中安网星
Make Security Easy Again

从NTLM Relay看Windows RPC攻击面

中安网星

Make Security Easy Again

分享人

中安网星高级安全专家——李帅臻

◆负责攻防对抗、漏洞研究、攻击建模、漏洞武器化等工作

◆专注于内网横向、域渗透在攻击场景中的利用

◆具备丰富的攻防实战经验

◆主要研究方向：Windows研究、内网高级攻击与防御、安全漏洞挖掘与利用等

目录

NTLM Relay

Printbug

SMB Auth
User:Pass

↓

Bind Rpc
12345678-1234-ABCD-EF00-0123456789AB

↓

RpcRemoteFindFirstPrinterChange NotificationEx()
pszLocalMachine=\\Attack\xxx

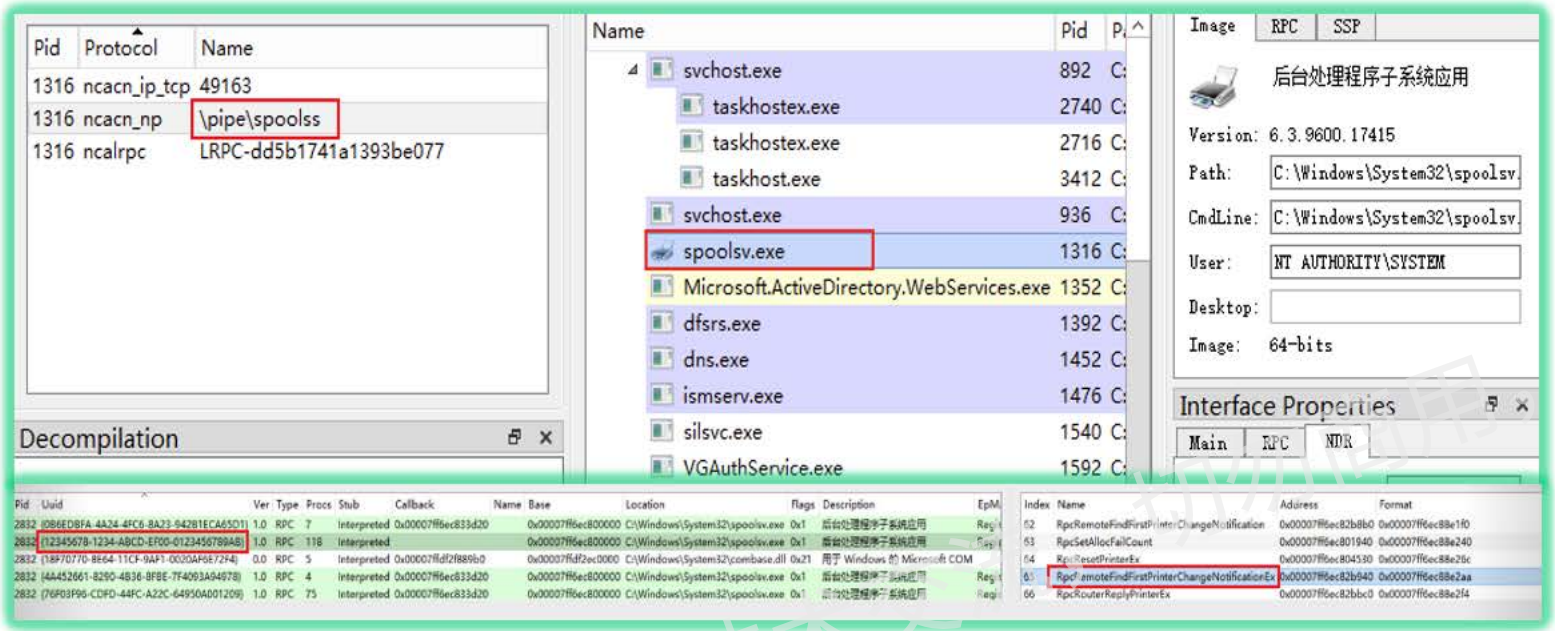
↓

NTLM Relay USER=DC$

↓

Complete

Printbug

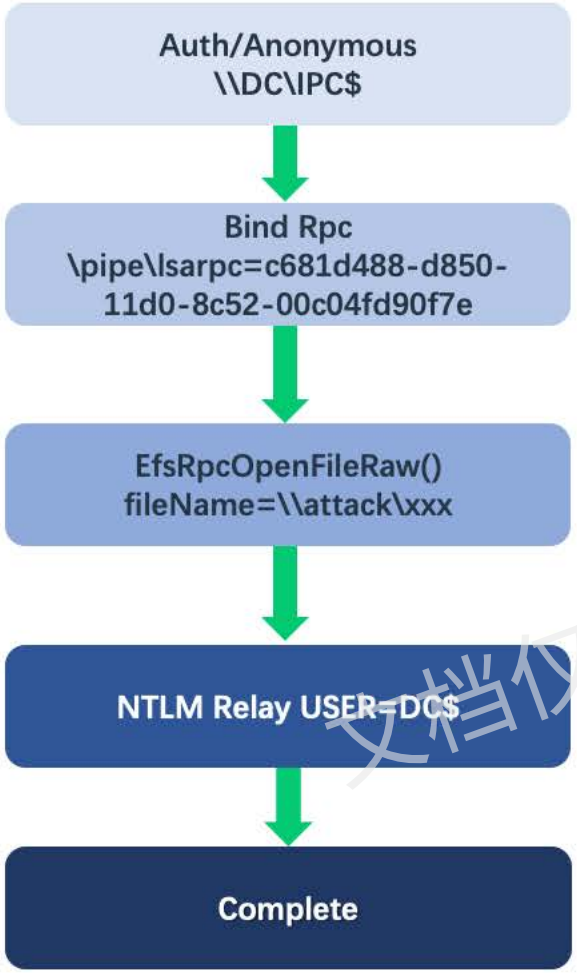


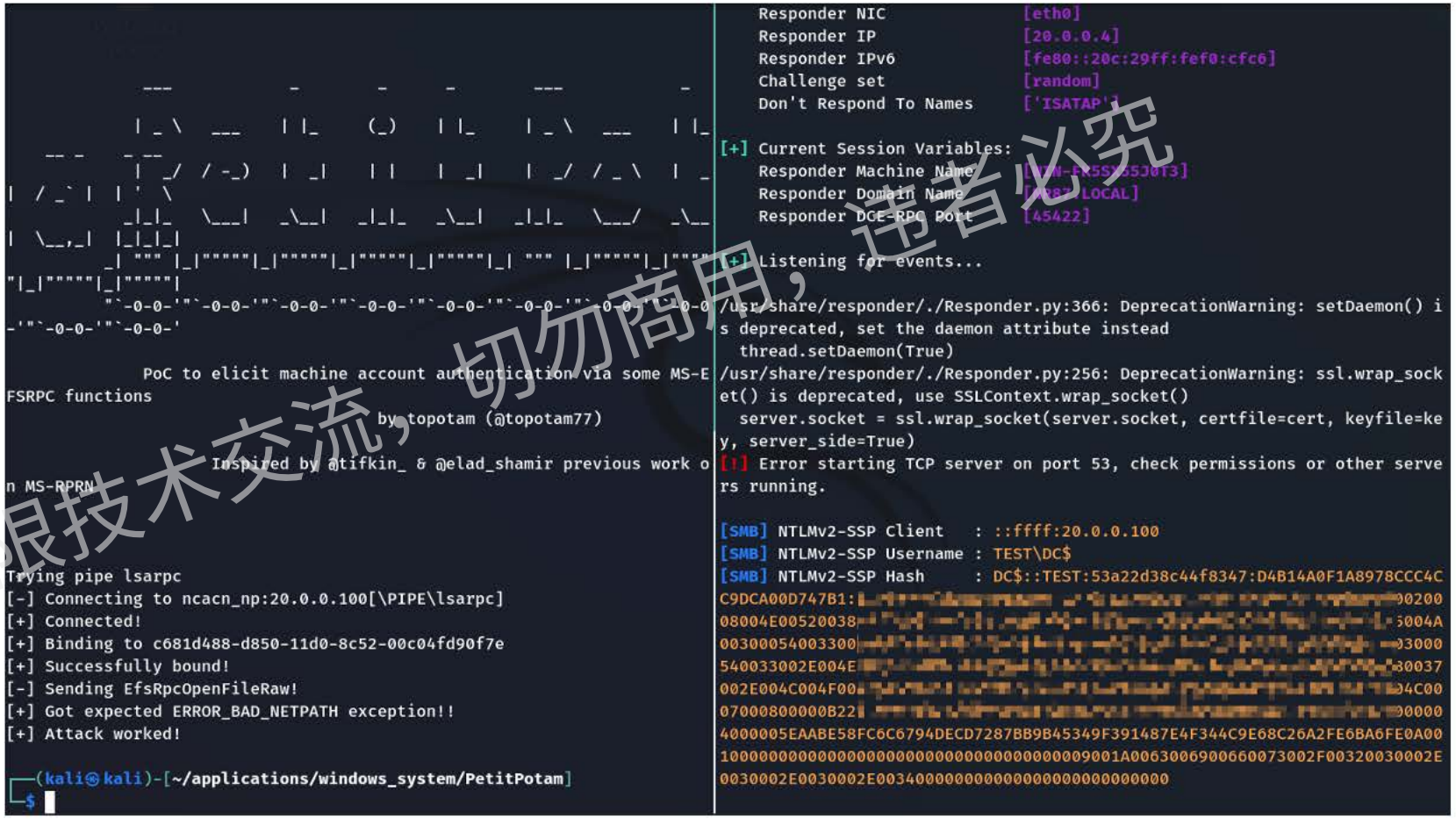
创建一个远程更改通知对象，该对象监视打印机对象的更改，并使用 ()将更改通知发送到打印客户端 RpcRouterReplyPrinter()或 RpcRouterReplyPrinterEx。

```
DWORD RpcRemoteFindFirstPrinterChangeNotificationEx(
  [in] PRINTER_HANDLE hPrinter,
  [in] DWORD fdwFlags,
  [in] DWORD fdwOptions,
  [in, string, unique] wchar_t* pszLocalMachine,
  [in] DWORD dwPrinterLocal,
  [in, unique] RPC_V2_NOTIFY_OPTIONS* pOptions
);
```

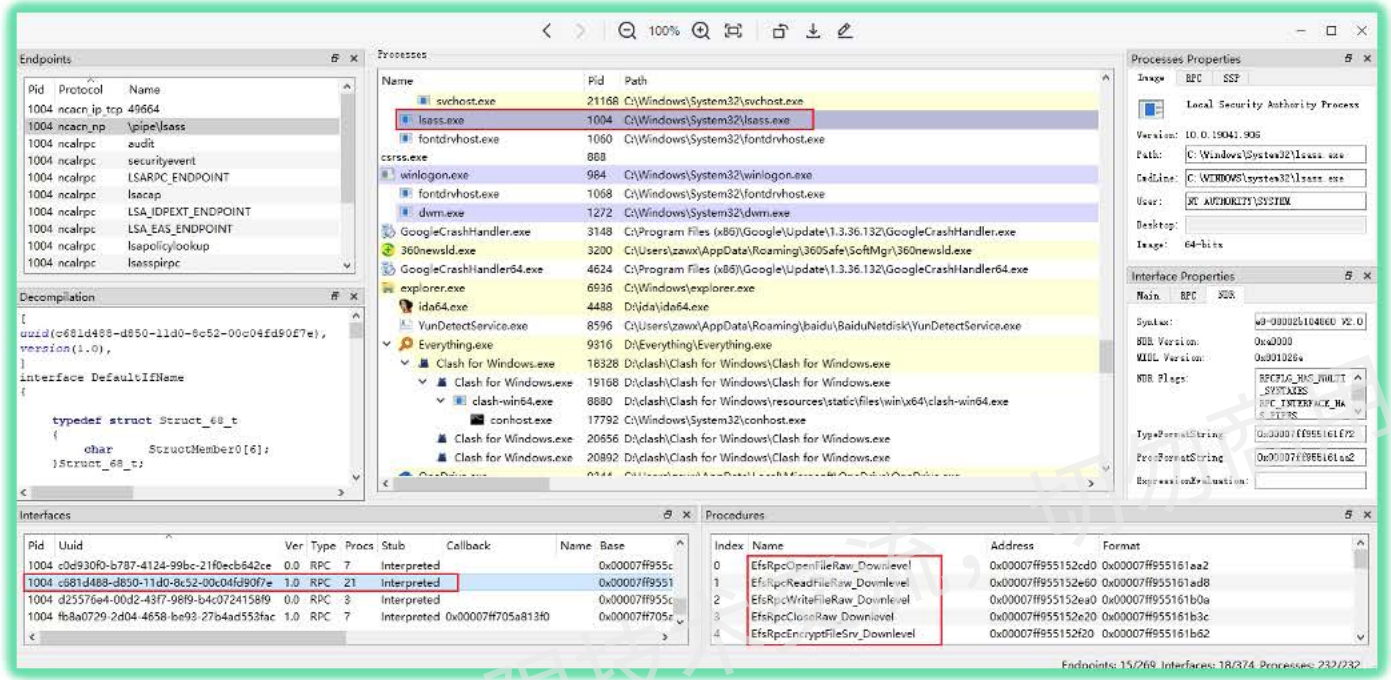
pszLocalMachine：指向表示客户端计算机名称的字符串的指针。

PetitPotam





PetitPotam



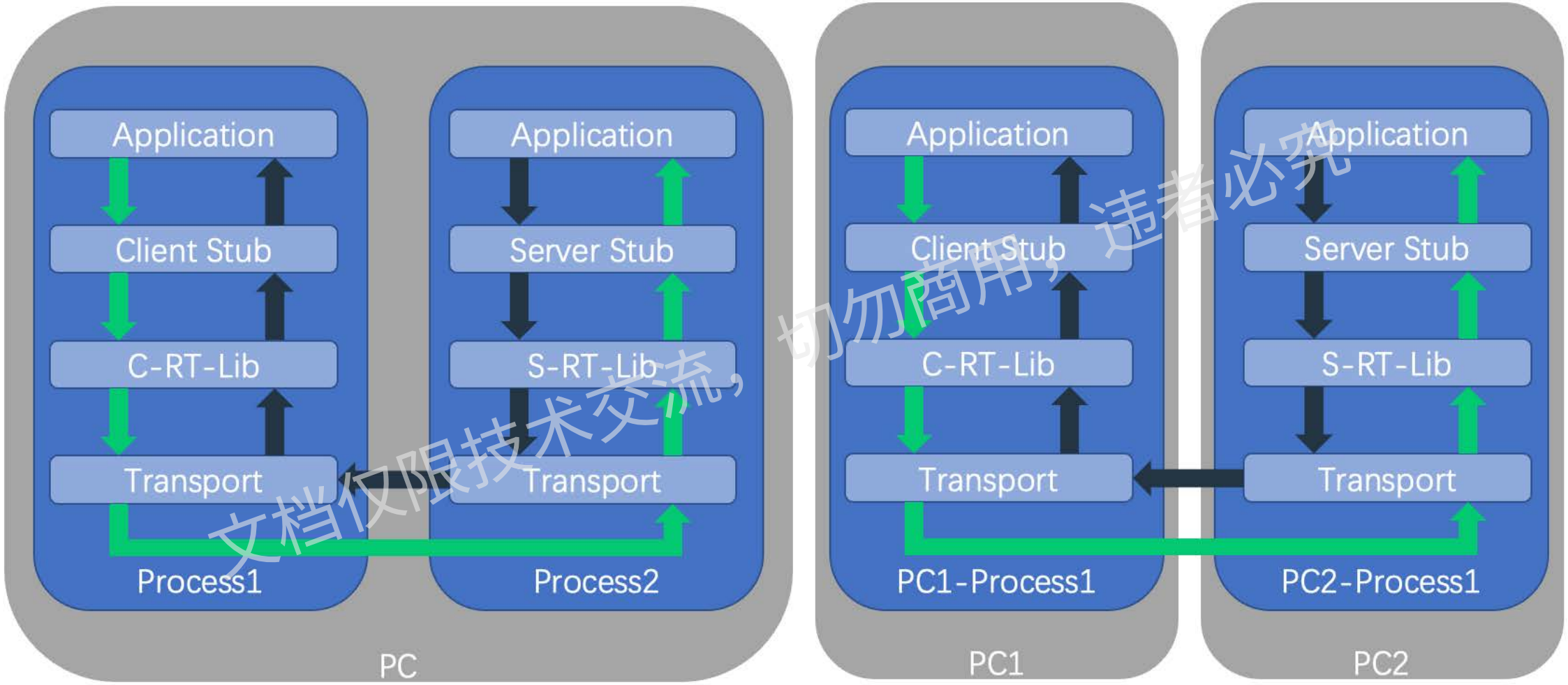
用于打开服务器上的加密对象以进行备份或还原。它分配必须通过调用 EfsRpcCloseRaw 方法释放的资源。

```
long EfsRpcOpenFileRaw(
  [in] handle_t binding_h,
  [out] PEXIMPORT_CONTEXT_HANDLE* hContext,
  [in, string] wchar_t* FileName,
  [in] long Flags
);
```

FileName： EFSRPC 标识符，指向远程服务器上的加密数据对象。应使用 Unc路径作为 EFSRPC 标识符。

RPC

RPC的两种调用方式

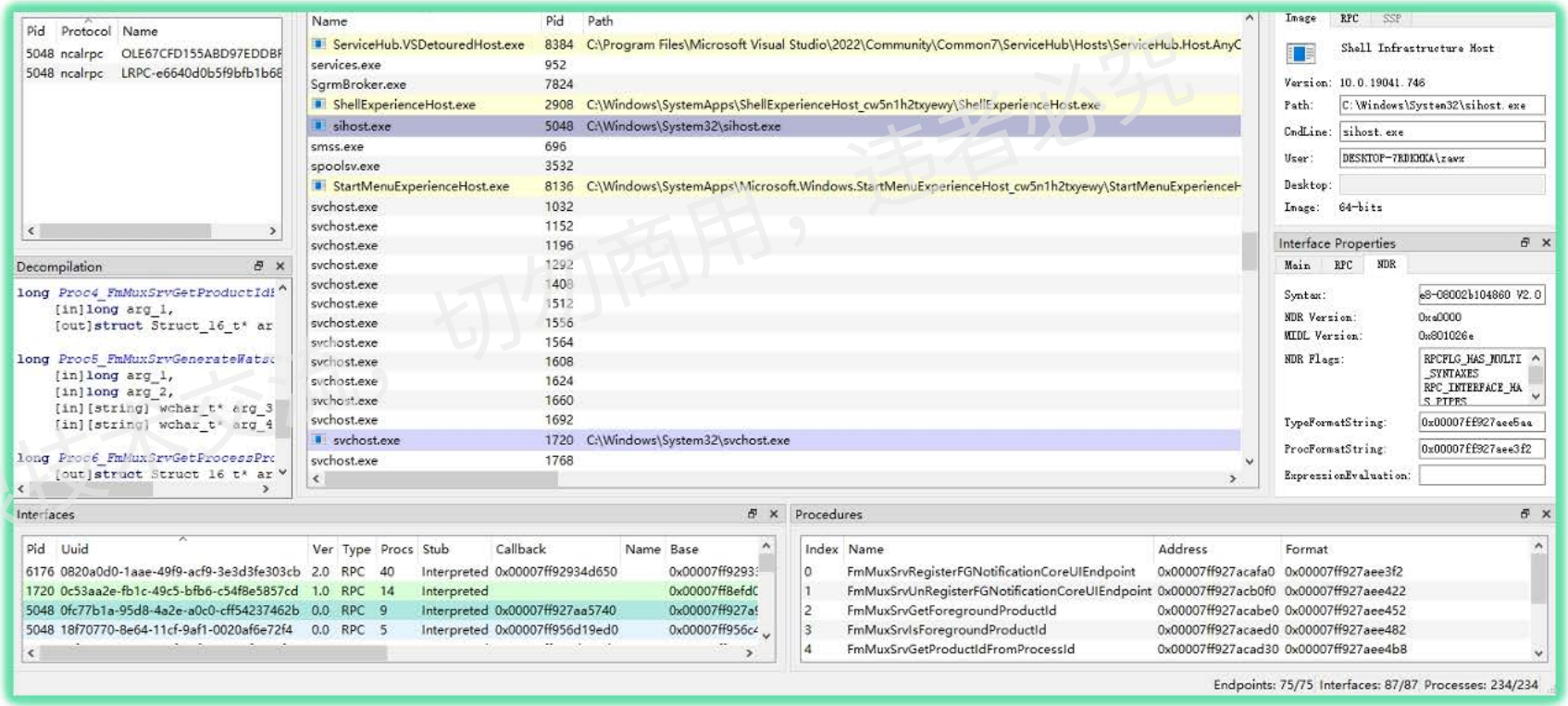


本地RPC调用

远程RPC调用

RPC应用场景

服务创建 (MS-SCMR)
目录复制服务 (MS-DRSR)
远程注册表 (MS-RRP)
计划任务 (MS-SCMR)
打印系统 (MS-RPRN)
Windows WMI(MS-WMI)
Netlogon 远程协议 (MS-NRPC)



国内外对RPC研究方向

← 推文

Compass Security
@compasssecurity

NTLM Relay over RPC: our analyst Sylvain Heiniger @sploutchy explored new attack vectors and discovered a vulnerability in the Windows Task Scheduler.

Ophir Harpaz
@OphirHarpaz

Yesterday, @nachoskrnl and I presented some of the research that has been going on in our team on MS-RPC. Long story short, Ben found a new auth coercion vulnerability on which you can read here akamai.com/blog/security/...
I'd like to highlight a couple more things from the talk. >>

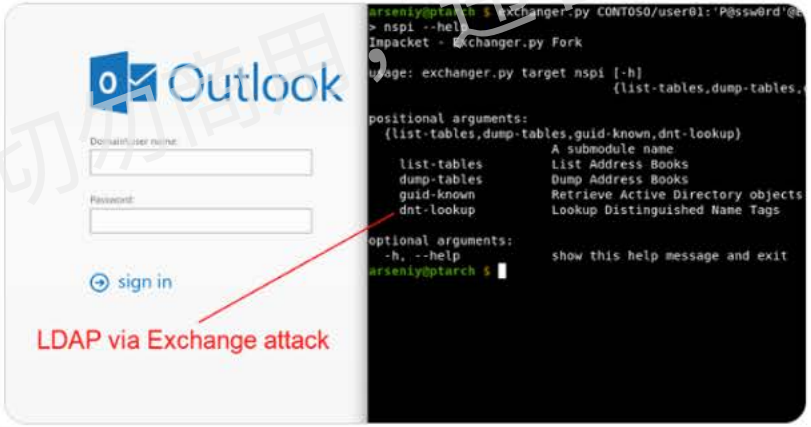
← 推文

Ophir Harpaz
@OphirHarpaz

Everyone's talking about the 9.8 RCE bug in Windows RPC runtime (CVE-2022-26809). @nachoskrnl bin-diffed rpcrt4.dll and located the integer overflow that was patched. Read about it here - akamai.com/blog/security/...
Patch now, and ffs don't expose TCP 445 to the internet.

PT SWARM
@ptswarm

New attack! Our researcher Arseniy Sharoglazov has discovered a method to connect to LDAP via #MSExchange from the Internet and access the whole Active Directory database. Read the research: swarm.ptsecurity.com/attacking-ms-e...
翻译推文

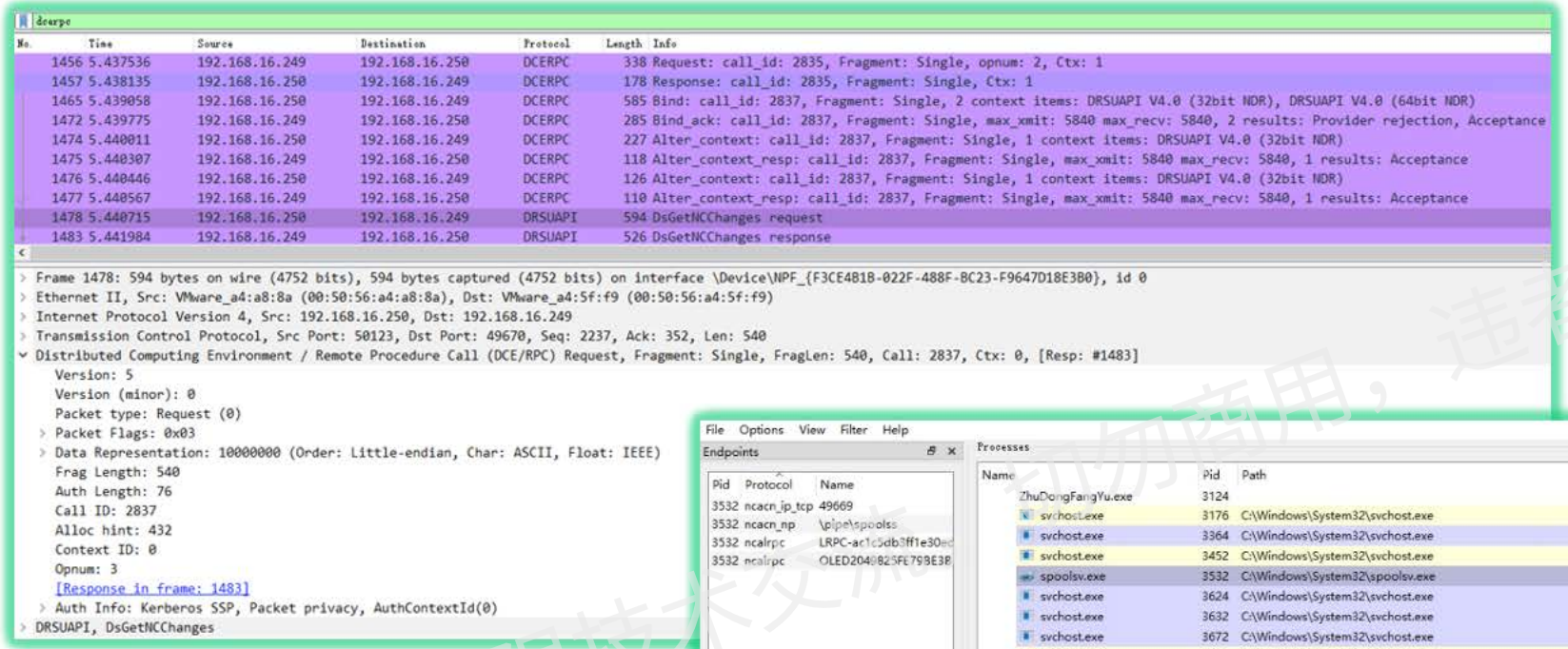


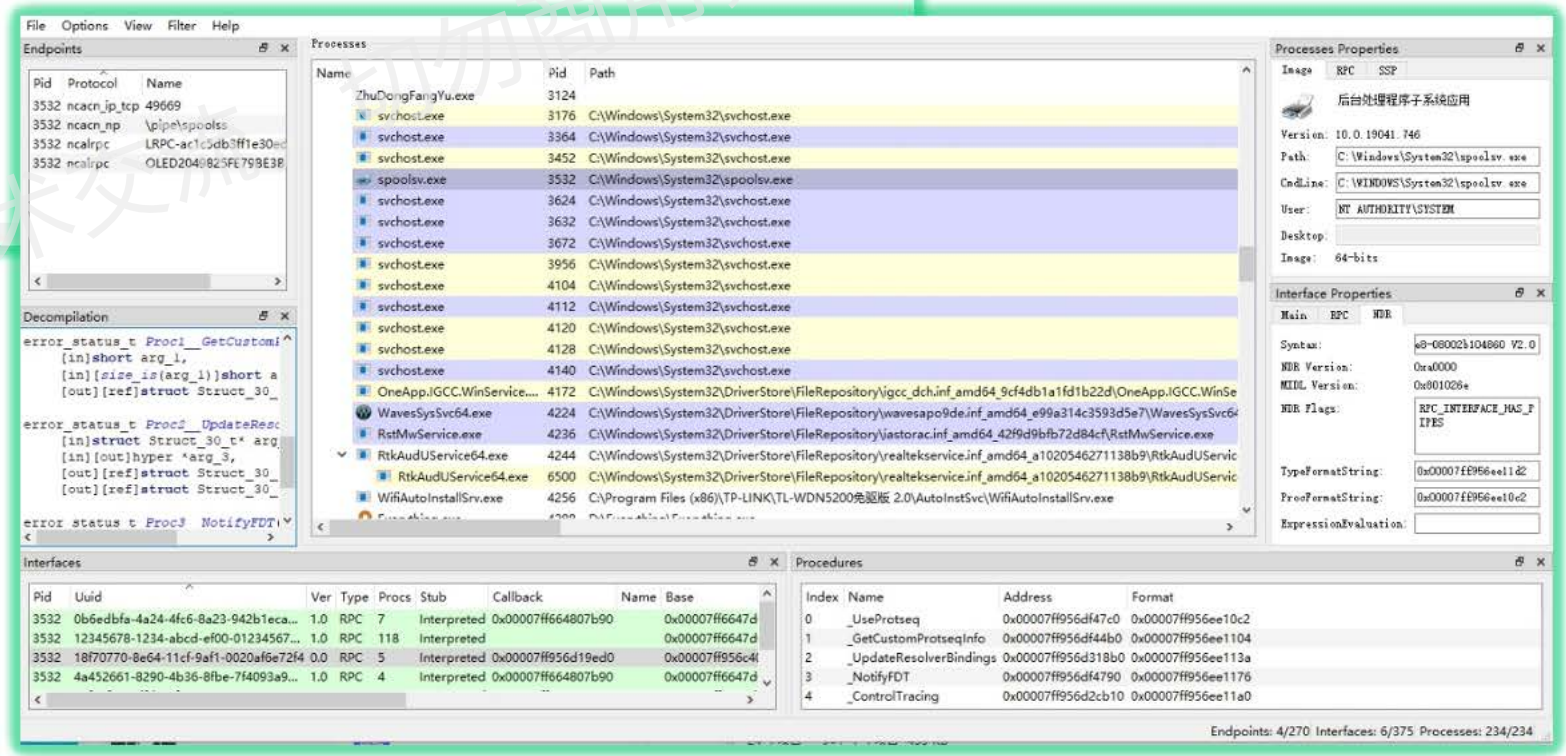
Jonas Vestberg
@bugch3ck

回复 @lkarlslund

My bet is something exposed over MS-RPC. That attack surface is huge and fairly unexplored. But I wouldn't be surprised if it was Exchange again 😅 (even though I would not consider it "Windows system").

RPC分析工具

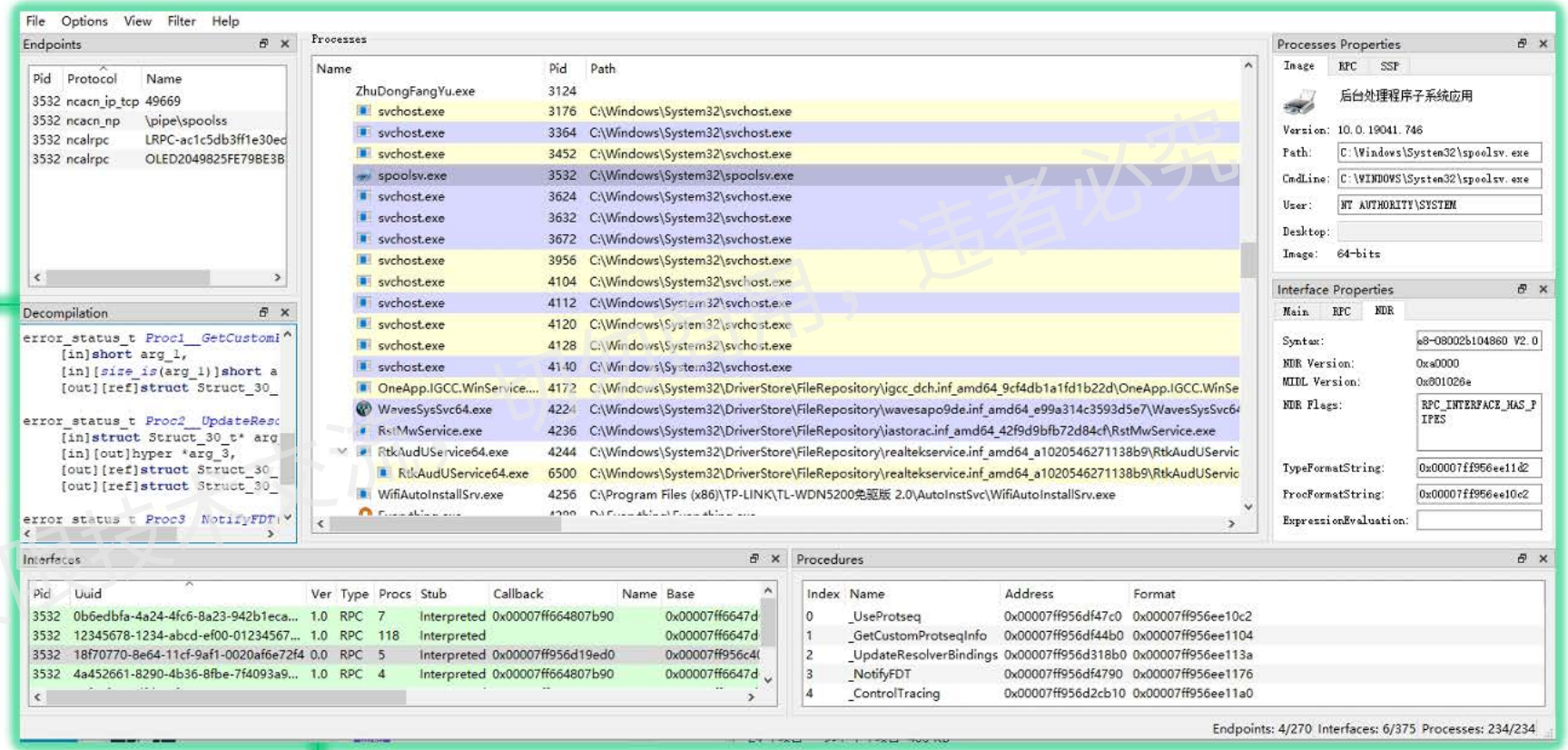




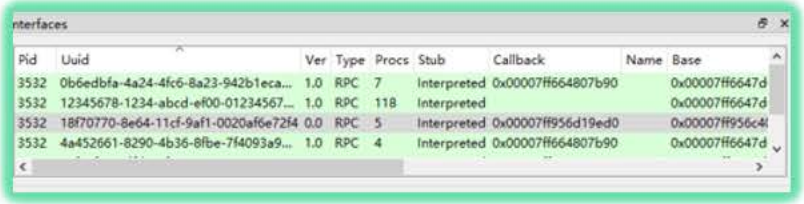
Wireshark
RPCView
RPCDump
PortQry

RPC参数详解

- Interfaces
- Interface UUID
- Opnum
- Procedures
- Endpoints
- RPC protocol sequence



RPC调用分析



UUID

```
[
uuid(18f70770-8e64-11cf-9af1-0020af6e72f4),
version(0.0),
]
interface DefaultIfName
{

    typedef struct Struct_30_t
    {
        short    StructMember0;
        short    StructMember1;
    [size_is(StructMember0)]short StructMember2[];
        }Struct_30_t;

error_status_t Proc0__UseProtseq(
    [in]short arg_1,
    [in][unique][string] wchar_t* arg_2,
    [out]long *arg_3,
    [out][ref]struct Struct_30_t** arg_4,
    [out][ref]struct Struct_30_t** arg_5);

error_status_t Proc1__GetCustomProtseqInfo(
    [in]short arg_1,
    [in][size_is(arg_1)]short arg_2[],
    [out][ref]struct Struct_30_t** arg_3);

error_status_t Proc2__UpdateResolverBindings(
    [in]struct Struct_30_t* arg_2,
    [in][out]hyper *arg_3,
    [out][ref]struct Struct_30_t** arg_4,
    [out][ref]struct Struct_30_t** arg_5);
```

IDL

Constant/value	Description
ncacn_nb_tcp Connection-oriented NetBIOS over Transmission Control Protocol (TCP)	Client only: MS-DOS, Windows 3.x Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT
ncacn_nb_ipx Connection-oriented NetBIOS over Internet Packet Exchange (IPX)	Client only: MS-DOS, Windows 3.x Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT
ncacn_nb_nb Connection-oriented NetBIOS Enhanced User Interface (NetBEUI)	Client only: MS-DOS, Windows 3.x Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT, Windows Me, Windows 98, Windows 95
ncacn_ip_tcp Connection-oriented Transmission Control Protocol/Internet Protocol (TCP/IP)	Client only: MS-DOS, Windows 3.x, and Apple Macintosh Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT, Windows Me, Windows 98, Windows 95
ncacn_np Connection-oriented named pipes	Client only: MS-DOS, Windows 3.x, Windows 95 Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT
ncacn_spx Connection-oriented Sequenced Packet Exchange (SPX)	Client only: MS-DOS, Windows 3.x Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT, Windows Me, Windows 98, Windows 95
ncacn_dnet_nsp Connection-oriented DECnet transport	Client only: MS-DOS, Windows 3.x
ncacn_at_dsp Connection-oriented AppleTalk DSP	Client: Apple Macintosh Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT
ncacn_vns_spp Connection-oriented Vines scalable parallel processing (SPP) transport	Client only: MS-DOS, Windows 3.x Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT
ncadg_ip_udp Datagram (connectionless) User Datagram Protocol/Internet Protocol (UDP/IP)	Client only: MS-DOS, Windows 3.x Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT
ncadg_ipx Datagram (connectionless) IPX	Client only: MS-DOS, Windows 3.x Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT
ncadg_mq Datagram (connectionless) over the Microsoft Message Queue Server (MSMQ)	Client only: Windows Me/98/95 Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT Server 4.0 with SP3 and later
ncacn_http Connection-oriented TCP/IP using Microsoft Internet Information Server as HTTP proxy	Client only: Windows Me/98/95 Client and Server: Windows Server 2003, Windows XP, Windows 2000
ncalrpc Local procedure call	Client and Server: Windows Server 2003, Windows XP, Windows 2000, Windows NT, Windows Me, Windows 98, Windows 95

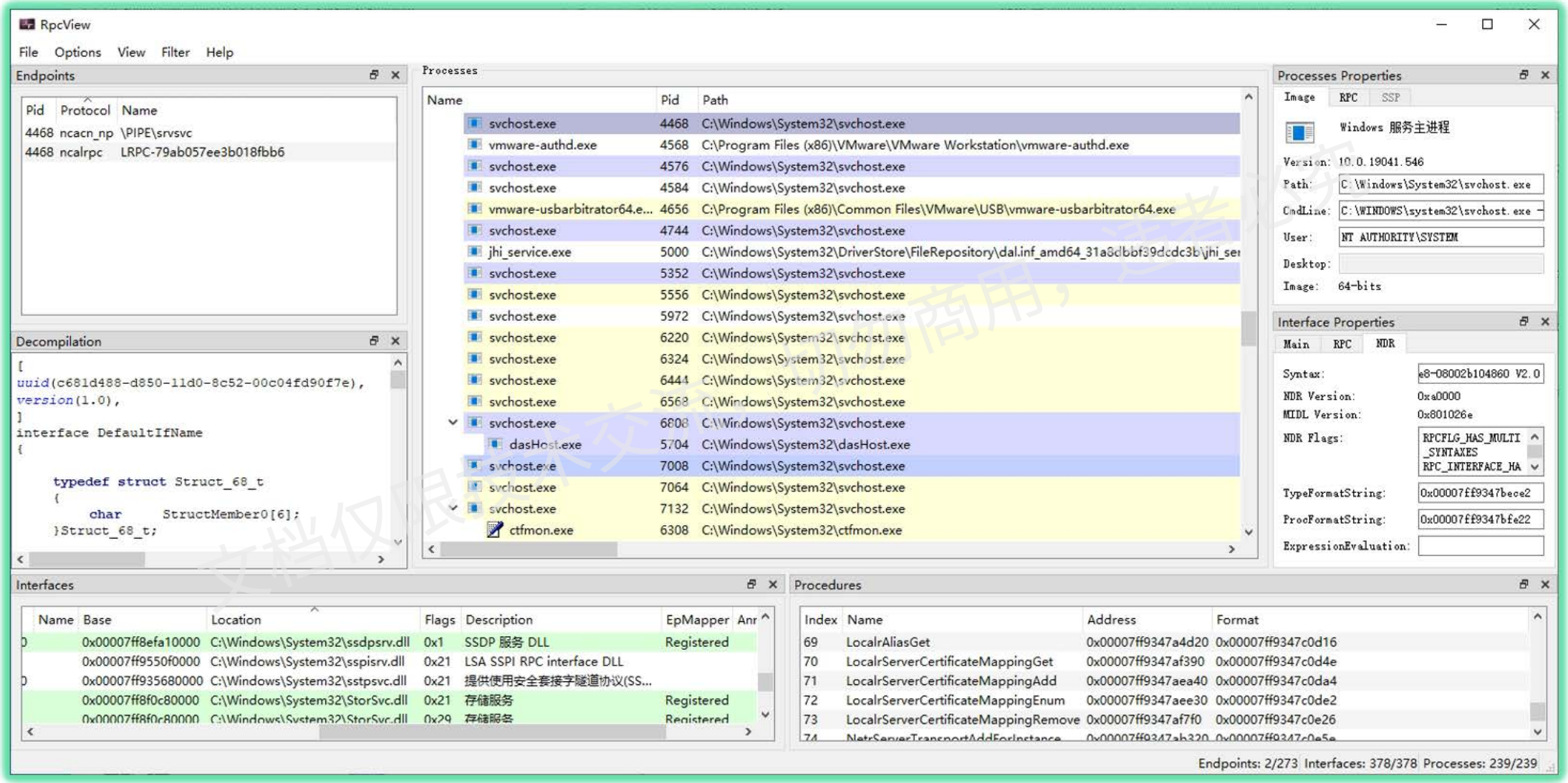
RPC protocol sequence

RPC相关漏洞

- Potato
- Zerologon
- PrinterNightMare

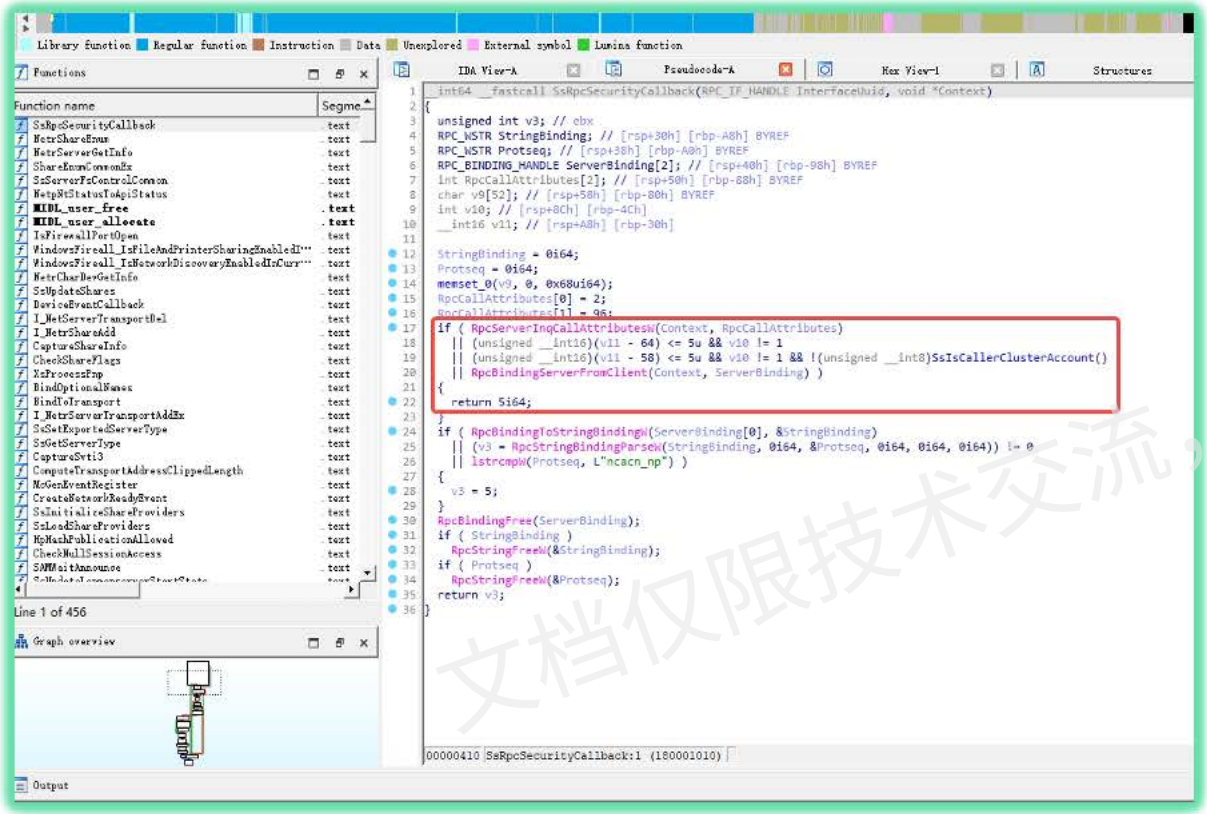
CVE-2022-30216

漏洞原理

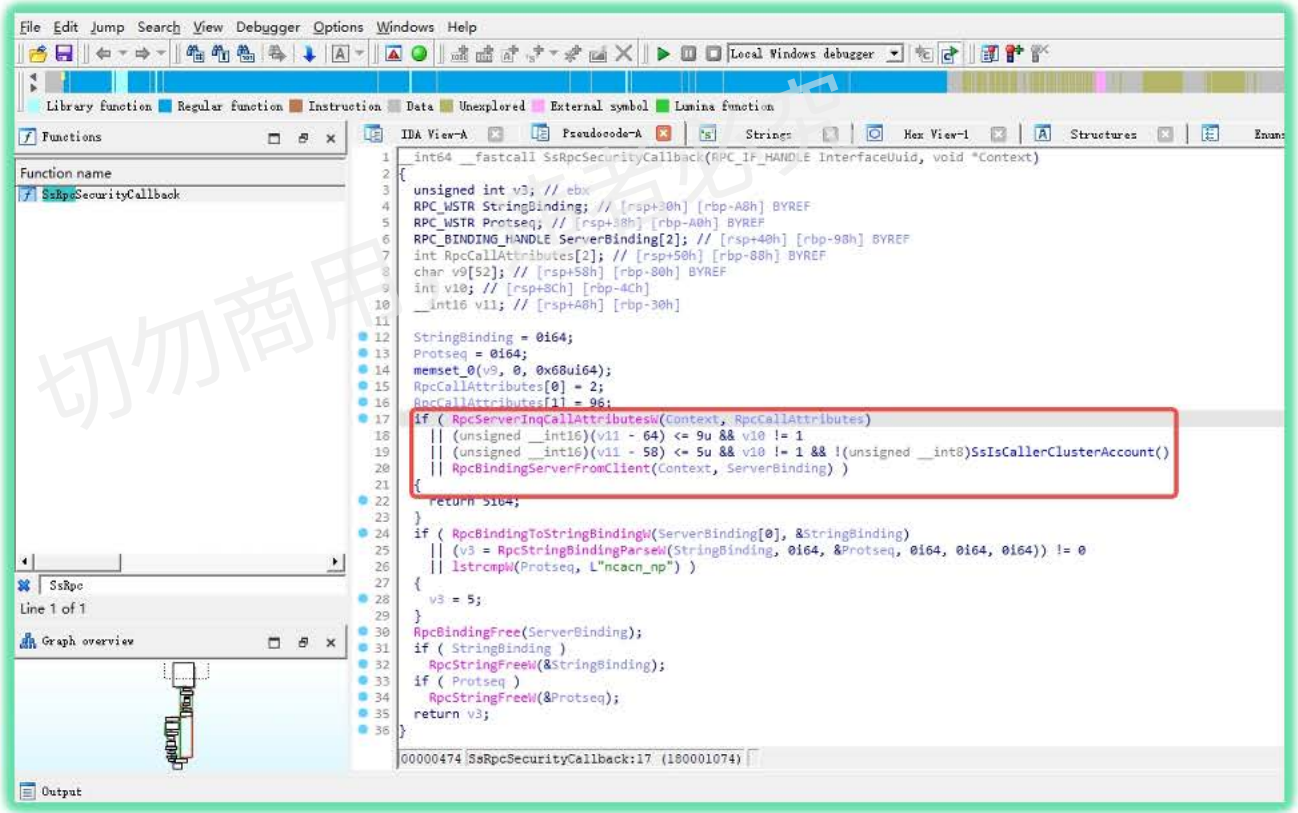


srvsvc.dll

历史版本实现



Windows 10 19H2

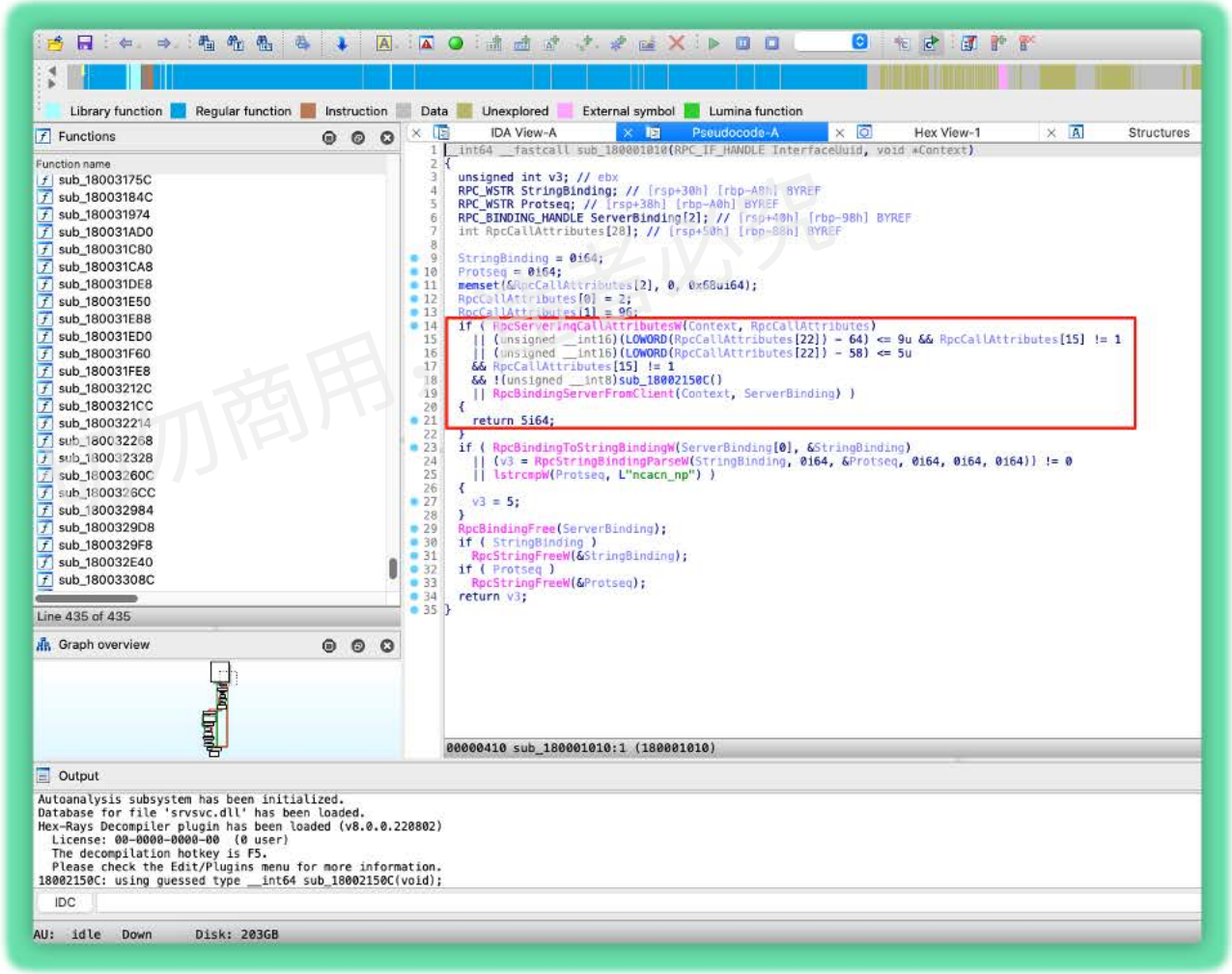


Windows 10 20H2

漏洞分析

```
.rdata:00007FFEEE276670                 dq offset LocalrServerCertificateMappingGet
.rdata:00007FFEEE276678                 dq offset LocalrServerCertificateMappingAdd
.rdata:00007FFEEE276680                 dq offset LocalrServerCertificateMappingEnum
.rdata:00007FFEEE276688                 dq offset LocalrServerCertificateMappingRemove
.rdata:00007FFEEE276690                 dq offset LocalrServerCertificateMappingModify
```

```
LocalrServerCertificateMappingModify(
    [in, string, unique] SRVSVC_HANDLE ServerName,
    [in]long arg_1,
    [in][out][switch_is(arg_1)]union certificate_container* arg_2
);
```



Windows 11/Server 2022

漏洞利用

攻击监测

中安网星
Make Security Easy Again

THANK YOU