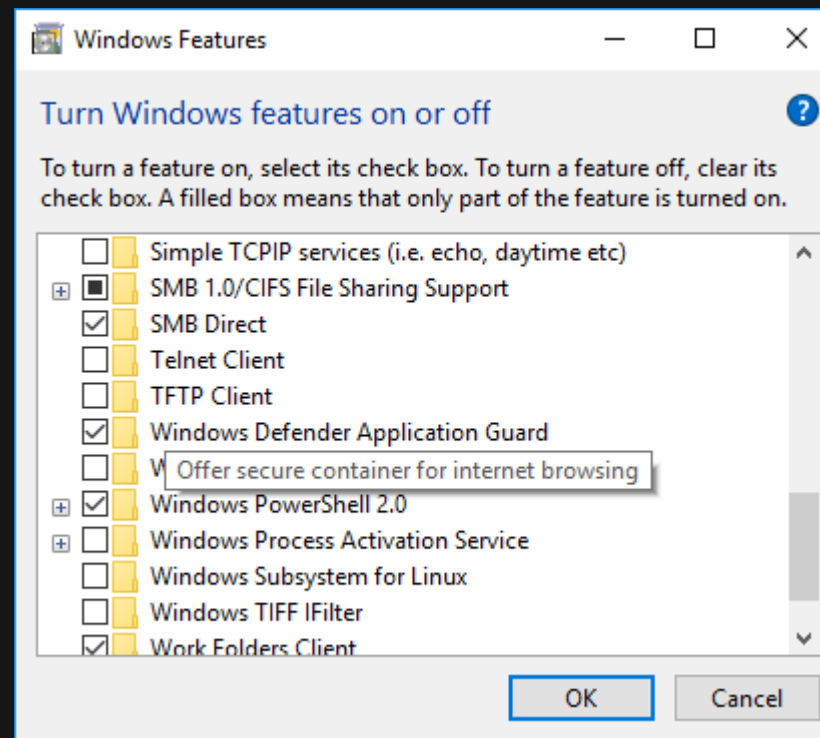


# ▶▶ How to use WDAG

## ❑ WDAG is not installed by default

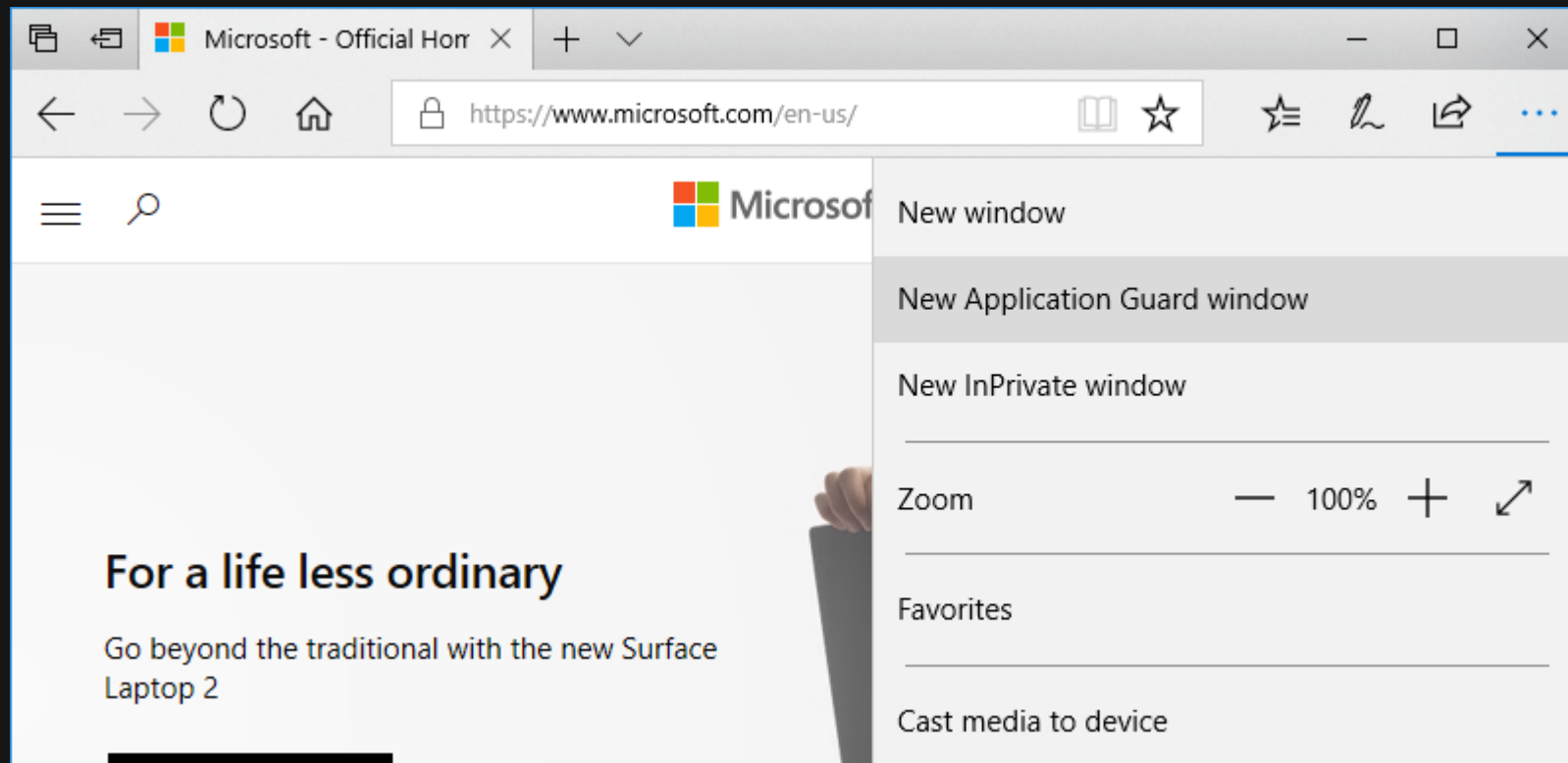
### • System Requirement

- Support SLAT and VT-x or AMD-V
- More than 4 CPU cores
- More than 8GB memory
- More than 5GB disk space



# ▶▶ How to use WDAG

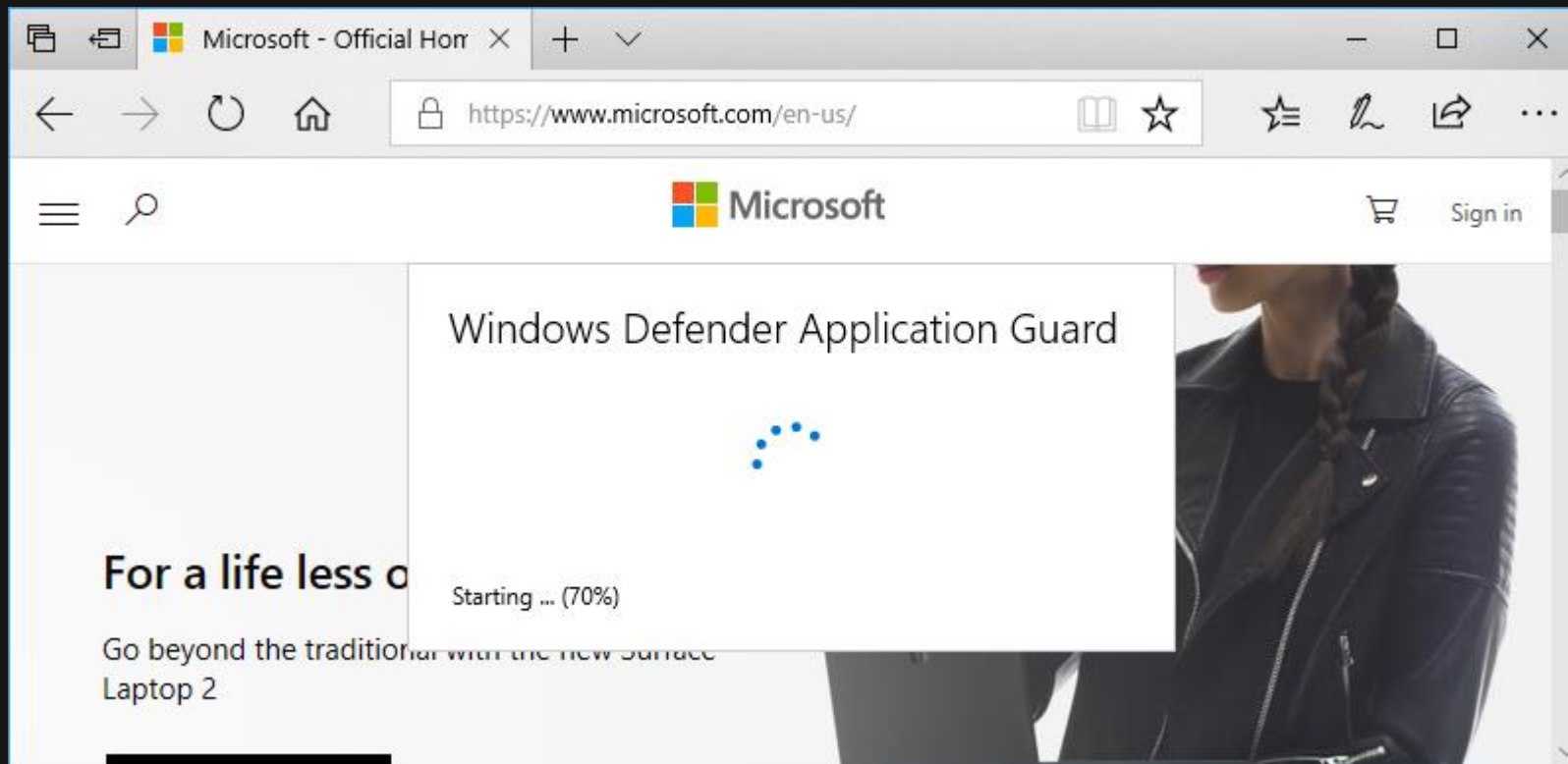
## ▣ New menu item in Microsoft Edge





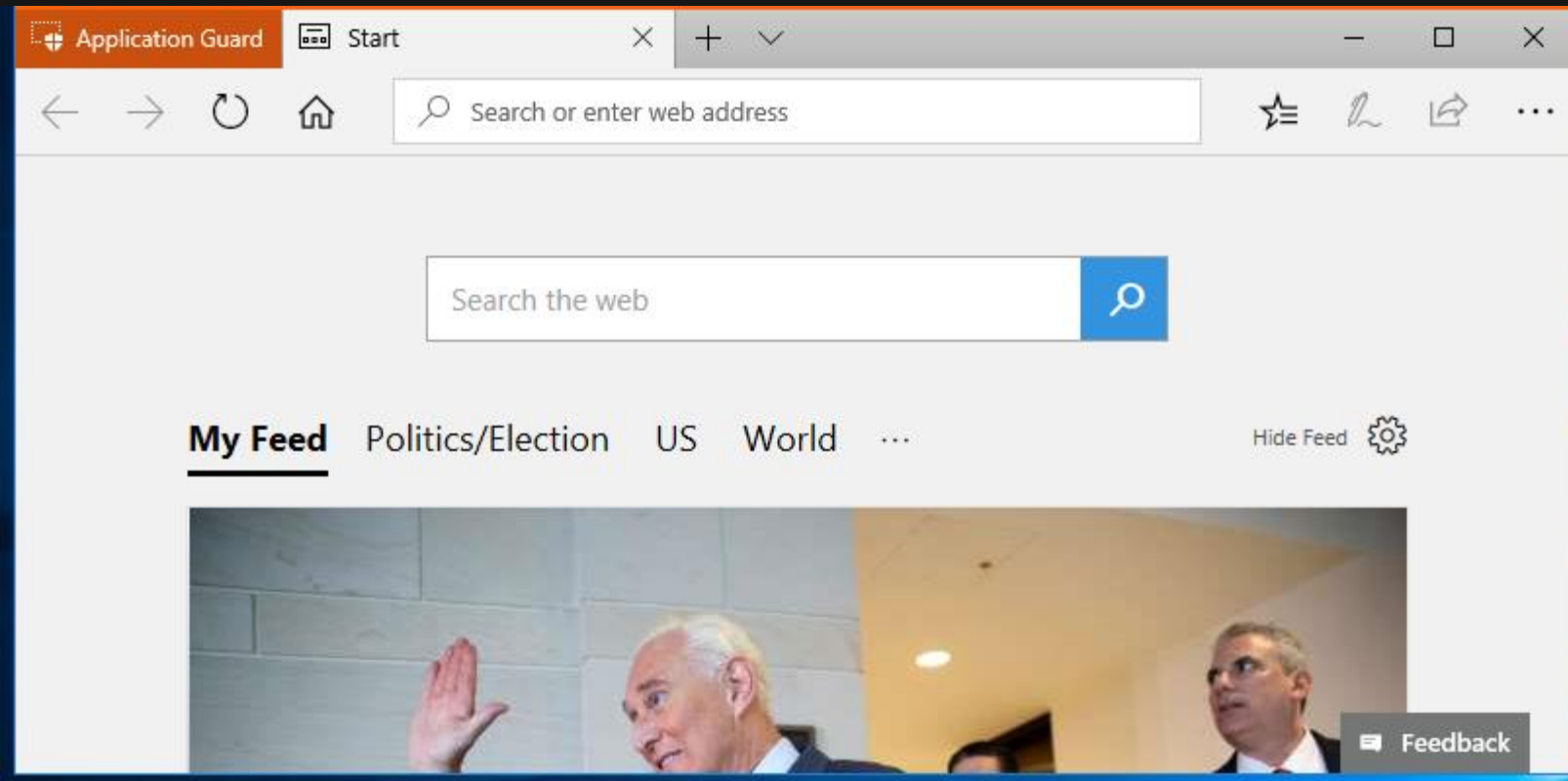
# ▶▶ How to use WDAG

## ▣ Starting WDAG



# ▶▶ How to use WDAG

## ▣ Microsoft Edge inside WDAG





# ▶▶ WDAG Architecture



MicrosoftEdge.exe



browser\_broker.exe



hvsimgr.exe



hvsirpcd.exe



hvsirdpclient.exe



svchost.exe

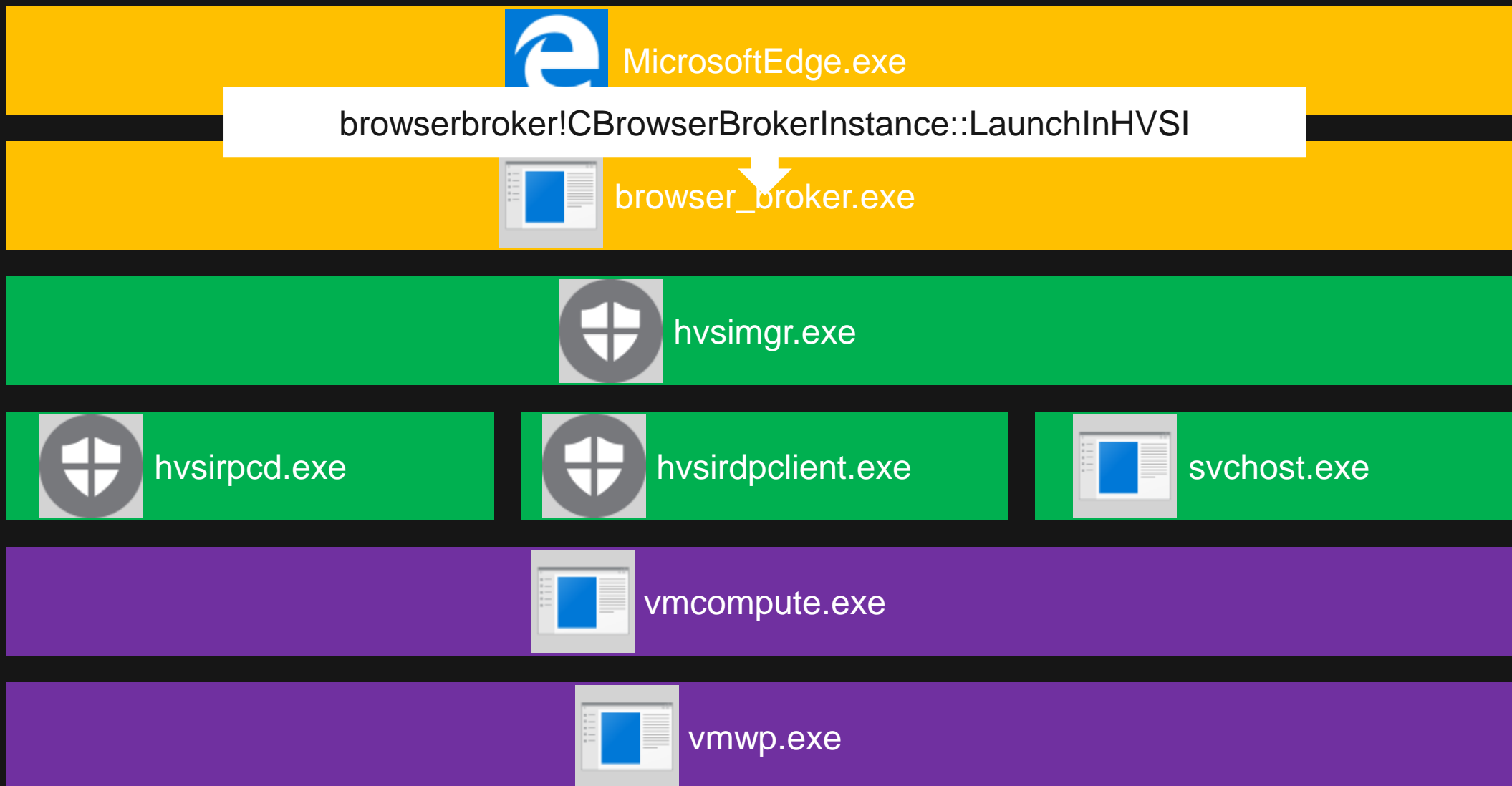


vmcompute.exe

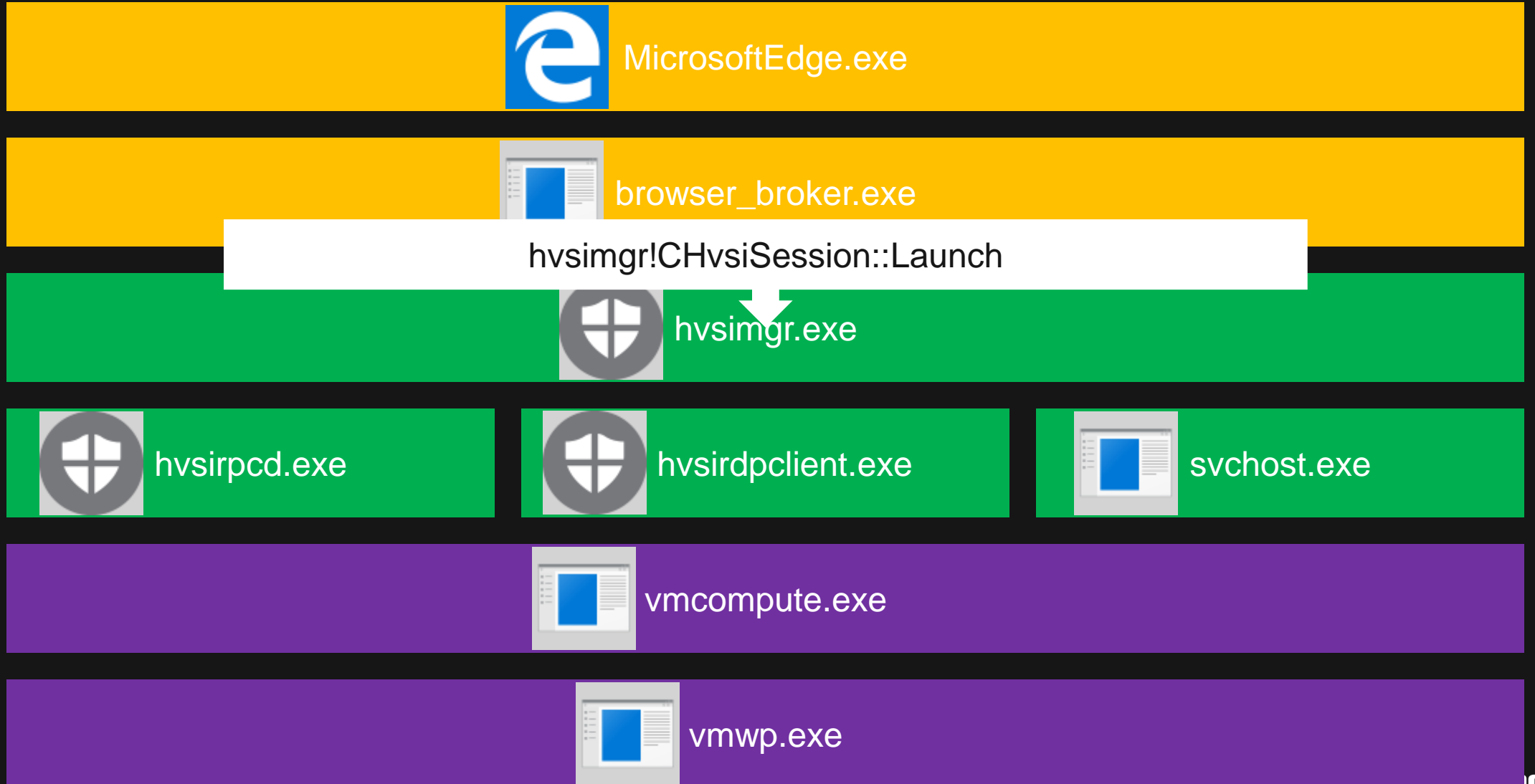


vmwp.exe

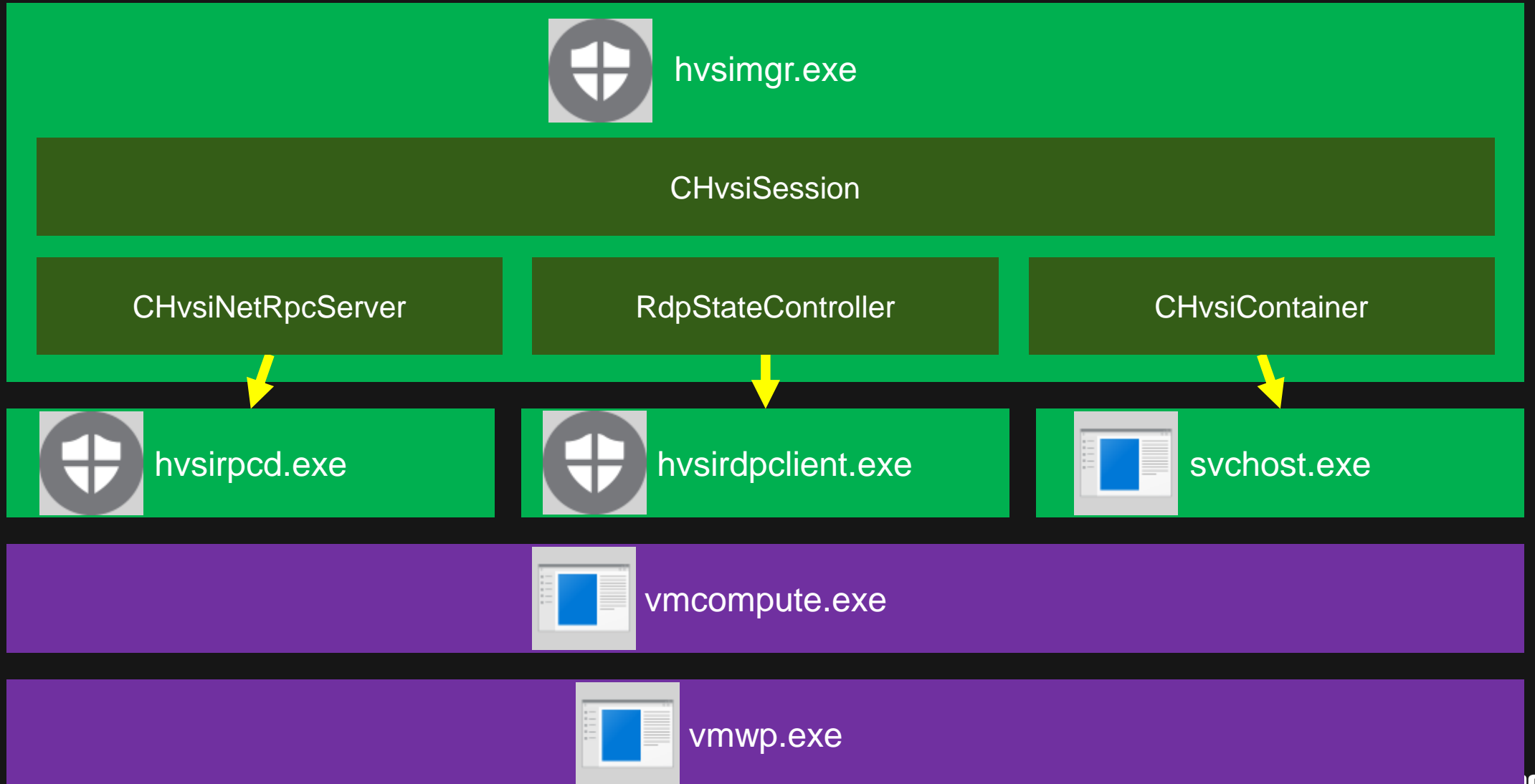
# ▶▶ WDAG Architecture



# ▶▶ WDAG Architecture



# ▶▶ WDAG Architecture



# ▶▶ WDAG Architecture



svchost.exe(Application Guard Container Service)

CHvsiContainerManager

CHvsiContainerServiceManager

CXenonManager

CXenonContainer

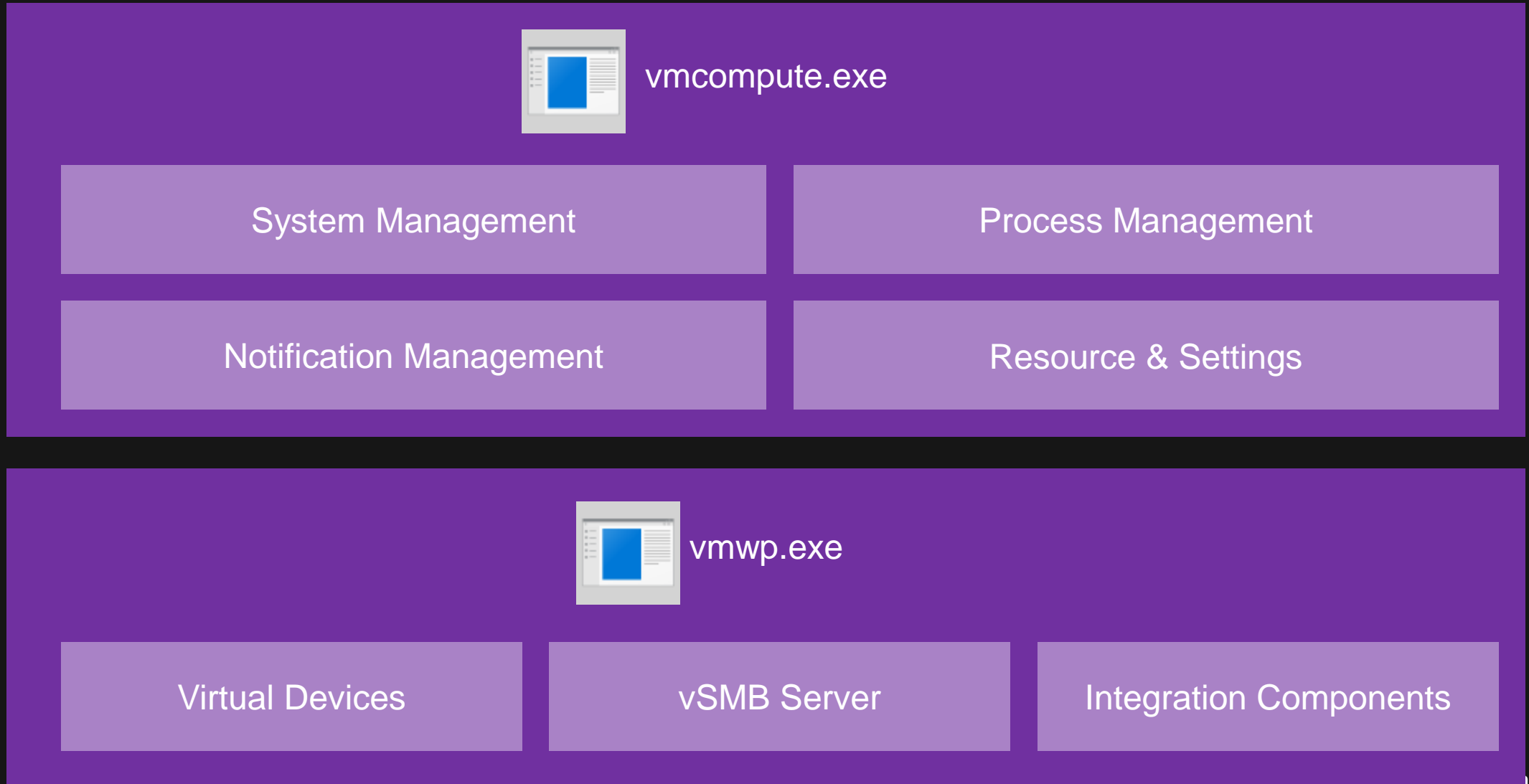


vmcompute.exe



vmwp.exe

# ▶▶ WDAG Architecture



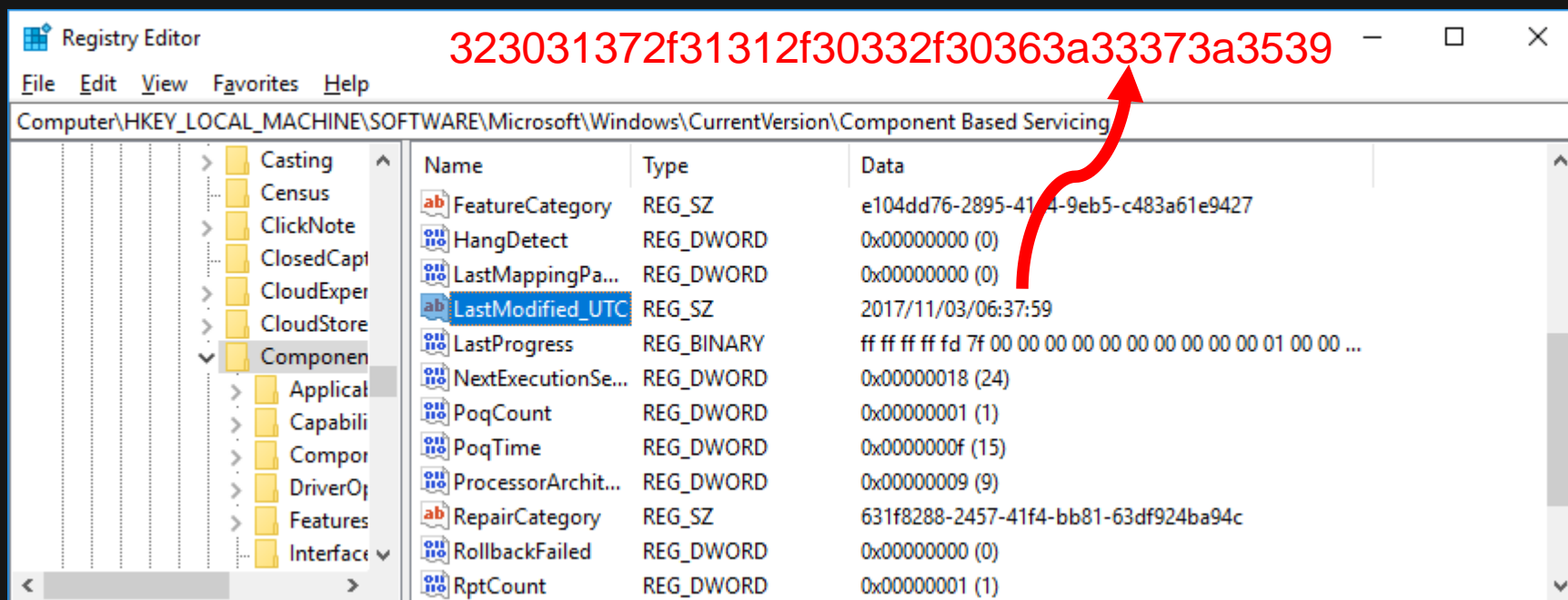


# ▶▶ WDAG Internals

## ❑ Terminology

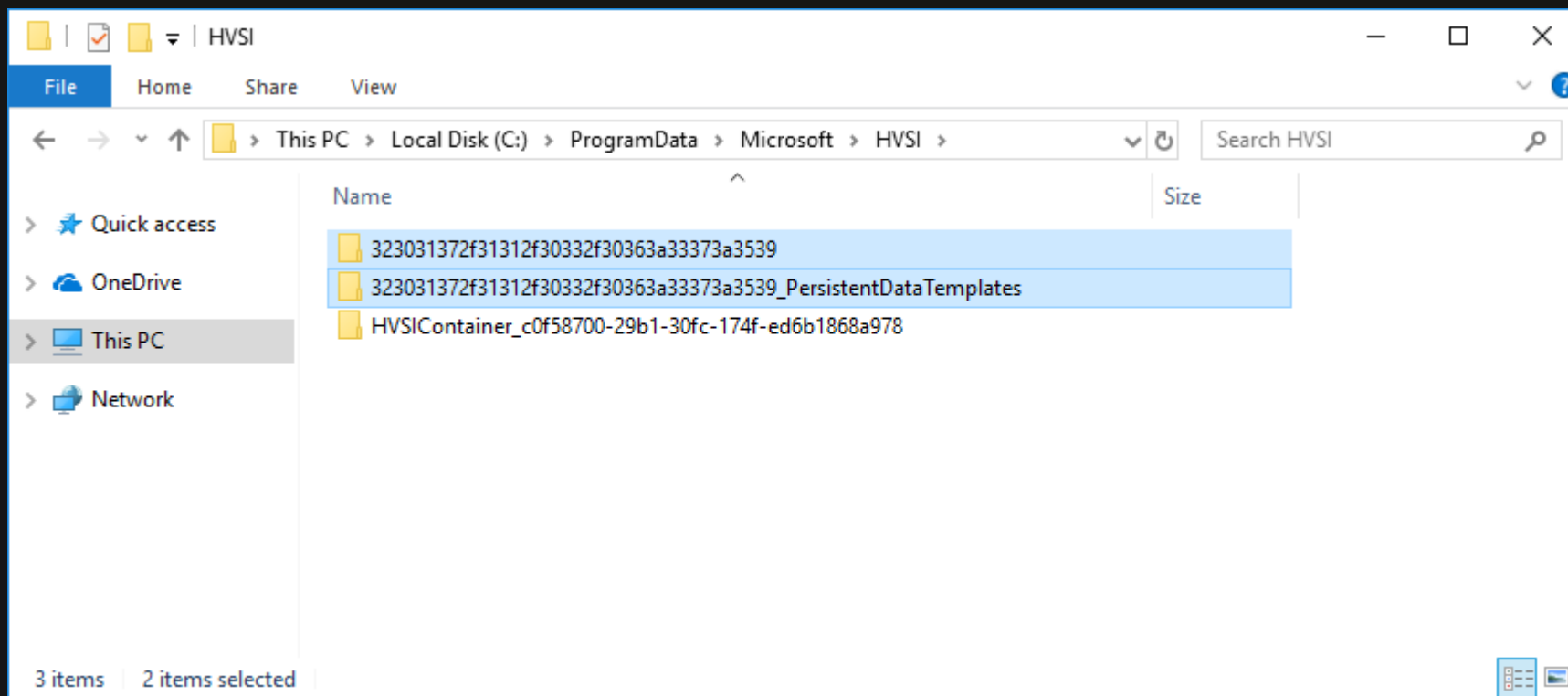
- Image Name

- Hex string of HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\LastModified\_UTC



# ▶▶ WDAG Internals

- ❑ Terminology
  - Image Name



# ▶▶ WDAG Internals

- Terminology
  - Container ID

**SHA256(**

Computer Name

User Sid

**)**

# ▶▶ WDAG Internals

## ❑ Terminology

- Container ID

SHA256(

Computer Name

User Sid

)

DESKTOP-7R43750

# ▶▶ WDAG Internals

- Terminology
  - Container ID

SHA256(

Computer Name

User Sid

)

S-1-5-21-2036491302-699820345-3847261429-1001

# ▶▶ WDAG Internals

## □ Terminology

- Container ID

SHA256(

Computer Name

User Sid

)

DESKTOP-7R43750S-1-5-21-2036491302-699820345-3847261429-1001



# ▶▶ WDAG Internals

- Terminology
  - Container ID

**SHA256(**

Computer Name

User Sid

**)**

DESKTOP-7R43750S-1-5-21-2036491302-699820345-3847261429-1001

SHA256

c0f58700-29b1-30fc-174f-ed6b1868a978

# ▶▶ WDAG Internals

- Terminology
  - Container Name

HVSIContainer\_

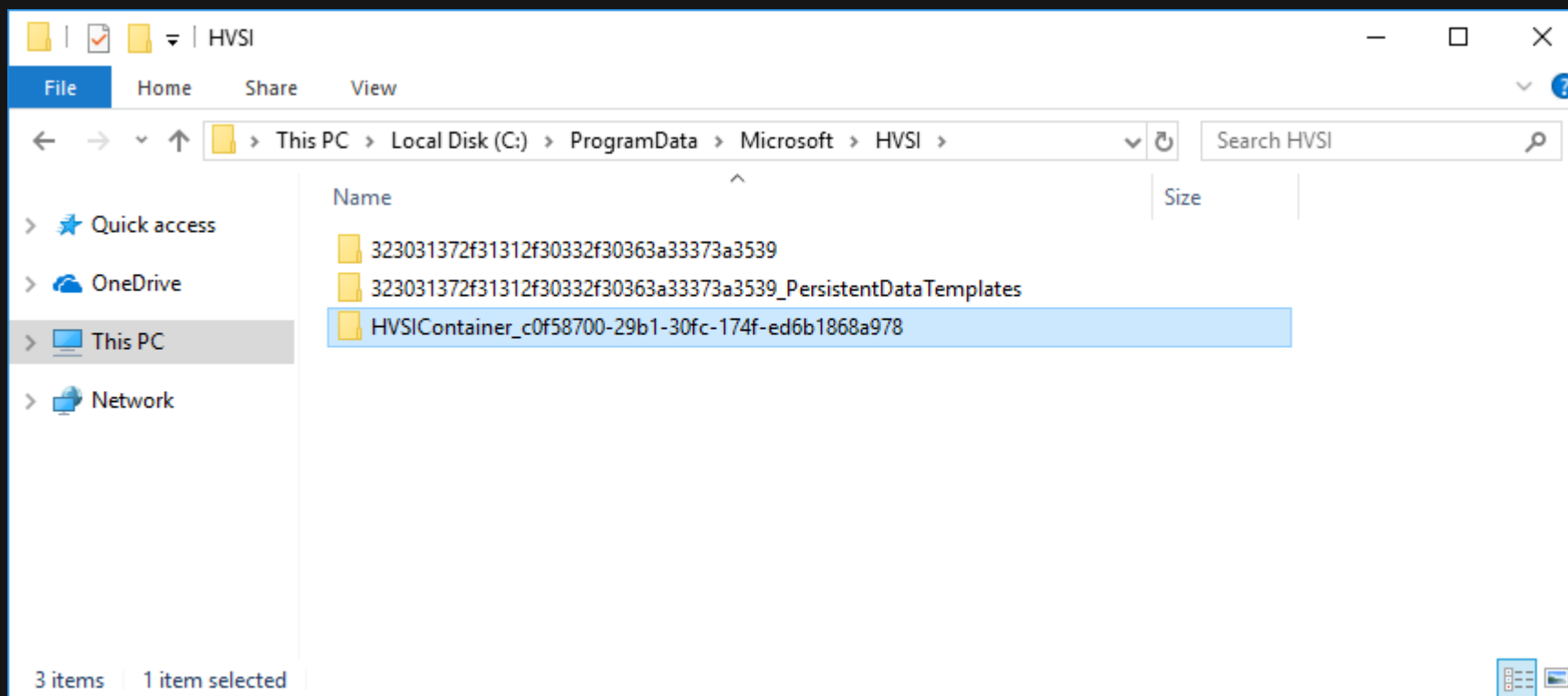
Container ID

HVSIContainer\_c0f58700-29b1-30fc-174f-ed6b1868a978

# ▶▶ WDAG Internals

## ❑ Terminology

- Container Name



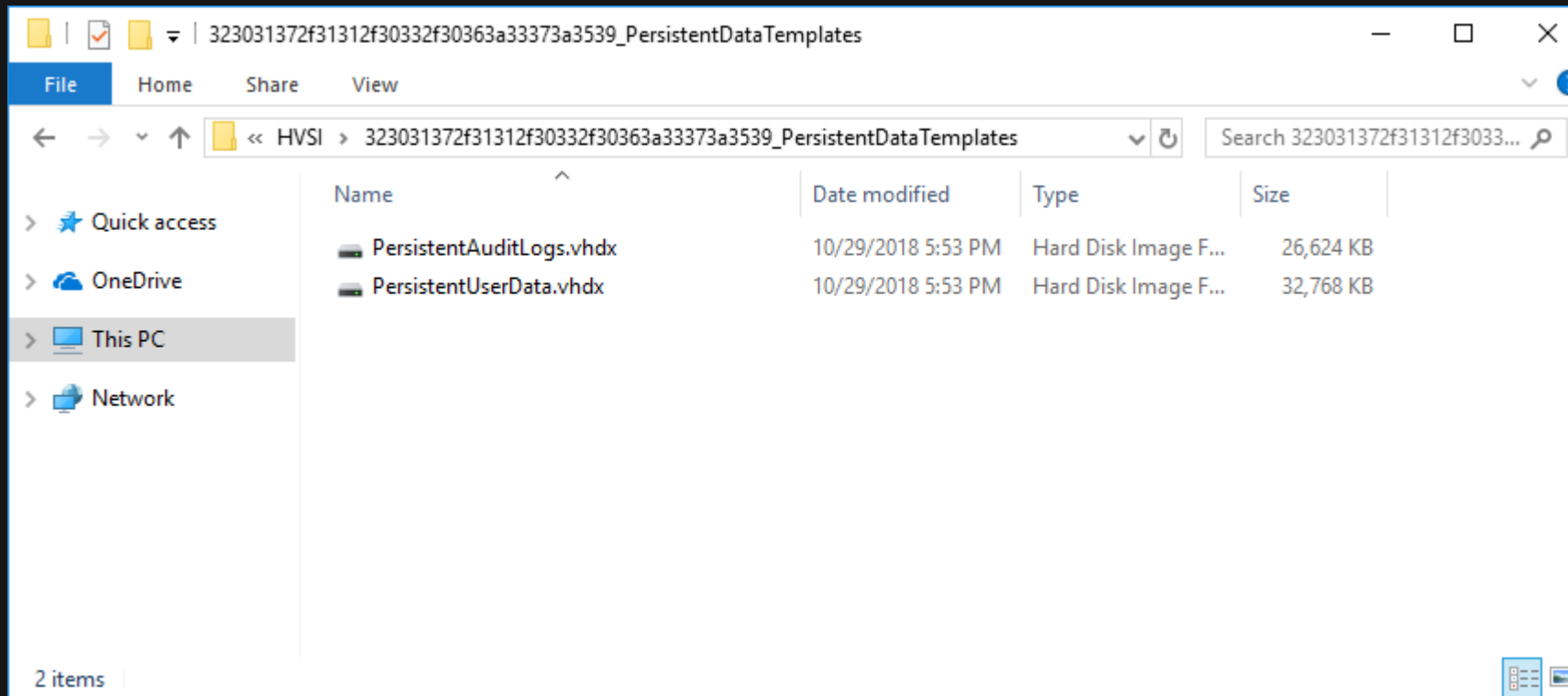
# ▶▶ WDAG Internals

## □ Terminology

- Runtime ID
  - Dynamic generated GUID for container instance
  - Generated each time when container is created

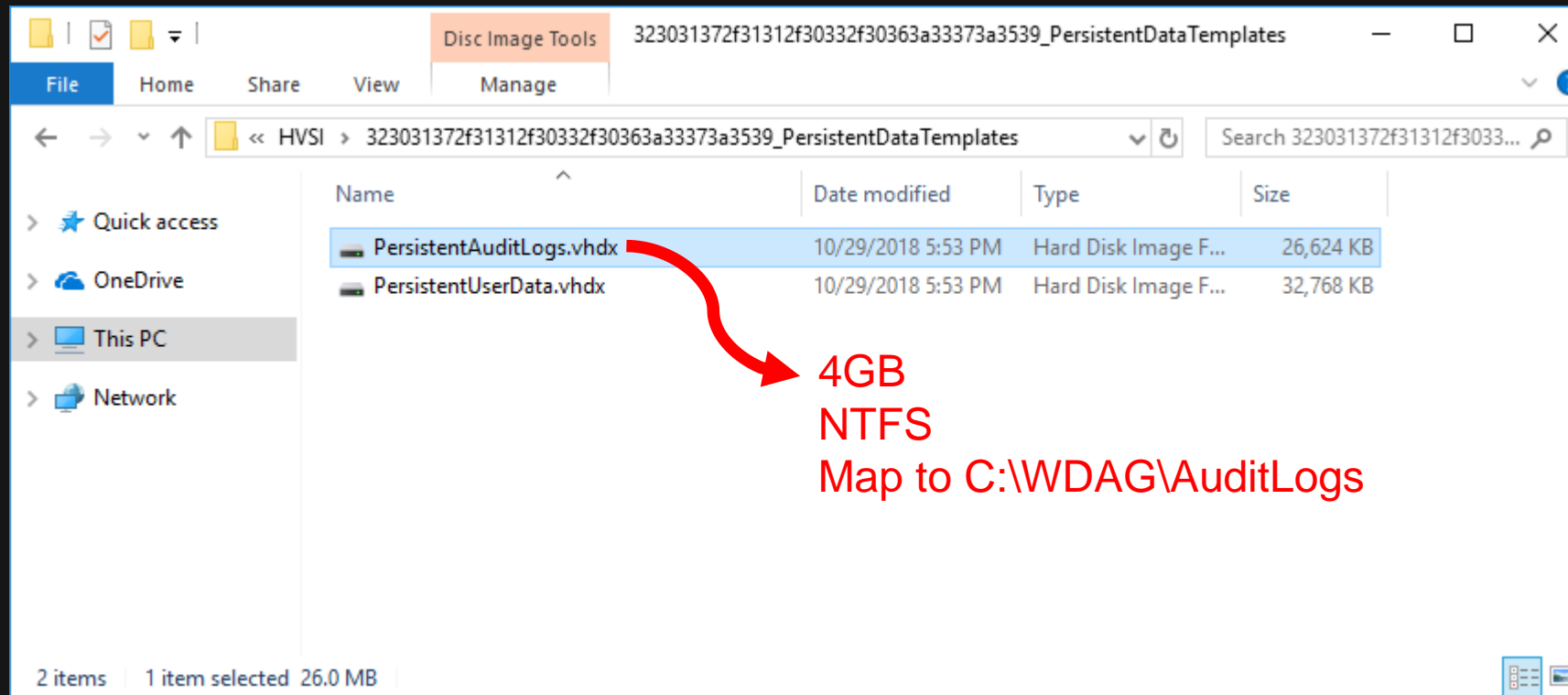
# ▶▶ WDAG Internals

- How is the container created
  - Create Template Persistent Data Stores



# ▶▶ WDAG Internals

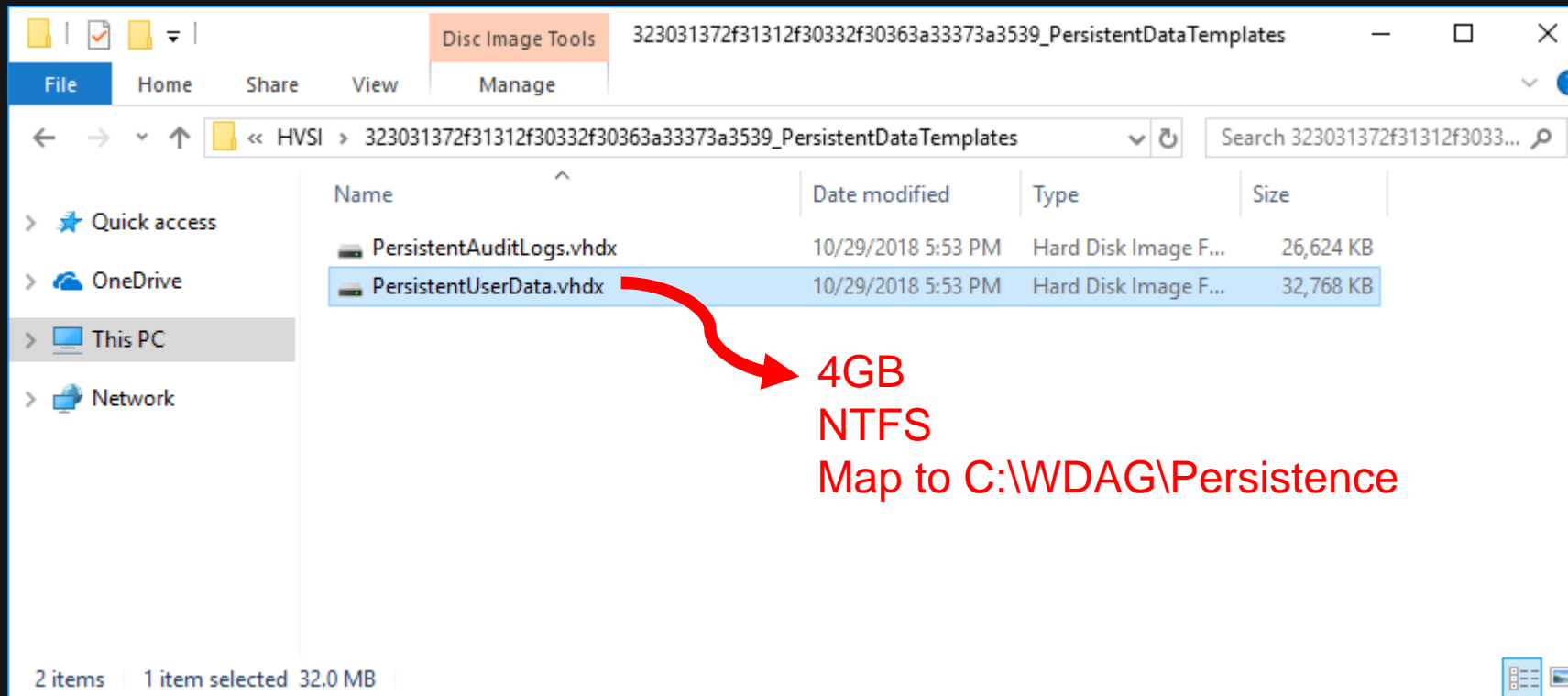
- How is the container created
  - Create Template Persistent Data Stores





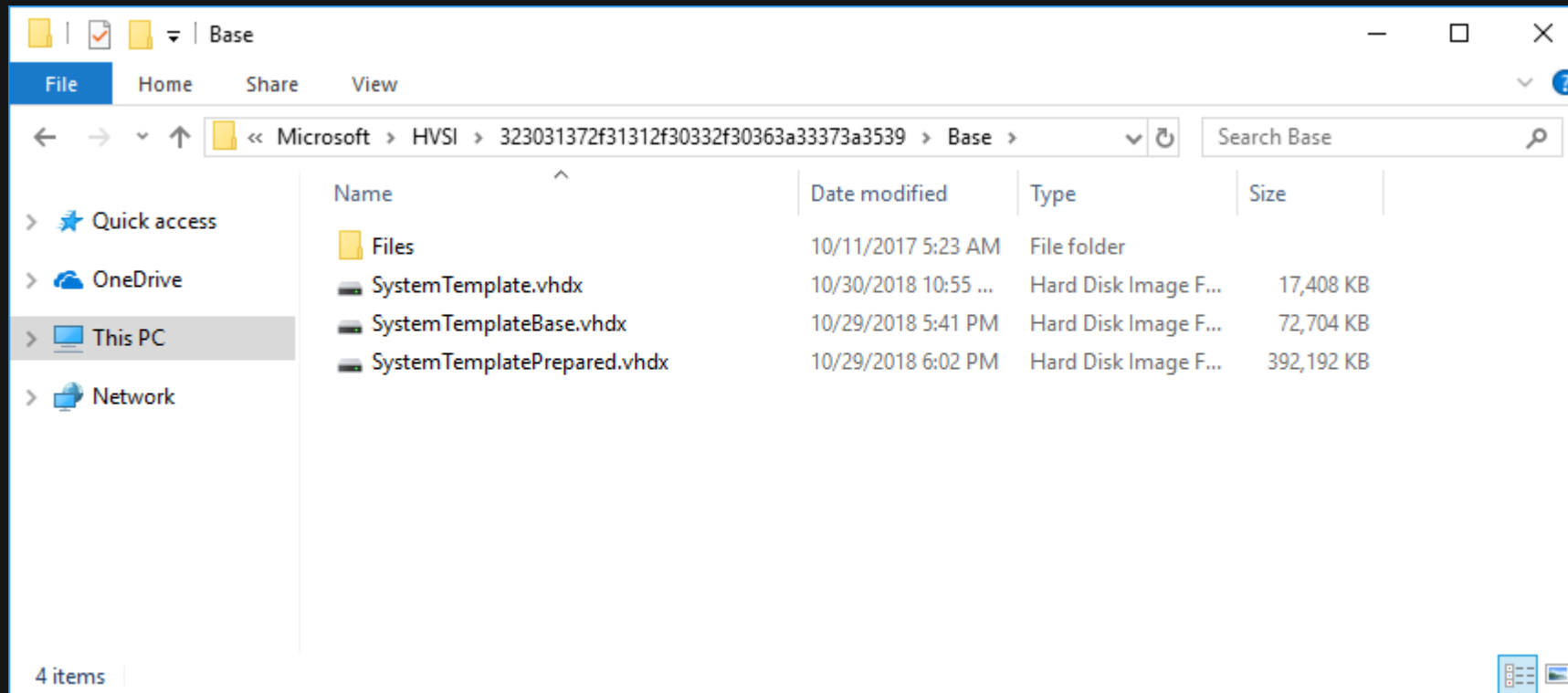
# ▶▶ WDAG Internals

- How is the container created
  - Create Template Persistent Data Stores



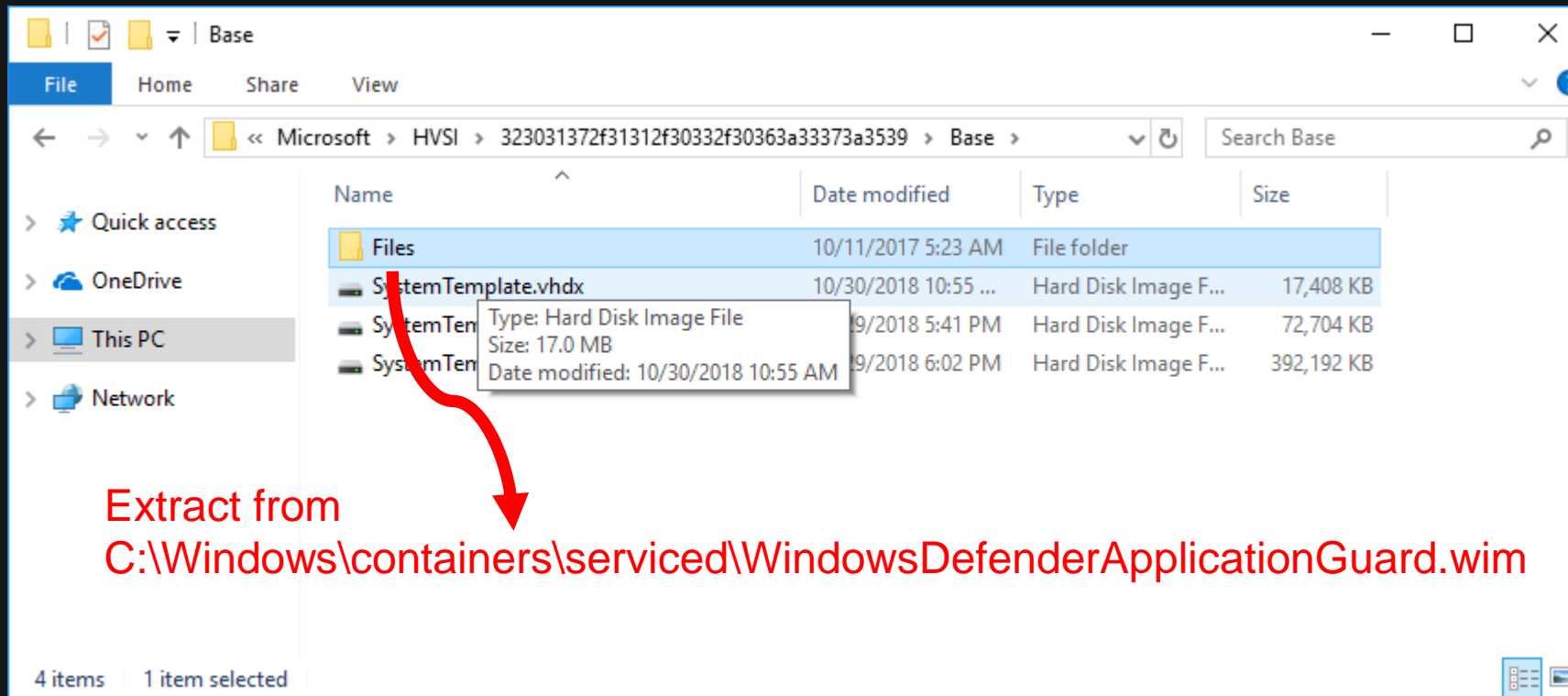
# ▶▶ WDAG Internals

- How is the container created
  - Create Base Image



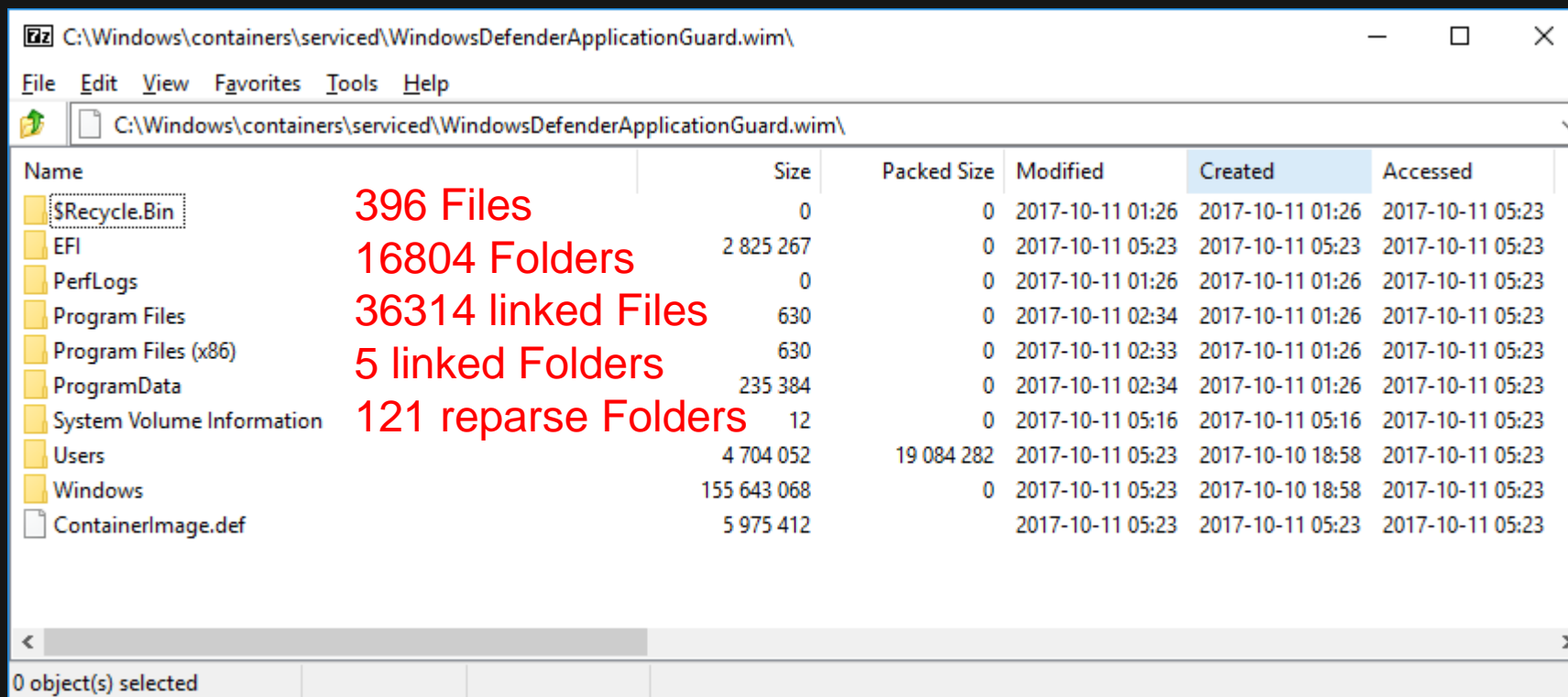
# ▶▶ WDAG Internals

- How is the container created
  - Create Base Image



# ▶▶ WDAG Internals

- How is the container created
  - Create Base Image

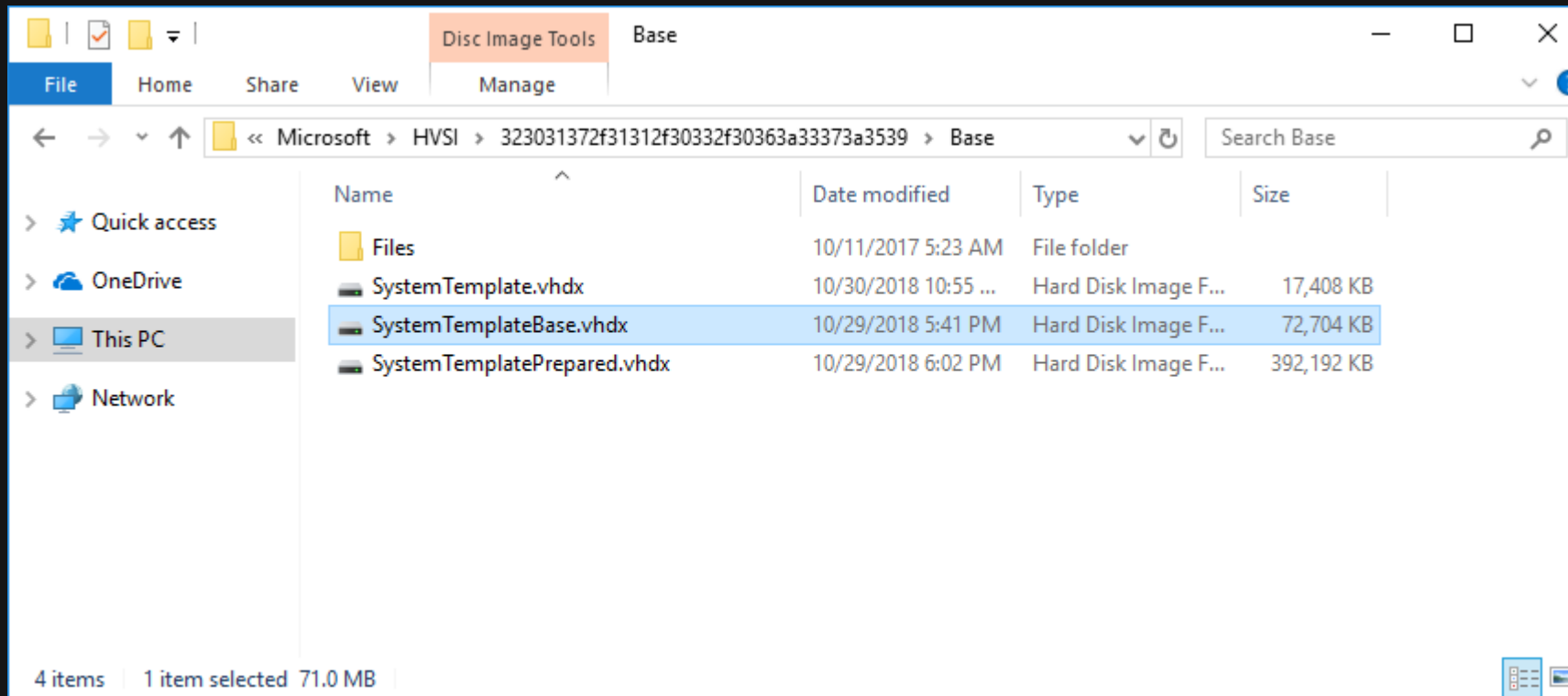


The screenshot shows a Windows Explorer window with the address bar set to `C:\Windows\containers\serviced\WindowsDefenderApplicationGuard.wim\`. The window displays a list of files and folders. Overlaid on the right side of the file list are red text annotations: "396 Files" next to \$Recycle.Bin, "16804 Folders" next to EFI, "36314 linked Files" next to PerfLogs, "5 linked Folders" next to Program Files, and "121 reparse Folders" next to System Volume Information.

Name	Size	Packed Size	Modified	Created	Accessed
\$Recycle.Bin	0	0	2017-10-11 01:26	2017-10-11 01:26	2017-10-11 05:23
EFI	2 825 267	0	2017-10-11 05:23	2017-10-11 05:23	2017-10-11 05:23
PerfLogs	0	0	2017-10-11 01:26	2017-10-11 01:26	2017-10-11 05:23
Program Files	630	0	2017-10-11 02:34	2017-10-11 01:26	2017-10-11 05:23
Program Files (x86)	630	0	2017-10-11 02:33	2017-10-11 01:26	2017-10-11 05:23
ProgramData	235 384	0	2017-10-11 02:34	2017-10-11 01:26	2017-10-11 05:23
System Volume Information	12	0	2017-10-11 05:16	2017-10-11 05:16	2017-10-11 05:23
Users	4 704 052	19 084 282	2017-10-11 05:23	2017-10-10 18:58	2017-10-11 05:23
Windows	155 643 068	0	2017-10-11 05:23	2017-10-10 18:58	2017-10-11 05:23
ContainerImage.def	5 975 412		2017-10-11 05:23	2017-10-11 05:23	2017-10-11 05:23

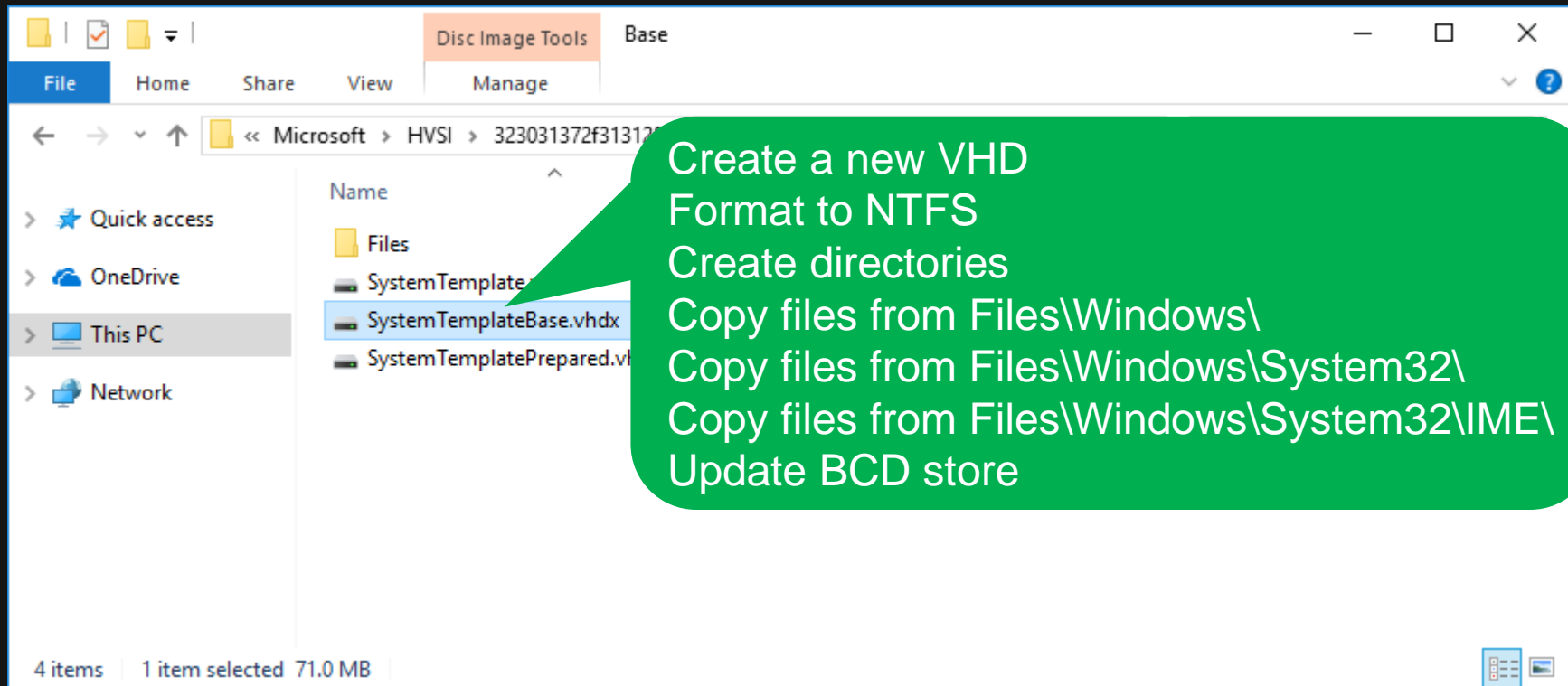
# ▶▶ WDAG Internals

- How is the container created
  - Create Base Image



# ▶▶ WDAG Internals

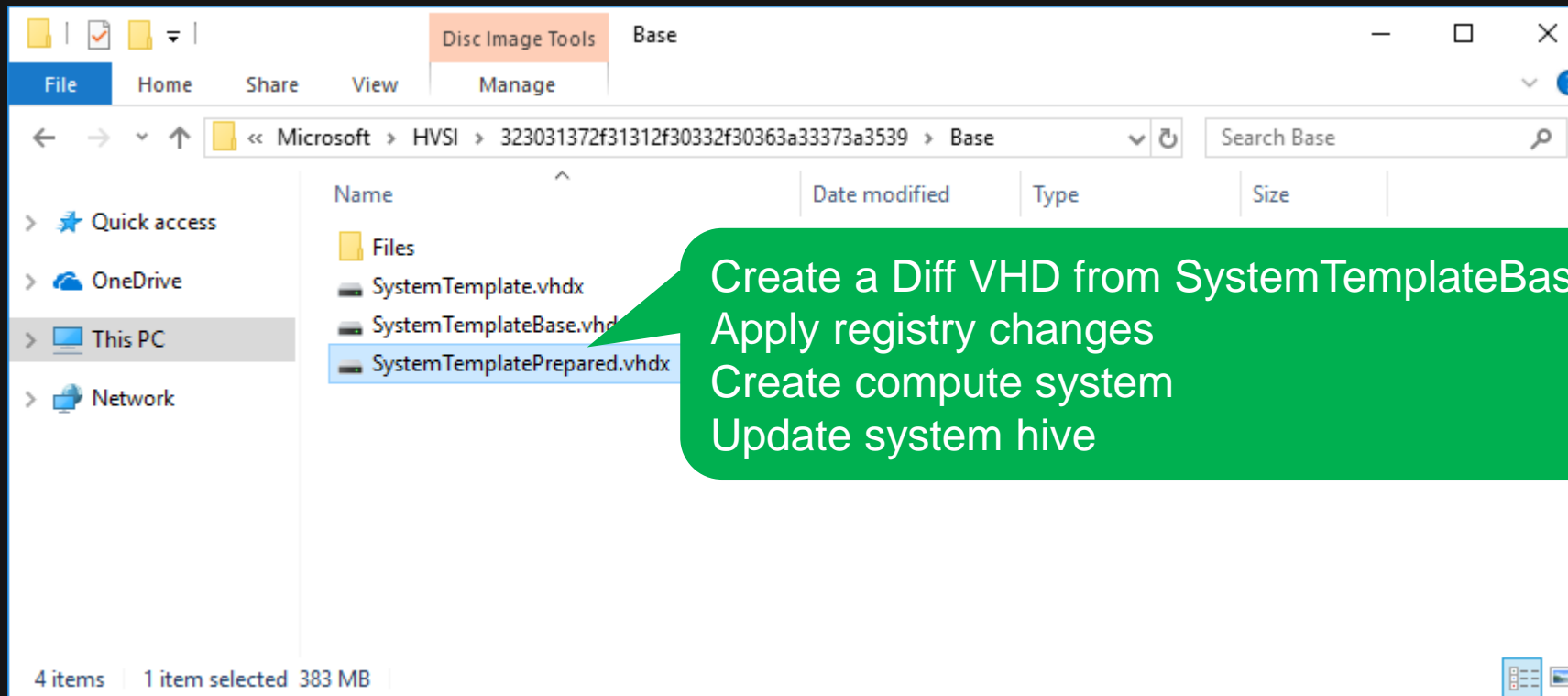
- How is the container created
  - Create Base Image





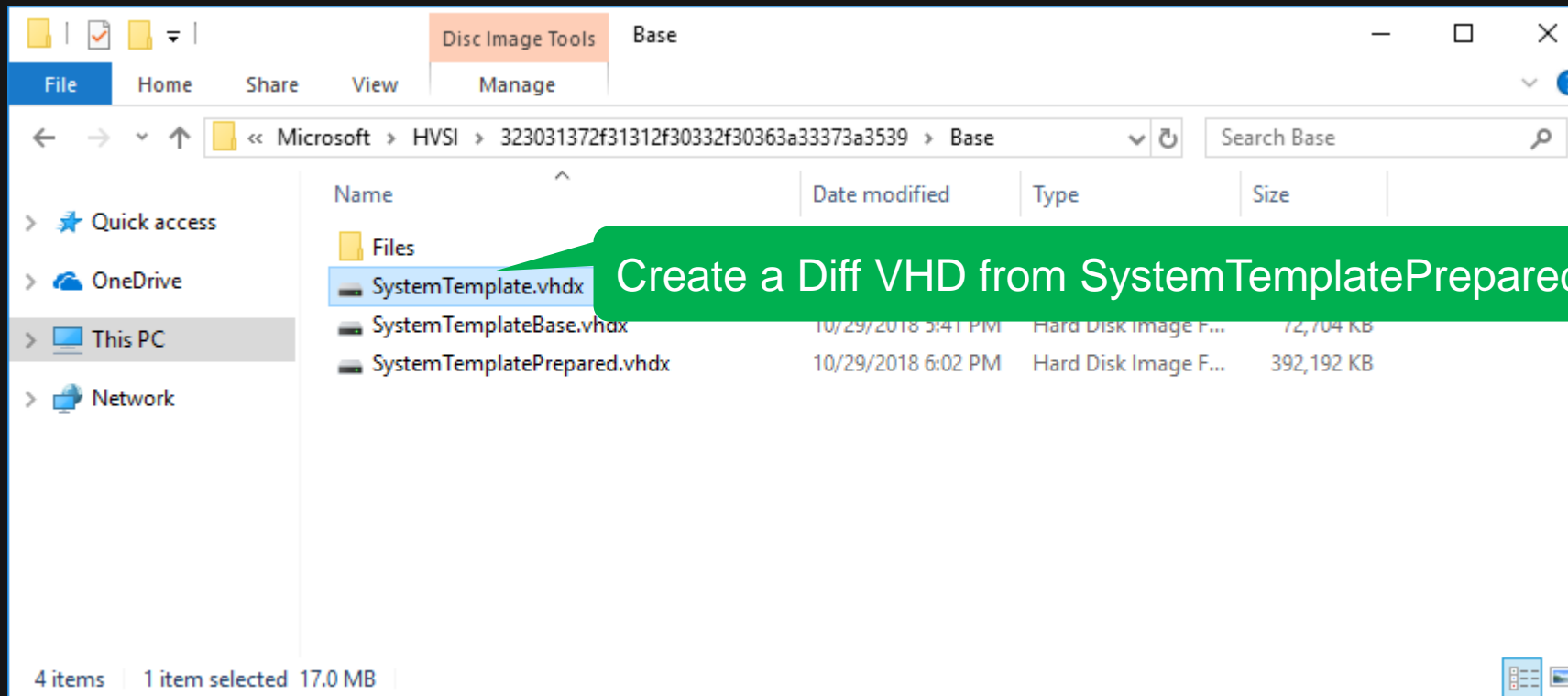
# ▶▶ WDAG Internals

- How is the container created
  - Create Base Image



# ▶▶ WDAG Internals

- ❑ How is the container created
  - Create Base Image



# ▶▶ WDAG Internals

- How is the container created
  - Create Base Image

SystemTemplate.vhdx

SystemTemplatePrepared.vhdx

SystemTemplateBase.vhdx

Files <= WindowsDefenderApplicationGuard.wim

# ▶▶ WDAG Internals

## □ How is the container created

- Create Container
  - Generate Runtime ID
  - Prepare HVSI NAT
  - Attach Persistent Data Stores
  - Create Container Settings
  - Create Sandbox Layer
  - Create Compute System
  - Create Container Credential
  - Start Compute System
  - Apply Settings to Container
  - Init RDP Logon

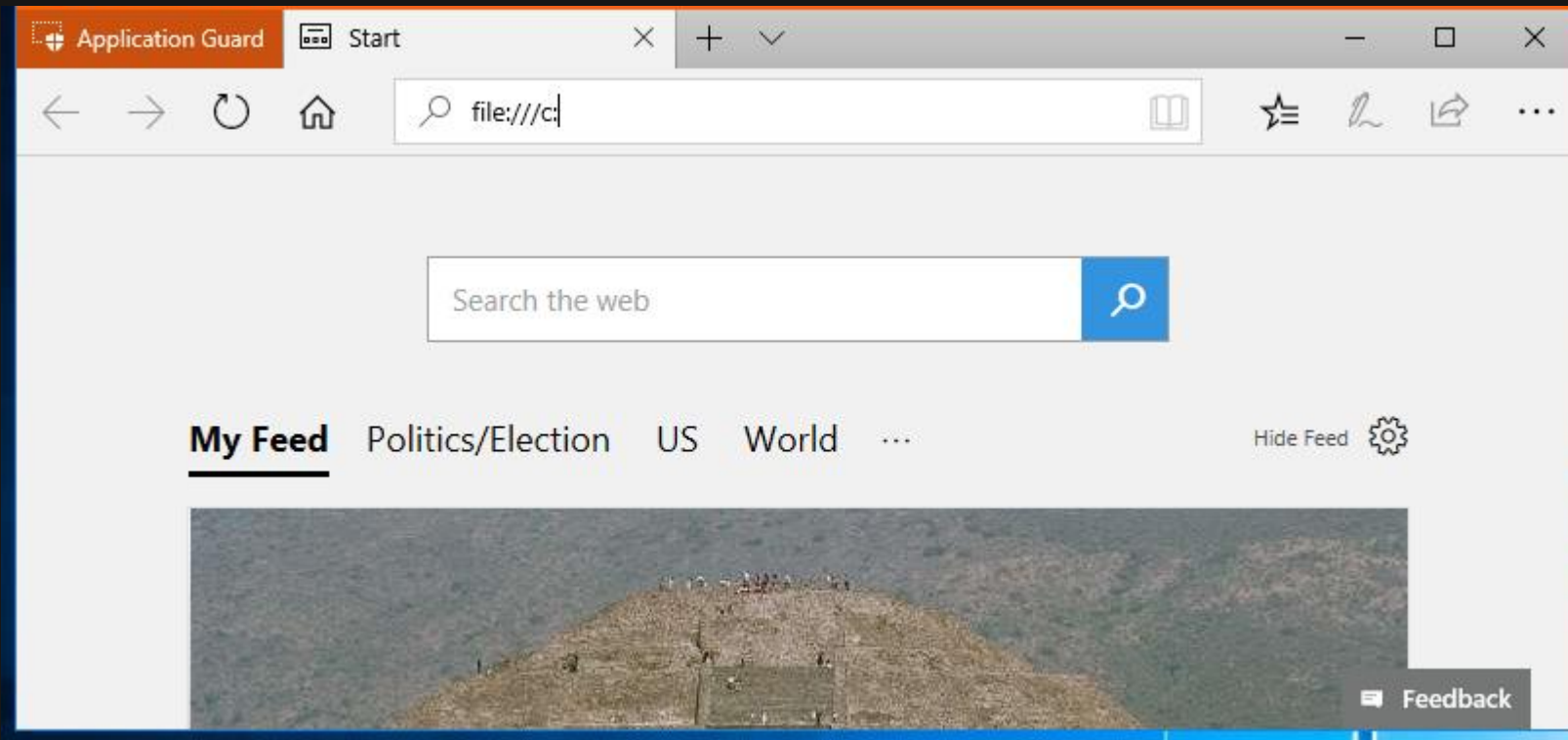
```

{
  "SystemType":"Container",
  "Name":"HVSContainer_c0f58700-29b1-30fc-174f-ed6b1868a978",
  "HvPartition":true,
  "Owner":"HVSI",
  "HvRuntime":{
    "RuntimeId":"3c810477-6845-43fd-aba0-c29d4d430998",
    "SkipTemplate":true,
    "EnableRdp":true,
    "RdpAccessSids":["S-1-5-21-2036491302-699820345-3847261429-1001","S-1-15-2-4241113689-1525372122-3928165819-2899915964-1654067008-1728629048-1671459956" ],
    "SynchronizeQPC":true,
    "BootFromLayers":true,
    "EnableMemoryHotHint":true,
    "EnableMemoryColdHint":true,
    "EnablePrivateMemoryCompressionStore":true,
    "EnableBattery":true,
    "BugcheckSavedStateFileName":"wdag.vmps"
  },
  "HostName":"3c810477-6",
  "RegistryChanges":{"AddValues":[{"Key":{"Hive":"System","Name":"ControlSet001\\Services\\EventLog\\Security"},"Name":"MaxSize","Type":"DWord","DWordValue":20971520},...]},
  "MemoryMaximumInMB":4000,
  "ProcessorCount":4,
  "DirectFileMappingMB":1024,
  "SharedMemoryMB":1024,
  "SandboxPath":"C:\\ProgramData\\Microsoft\\HVS\\HVSContainer_c0f58700-29b1-30fc-174f-ed6b1868a978",
  "Layers":[{"Id":"1b3979c8-279b-42eb-b2b9-750767ee9e3f","Path":"C:\\ProgramData\\Microsoft\\HVS\\323031372f31312f30332f30363a33373a3539\\Base"}],
  "MappedVirtualDisks":[
    {"HostPath":"C:\\Users\\test\\AppData\\Local\\Microsoft\\WDAG\\PersistentAuditLogs.vhdx","ContainerPath":"C:\\WDAG\\AuditLogs","OverwriteIfExists":true},
    {"HostPath":"C:\\Users\\test\\AppData\\Local\\Microsoft\\WDAG\\PersistentUserData.vhdx","ContainerPath":"C:\\WDAG\\Persistence","OverwriteIfExists":true}
  ],
  "NetworkEndpoints":[{"
    "Id":"00000000-0000-0000-0000-000000000000",
    "EndpointName":"3c810477-6845-43fd-aba0-c29d4d430998",
    "StaticMacAddress":"02174FED6B18",
    "NetworkId":"161df6ed-7ce7-450f-8ddb-4603ff64edfc"
  }],
  "VsockStdioPortRange":{"Min":0,"Max":0},
  "EnableUtcRelay":true,
  "HvSocketConfig":{
    "ServiceTable":{
      "abd802e8-ffcc-40d2-a5f1-f04b1d12cbc8":{"BindSecurityDescriptor":"D:P(A;;;FA;;;WD)(A;;;FA;;;S-1-15-3-3)","ConnectSecurityDescriptor":"D:P(D;;;FA;;;WD)"}
    }
  }
}

```

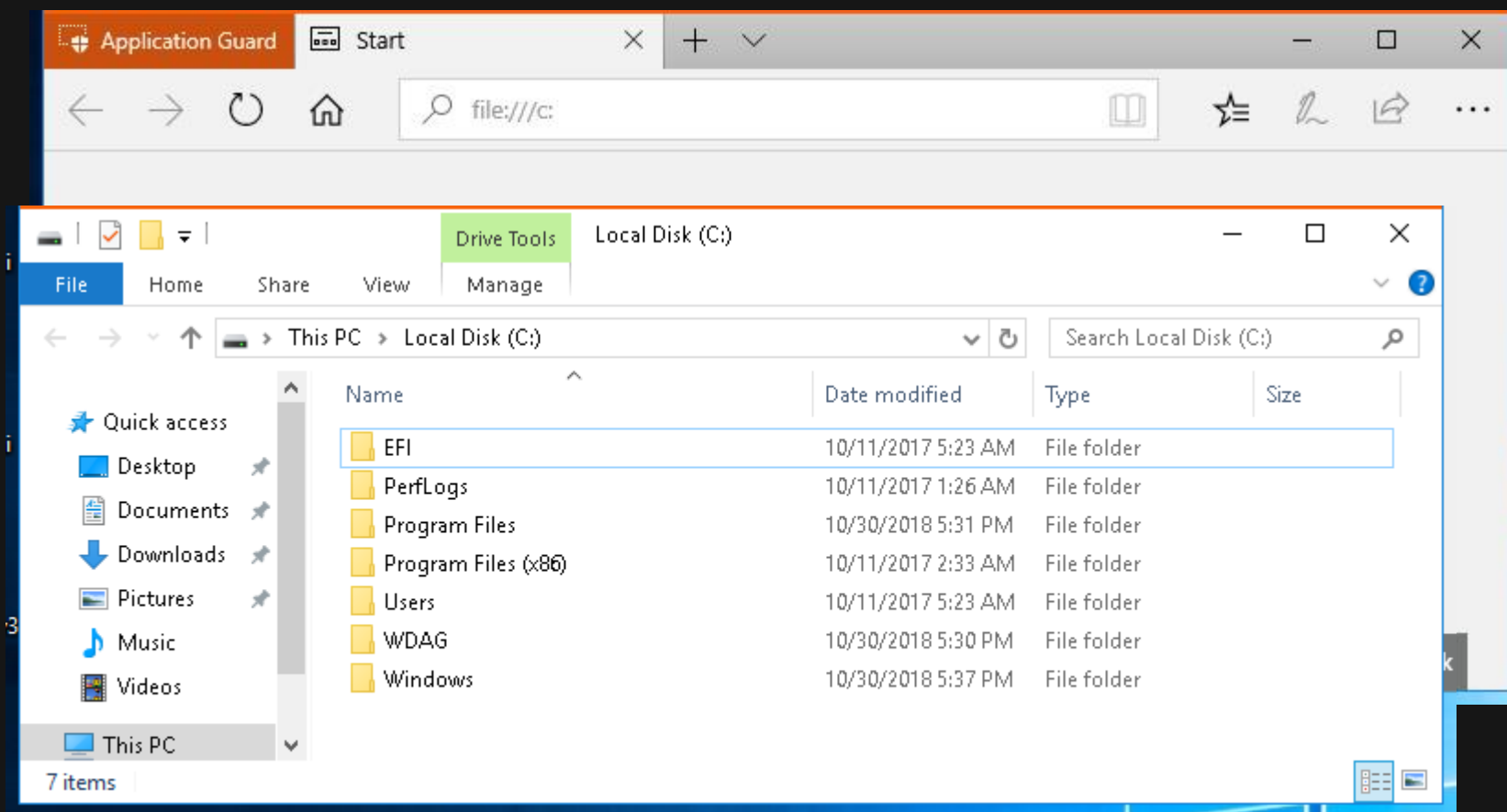
# ▶▶ Reform WDAG for Research

## □ Step 1: Launch File Explorer in WDAG



# ▶▶ Reform WDAG for Research

## □ Step 1: Launch File Explorer in WDAG



# ▶▶ Reform WDAG for Research

## □ Step 2: Modify Device Guard Rule

- WDAG deploy a very strict rule inside the container
  - UMCI is enabled
  - Only Microsoft Signers are allowed
  - 171 files are explicitly denied
    - cmd.Exe
    - CONTROL.EXE
    - mmc.exe
    - netsh.exe
    - regedit.exe
    - windbg.Exe
    - wmic.exe
    - wscript.exe
    - ...



# ▶▶ Reform WDAG for Research

- ❑ Step 2: Modify Device Guard Rule
  - WDAG deploy a very strict rule inside the container

This app can't run in Windows Defender Application Guard.

C:\Windows\System32\cmd.exe

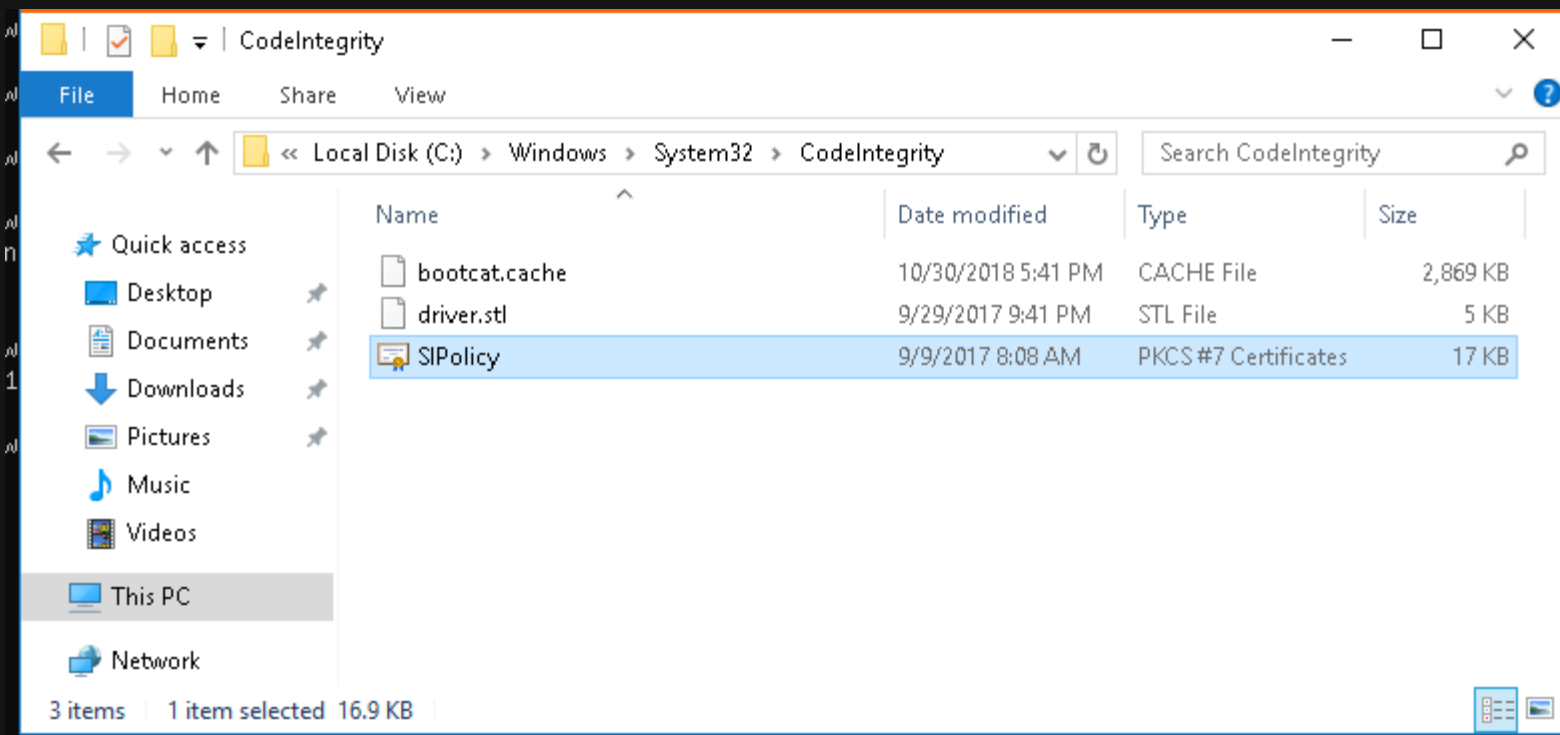
Please contact your administrator for help.

Copy to clipboard

Close

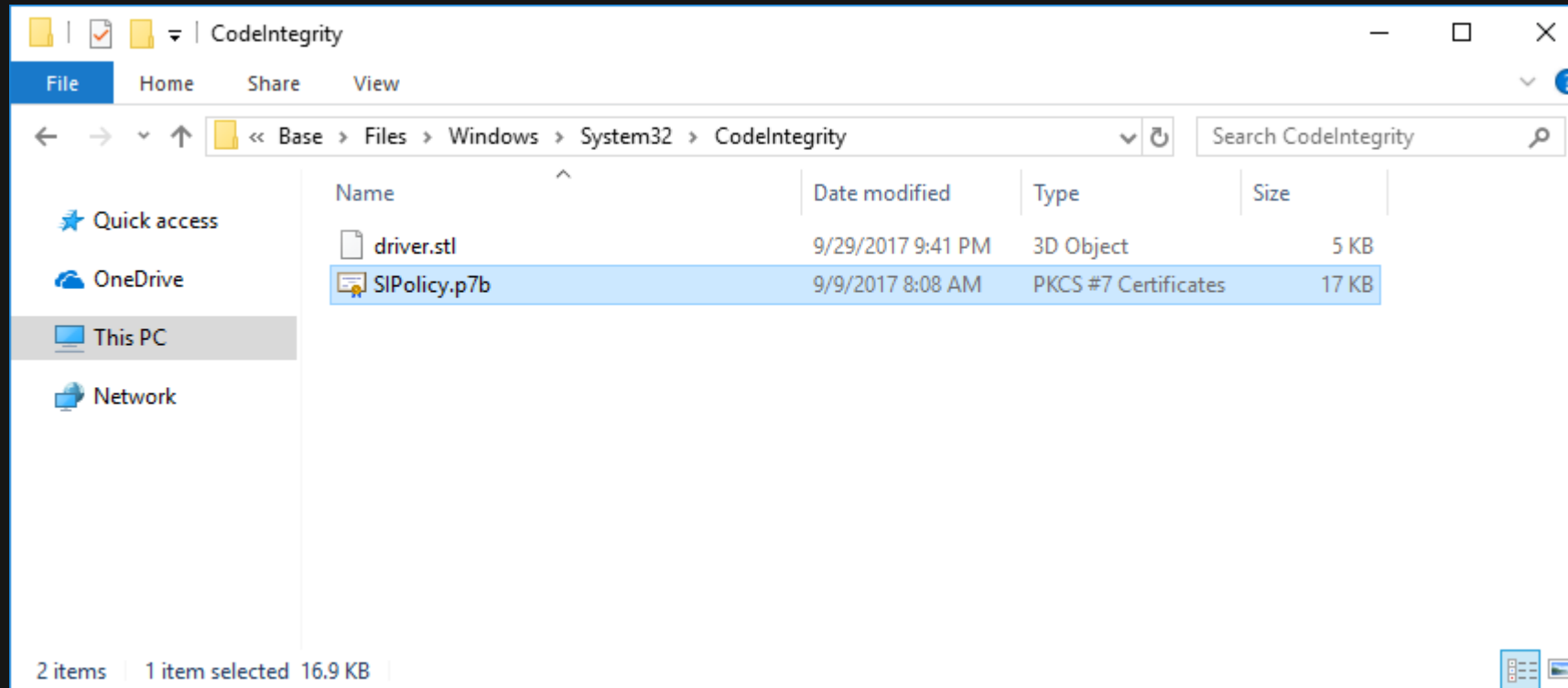
# ▶▶ Reform WDAG for Research

- ❑ Step 2: Modify Device Guard Rule
  - The policy file can be modified outside the container



# ▶▶ Reform WDAG for Research

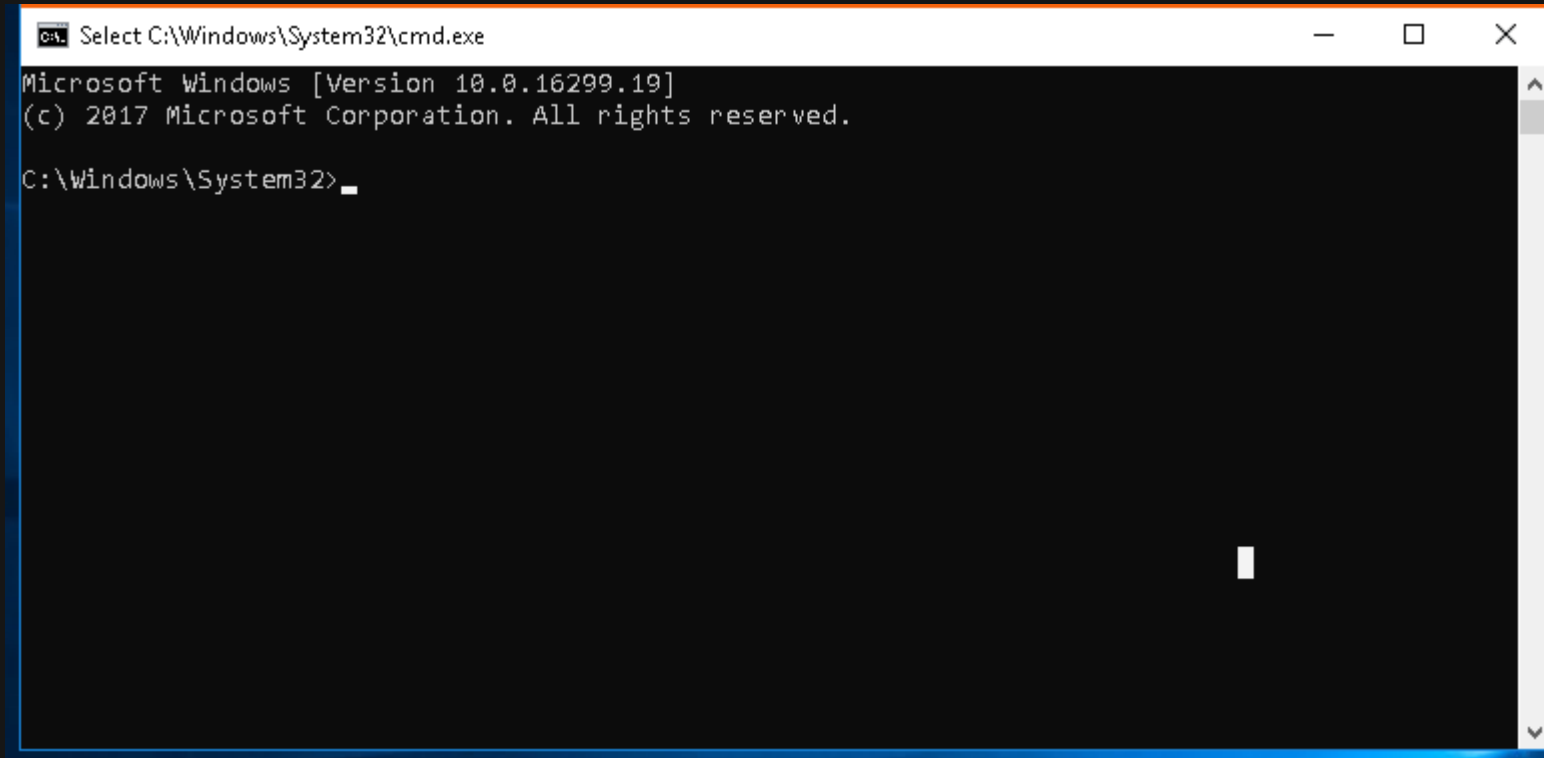
- ❑ Step 2: Modify Device Guard Rule
  - The policy file can be modified outside the container



# ▶▶ Reform WDAG for Research

## ❑ Step 2: Modify Device Guard Rule

- The policy file can be modified outside the container



```

Select C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.16299.19]
(c) 2017 Microsoft Corporation. All rights reserved.

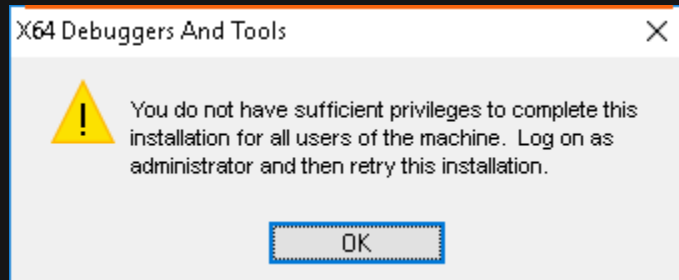
C:\Windows\System32>

```

# ▶▶ Reform WDAG for Research

## □ Step 3: Install WinDbg

- We do not have sufficient privileges to install program
  - The logged on user is a normal user
  - The administrator user in the container is disabled



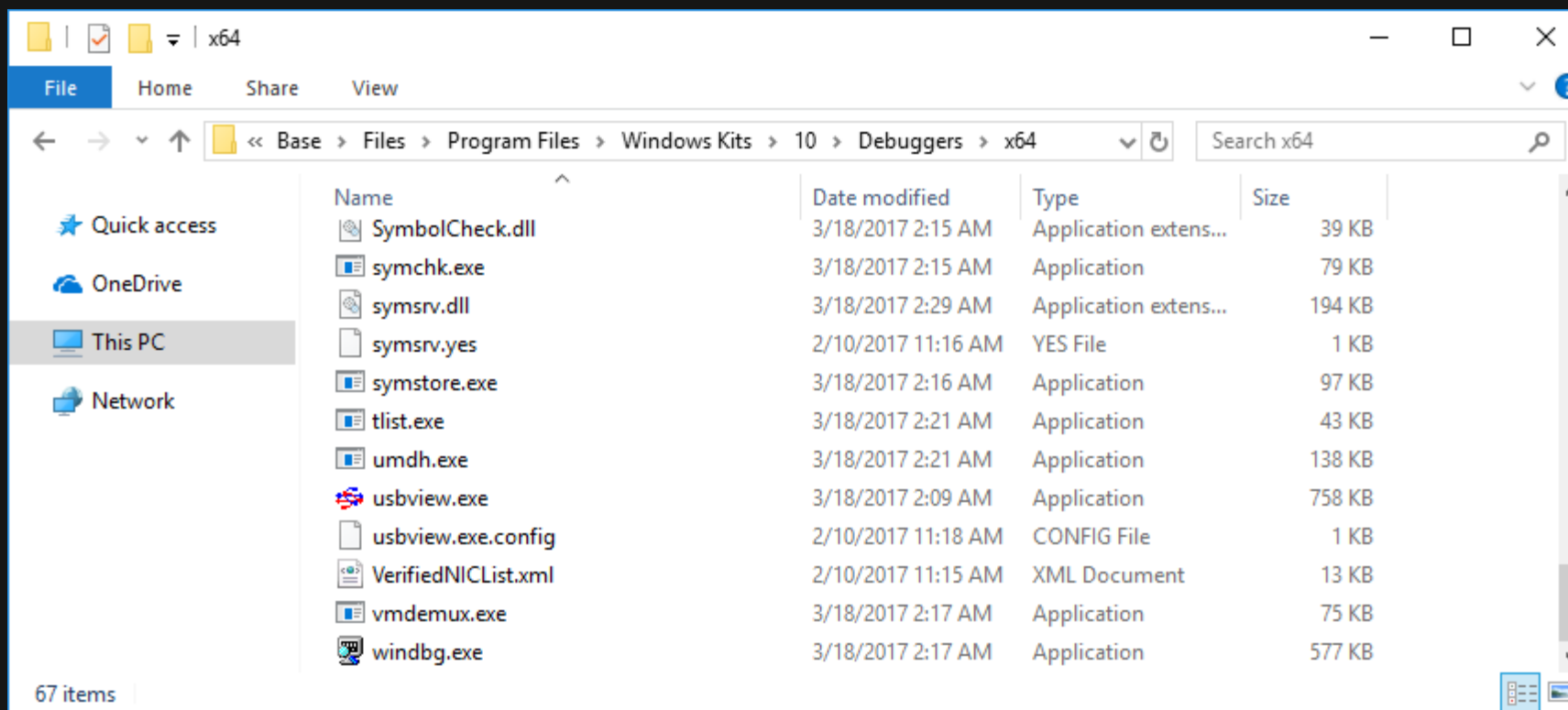
# ▶▶ Reform WDAG for Research

## □ Step 3: Install WinDbg

- 2 choices
  - Exploit an EoP vulnerability
  - Copy an installed version into the container

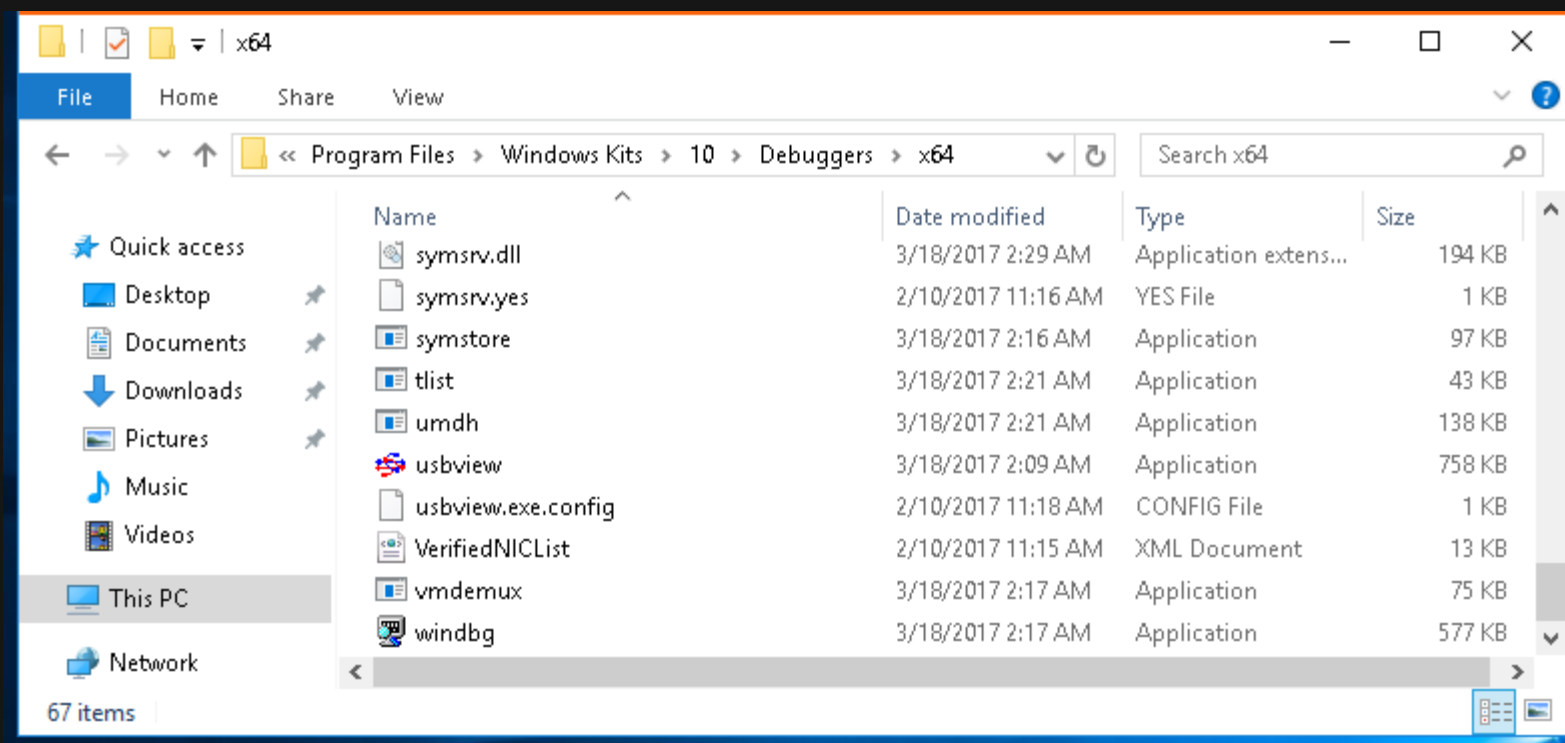
# ▶▶ Reform WDAG for Research

- Step 3: Install WinDbg
  - Copy files to Base Files



# ▶▶ Reform WDAG for Research

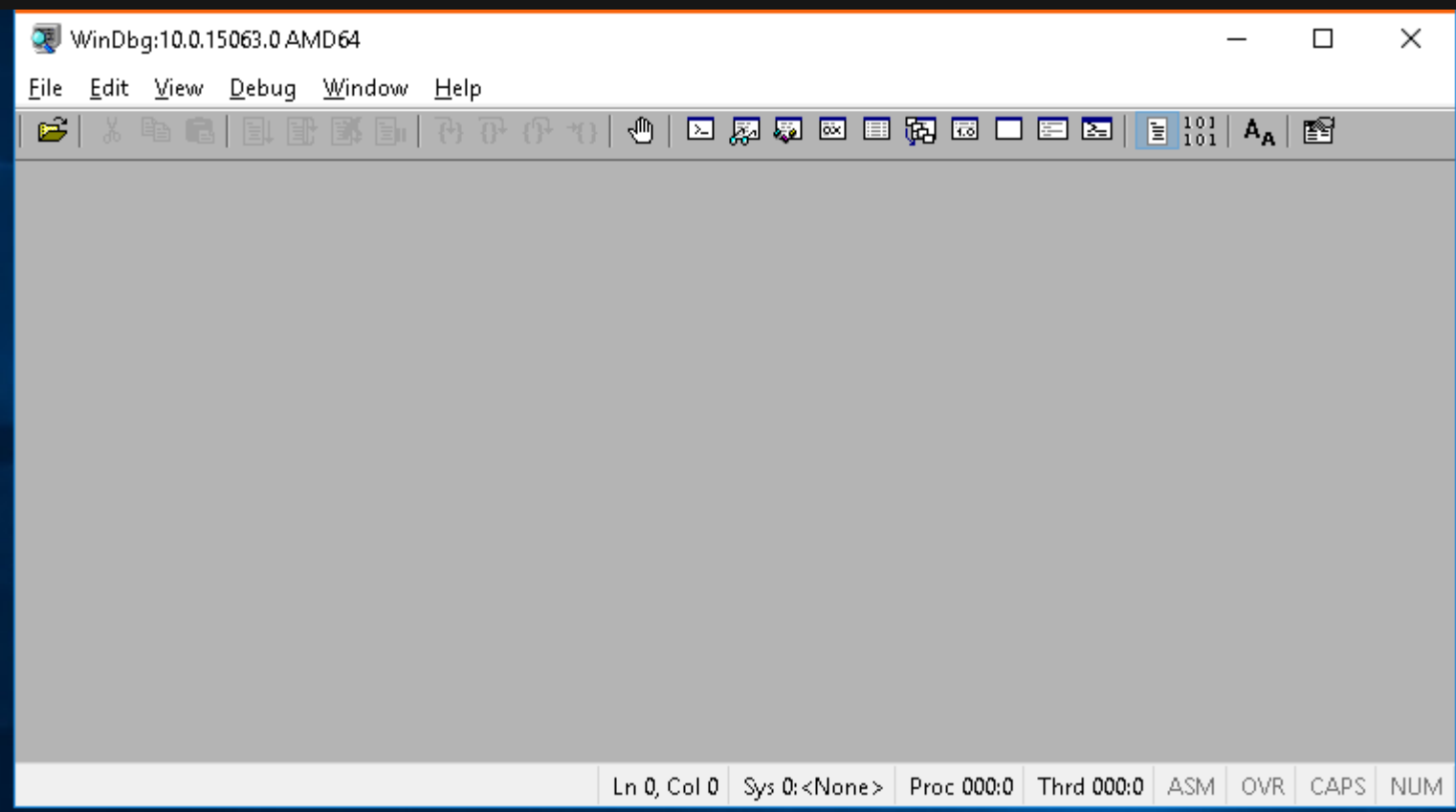
- ❑ Step 3: Install WinDbg
  - They will appear in the container immediately





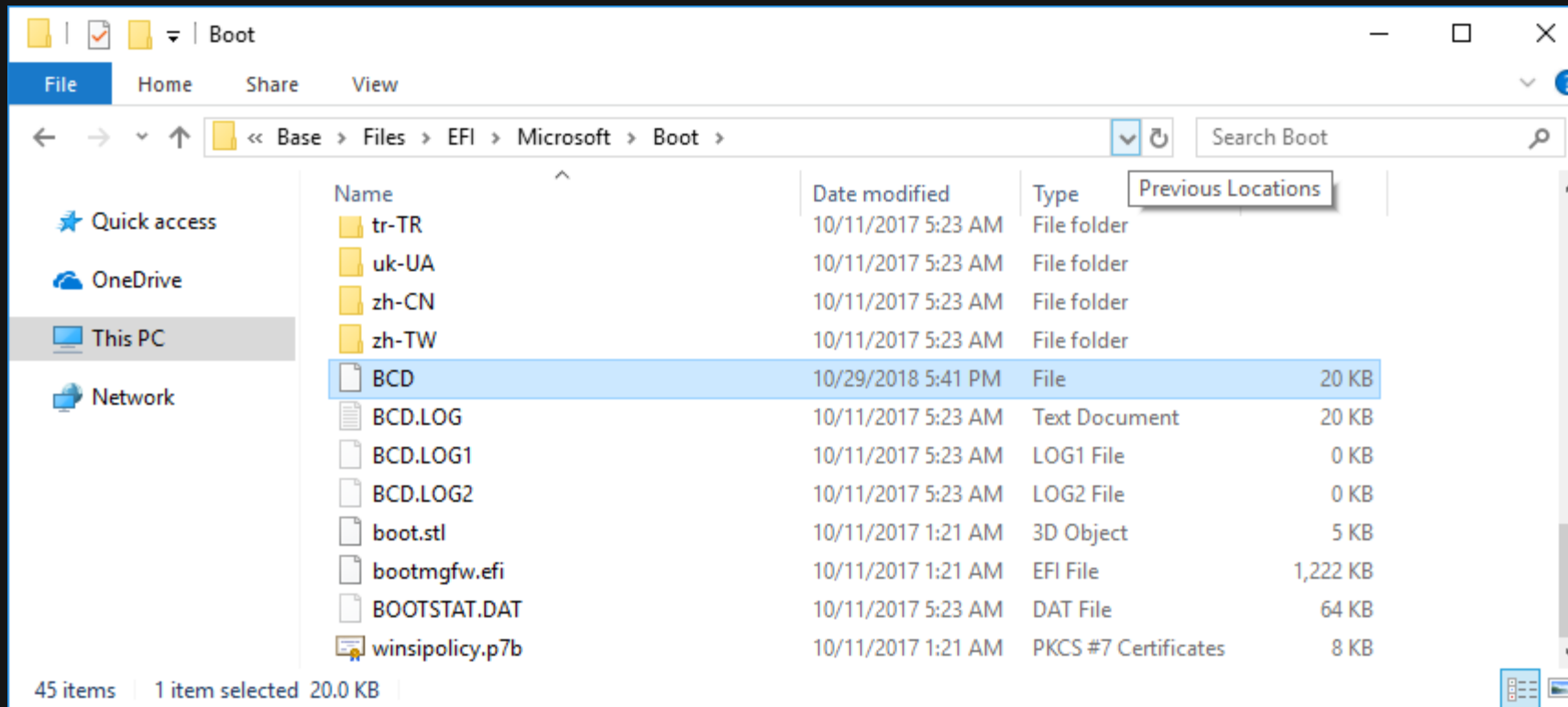
# ▶▶ Reform WDAG for Research

## □ Step 3: Install WinDbg



# ▶▶ Reform WDAG for Research

- ❑ Step 4: Setting Up Kernel Debugging
  - Edit BCD store of the container

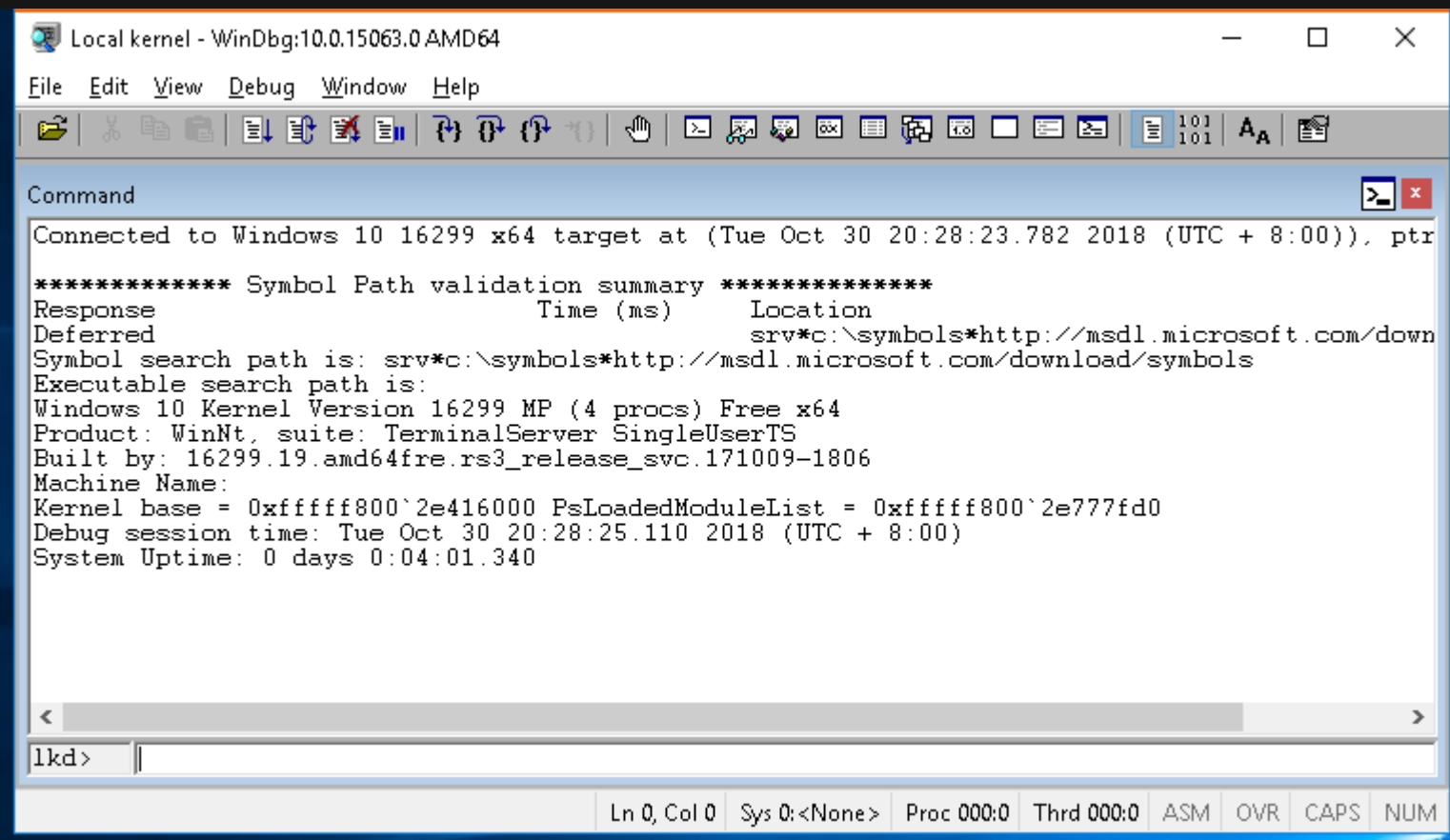


# ▶▶ Reform WDAG for Research

- Step 4: Setting Up Kernel Debugging
  - Currently only local debugging is possible
    - No COM port or USB or 1394
    - Network connection is restricted

# ▶▶ Reform WDAG for Research

## □ Step 4: Setting Up Kernel Debugging

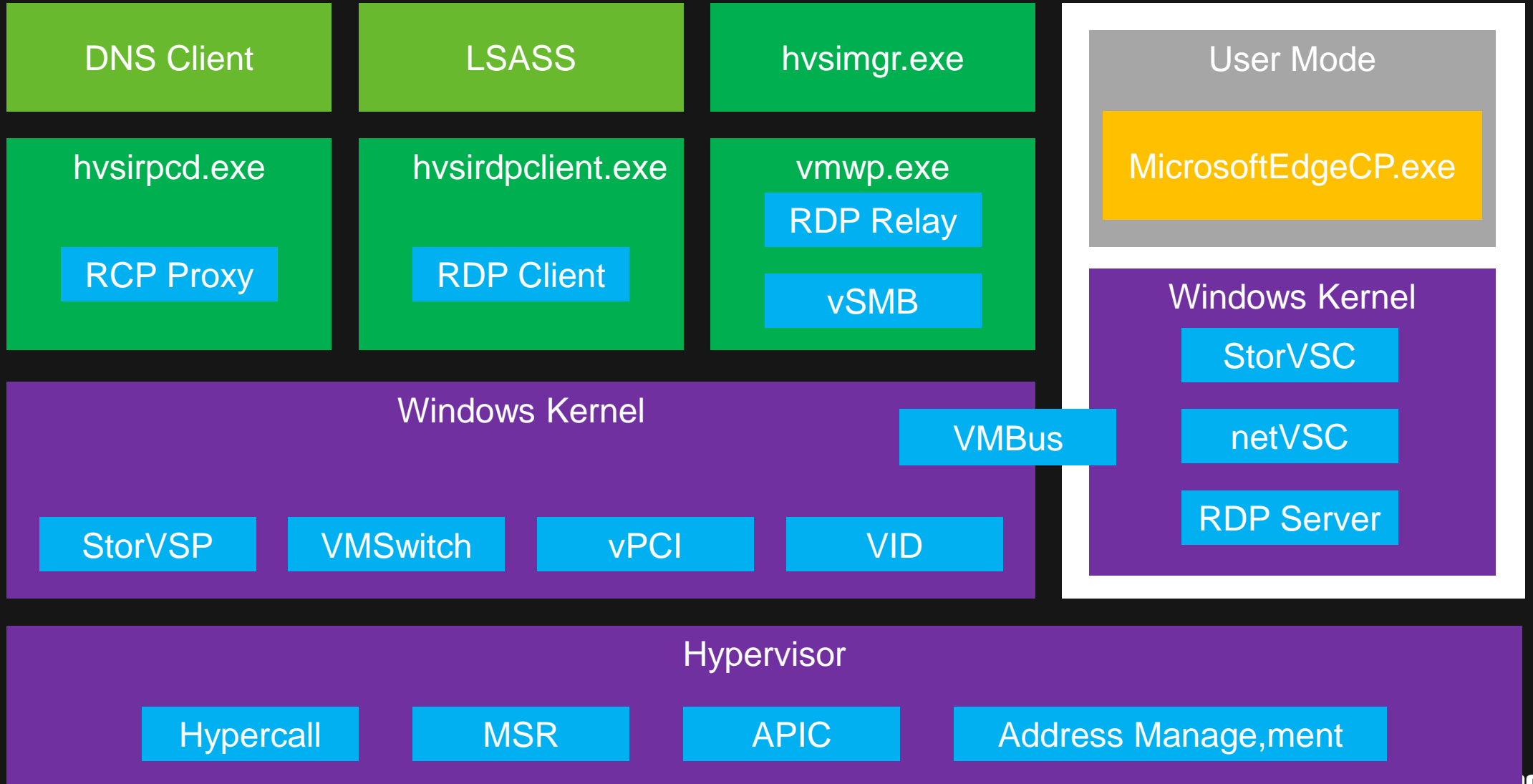


The screenshot shows the WinDbg interface with the title bar "Local kernel - WinDbg:10.0.15063.0 AMD64". The menu bar includes File, Edit, View, Debug, Window, and Help. The toolbar contains various icons for file operations, debugging, and viewing. The Command window displays the following text:

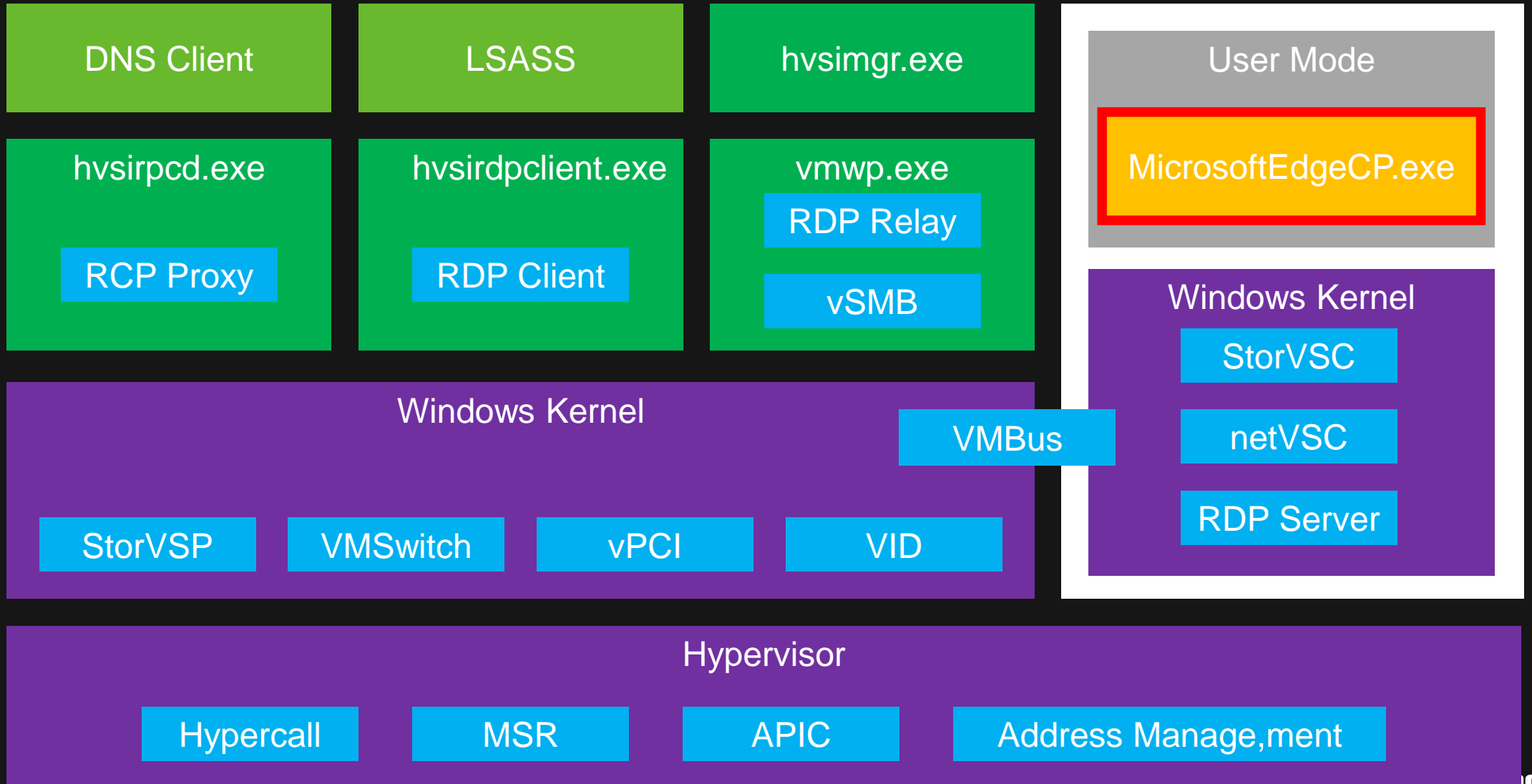
```
Connected to Windows 10 16299 x64 target at (Tue Oct 30 20:28:23.782 2018 (UTC + 8:00)), ptr
***** Symbol Path validation summary *****
Response          Time (ms)      Location
Deferred          101           srv*c:\symbols*http://msdl.microsoft.com/down
Symbol search path is: srv*c:\symbols*http://msdl.microsoft.com/download/symbols
Executable search path is:
Windows 10 Kernel Version 16299 MP (4 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Built by: 16299.19.amd64fre.rs3_release_svc.171009-1806
Machine Name:
Kernel base = 0xfffff800`2e416000 PsLoadedModuleList = 0xfffff800`2e777fd0
Debug session time: Tue Oct 30 20:28:25.110 2018 (UTC + 8:00)
System Uptime: 0 days 0:04:01.340
```

The status bar at the bottom shows "Ln 0, Col 0", "Sys 0:<None>", "Proc 000:0", "Thrd 000:0", and tabs for ASM, OVR, CAPS, and NUM.

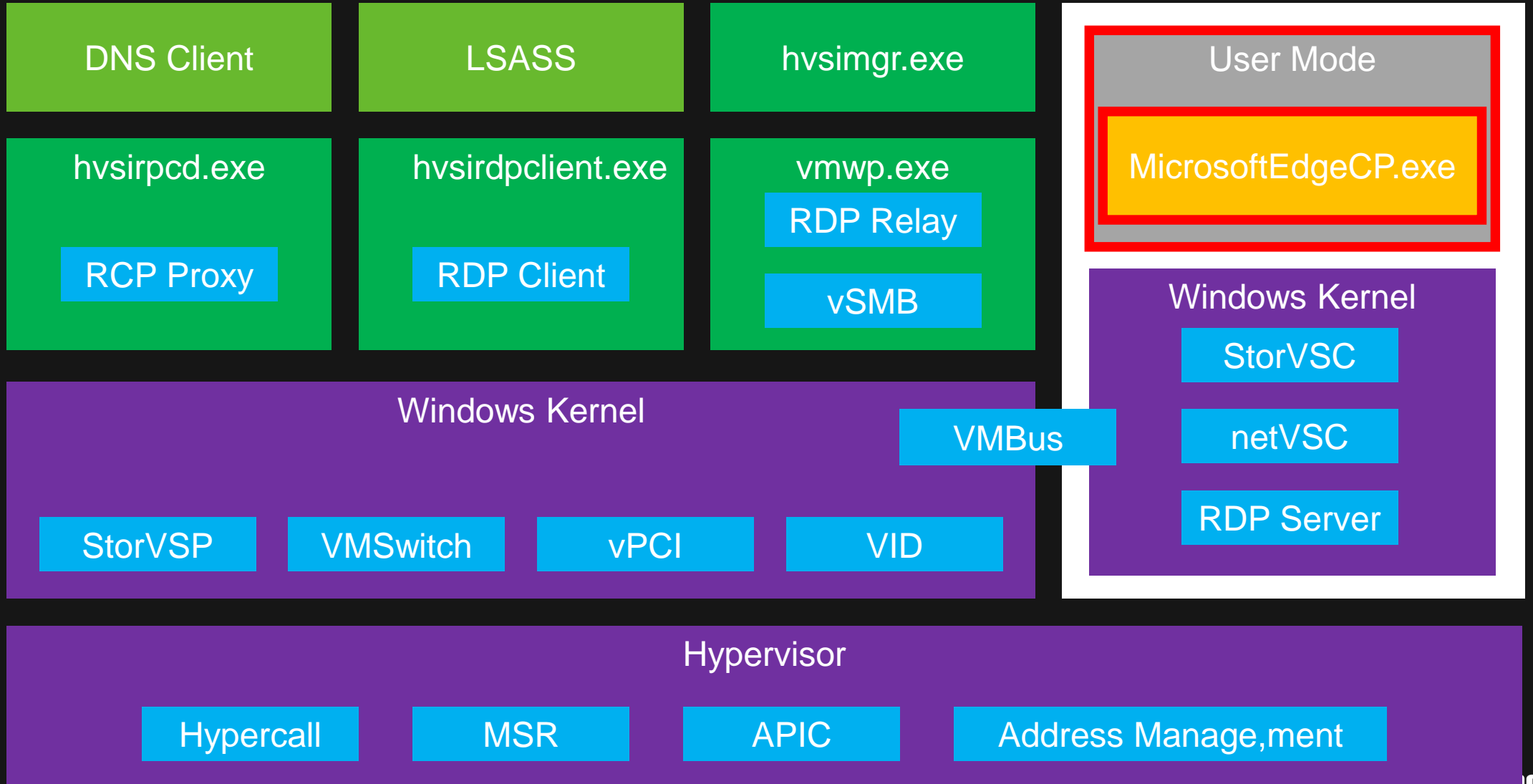
# ▶▶ WDAG Attack Surface



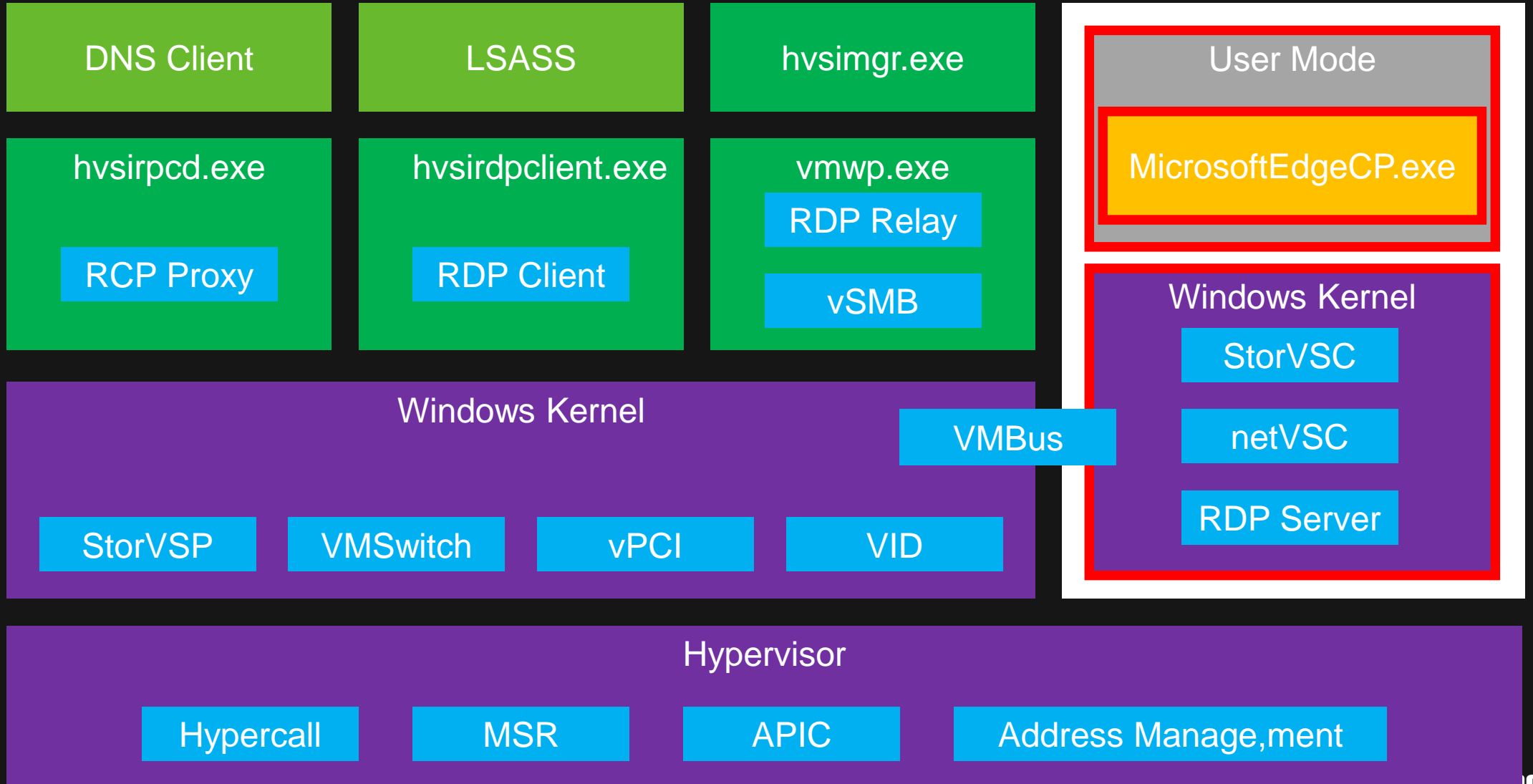
# ▶▶ WDAG Attack Surface



# ▶▶ WDAG Attack Surface

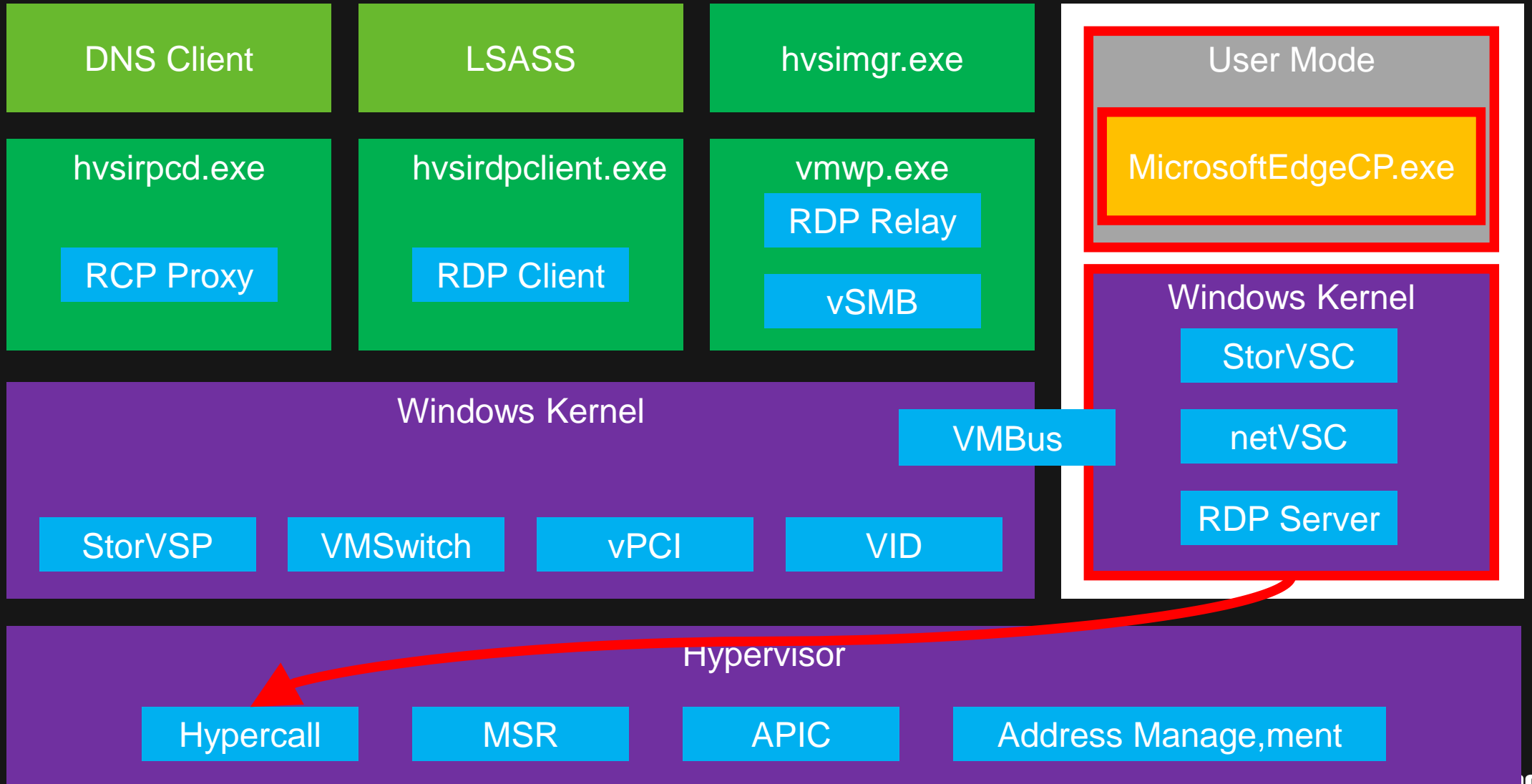


# ▶▶ WDAG Attack Surface

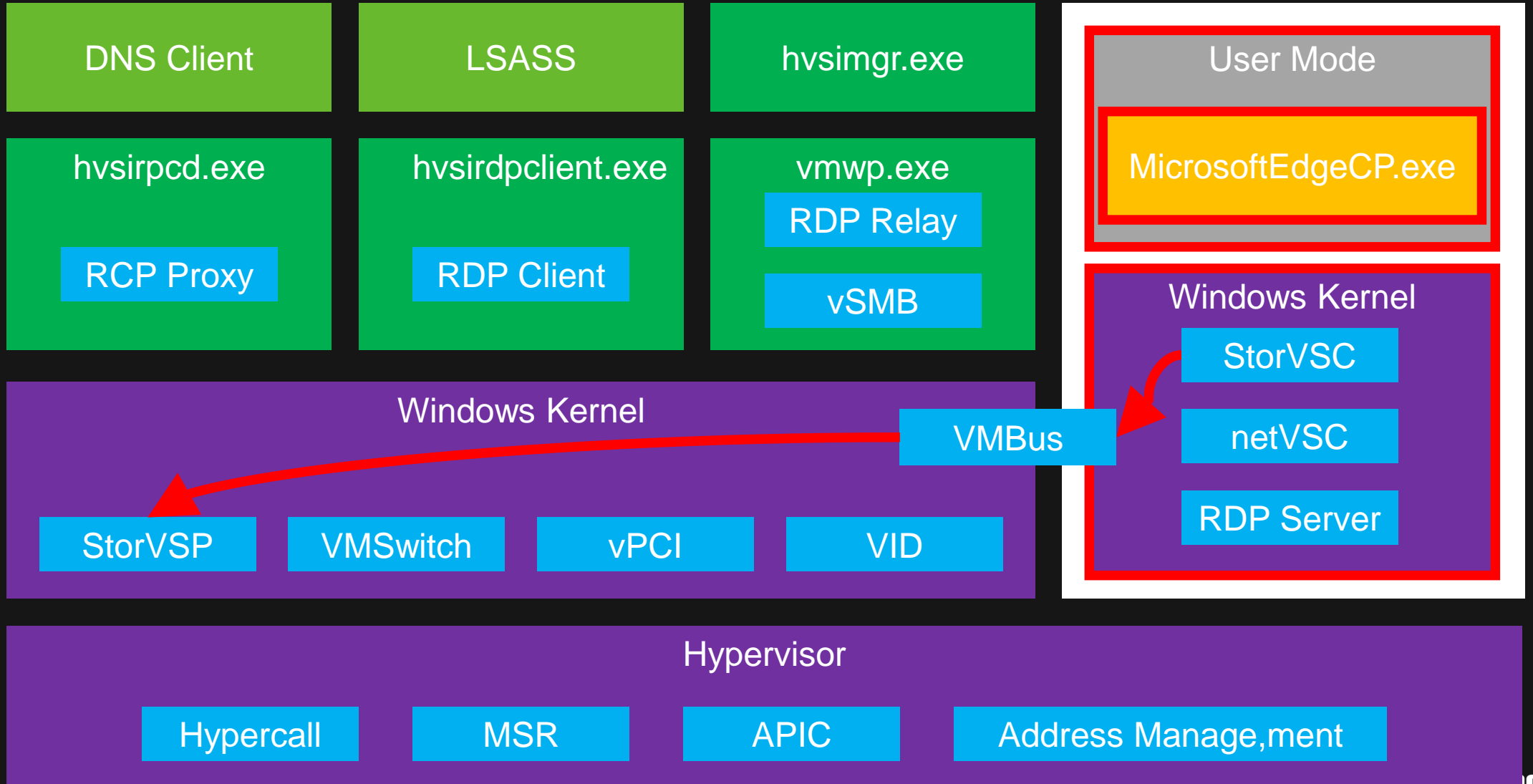




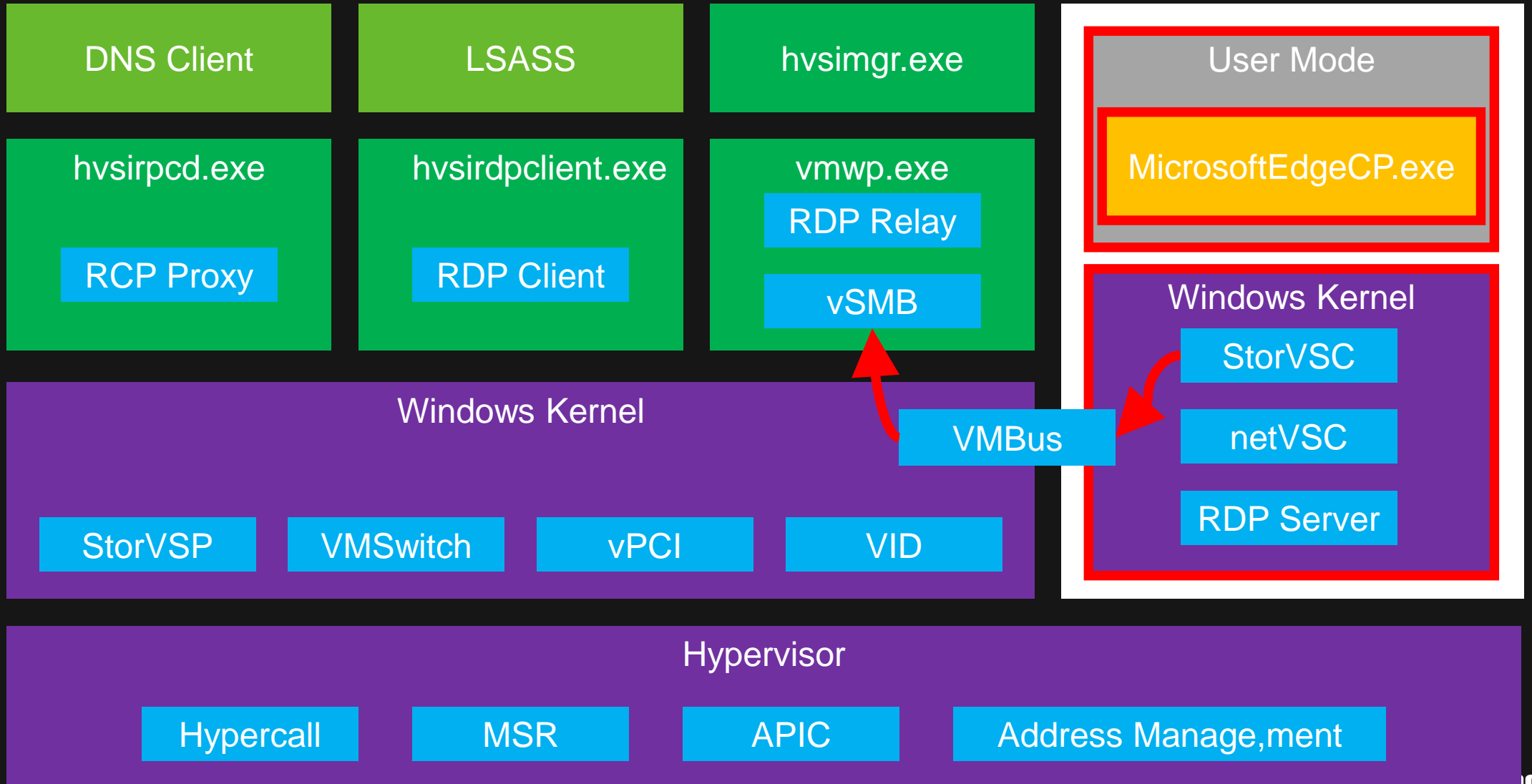
# ▶▶ WDAG Attack Surface



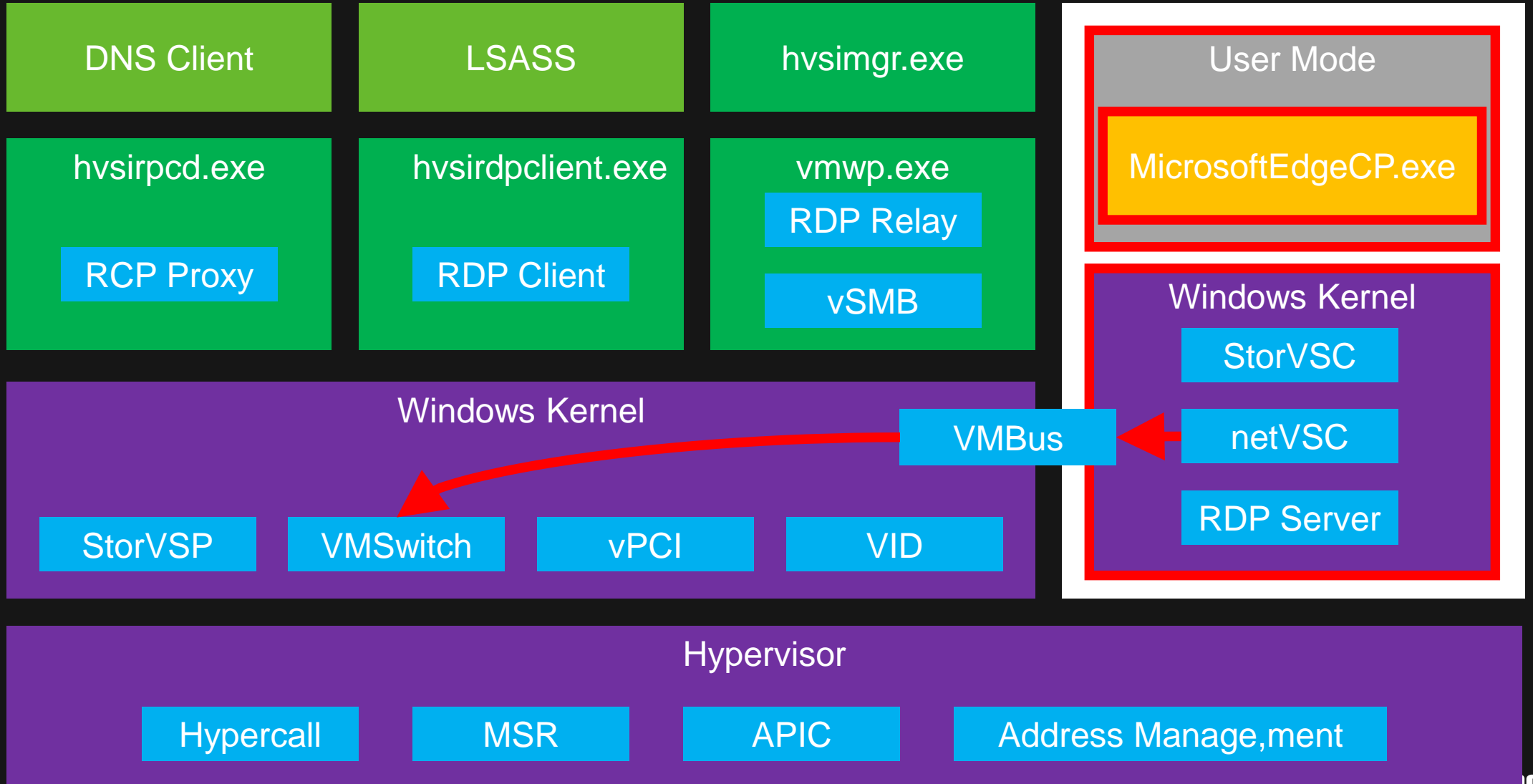
# ▶▶ WDAG Attack Surface



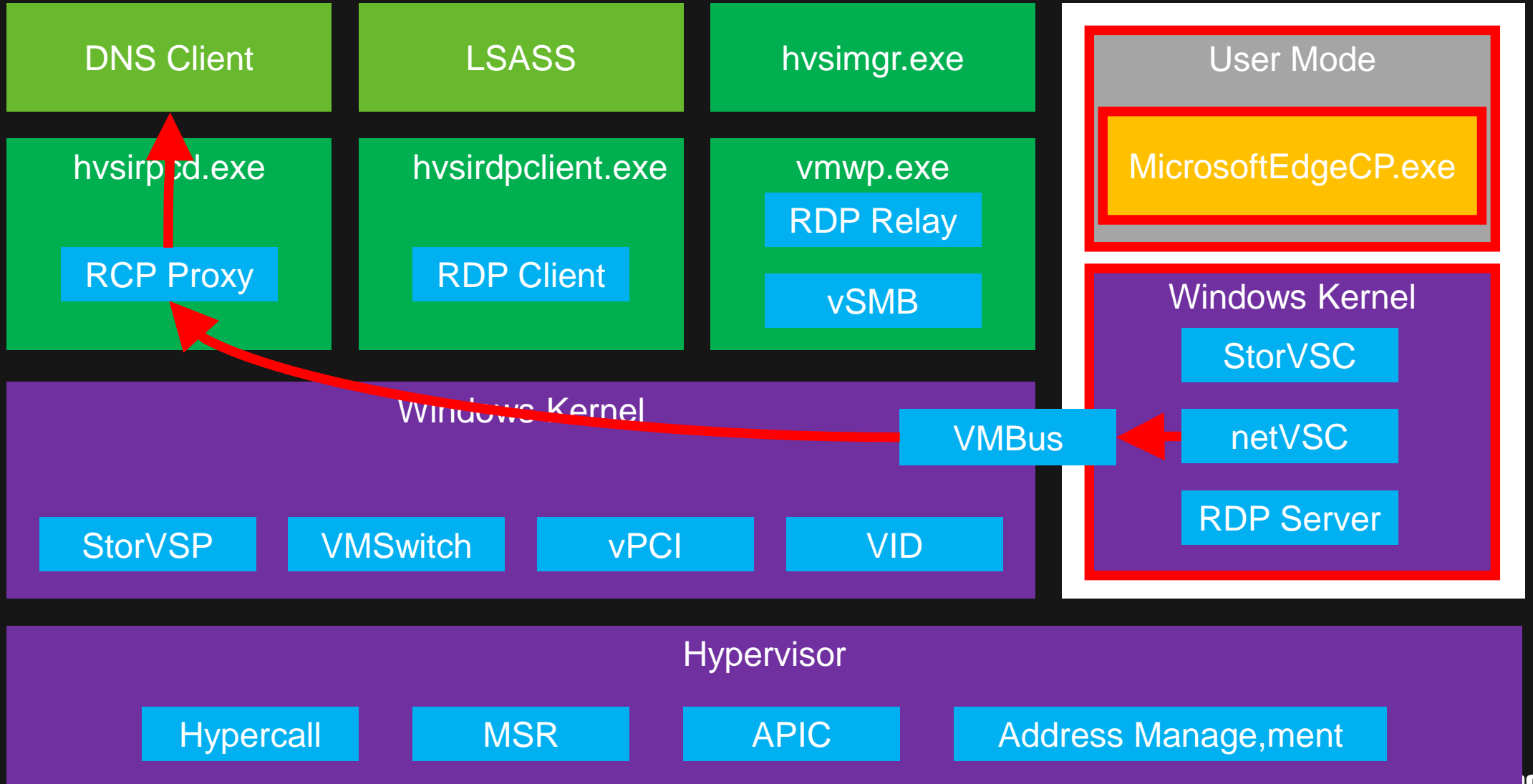
# ▶▶ WDAG Attack Surface



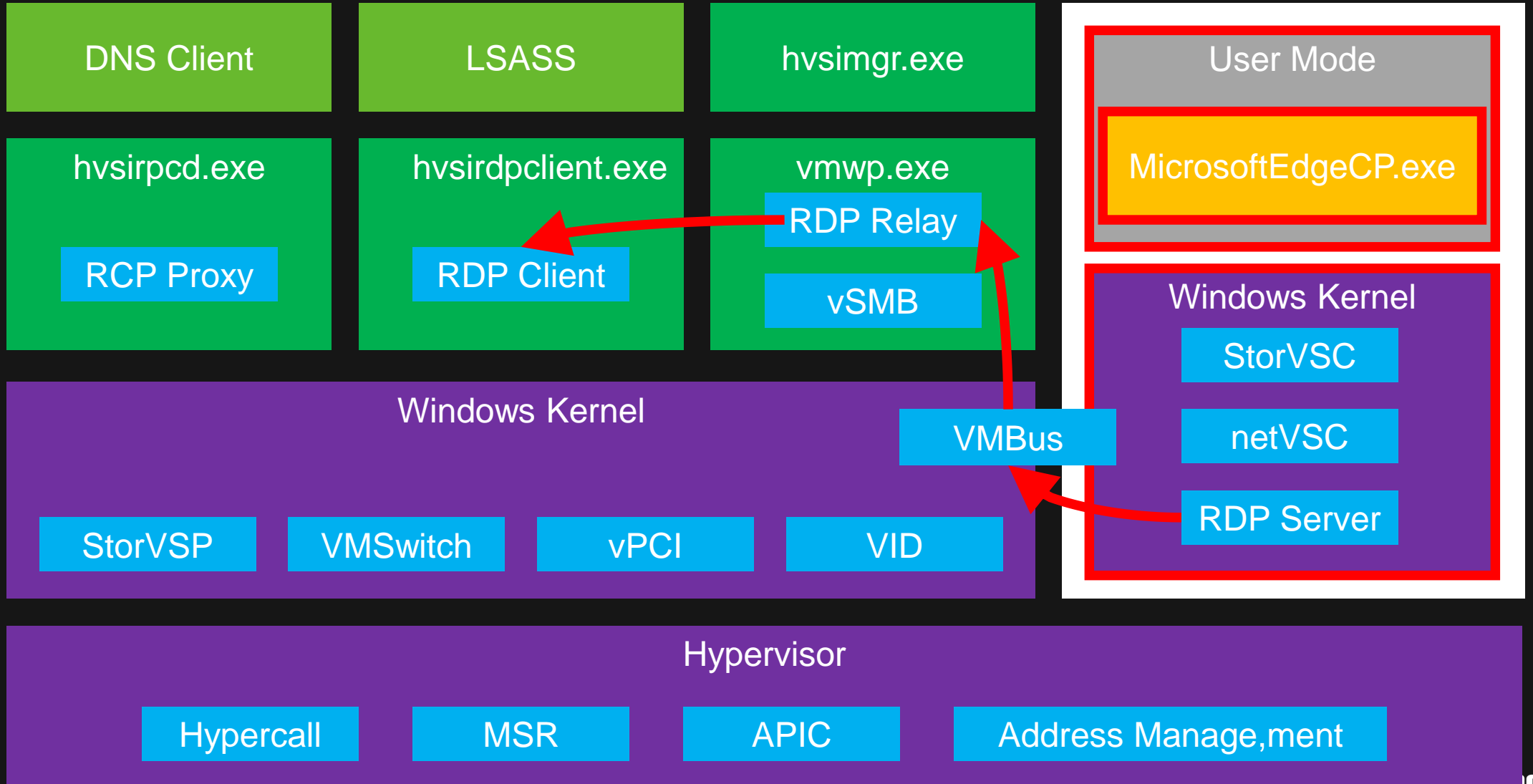
# ▶▶ WDAG Attack Surface



# ▶▶ WDAG Attack Surface



# ▶▶ WDAG Attack Surface





# Q&A







# Thanks!

