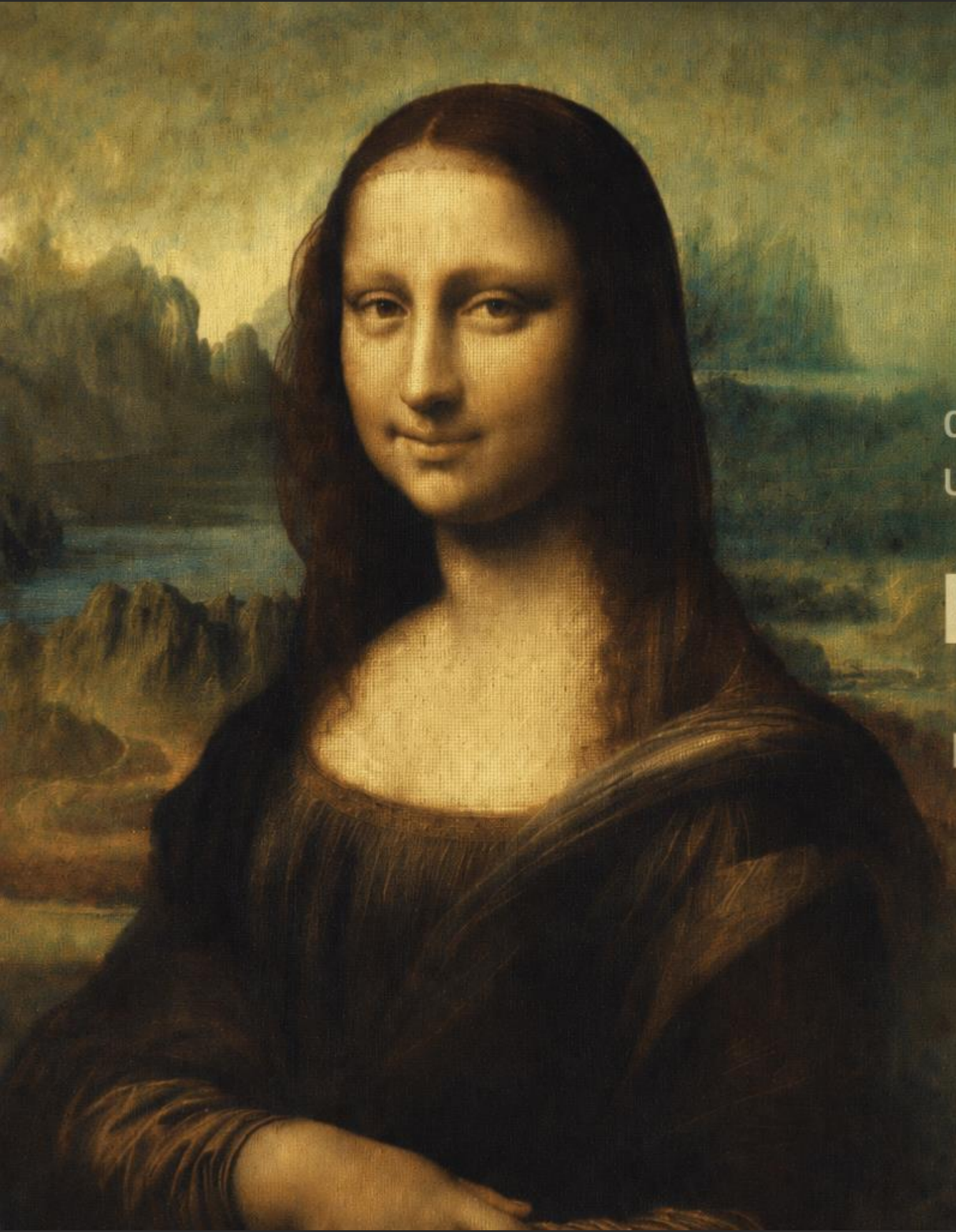


kaspersky

0x800706BA: RPC_S_SERVER
UNAVAILABLE (1722)

PhantomRPC

Haidar Kabibo

black hat®

Whoami?

- Industrial Security Services team, Kasperksy
- Windows Security Researches
- Masters of None:
  - Pentest
  - RE
  - AppSec
  - ICS
  - Network
  - Radio

https://sud0ru.ghost.io/research-work/





The Exception that Started Everything

svchost.exe - PID: 1308 - Module: kernelbase.dll - Thread: 5228 - x64dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help Aug 15 2023 (TitanEngine)

CPU | Log | Notes | Breakpoints | Memory Map | Call Stack | SEH | Script | Symbols | Source | References | Threads | Handles | Trace

```
RIP→ 00007FFACC8BFF6C   0F1F4400 00          nop dword pt
     00007FFACC8BFF71   48:8B8C24 C0000000  mov rcx,qwo
     00007FFACC8BFF79   48:33CC             xor rcx,rsp
     00007FFACC8BFF7C   E8 AFC50800         call kernell
     00007FFACC8BFF81   48:81C4 D8000000    add rsp,D8
     00007FFACC8BFF88   C3                  ret
     00007FFACC8BFF89   CC                  int3
     00007FFACC8BFF8A   836424 38 00        and dword pt
     00007FFACC8BFF8F   EB CF               jmp kernelba
     00007FFACC8BFF91   CC                  int3
     00007FFACC8BFF92   CC                  int3
     00007FFACC8BFF93   CC                  int3
     00007FFACC8BFF94   CC                  int3
     00007FFACC8BFF95   CC                  int3
     00007FFACC8BFF96   CC                  int3
```

```
dword ptr ds:[rax+rax*1]=[A000A0]=???
eax=500050

.text:00007FFACC8BFF6C kernelbase.dll:$1FF6C #1FF6C
```

Hide FPU

```
RAX   0000000000500050
RBX   0000000000000000
RCX   0000000000082867
RDX   000001F7826A1900
RBP   0000000000000008
RSP   000000C2329FF430
RSI   000000C2329FF450
RDI   000000C2329FEE00

R8    000000000000000A
R9    0000000000000030      '0'
R10   0000000000000008
R11   0000000000000030      '0'
R12   00000000000006BA      L'º'
R13   0000000000000000
R14   000001F782823B40
R15   000000C2329FF6B0

RIP   00007FFACC8BFF6C      kernelbase.00007FFACC8BFF6C

RFLAGS   0000000000000204
ZF 0  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1
```

Default (x64 fastcall) 5 Unlocked

```
1: rcx 0000000000082867 0000000000082867
2: rdx 000001F7826A1900 000001F7826A1900
3: r8 000000000000000A 000000000000000A
4: r9 0000000000000030 0000000000000030
5: [rsp+28] 0000000000000000 0000000000000000
```

Dump 1 | Dump 2 | Dump 3 | Dump 4 | Dump 5 | Watch 1 | [x=] Locals | Struct

Address	Hex	ASCII
00007FFACF230000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....ÿÿ..
00007FFACF230010	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	¸.......@.......
00007FFACF230020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00007FFACF230030	00 00 00 00 00 00 00 00 00 00 00 00 E0 00 00 00	............à...
00007FFACF230040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	..º..´.Í!¸.LÍ!Th
00007FFACF230050	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
00007FFACF230060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
00007FFACF230070	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode....$.......
00007FFACF230080	DC 40 BF 0D 98 21 D1 5E 98 21 D1 5E 98 21 D1 5E	Ü@¿..!Ñ^.!Ñ^.!Ñ^
00007FFACF230090	7C 51 D1 5F 99 21 D1 5E 7C 51 D2 5F BE 21 D1 5E	|QÑ_.!Ñ^|QÒ_¾!Ñ^
00007FFACF2300A0	7C 51 D5 5F 1A 21 D1 5E 7C 51 DC 5F B3 20 D1 5E	|QÕ_.!Ñ^|QÜ_³ Ñ^

```
000000C2329FF430   000001F782862400
000000C2329FF438   00000000000006BA
000000C2329FF440   0000000000000000
000000C2329FF448   00007FFACF24B3FD
000000C2329FF450   00000081000006BA
000000C2329FF458   0000000000000000
000000C2329FF460   00007FFACC8BFF6C
000000C2329FF468   0000000A00000000
000000C2329FF470   0000000000000002
000000C2329FF478   0000000000000003
000000C2329FF480   000001F78286F070
000000C2329FF488   00007FFACE9C3693
000000C2329FF490   000001F7828623A0
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx Default

Paused | First chance exception on 00007FFACC8BFF6C (000006BA, RPC_S_SERVER_UNAVAILABLE)! | Time Wasted Debugging: 0:04:07:25

svchost.exe - PID: 1308 - Module: kernelbase.dll - Thread: 5228 - x64dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help Aug 15 2023 (TitanEngine)

CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace

```
RIP→ 00007FFACC8BFF6C   0F1F4400 00          nop dword pt
     00007FFACC8BFF71   48:8B8C24 C0000000  mov rcx,qwo
     00007FFACC8BFF79   48:33CC             xor rcx,rsp
     00007FFACC8BFF7C   E8 AFC50800         call kernell
     00007FFACC8BFF81   48:81C4 D8000000    add rsp,D8
     00007FFACC8BFF88   C3                  ret
     00007FFACC8BFF89   CC                  int3
     00007FFACC8BFF8A   836424 38 00        and dword pt
     00007FFACC8BFF8E   EB CE               jmp kernelba
     00007FFACC8BFF93   CC                  int3
     00007FFACC8BFF94   CC                  int3
     00007FFACC8BFF95   CC                  int3
     00007FFACC8BFF96   CC                  int3
```

Paused — First chance exception on 00007FFACC8BFF6C (000006BA, RPC_S_SERVER_UNAVAILABLE)!

```
RAX 0000000000500050
RBX 0000000000000000
RCX 0000000000082867
RDX 000001F7826A1900
RBP 0000000000000008
RSP 000000C2329FF430
RSI 000000C2329FF450
RDI 000000C2329FEE00

R8  000000000000000A
R9  0000000000000030   '0'
R10 0000000000000008
R11 0000000000000030   '0'
R12 00000000000006BA   L'º'
R13 0000000000000000
R14 000001F782823B40

RFLAGS 0000000000000204
ZF 0  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1
```

Hide FPU

```
dword ptr ds:[rax+rax*1]=[A000A0]=???
eax=500050

.text:00007FFACC8BFF6C kernelbase.dll:$1FF6C #1FF6C
```

Default (x64 fastcall) 5 Unlocked

```
1: rcx 0000000000082867 0000000000082867
2: rdx 000001F7826A1900 000001F7826A1900
3: r8 000000000000000A 000000000000000A
4: r9 0000000000000030 0000000000000030
5: [rsp+28] 0000000000000000 0000000000000000
```

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals Struct

Address	Hex	ASCII
00007FFACF230000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ.....ÿÿ..
00007FFACF230010	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	¸.......@.......
00007FFACF230020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
00007FFACF230030	00 00 00 00 00 00 00 00 00 00 00 00 E0 00 00 00	............à...
00007FFACF230040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	..º..´.Í!¸.LÍ!Th
00007FFACF230050	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
00007FFACF230060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
00007FFACF230070	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode....$.......
00007FFACF230080	DC 40 BF 0D 98 21 D1 5E 98 21 D1 5E 98 21 D1 5E	Ü@¿..!Ñ^.!Ñ^.!Ñ^
00007FFACF230090	7C 51 D1 5F 99 21 D1 5E 7C 51 D2 5F BE 21 D1 5E	|QÑ_.!Ñ^|QÒ_¾!Ñ^
00007FFACF2300A0	7C 51 D5 5F 1A 21 D1 5E 7C 51 DC 5F B3 20 D1 5E	|QÕ_.!Ñ^|QÜ_³ Ñ^

```
000000C2329FF430  000001F782862400
000000C2329FF438  00000000000006BA
000000C2329FF440  0000000000000000
000000C2329FF448  00007FFACF24B3FD
000000C2329FF450  00000081000006BA
000000C2329FF458  0000000000000000
000000C2329FF460  00007FFACC8BFF6C
000000C2329FF468  0000000A00000000
000000C2329FF470  0000000000000002
000000C2329FF478  0000000000000003
000000C2329FF480  000001F78286F070
000000C2329FF488  00007FFACE9C3693
000000C2329FF490  000001F7828623A0
```

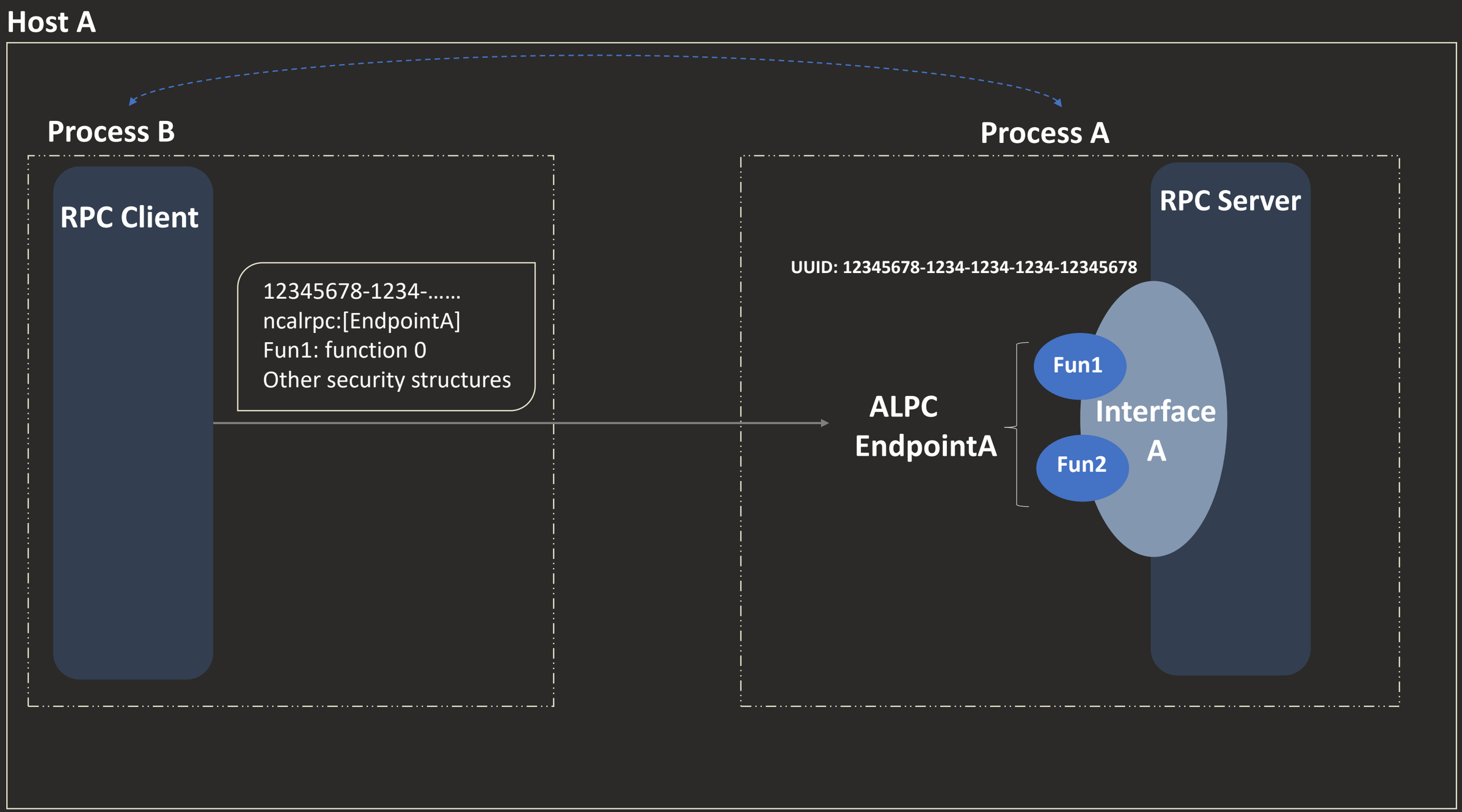
Command: Commands are comma separated (like assembly instructions): mov eax, ebx — Default

Paused — First chance exception on 00007FFACC8BFF6C (000006BA, RPC_S_SERVER_UNAVAILABLE)! — Time Wasted Debugging: 0:04:07:25

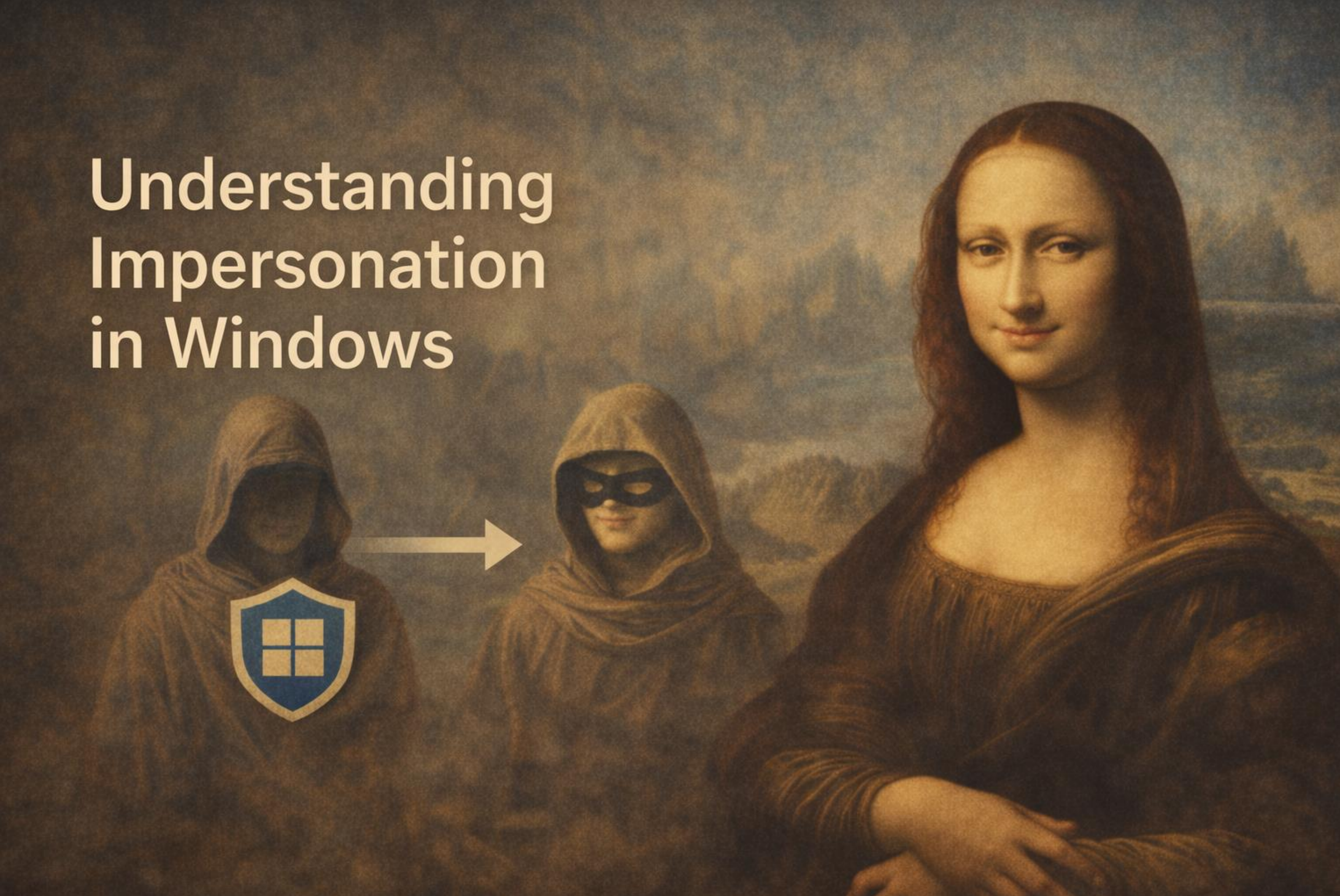


RPC crash course

What Is MSRPC?



Understanding Impersonation in Windows



What Is Impersonation?

- Impersonation allows a process with one identity to temporarily assume another identity for the purpose of access checks.
- In this presentation, we focus on impersonation in RPC.
- In RPC, the server can impersonate the client using the **RpcImpersonateClient** API.

- Security Quality of Service (SQoS) features control the server’s ability to impersonate a client.
- They are defined by the _SECURITY_QUALITY_OF_SERVICE structure.

What Is Impersonation?

- Security Quality of Service (SQoS) features control the server’s ability to impersonate a client.
- They are defined by the _SECURITY_QUALITY_OF_SERVICE structure.

What Is Impersonation?

- Security Quality of Service (SQoS) features control the server’s ability to impersonate a client.
- They are defined by the _SECURITY_QUALITY_OF_SERVICE structure.

C++

```
typedef struct _SECURITY_QUALITY_OF_SERVICE {
  DWORD                            Length;
  SECURITY_IMPERSONATION_LEVEL     ImpersonationLevel;
  SECURITY_CONTEXT_TRACKING_MODE ContextTrackingMode;
  BOOLEAN                          EffectiveOnly;
} SECURITY_QUALITY_OF_SERVICE, *PSECURITY_QUALITY_OF_SERVICE;
```

What Is Impersonation?

- Security Quality of Service (SQoS) features control the server's ability to impersonate a client.
- They are defined by the _SECURITY_QUALITY_OF_SERVICE structure.
- SQoS provides four impersonation levels:
  - Anonymous
  - Identification
  - Impersonation
  - Delegation

```C++
typedef struct _SECURITY_QUALITY_OF_SERVICE {
  DWORD                            Length;
  SECURITY_IMPERSONATION_LEVEL     ImpersonationLevel;
  SECURITY_CONTEXT_TRACKING_MODE   ContextTrackingMode;
  BOOLEAN                          EffectiveOnly;
} SECURITY_QUALITY_OF_SERVICE, *PSECURITY_QUALITY_OF_SERVICE;
```

- For an RPC server process to impersonate an RPC client, the server process must have the SeImpersonatePrivilege enabled in its token.

The Exception That Changed Everything

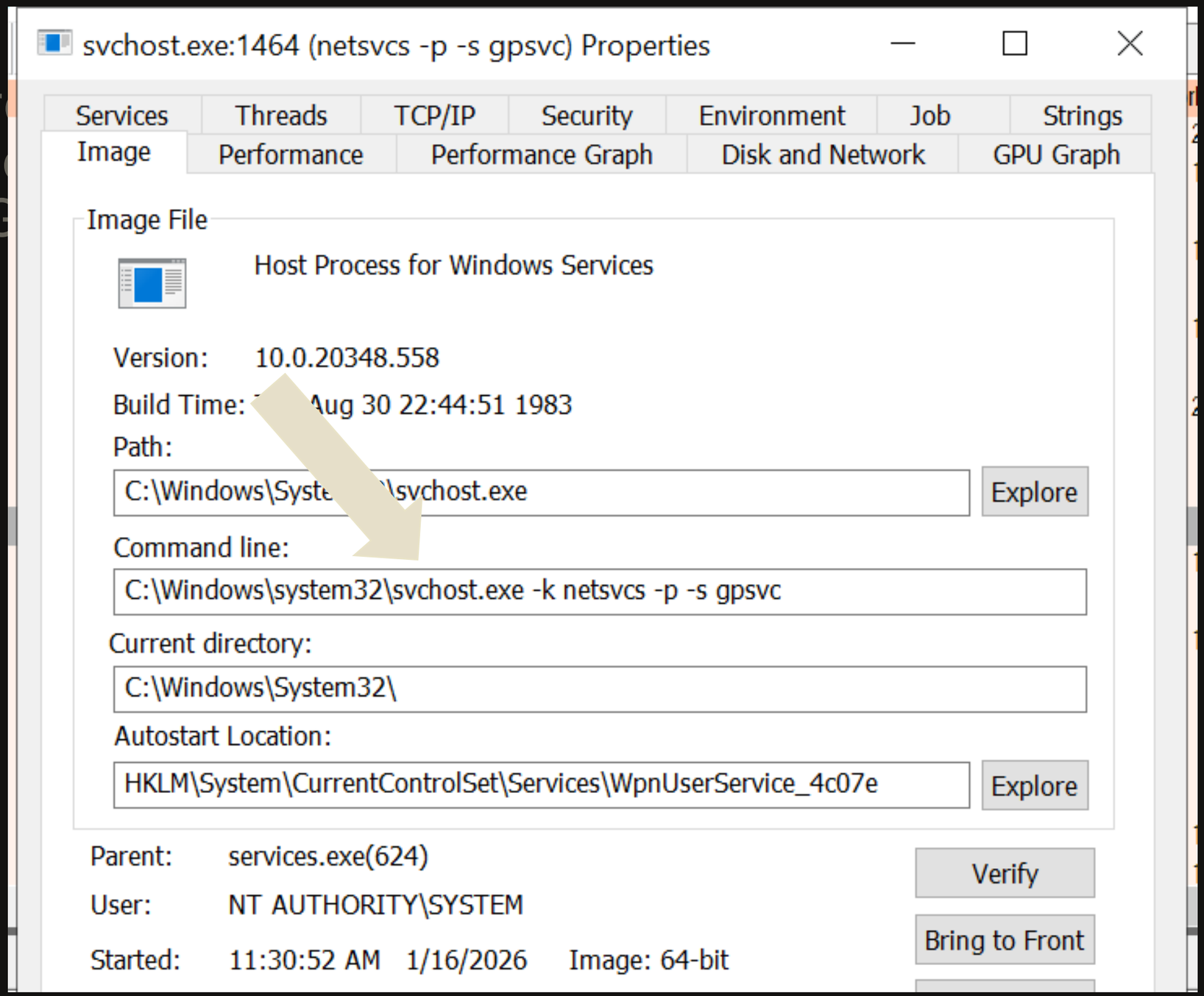


GPSVC Service

- GPSVC (Group Policy Client Service) is a core Windows service responsible for applying and enforcing Group Policy settings on a system.

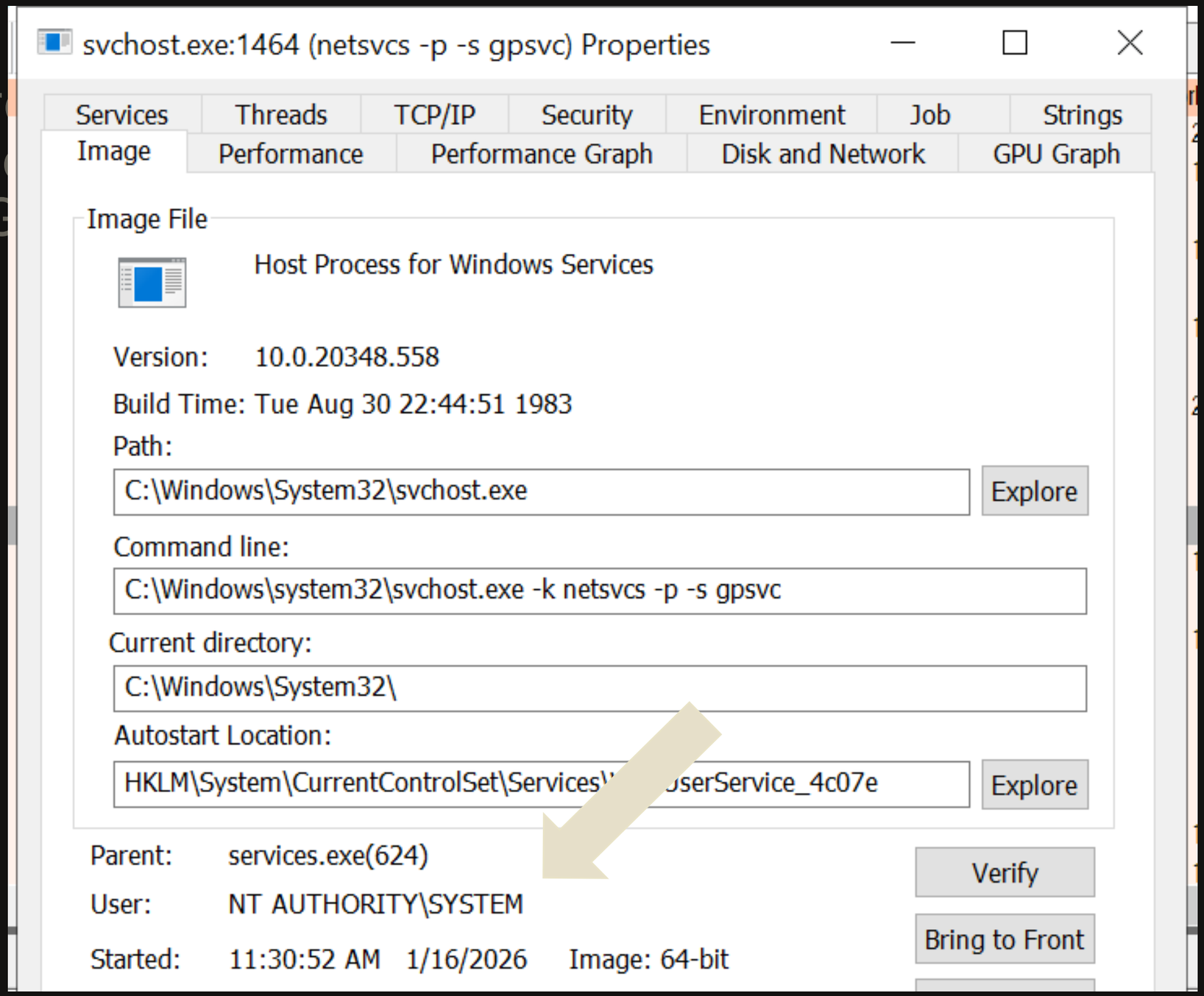
GPSVC Service

- GPSVC (Gr
  Windows s
  enforcing G



GPSVC Service

- GPSVC (Gr
  Windows s
  enforcing G



GPSVC Service

- GPSVC (Group Policy Client Service) is a core Windows service responsible for applying and enforcing Group Policy settings on a system.

- It runs as SYSTEM under svchost.exe.

- While debugging this service, an exception consistently occurred when triggering a policy refresh using gpupdate /force.

Follow the Exception

First chance exception on 00007FFACC8BFF6C (000006BA, RPC_S_SERVER_UNAVAILABLE)!

Follow the Exception

```
First chance exception on 00007FFACC8BFF6C (000006BA, RPC_S_SERVER_UNAVAILABLE)!
```

- The exception encountered was **0x800706BA**
  - RPC_S_SERVER_UNAVAILABLE, 1722
- “RPC client could not reach the target server”
- The exception was raised by rpcrt4.dll

Follow the Exception

- The root cause was a call to NtAlpcConnectPort, used by RPC to establish an ALPC connection between processes.

Follow the Exception

- The root cause was a call to NtAlpcConnectPort, used by RPC to establish an ALPC connection between processes.

```
NTSTATUS NTAPI NtAlpcConnectPort(
    _Out_ PHANDLE PortHandle,
    _In_ PUNICODE_STRING PortName,
    _In_opt_ POBJECT_ATTRIBUTES ObjectAttributes,
    _In_opt_ PALPC_PORT_ATTRIBUTES PortAttributes,
    _In_ DWORD ConnectionFlags,
    _In_opt_ PSID RequiredServerSid,
    _In_opt_ PPORT_MESSAGE ConnectionMessage,
    _Inout_opt_ PSIZE_T ConnectMessageSize,
    _In_opt_ PALPC_MESSAGE_ATTRIBUTES OutMessageAttributes,
    _In_opt_ PALPC_MESSAGE_ATTRIBUTES InMessageAttributes,
    _In_opt_ PLARGE_INTEGER Timeout
);
```

Follow the Exception

- The root cause was a call to NtAlpcConnectPort, used by RPC to establish an ALPC connection between processes.

```
typedef struct _ALPC_PORT_ATTRIBUTES
{
    unsigned long Flags;
    SECURITY_QUALITY_OF_SERVICE SecurityQos;
    unsigned __int64 MaxMessageLength;
    unsigned __int64 MemoryBandwidth;
    unsigned __int64 MaxPoolUsage;
    unsigned __int64 MaxSectionSize;
    unsigned __int64 MaxViewSize;
    unsigned __int64 MaxTotalSectionSize;
    ULONG DupObjectTypes;
```

```
NTSTATUS NTAPI NtAlpcConnectPort(
    _Out_ PHANDLE PortHandle,
    _In_ PUNICODE_STRING PortName,
    _In_opt_ POBJECT_ATTRIBUTES ObjectAttributes,
    _In_opt_ PALPC_PORT_ATTRIBUTES PortAttributes,
    _In_ DWORD ConnectionFlags,
    _In_opt_ PSID RequiredServerSid,
    _In_opt_ PPORT_MESSAGE ConnectionMessage,
    _Inout_opt_ PSIZE_T ConnectMessageSize,
    _In_opt_ PALPC_MESSAGE_ATTRIBUTES OutMessageAttributes,
    _In_opt_ PALPC_MESSAGE_ATTRIBUTES InMessageAttributes,
    _In_opt_ PLARGE_INTEGER Timeout
);
```

C++

```
typedef struct _SECURITY_QUALITY_OF_SERVICE {
  DWORD                        Length;
  SECURITY_IMPERSONATION_LEVEL   ImpersonationLevel;
  SECURITY_CONTEXT_TRACKING_MODE ContextTrackingMode;
  BOOLEAN                      EffectiveOnly;
} SECURITY_QUALITY_OF_SERVICE, *PSECURITY_QUALITY_OF_SERVICE;
```

Follow the Exception

```
00007FFF3A91F665    mov qword ptr ss:[rsp+50],r12
00007FFF3A91F66A    lea rax,qword ptr ss:[rbp+60]
00007FFF3A91F66E    mov qword ptr ss:[rsp+48],rax
00007FFF3A91F673    lea r8,qword ptr ss:[rbp-58]
00007FFF3A91F677    mov qword ptr ss:[rsp+40],r11
00007FFF3A91F67C    lea rdx,qword ptr ss:[rbp-68]
00007FFF3A91F680    mov qword ptr ss:[rsp+38],r11
00007FFF3A91F685    mov qword ptr ss:[rsp+30],r11
00007FFF3A91F68A    mov qword ptr ss:[rsp+28],rbx
00007FFF3A91F68F    mov dword ptr ss:[rsp+20],r9d
00007FFF3A91F694    lea r9,qword ptr ss:[rbp+10]
00007FFF3A91F698    call qword ptr ds:[<NtAlpcConnectPort>]
```

Follow the Exception

```
00007FFF3A91F665    mov qword ptr ss:[rsp+50],r12
00007FFF3A91F66A    lea rax,qword ptr ss:[rbp+60]
00007FFF3A91F66E    mov qword ptr ss:[rsp+48],rax
00007FFF3A91F673    lea r8,qword ptr ss:[rbp-58]
00007FFF3A91F677    mov qword ptr ss:[rsp+40],r11
00007FFF3A91F67C    lea rdx,qword ptr ss:[rbp-68]
00007FFF3A91F680    mov qword ptr ss:[rsp+38],r11
00007FFF3A91F685    mov qword ptr ss:[rsp+30],r11
00007FFF3A91F68A    mov qword ptr ss:[rsp+28],rbx
00007FFF3A91F68F    mov dword ptr ss:[rsp+20],r9d
00007FFF3A91F694    lea r9,qword ptr ss:[rbp+10]
00007FFF3A91F698    call qword ptr ds:[<NtAlpcConnectPort>]
```

```
NTSTATUS NTAPI NtAlpcConnectPort(
    _Out_ PHANDLE PortHandle,
    _In_ PUNICODE_STRING PortName,
    _In_opt_ POBJECT_ATTRIBUTES ObjectAttributes,
    _In_opt_ PALPC_PORT_ATTRIBUTES PortAttributes,
    _In_ DWORD ConnectionFlags,
    _In_opt_ PSID RequiredServerSid,
    _In_opt_ PPORT_MESSAGE ConnectionMessage,
    _Inout_opt_ PSIZE_T ConnectMessageSize,
    _In_opt_ PALPC_MESSAGE_ATTRIBUTES OutMessageAttributes,
    _In_opt_ PALPC_MESSAGE_ATTRIBUTES InMessageAttributes,
    _In_opt_ PLARGE_INTEGER Timeout
);
```

Follow the Exception

```
00007FFF3A91F665    mov qword ptr ss:[rsp+50],r12
00007FFF3A91F66A    lea rax,qword ptr ss:[rbp+60]
00007FFF3A91F66E    mov qword ptr ss:[rsp+48],rax
00007FFF3A91F673    lea r8,qword ptr ss:[rbp-58]
00007FFF3A91F677    mov qword ptr ss:[rsp+40],r11
00007FFF3A91F67C    lea rdx,qword ptr ss:[rbp-68]
00007FFF3A91F680    mov qword ptr ss:[rsp+38],r11
00007FFF3A91F685    mov qword ptr ss:[rsp+30],r11
00007FFF3A91F68A    mov qword ptr ss:[rsp+28],rbx
00007FFF3A91F68F    mov dword ptr ss:[rsp+20],r9d
00007FFF3A91F694    lea r9,qword ptr ss:[rbp+10]
00007FFF3A91F698    call qword ptr ds:[<NtAlpcConnectPort>]
```

Hex												ASCII
5C	00	52	00	50	00	43	00	20	00	43	00	\.R.P.C. .C.
6F	00	6E	00	74	00	72	00	6F	00	6C	00	o.n.t.r.o.l.
5C	00	54	00	65	00	72	00	6D	00	53	00	\.T.e.r.m.S.
72	00	76	00	41	00	70	00	69	00	00	00	r.v.A.p.i...

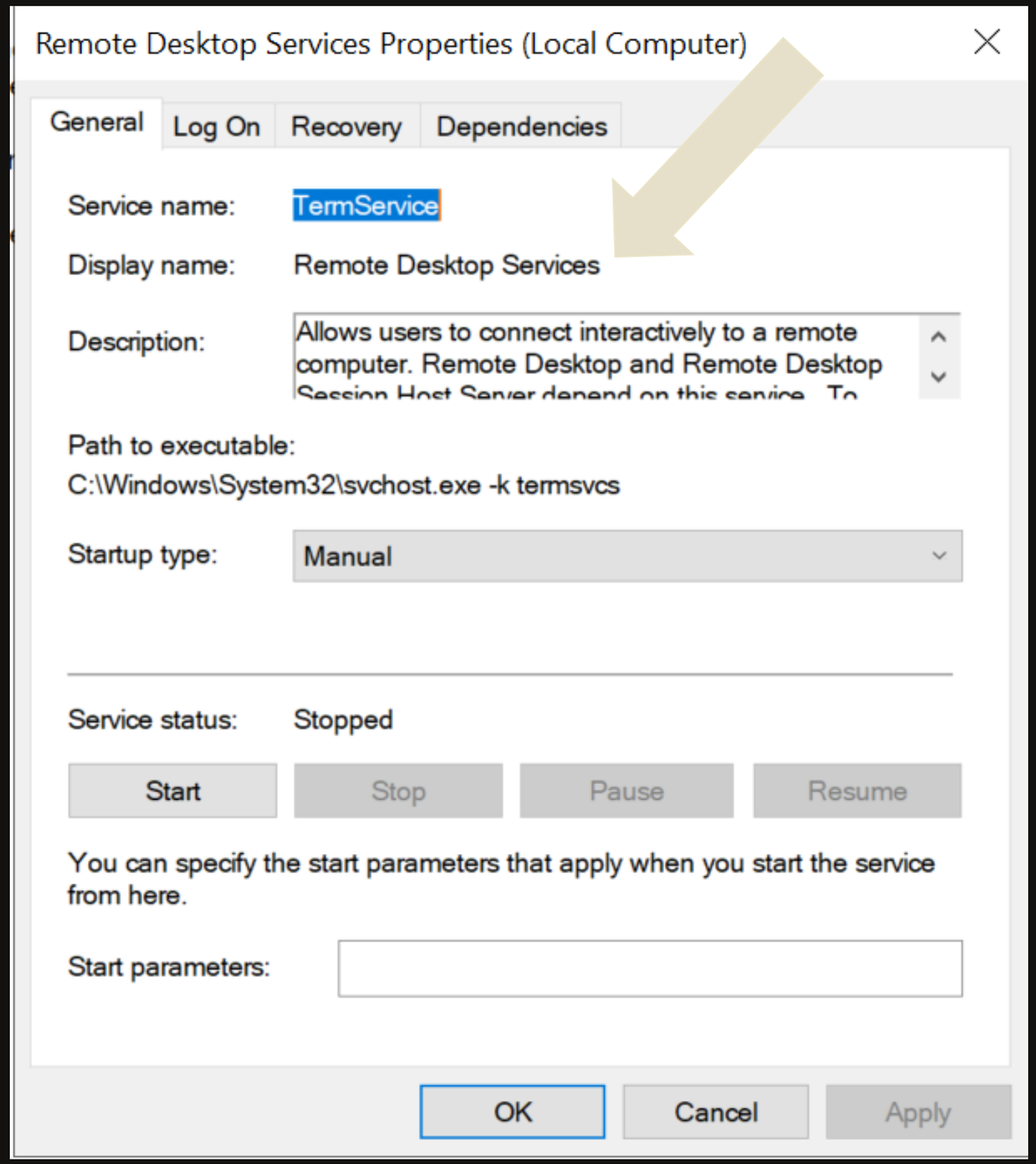
```
NTSTATUS NTAPI NtAlpcConnectPort(
    _Out_ PHANDLE PortHandle,
    _In_ PUNICODE_STRING PortName,
    _In_opt_ POBJECT_ATTRIBUTES ObjectAttributes,
    _In_opt_ PALPC_PORT_ATTRIBUTES PortAttributes,
    _In_ DWORD ConnectionFlags,
    _In_opt_ PSID RequiredServerSid,
    _In_opt_ PPORT_MESSAGE ConnectionMessage,
    _Inout_opt_ PSIZE_T ConnectMessageSize,
    _In_opt_ PALPC_MESSAGE_ATTRIBUTES OutMessageAttributes,
    _In_opt_ PALPC_MESSAGE_ATTRIBUTES InMessageAttributes,
    _In_opt_ PLARGE_INTEGER Timeout
);
```

TermService:

- RPC Control/ TermSrvApi endpoint belongs to TermService

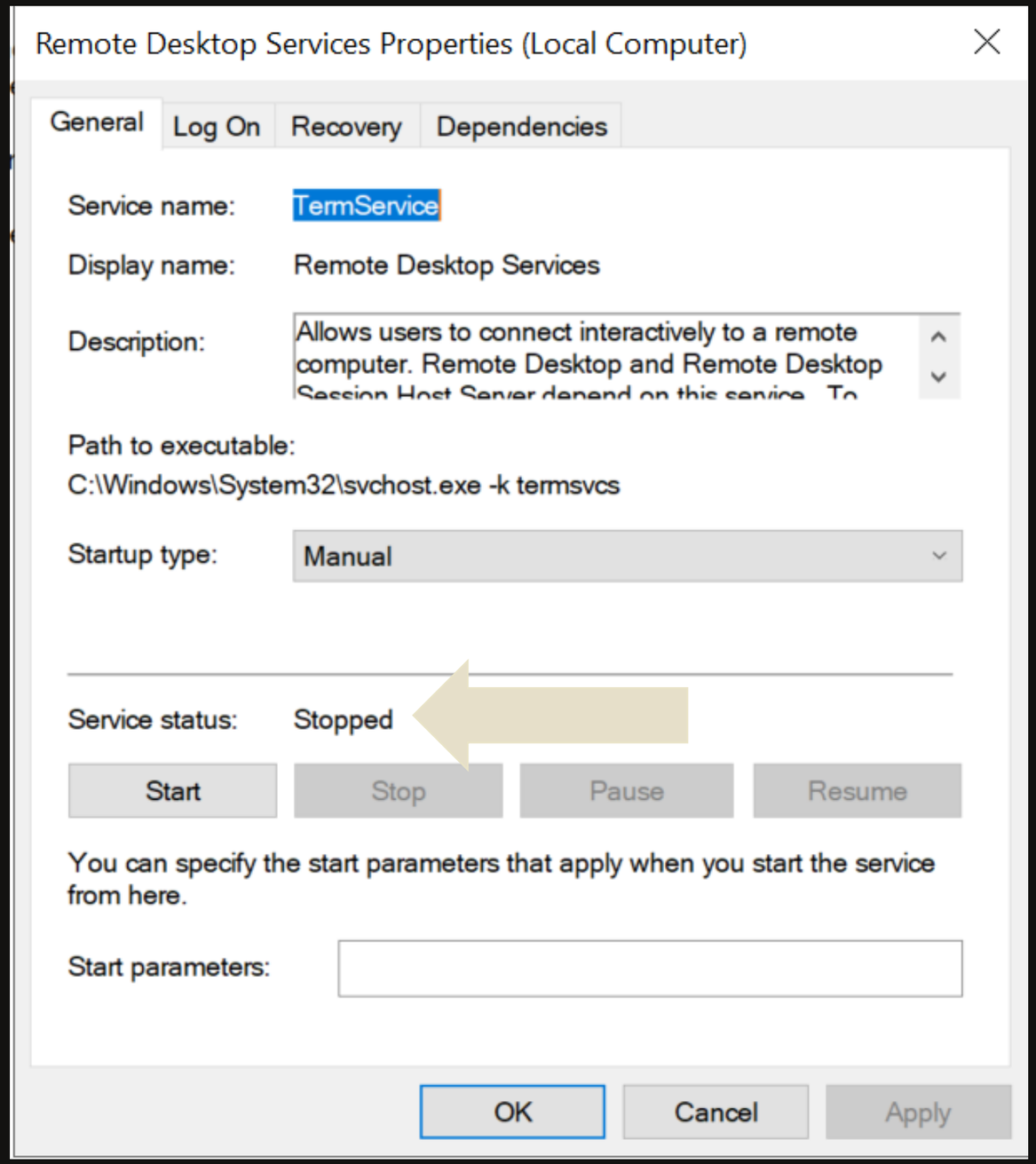
TermService:

- RPC Control/ TermSrvApi endpoint belongs to TermService



TermService:

- RPC Control/ TermSrvApi endpoint belongs to TermService



TermService:

- RPC Control/ TermSrvApi endpoint belongs to TermService
- This service is responsible for remote desktop. By default, it is turned off.

TermService:

- RPC Control/ TermSrvApi endpoint belongs to TermService
- This service is responsible for remote desktop. By default, it is turned off.
- Once the service is enabled and Remote Desktop access is activated, it exposes an RPC server with multiple interfaces and endpoints.
- This service works under NT AUTHORITY\Network Service





WHAT IF I MIMIC THE SERVER !?

Follow the Exception

```
typedef struct _ALPC_PORT_ATTRIBUTES
{
    unsigned long Flags;
    SECURITY_QUALITY_OF_SERVICE SecurityQos;
    unsigned __int64 MaxMessageLength;
    unsigned __int64 MemoryBandwidth;
    unsigned __int64 MaxPoolUsage;
    unsigned __int64 MaxSectionSize;
    unsigned __int64 MaxViewSize;
    unsigned __int64 MaxTotalSectionSize;
    ULONG DupObjectTypes;
```

```
NTSTATUS NTAPI NtAlpcConnectPort(
    _Out_ PHANDLE PortHandle,
    _In_ PUNICODE_STRING PortName,
    _In_opt_ POBJECT_ATTRIBUTES ObjectAttributes,
    _In_opt_ PALPC_PORT_ATTRIBUTES PortAttributes,
    _In_ DWORD ConnectionFlags,
    _In_opt_ PSID RequiredServerSid,
    _In_opt_ PPORT_MESSAGE ConnectionMessage,
    _Inout_opt_ PSIZE_T ConnectMessageSize,
    _In_opt_ PALPC_MESSAGE_ATTRIBUTES OutMessageAttributes,
    _In_opt_ PALPC_MESSAGE_ATTRIBUTES InMessageAttributes,
    _In_opt_ PLARGE_INTEGER Timeout
));
```

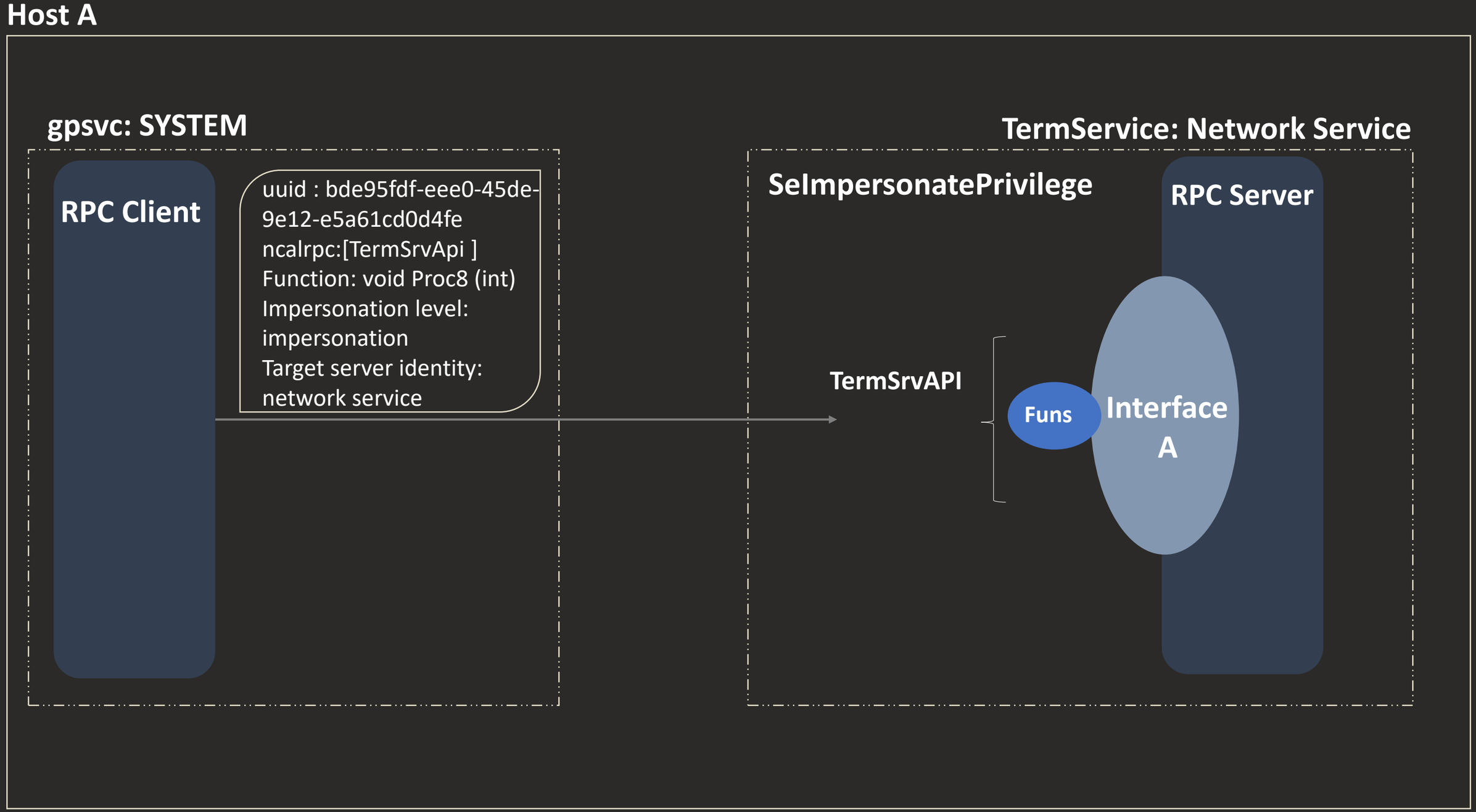
C++

```
typedef struct _SECURITY_QUALITY_OF_SERVICE {
  DWORD                        Length;
  SECURITY_IMPERSONATION_LEVEL ImpersonationLevel;
  SECURITY_CONTEXT_TRACKING_MODE ContextTrackingMode;
  BOOLEAN                      EffectiveOnly;
} SECURITY_QUALITY_OF_SERVICE, *PSECURITY_QUALITY_OF_SERVICE;
```

ImpersonationLevel = Impersonation

😈

GPSVC to RDP


Host A
gpsvc: SYSTEM
RPC Client
uuid : bde95fdf-eee0-45de-9e12-e5a61cd0d4fe
ncalrpc:[TermSrvApi]
Function: void Proc8 (int)
Impersonation level: impersonation
Target server identity: network service
TermService: Network Service
SeImpersonatePrivilege
RPC Server
TermSrvAPI
Funs
Interface A


CASE ONE:
COERCING GROUP
POLICY SERVICE

Exploit/low privilege

SeImpersonatePrivilege

NT AUTHORITY\NETWORK SERVICE

gpupdate.exe /force

??

gpsvc: SYSTEM

RPC Client

Level: Impersonate

??

NT AUTHORITY\NETWORK SERVICE

Malicious executable

RPC Server

UUID

bde95fdf-eee0-45de-9e12-e5a61cd0d4fe

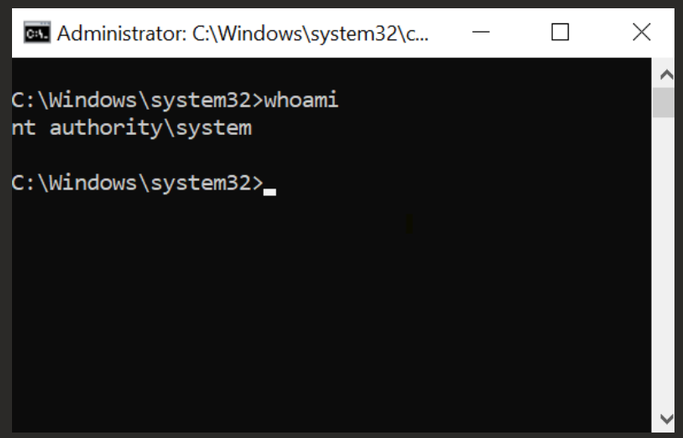
TermSrvAPI

Proc8

Interface

SeImpersonatePrivilege

RpcImpersonateClient





LIVE DEMO

Server 2022 - VMware Workstation 16 Player (Expired license)

Player

System Information

File Edit View Help

System Summary
- Hardware Resources
- Components
- Software Environment

Item	Value
OS Name	Microsoft Windows Server 2022 Standard Evaluation
Version	10.0.20348 Build 20348
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	DCSRV
System Manufacturer	VMware, Inc.
System Model	VMware7,1

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.20348.3207]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c45:491f:53de:b751%3
   IPv4 Address. . . . . . . . . . . : 192.168.177.177
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\Administrator>
```

Total Virtual Memory	2.09 GB
Available Virtual Memory	1.14 GB
Page File Space	704 MB
Page File	C:\pagefile.sys
Kernel DMA Protection	Off
Virtualization-based security	Not enabled
Device Encryption Support	Not Available
A hypervisor has been detecte...	

kali-pen - VMware Workstation 16 Player (Expired license)

Player

Web Command Executor | Web Command Executor

192.168.177.177

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Execute Command

Enter Command | Run Command

Output:

File Upload

Browse... No file selected. | Upload File

Upload Status:

Exploit/low privilege

SeImpersonatePrivilege

NT AUTHORITY\NETWORK SERVICE

gpupdate.exe /force

gpsvc: SYSTEM

RPC Client

Level: Impersonate

NT AUTHORITY\NETWORK SERVICE

Malicious executable

RPC Server

UUID

bde95fdf-eee0-45de-9e12-e5a61cd0d4fe

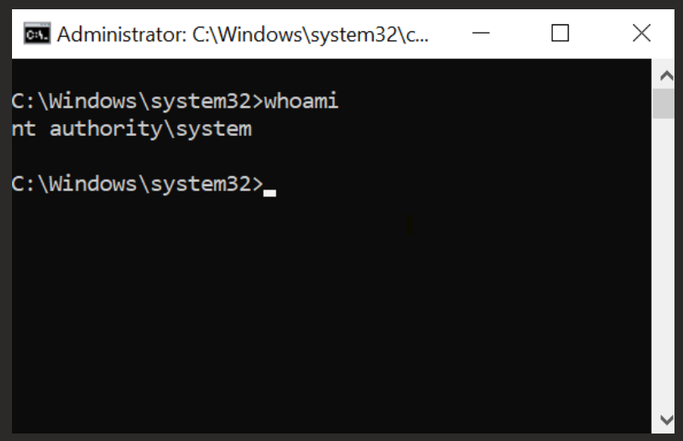
TermSrvAPI

Proc8

Interface

SeImpersonatePrivilege

RpcImpersonateClient

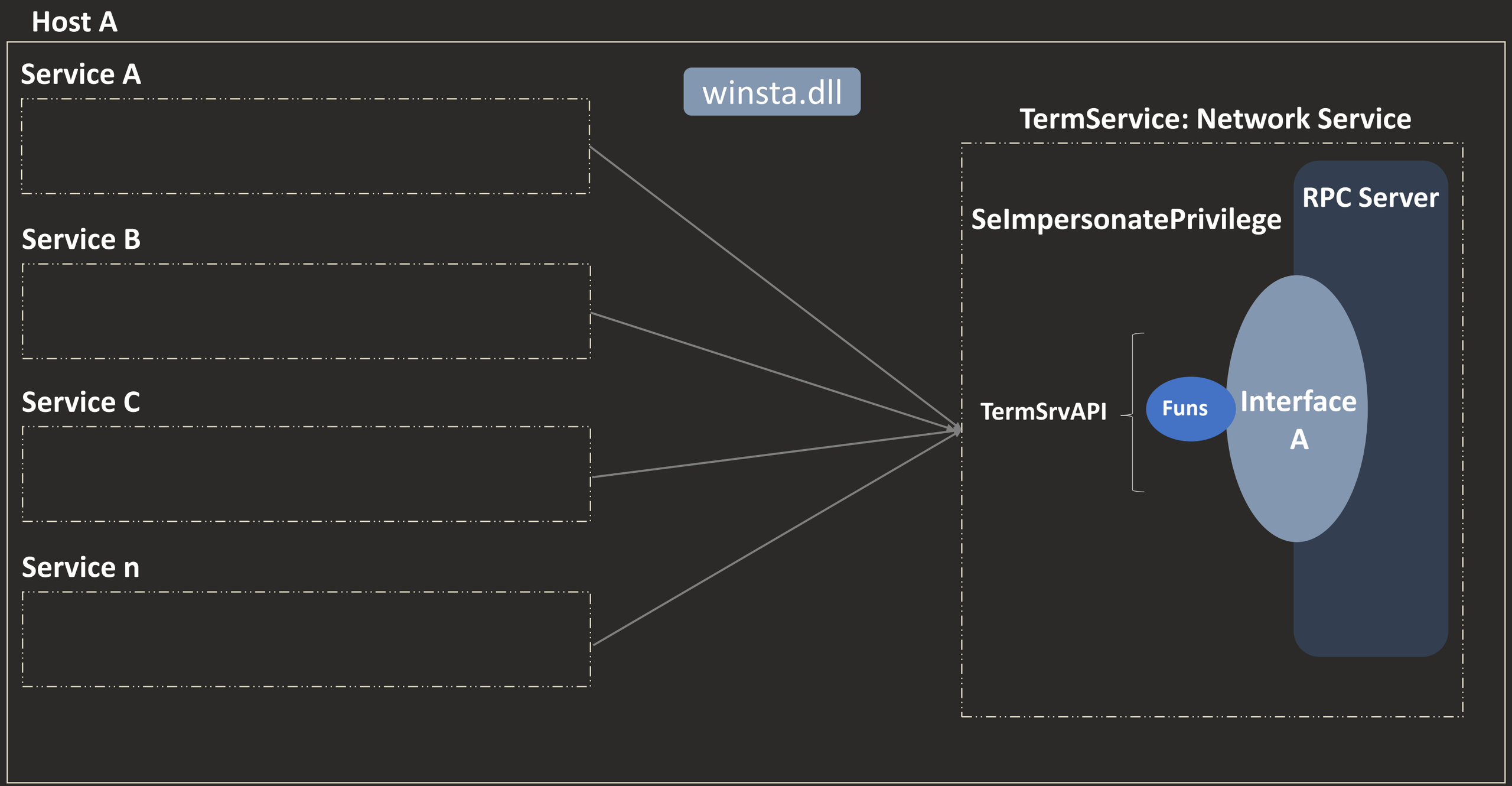


One group policy should be changed at least

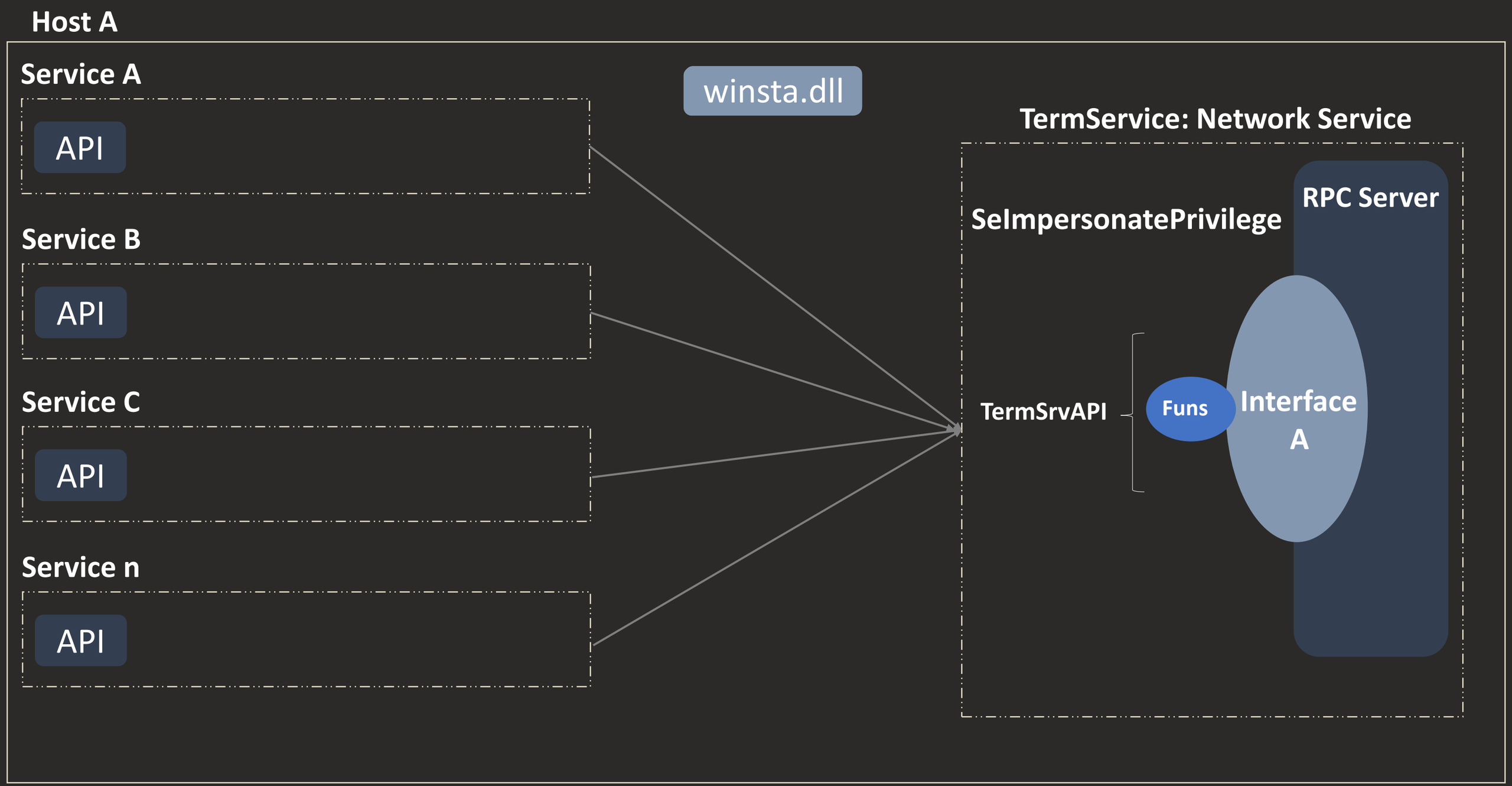

The Exception
That Cannot
Be Controlled

Applying computer settings

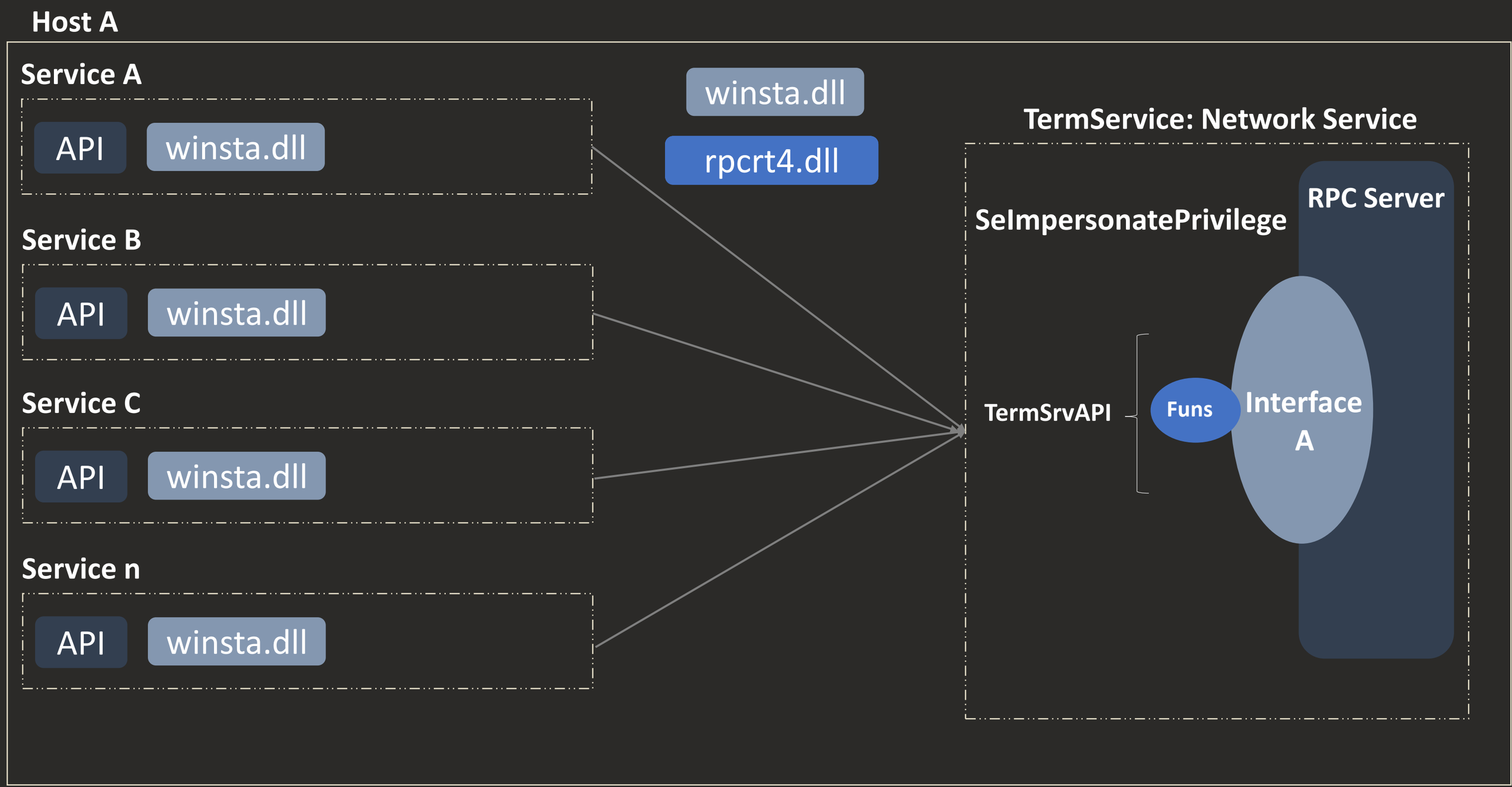
RPC Architecture Flow



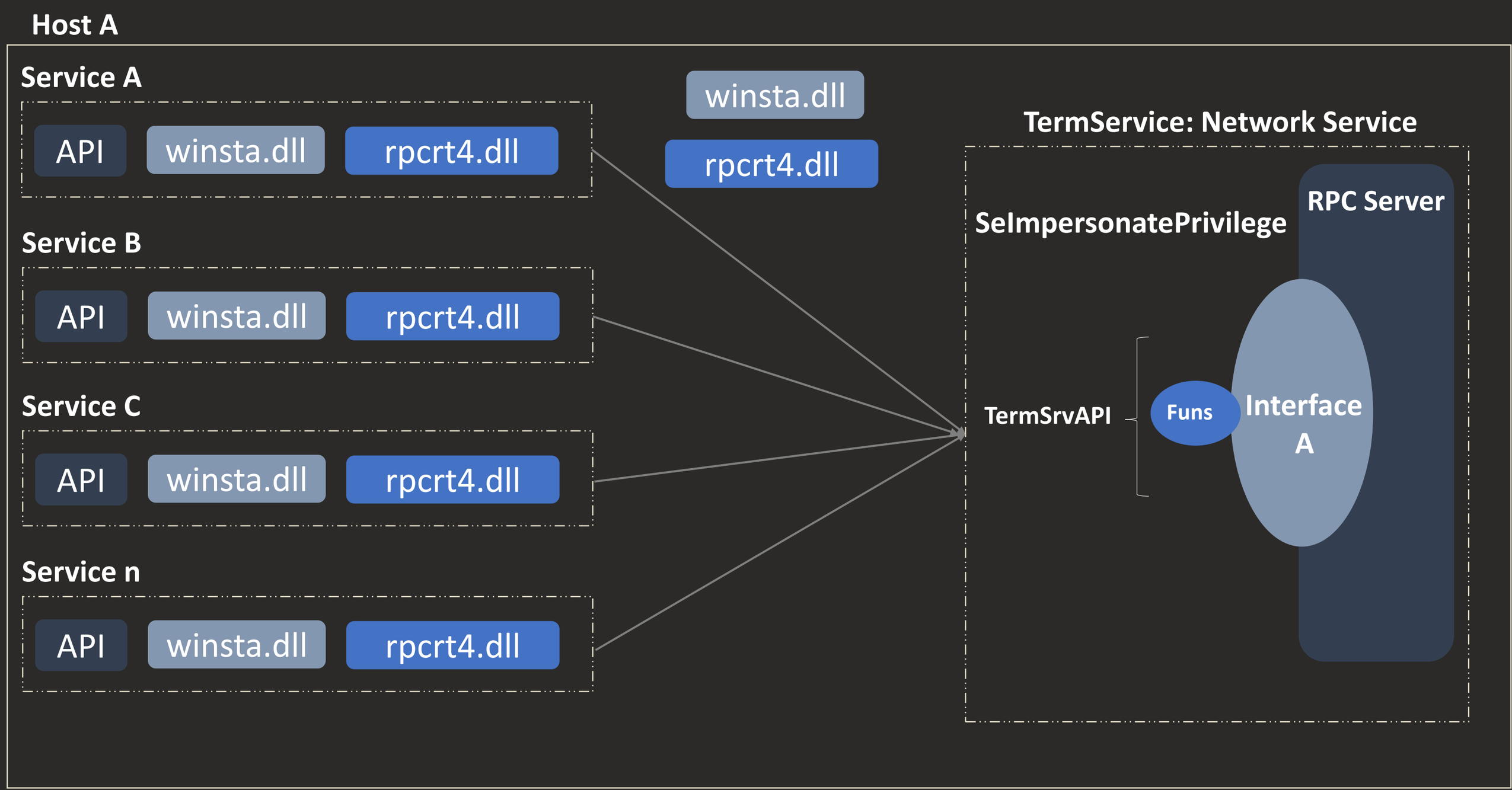
RPC Architecture Flow



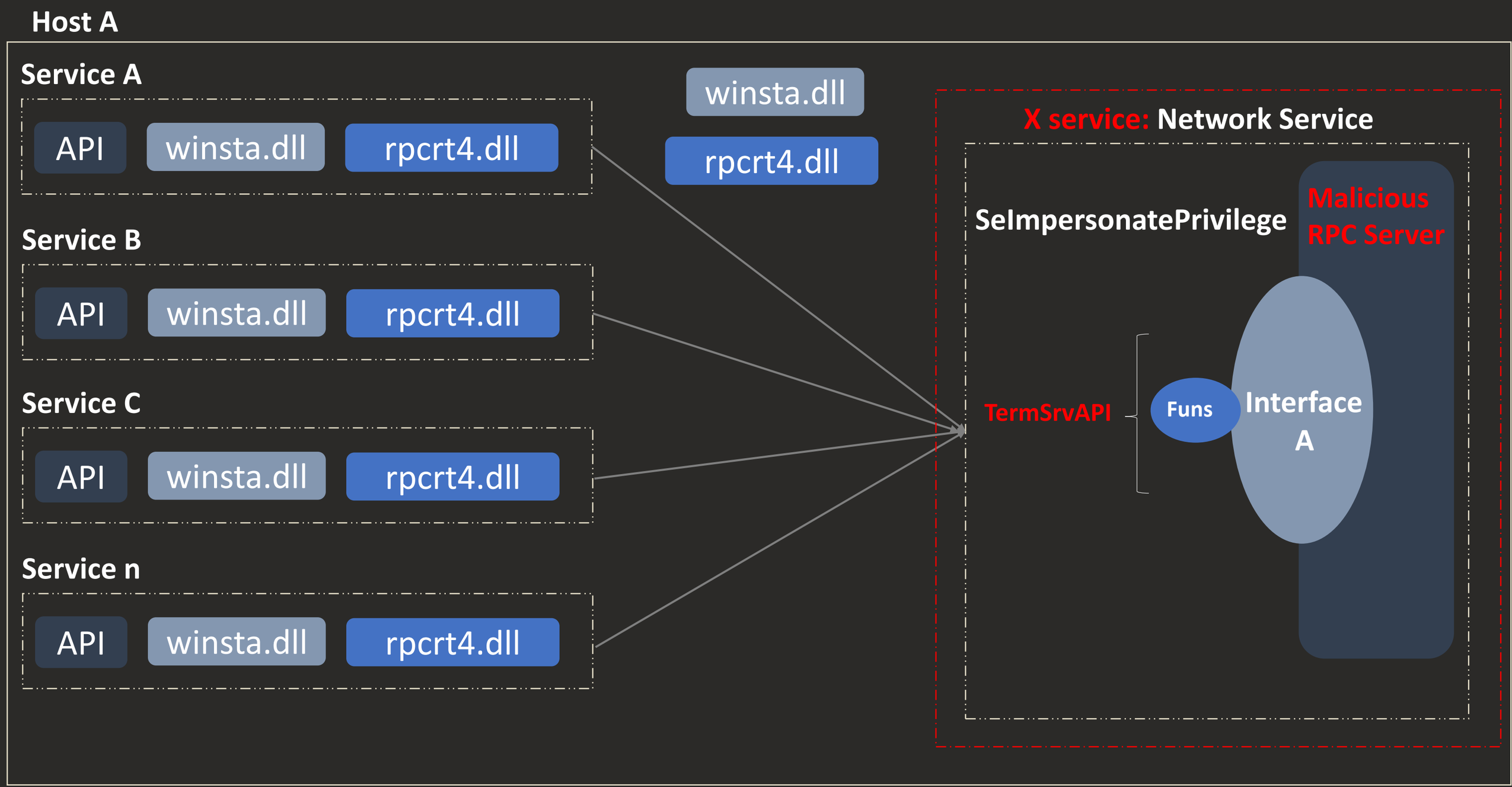
RPC Architecture Flow



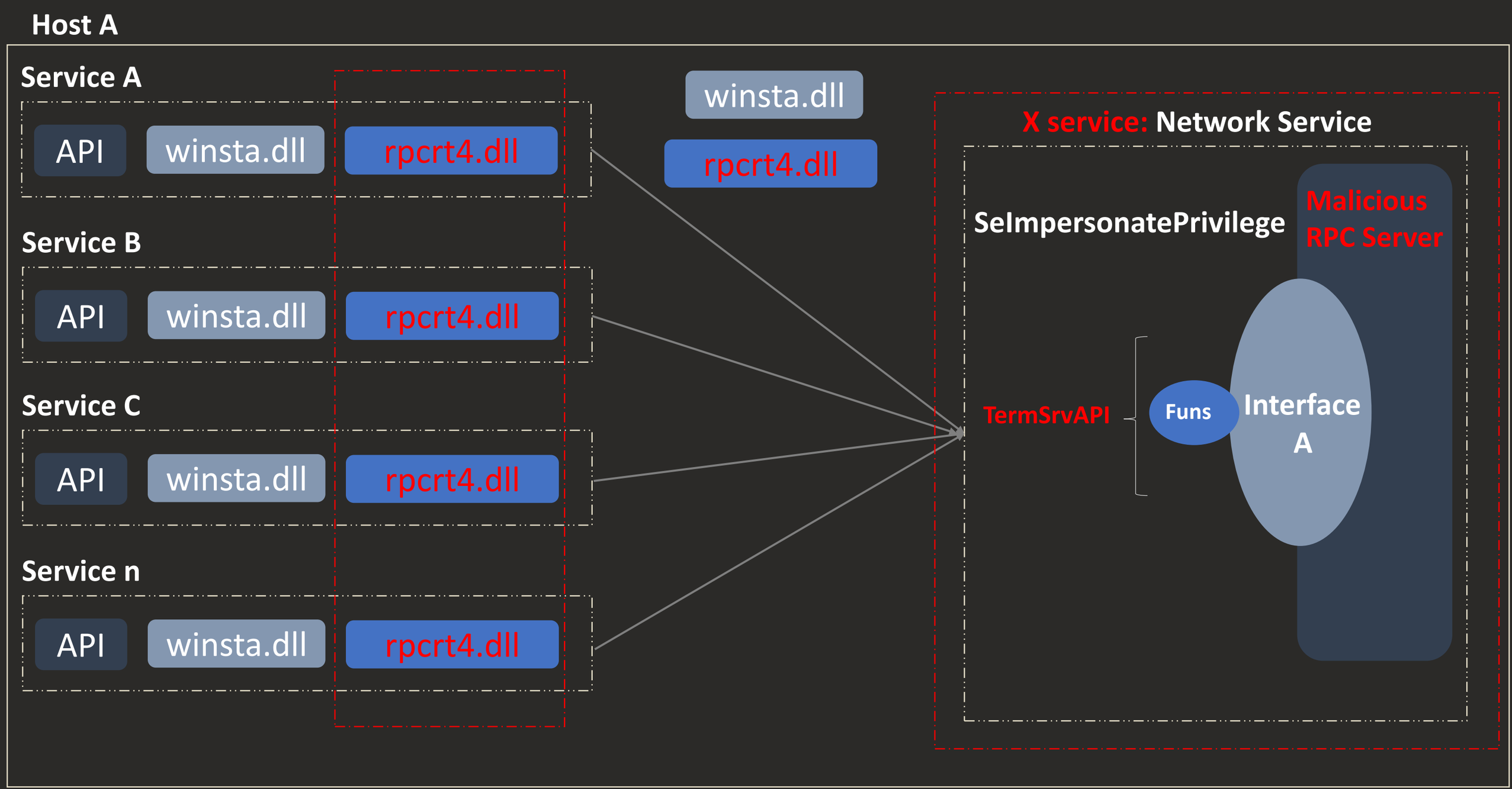
RPC Architecture Flow



RPC Architecture Flow



RPC Architecture Flow



RPC Architecture Flow

Host A

Service A

API

winsta.dll

winsta.dll

Service B

API

winsta.dll

Service C

API

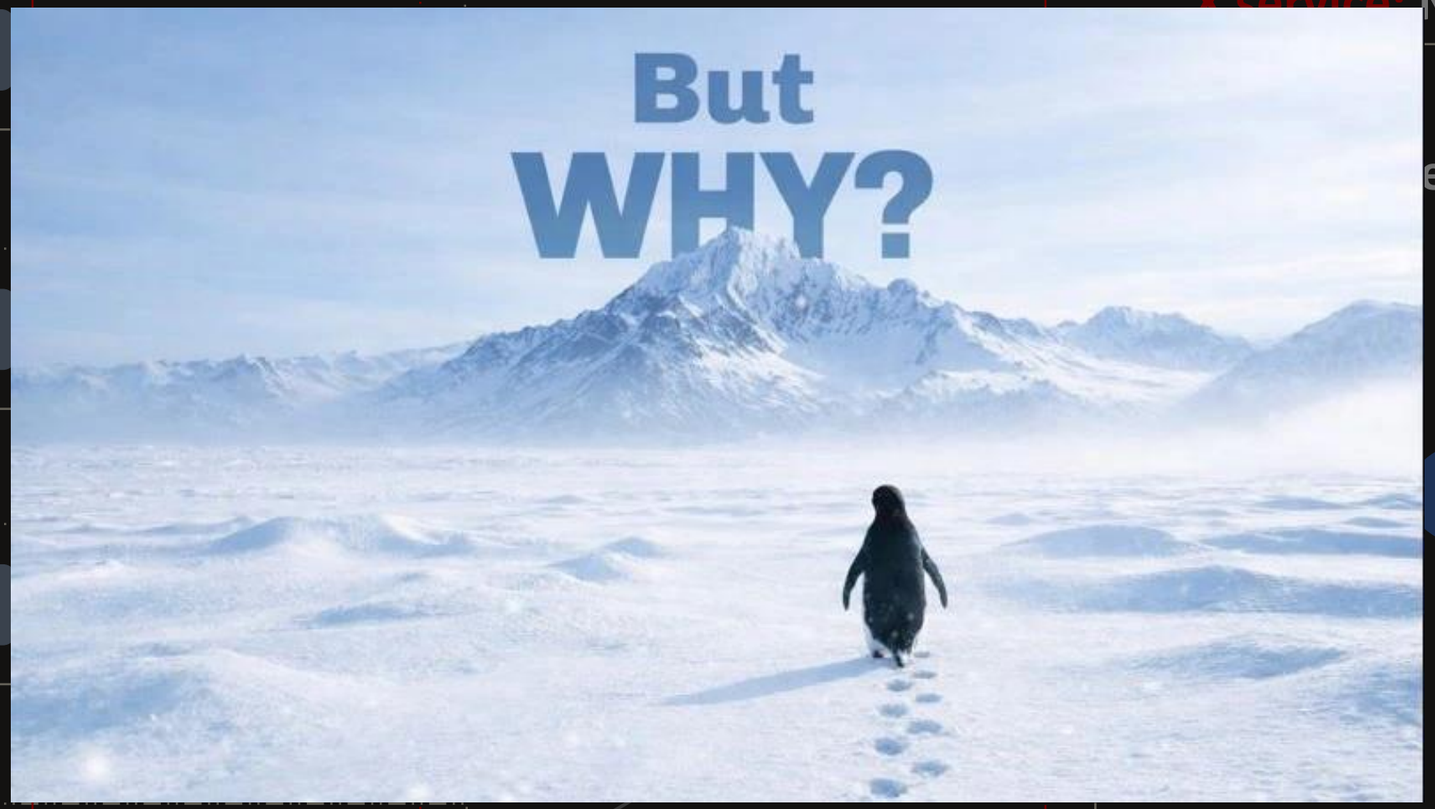
winsta.dll

Service n

API

winsta.dll

rpcrt4.dll



X service: Network Service

ePrivilege

Malicious
RPC Server

Funs

Interface
A

RPC Architecture Flow

Host A

Service A

API winsta.

Service B

API winsta.

Service C

API winsta.

Service n

API winsta.



ork Service

ege

Malicious RPC Server

Interface A

RPC Architecture Flow

- The RPC runtime (rpcrt4.dll) does not provide a mechanism to verify the legitimacy of RPC servers, to addition to that Windows will allow you to deploy the exact same RPC server exposed by legitimate process.

- As a result, this architecture exposes a large attack surface, since RPC is widely used across system DLLs.

- Applications calling seemingly benign APIs can unintentionally trigger local privilege escalation without user awareness.

The Exception That Is Hard to Collect



Properties

1- Exception Properties

- The target exception must be an RPC call failure with status RPC_S_SERVER_UNAVAILABLE.
- To be relevant, the exception should:
  - Originate from a high-privilege process
  - Use a high impersonation level

2- Monitoring Properties

- Allow extraction of key RPC metadata:
  - UUID, Endpoint, and OPNUM
  - Impersonation level and status code
  - Client process privilege, name, and module path

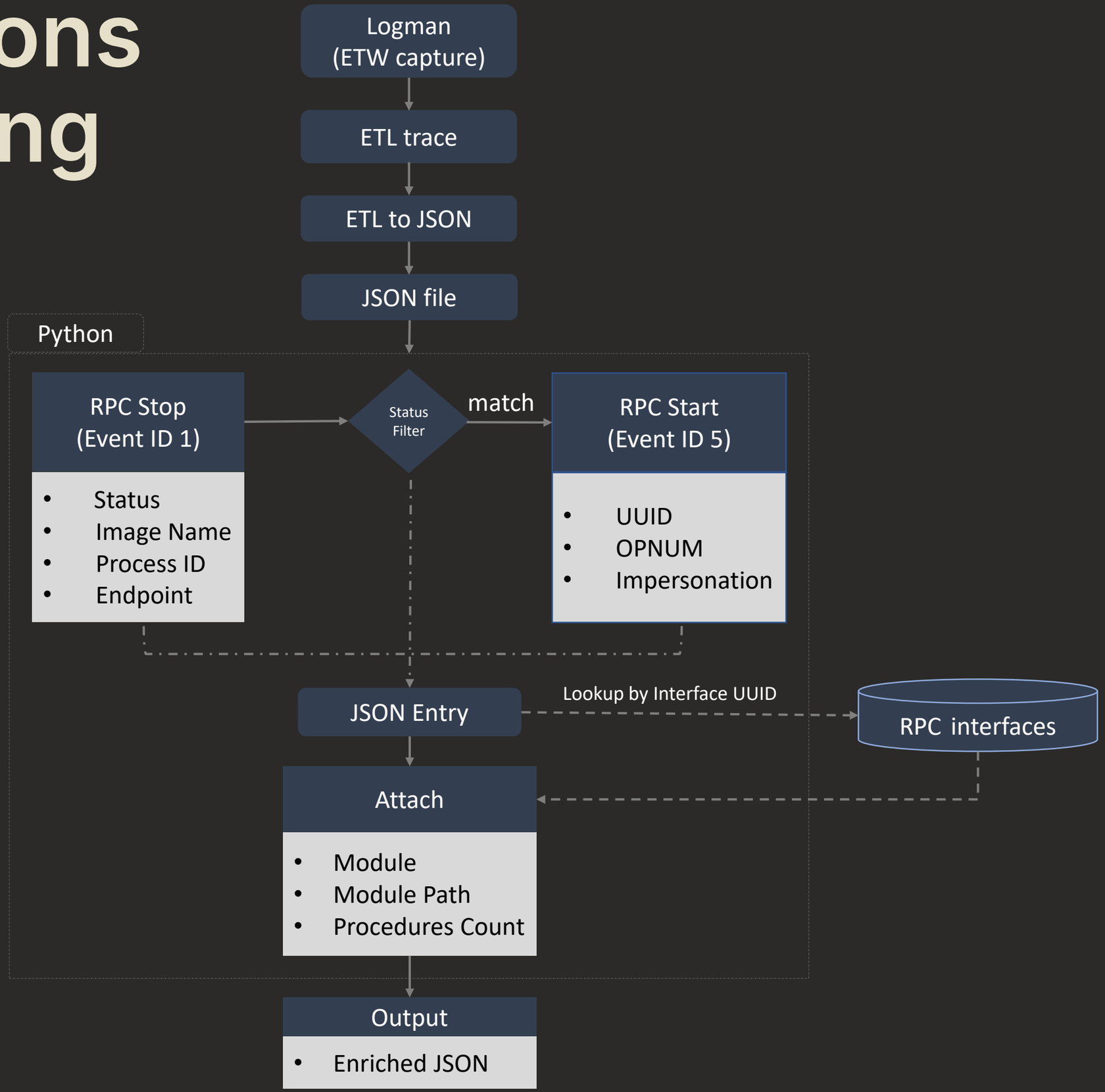
- This information enables mimicking the RPC server and understanding how the call is triggered.

ETW

- ETW (Event Tracing for Windows), Built-in Windows logging framework that captures kernel and user-mode events in real time.
- logman controls ETW by creating trace sessions, selecting providers, and setting verbosity.
- Tracing output is saved as an .etl file, which can be viewed in Event Viewer.
- ETW provides deep visibility into RPC client and server behavior without modifying applications.
- ETW captures RPC bindings, endpoints, interface UUIDs, authentication details, call flow, timing, and status code



Exceptions Collecting



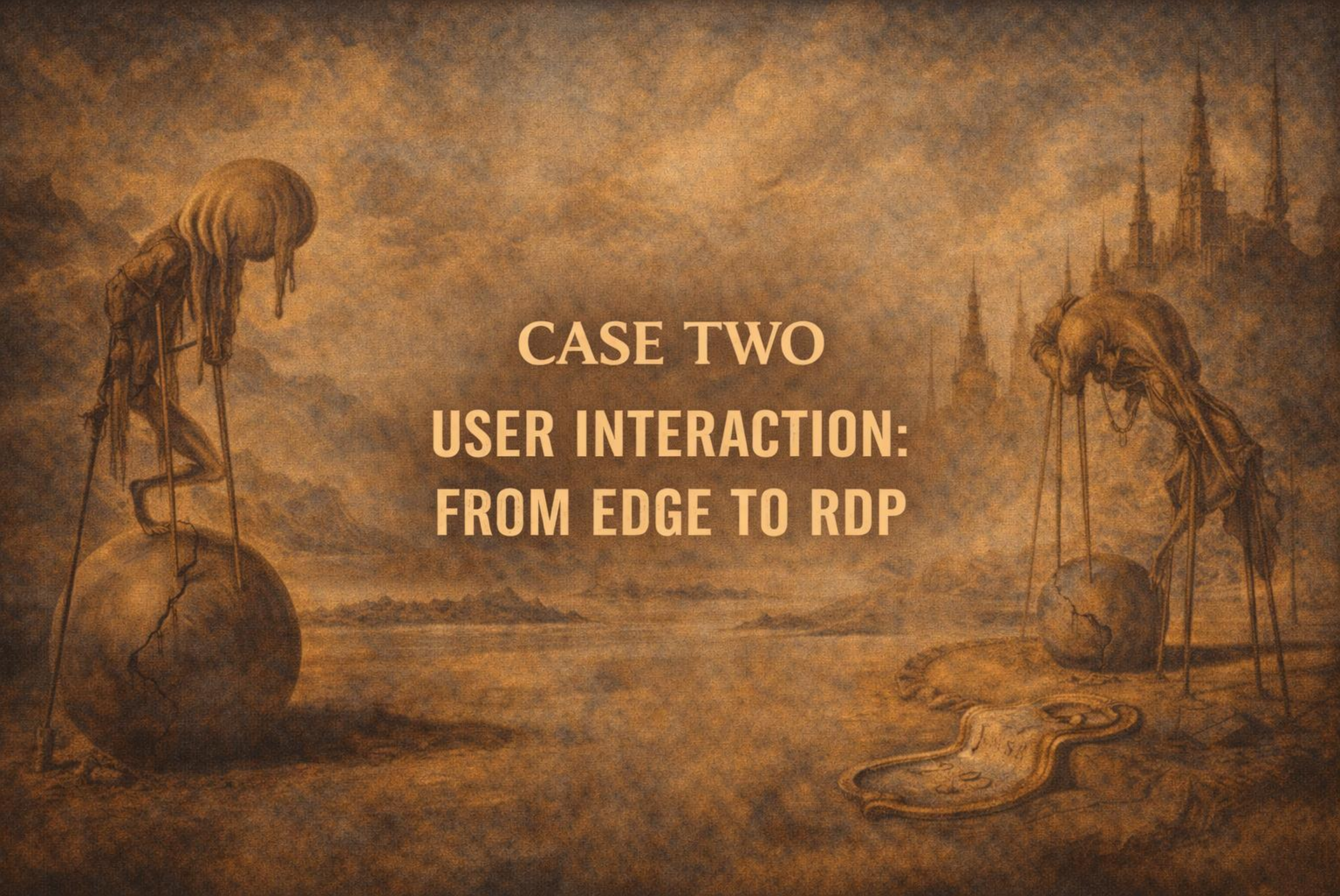
```
    {
      "ImageName": "wmiprvse.exe",
      "ProcessID": 2952,
      "EndPoint": "\\RPC Control\\TermSrvApi",
      "InterfaceUuid": "bde95fdf-eee0-45de-9e12-e5a61cd0d4fe",
      "ImpersonationLevel": 3,
      "ProcNum": 9,
      "Module": "termsrv.dll",
      "ModulePath": "C:\\Windows\\System32\\termsrv.dll",
      "ProceduresCount": 12
    },
    {
      "ImageName": "winlogon.exe",
      "ProcessID": 724,
      "EndPoint": "\\RPC Control\\TermSrvApi",
      "InterfaceUuid": "28098650-fe3c-4af4-8a41-8bcd284941c5",
      "ImpersonationLevel": 3,
      "ProcNum": 2,
      "Module": "termsrv.dll",
      "ModulePath": "C:\\Windows\\System32\\termsrv.dll",
      "ProceduresCount": 4
    },
    {
      "ImageName": "svchost.exe",
      "ProcessID": 1872,
      "EndPoint": "\\RPC Control\\TermSrvApi",
      "InterfaceUuid": "bde95fdf-eee0-45de-9e12-e5a61cd0d4fe",
      "ImpersonationLevel": 3,
      "ProcNum": 9,
      "Module": "termsrv.dll",
      "ModulePath": "C:\\Windows\\System32\\termsrv.dll",
      "ProceduresCount": 12
    },
```

Exceptions Generating

- After enabling logging, generate the exceptions by:
  - Rebooting the system
  - Running an automated script to perform random operations
  - Turning off each service and repeating the previous two steps

The Exceptions That Behave Differently




CASE TWO
USER INTERACTION:
FROM EDGE TO RDP

From EDGE to RDP

- Microsoft Edge browser (msedge.exe) is installed by default in Windows.

- When Edge starts, it triggers an RPC call to the Terminal Services service (RDP) with a high impersonation level.



Exploit/low privilege

SeImpersonatePrivilege

NT AUTHORITY\NETWORK SERVICE

Malicious executable

RPC Server

UUID

bde95fdf-eee0-45de-9e12-e5a61cd0d4fe

TermSrvAPI

Proc8

Interface

SeImpersonatePrivilege

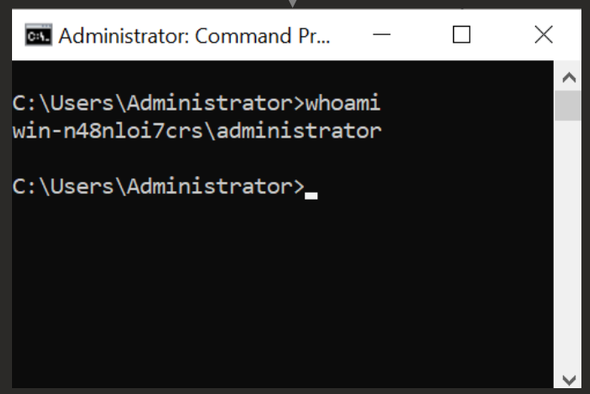
RpcImpersonateClient

Level: Impersonate

User Interaction

msedge.exe: Administrator

RPC Client



CASE THREE

ABUSING BACKGROUND SERVICES

From WDI to RDP

- There are some background Windows services that periodically attempt to make RPC calls to the RDP service without user interaction.

- One example of such a service is the WdiSystemHost service.

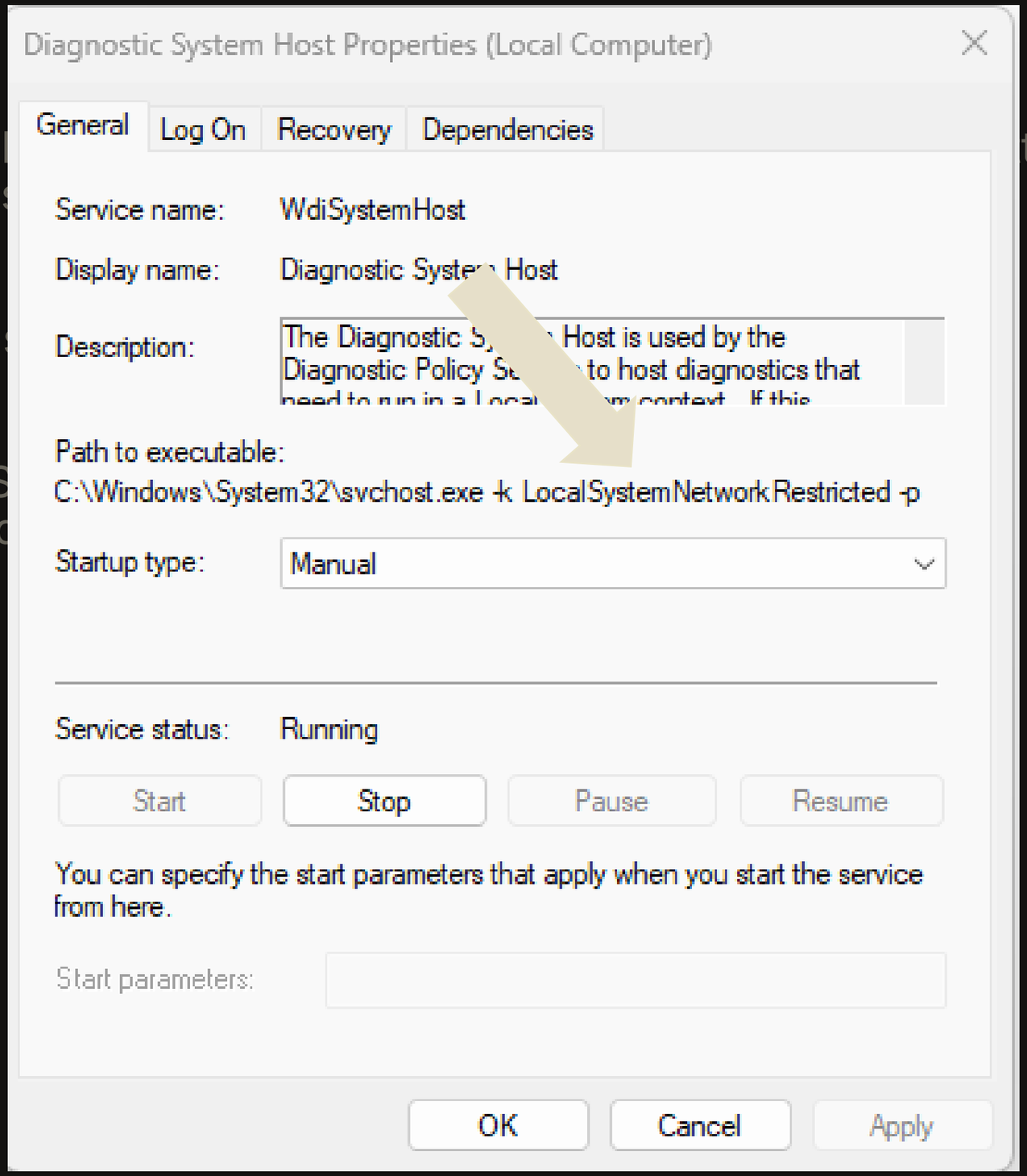
- The Diagnostic System Host Service is a built-in Windows service responsible for running system diagnostics and troubleshooting tasks.

From Wdi to RDP

- There are some
- One example of
- The Diagnostic S

tempt to make RPC calls to the RDP

responsible for running system

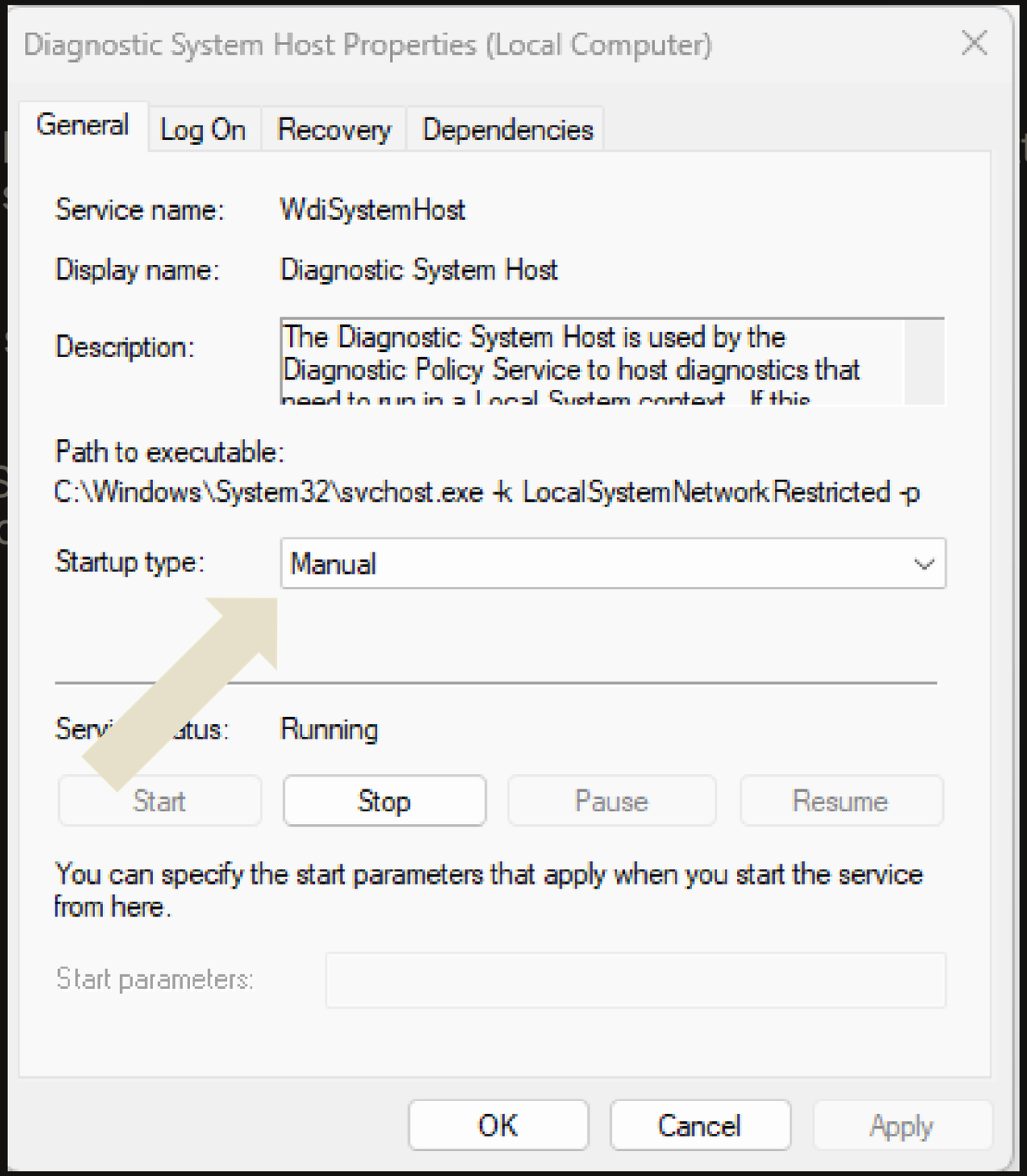


From Wdi to RDP

- There are some
- One example of
- The Diagnostic S

tempt to make RPC calls to the RDP

responsible for running system



Exploit/low privilege

SeImpersonatePrivilege

NT AUTHORITY\NETWORK SERVICE

Malicious executable

RPC Server

UUID

bde95fdf-eee0-45de-9e12-e5a61cd0d4fe

TermSrvAPI

Proc8

Interface

SeImpersonatePrivilege

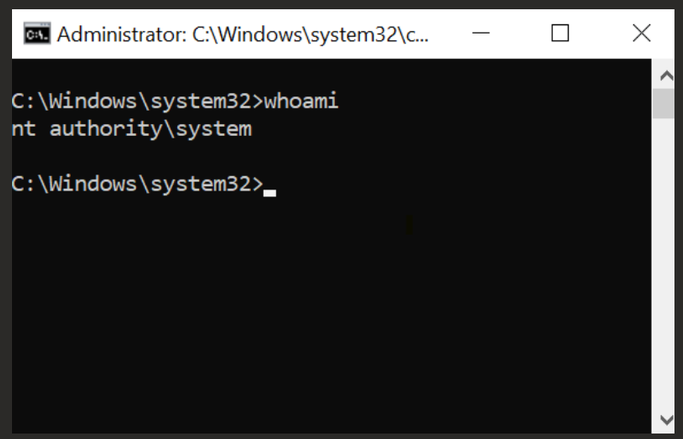
RpcImpersonateClient

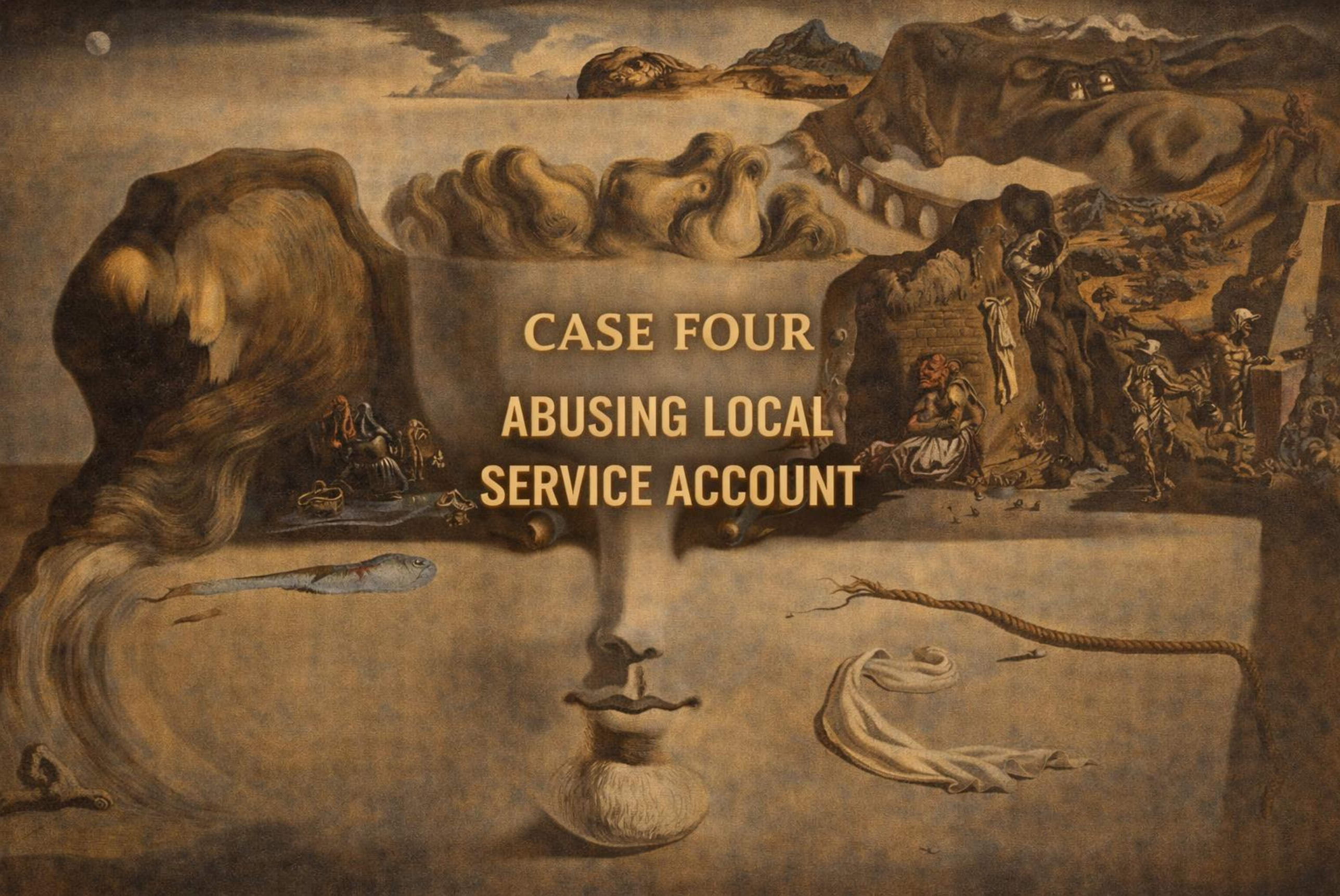
Level: Impersonate

Background service

WDI: SYSTEM

RPC Client



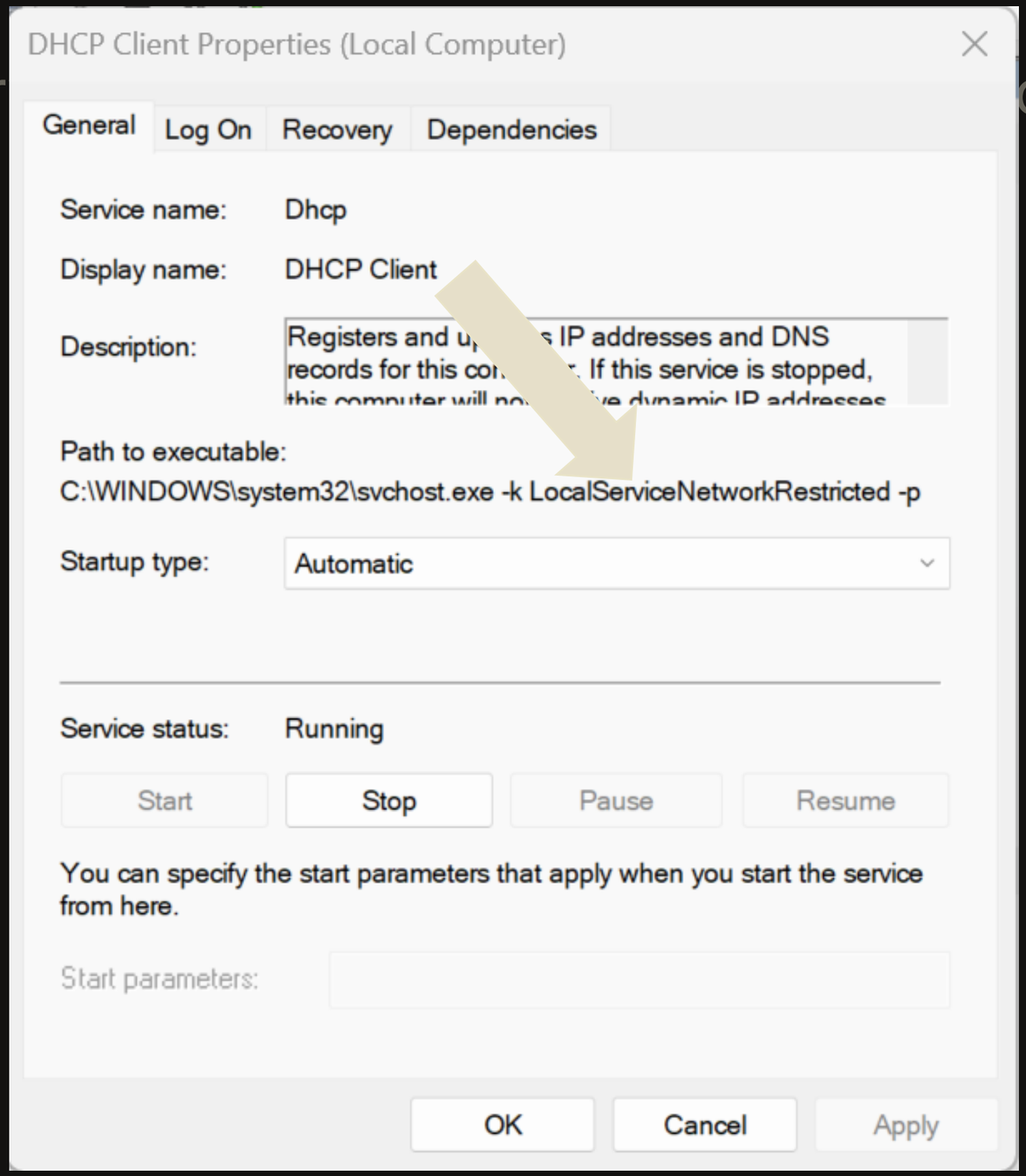

CASE FOUR
ABUSING LOCAL
SERVICE ACCOUNT

From ipconfig to DHCP

- The DHCP service (DHCP Client) is responsible for DHCP client operations.

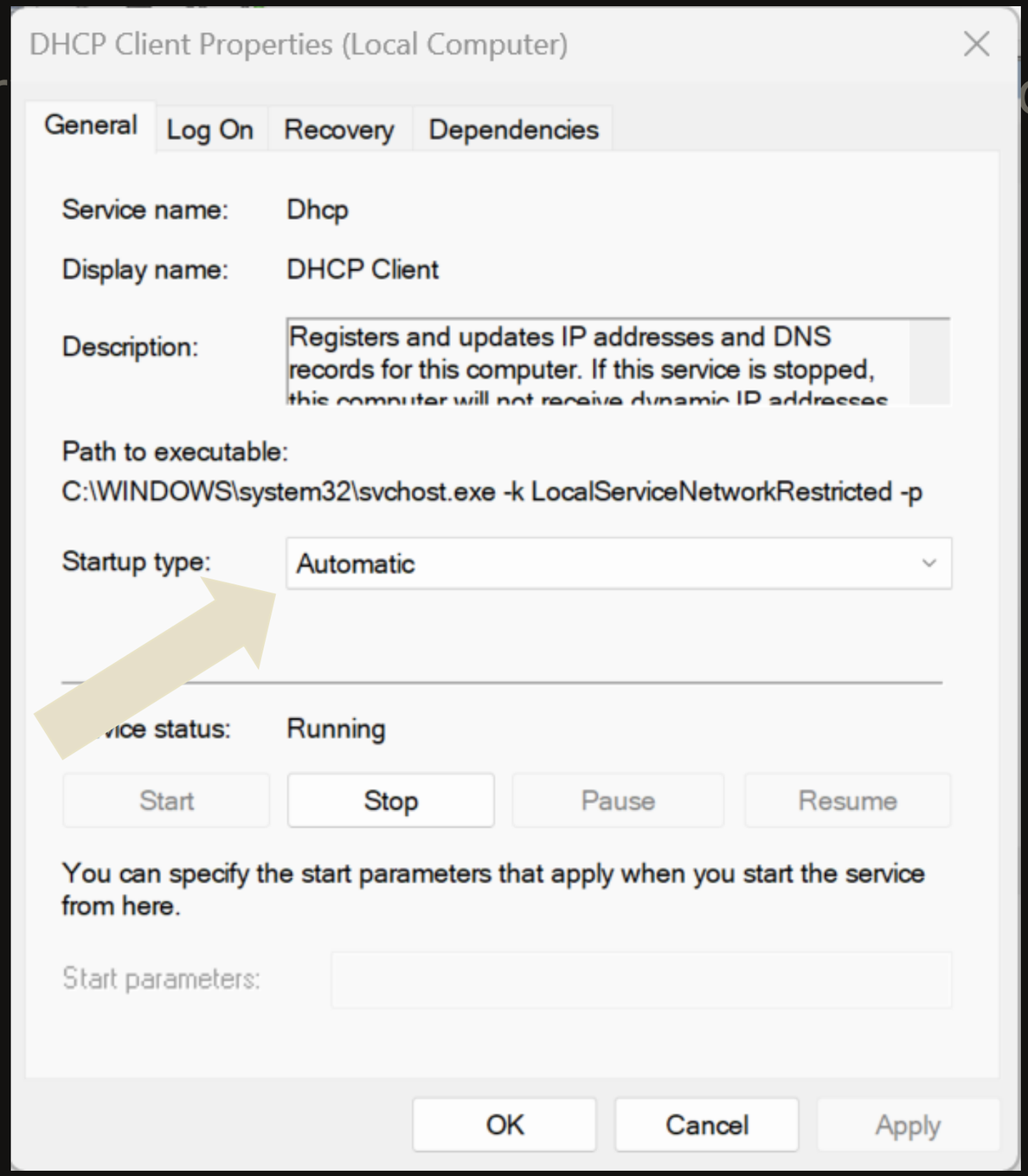
From ipconfig to DHCP

- The DHCP ser or DHCP client operations.



From ipconfig to DHCP

- The DHCP ser or DHCP client operations.



From ipconfig to DHCP

- The DHCP service (DHCP Client) is responsible for DHCP client operations.
- It runs under the Local Service account and is enabled by default.

From ipconfig to DHCP

- The DHCP service (DHCP Client) is responsible for DHCP client operations.
- It runs under the Local Service account and is enabled by default.
- This service exposes an RPC server with multiple interfaces and endpoints.
- The RPC server exposed by this service is called by various system DLLs using a high impersonation level.

Exploit/low privilege

SeImpersonatePrivilege

NT AUTHORITY\LOCAL SERVICE

Malicious executable

RPC Server

UUID

3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5

dhcpcsvc

Proc16

Interface

SeImpersonatePrivilege

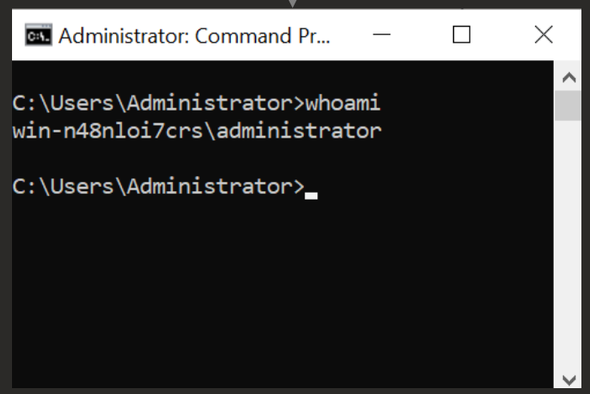
RpcImpersonateClient

Level: Impersonate

User Interaction

ipconfig.exe: Administrator

RPC Client



dhcp service need to be turned off

The Exception That Loves Ghosts



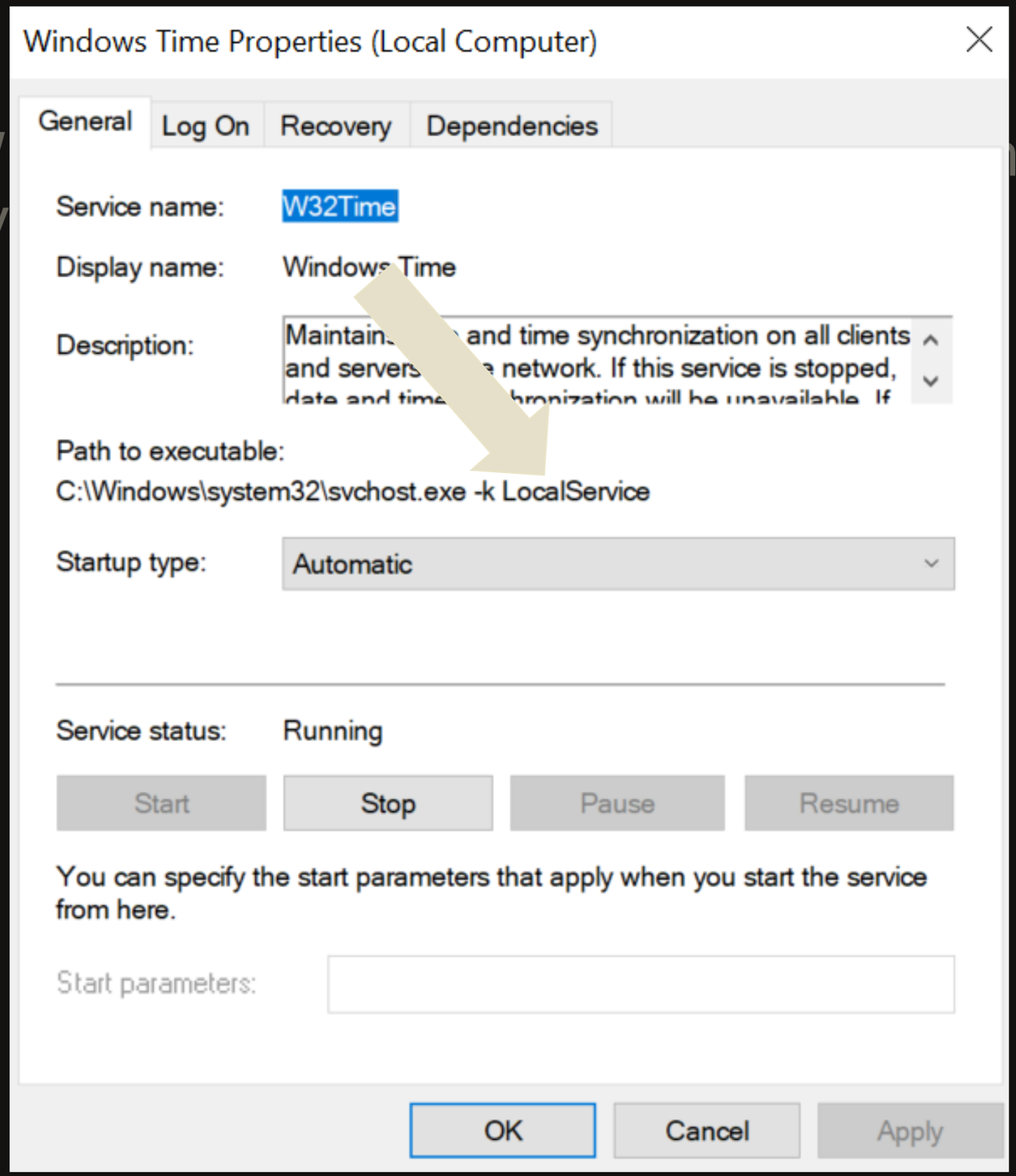
CASE FIVE
ABUSING TIME

Windows Time Service

- The Windows W32Time service is responsible for maintaining date and time synchronization across all clients and servers in the network.

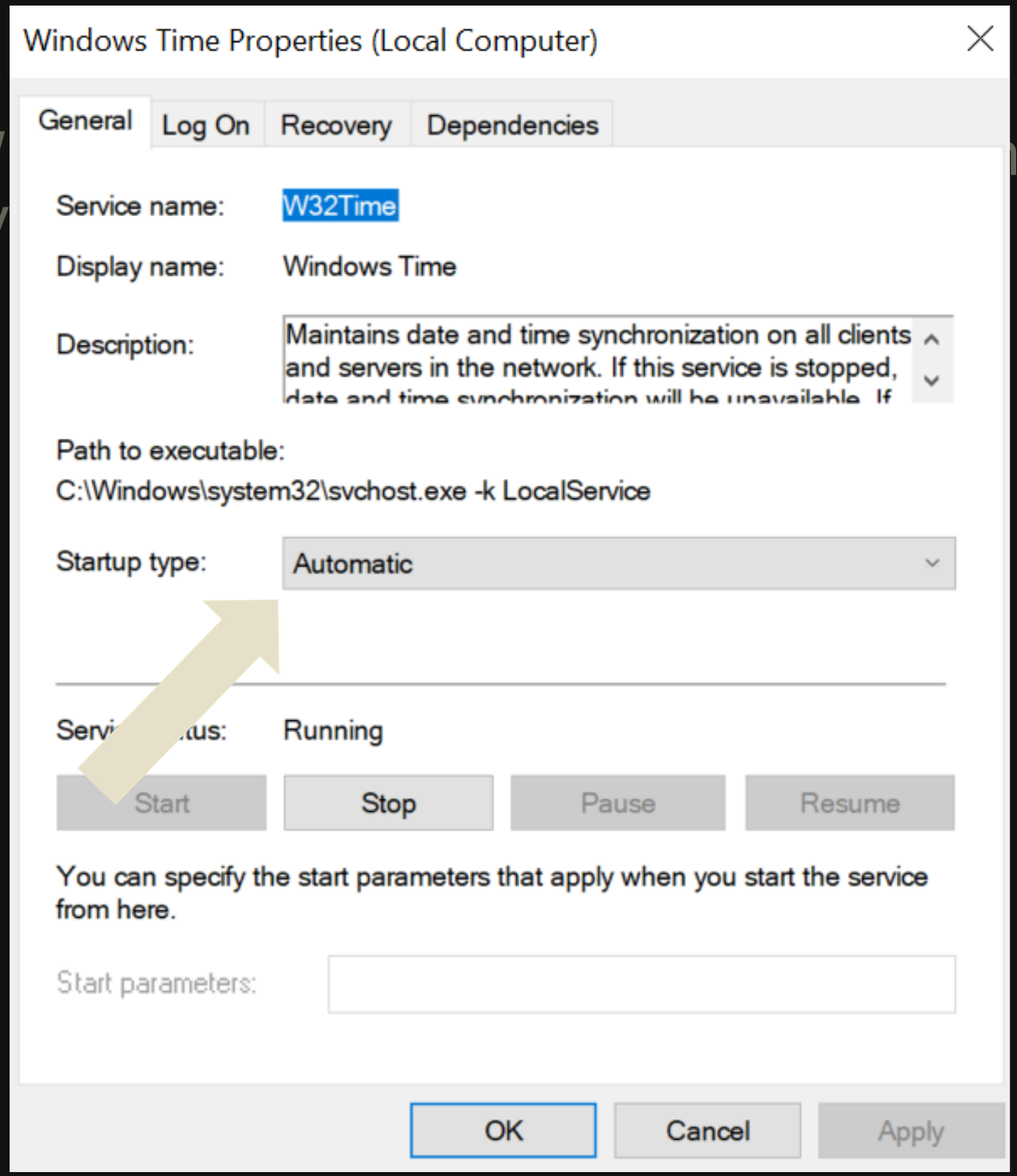
Windows Time Service

- The Windows W…aintaining date and time sy… servers in the network.



Windows Time Service

- The Windows W…aintaining date and time sy… servers in the network.



Windows Time Service

- The Windows W32Time service is responsible for maintaining date and time synchronization across all clients and servers in the network.

- It is enabled by default and runs under the Local Service account.

Windows Time Service

- The Windows W32Time service is responsible for maintaining date and time synchronization across all clients and servers in the network.

- It is enabled by default and runs under the Local Service account.

- This service exposes an RPC server with two endpoints:
  - \PIPE\W32TIME_ALT
  - \RPC Control\W32TIME_ALT

Windows Time Service

Host A

C:\Windows\System32\w32tm.exe

RPC Client

W32TIME

W32Time: Local Service

SeImpersonatePrivilege

RPC Server

W32TIME_ALT

Funs

Interface A

Windows Time Service

Host A

Ghost Lovers

C:\Windows\System32\w32tm.exe

RPC Client

W32TIME

W32Time: Local Service

SeImpersonatePrivilege

RPC Server

W32TIME_ALT

Funs

Interface A

Exploit/low privilege

SeImpersonatePrivilege

NT AUTHORITY\LOCAL SERVICE

Malicious executable

RPC Server

UUID

8fb6d884-2388-11d0-8c35-00c04fda2795

W32TIME

Proc6

Interface

SeImpersonatePrivilege

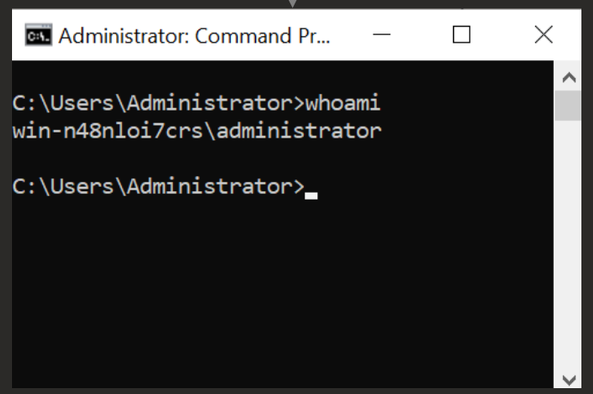
RpcImpersonateClient

Level: Impersonate

User Interaction

w32tm.exe : Administrator

RPC Client



No need to turn off Time service

How to Collect These Ghost Lovers?



The Exception That Was Never Confirmed



“After careful investigation, this case has been assessed as **Moderate severity** and does not meet Microsoft's bar for immediate servicing as this attack has to originate from a process with '**SeImpersonatePrivilege**' privileges. However, we have shared the report with the team responsible for maintaining the product or service. They will take appropriate action as needed to help keep customers protected.”

Detection and Defense



Detection and Defense

this type of activity cannot be prevented

The attack surface is extensive

Mitigation depends on Microsoft future updates

Detection can be by following the Potato detection

Research Repository



https://github.com/klsecservices/PhantomRPC

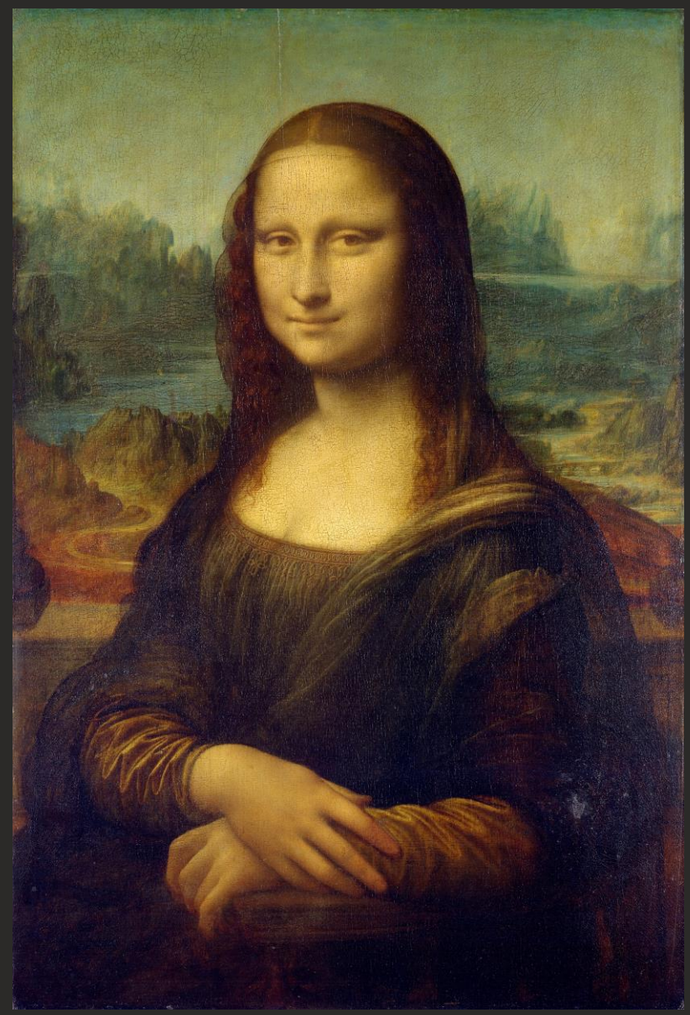
CONCLUSION

What Is Next?

- The provided POCs are simple examples, and additional cases are likely to exist

- All POCs were discovered and tested prior to the report date 29.09.2025

- Testing was performed on the latest versions of Windows Server 2022 and Windows Server 2025



What Is Next?

- The provided POCs are simple examples, and additional cases are likely to exist

- All POCs were discovered and tested prior to the report date 29.09.2025

- Testing was performed on the latest versions of Windows Server 2022 and Windows Server 2025



kaspersky

black hat

Thank you
Q&A

@haider_kabibo

PurpleShift blog