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：

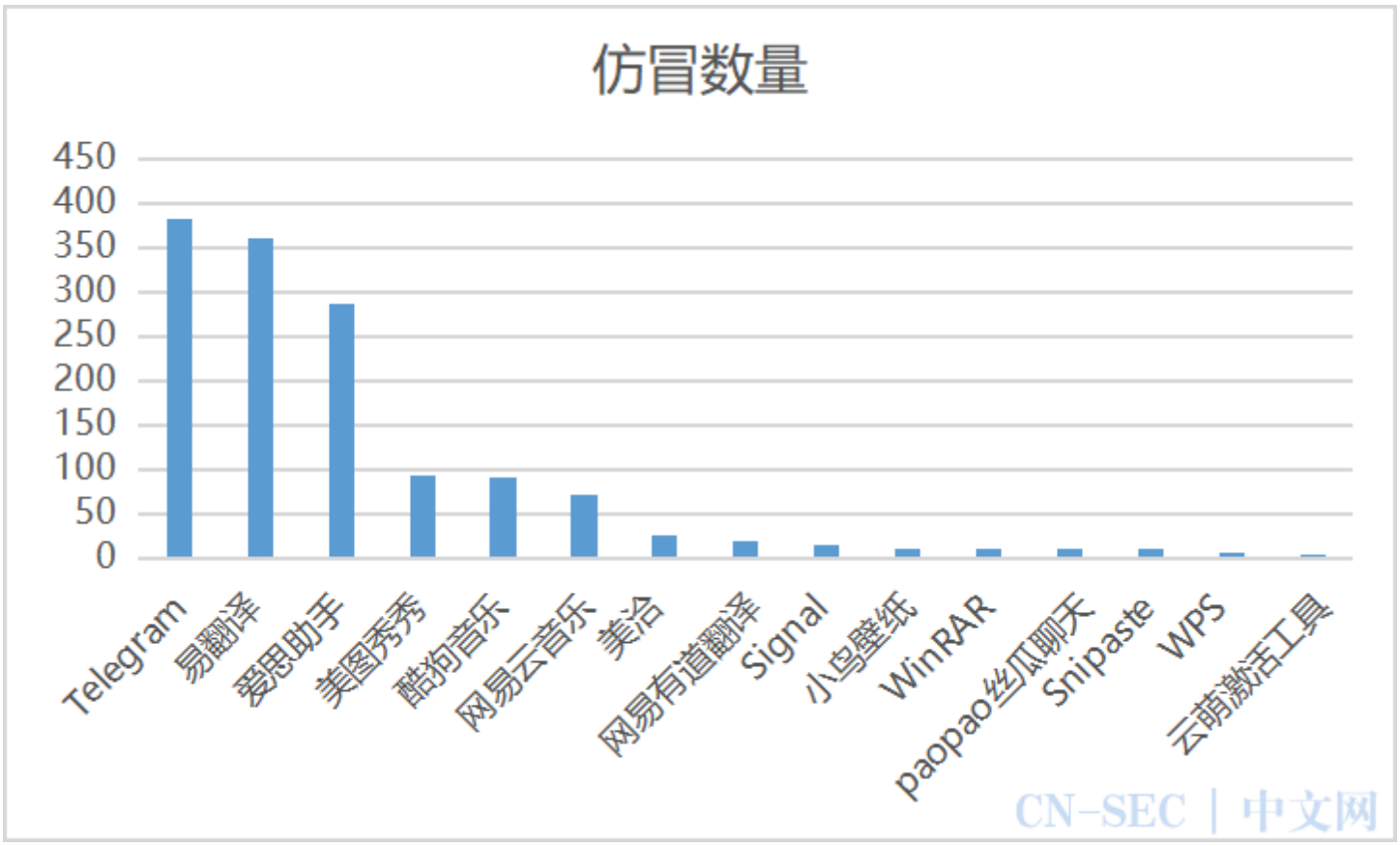
- 关闭安全软件：释放包含漏洞的Ping32、百度杀毒等安全软件驱动，触发漏洞后强行关闭失陷终端上的特定安全软件进程。
- 致盲行为检测：读写内核数据，定位并修改安全软件内核回调函数的地址，使安全软件在未被关闭的情况下，也无法采集与检测进程、线程、文件、注册表的行为。
- 指定进程隐身：通过InfinityHook技术实现RootKit，隐藏指定的恶意进程，即使找到这个进程也很难通过常规手段关闭。
- 屏蔽网络反连：劫持系统网络驱动，在底层过滤和篡改网络连接信息，使安全软件无法正确获取失陷终端与C2服务器之间的恶意反连。

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。

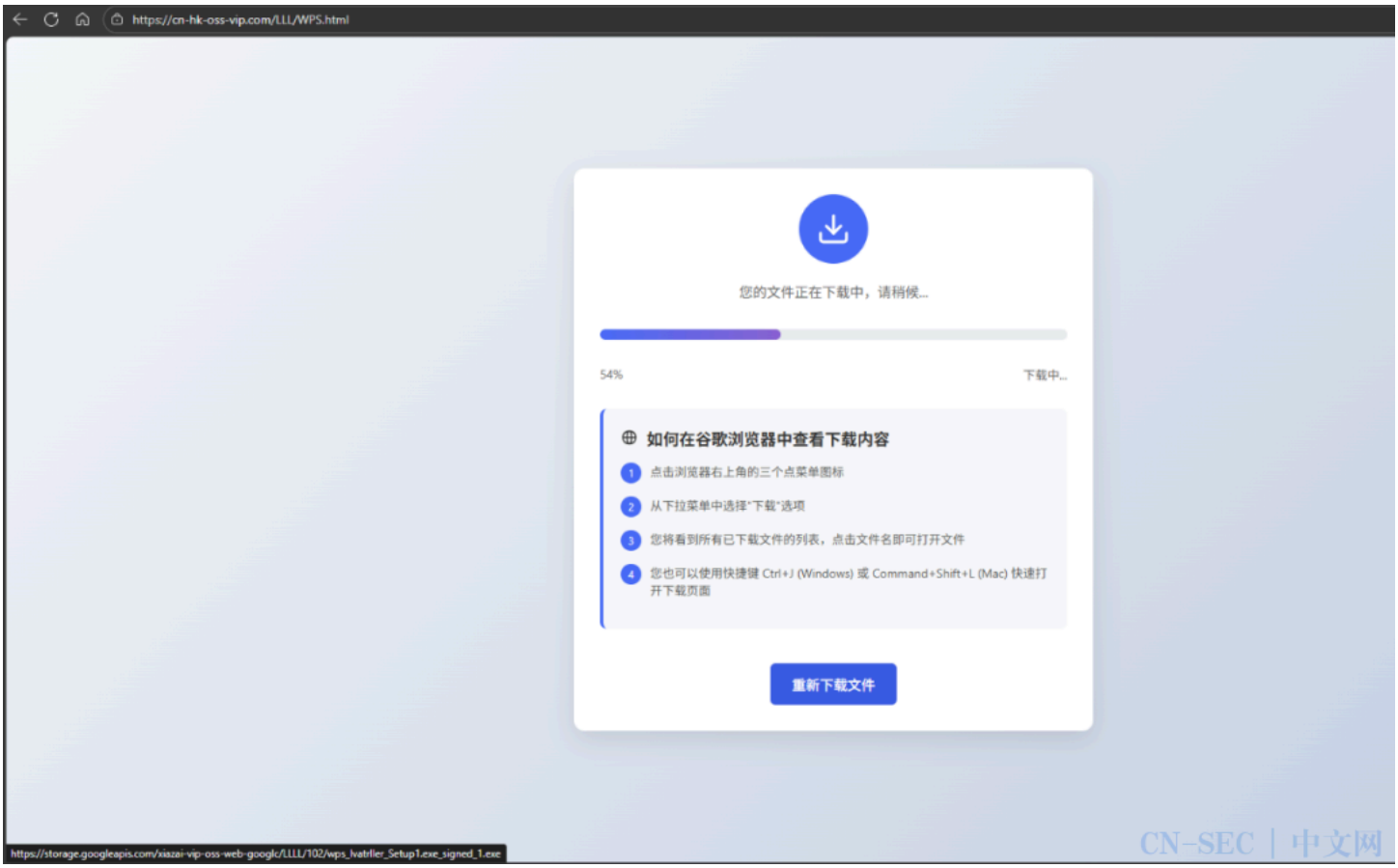
样本投递

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。



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

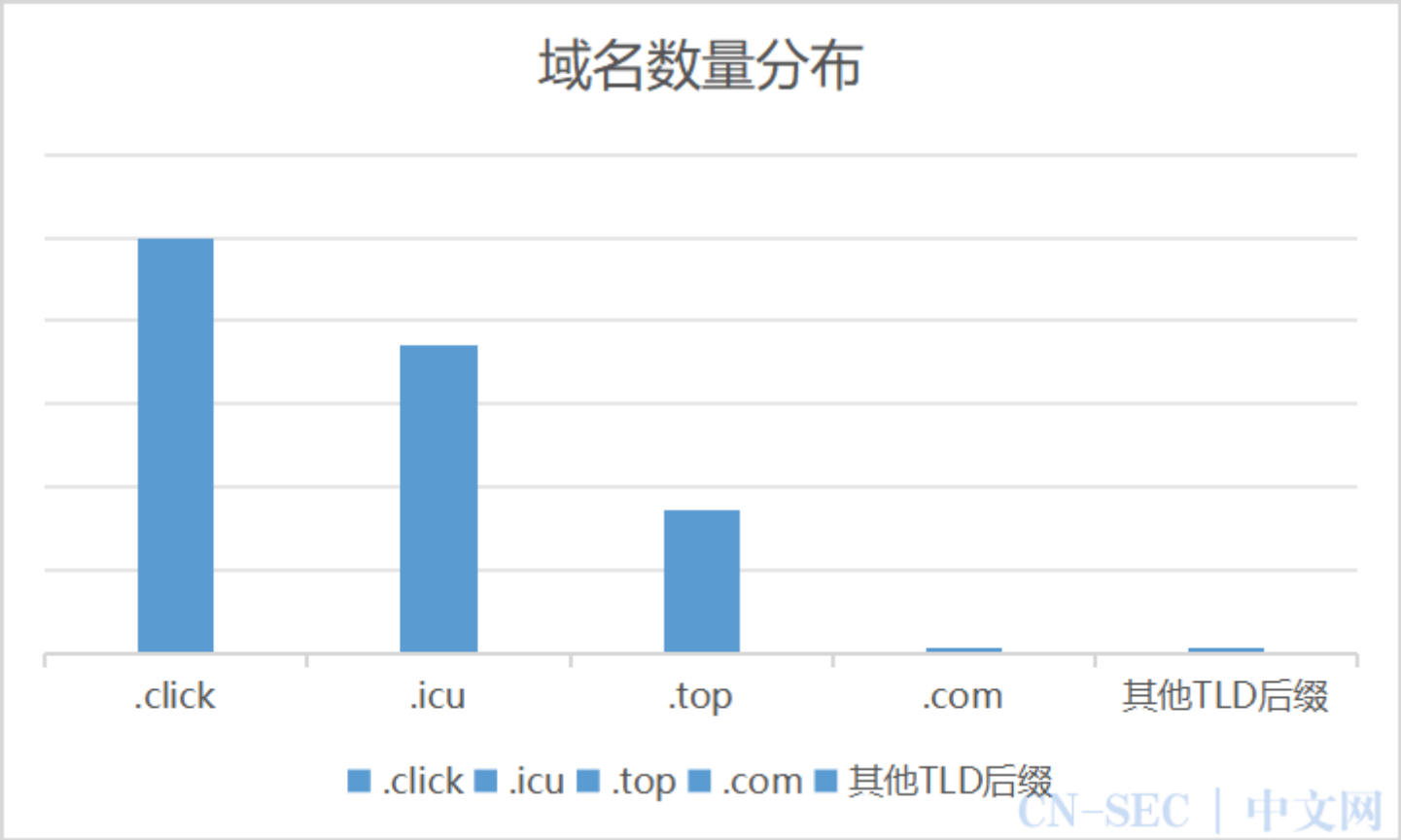
通过中转下载页面去下载放在Google文件存储服务上的安装包文件



这些钓鱼域名使用了随机字母的二级域名

```
ooxxwvenic.icu
bbzzdkem.icu
aisixxxz.top
xxsszzzw.click
ssuuxoxoxs.click
ssuuxoxozu.click
niimzw.click
yifanyxxz.top
ossonj.click
xiuxiua64.top
ossovu.click
yfyxxx.top
eexccsd.click
ossoxj.click
ossoxs.click
mtxxxx.top
vvxvvvu.click
eexcczw.click
vvxwvvzw.click
qsyyxx.top
```

以及廉价的TLD顶级域名后缀



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。

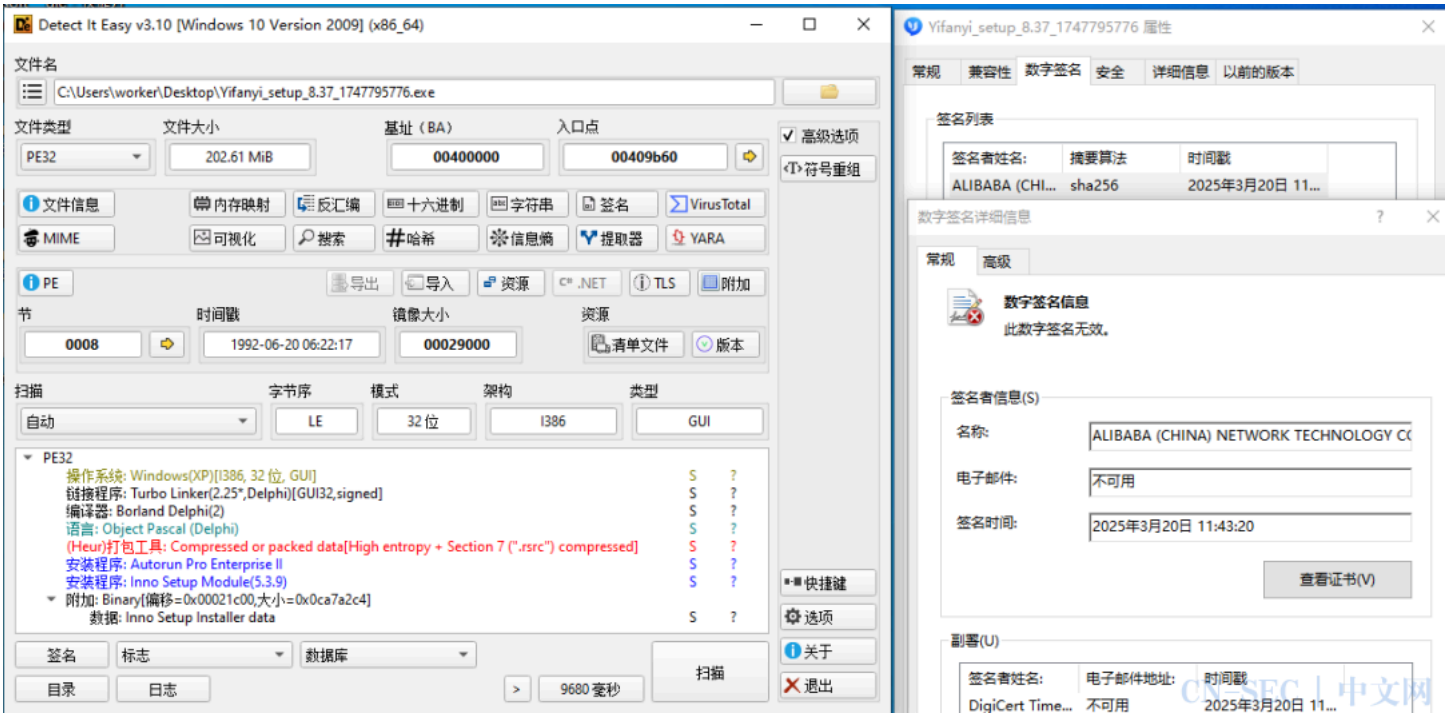
样本分析

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

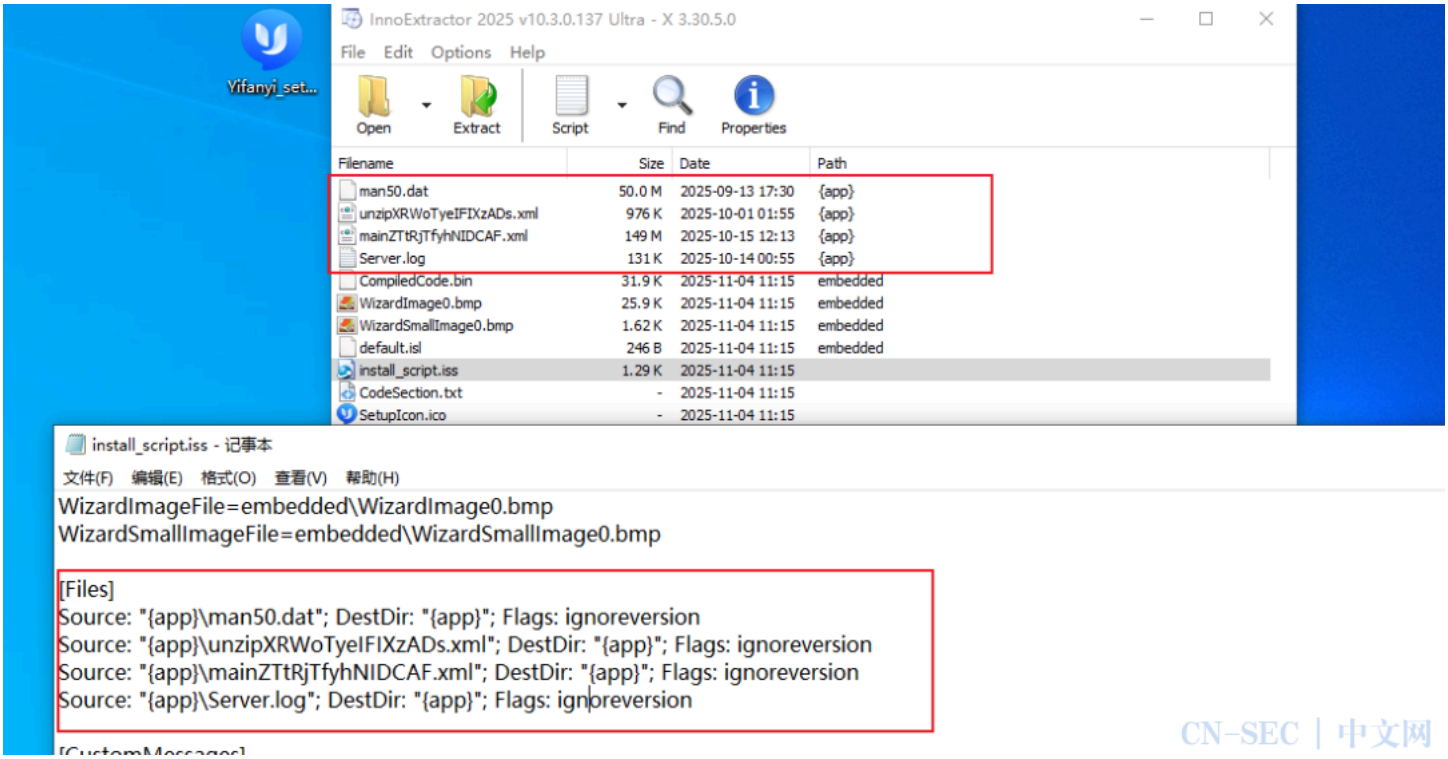
```
|p1:x-wwww.com|o1:8880|t1:1|p2:|o2:|t2:1|p3:127.0.0.1|o3:80|t3:1|dd:1|cl:1
|fz:精聊|bb:1.0|bz:2025. 6.15|jp:0|bh:0|ll:0|dl:1|sh:0|kl:0|bd:0|
```

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



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



OneSEC在早些时候，已能精准捕样本执行后的恶意行为。

线程创建

高危驱动加载

恶意反连

后门执行

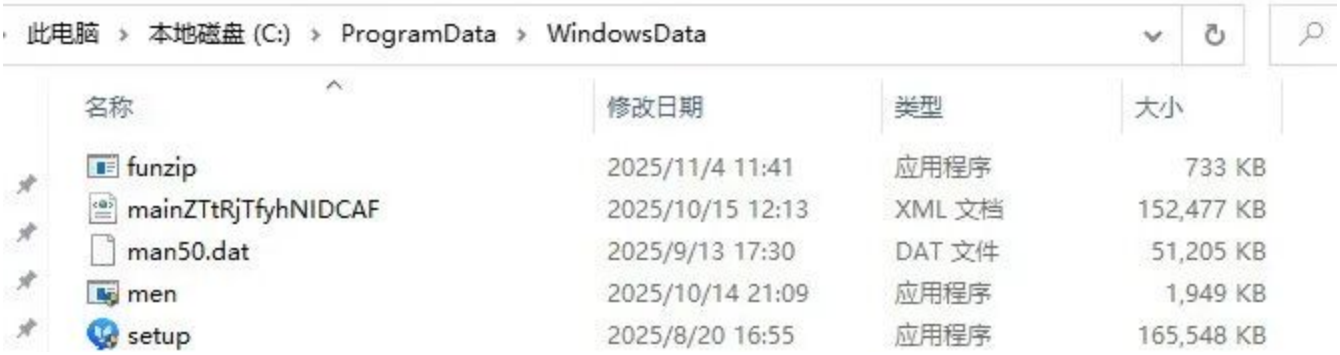
云沙箱S、沙箱分析平台OneSandbox也支持精确检测

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

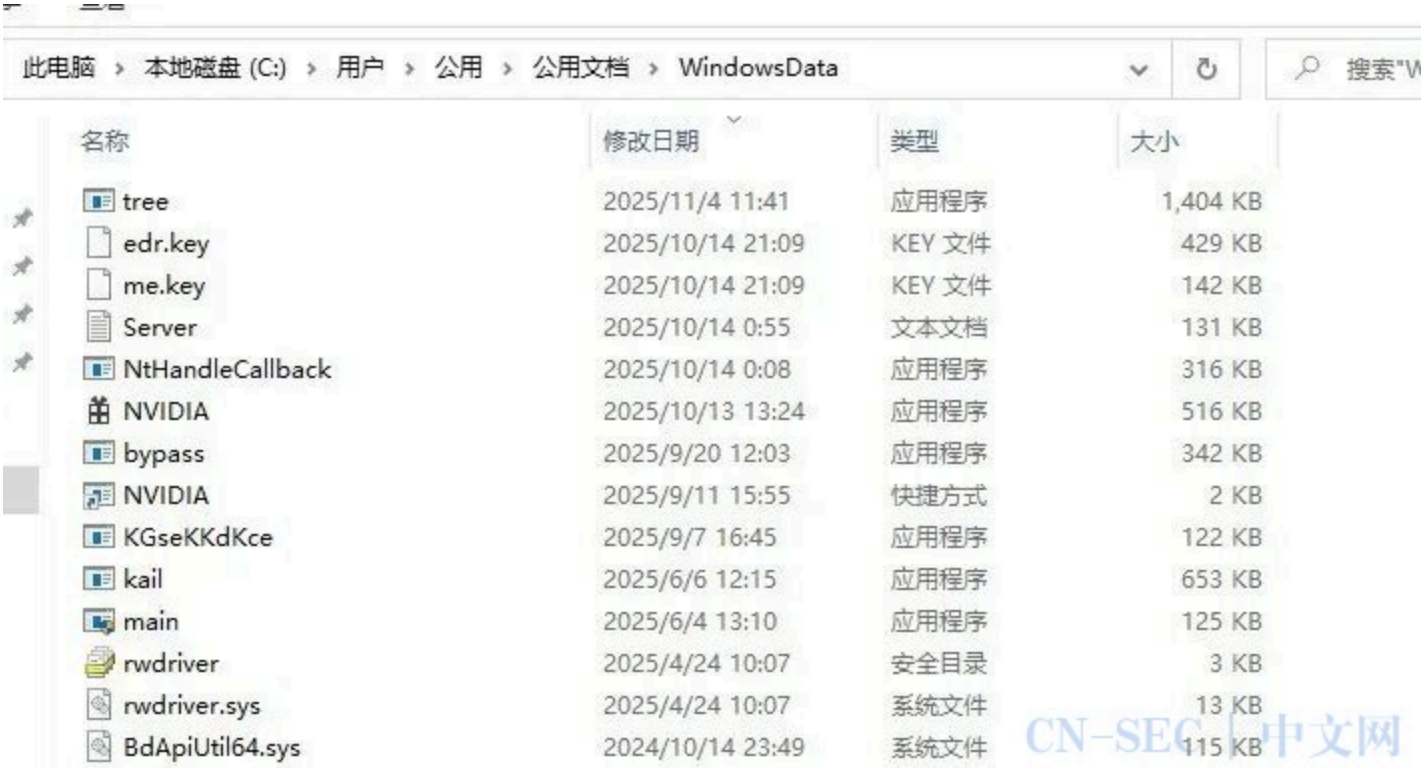


这些释放的文件功能为

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

后续在

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



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

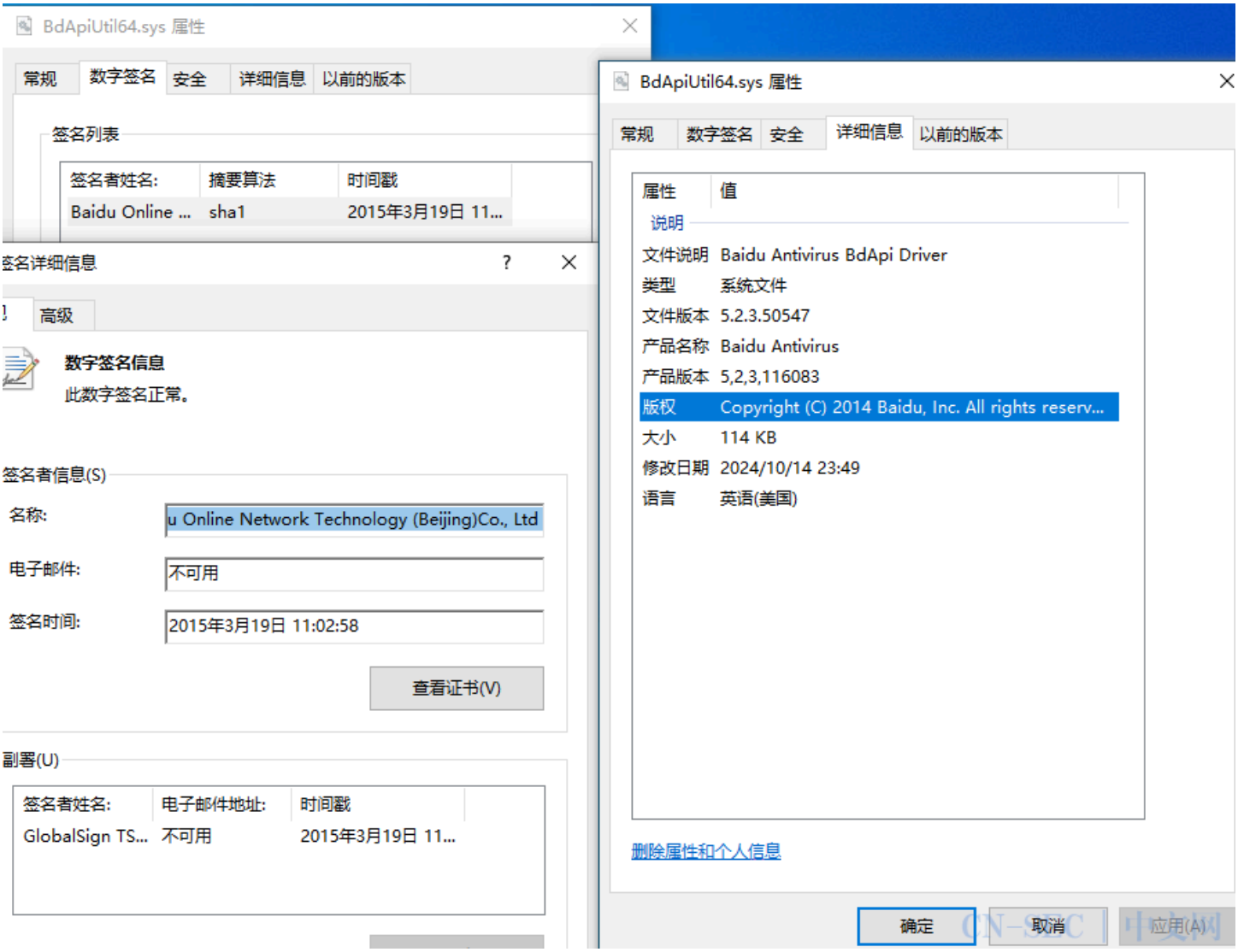
此外，程序运行时会动态加载其他两个驱动程序

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

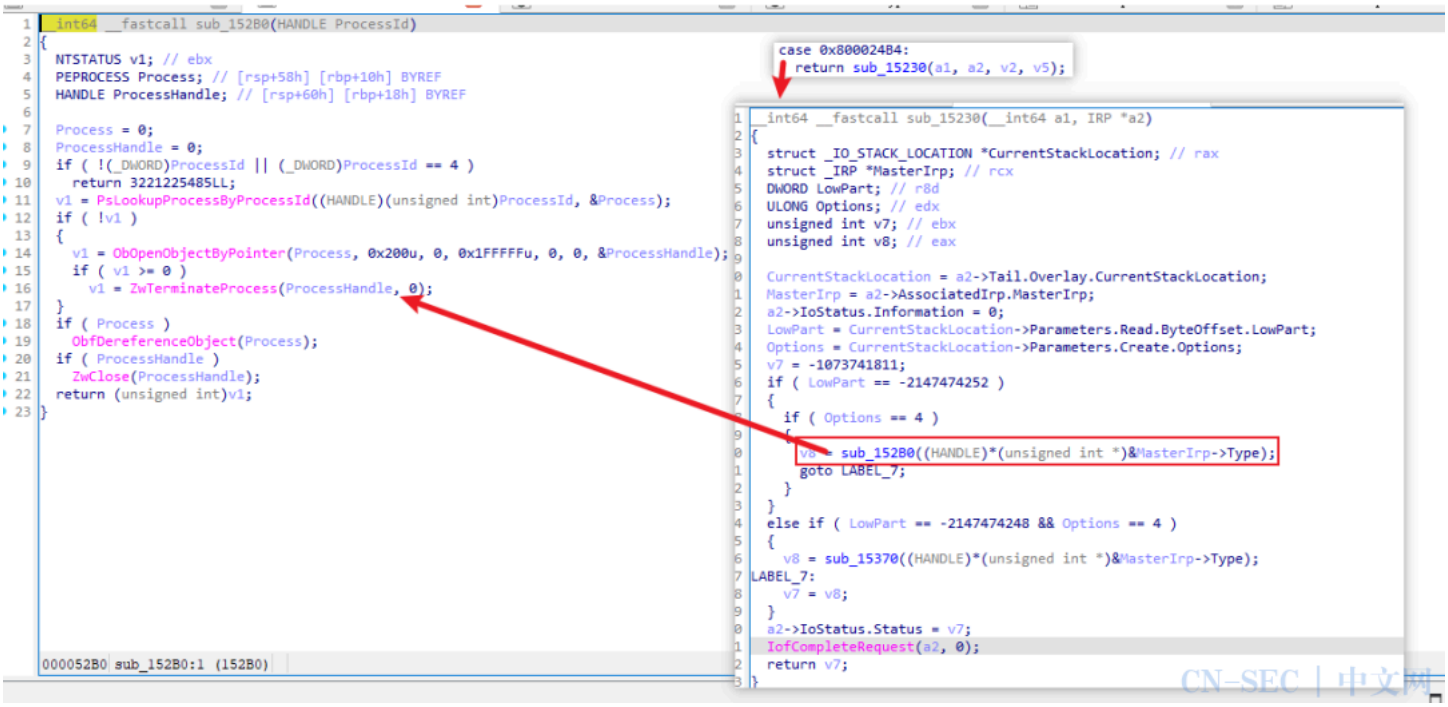
在本次样本中，程序共加载4个驱动程序，来负责银狐恶意进程信息隐藏，网络信息隐藏，内核内存的读写，以及BYOVD技术来关闭EDR和杀毒软件。

- 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



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

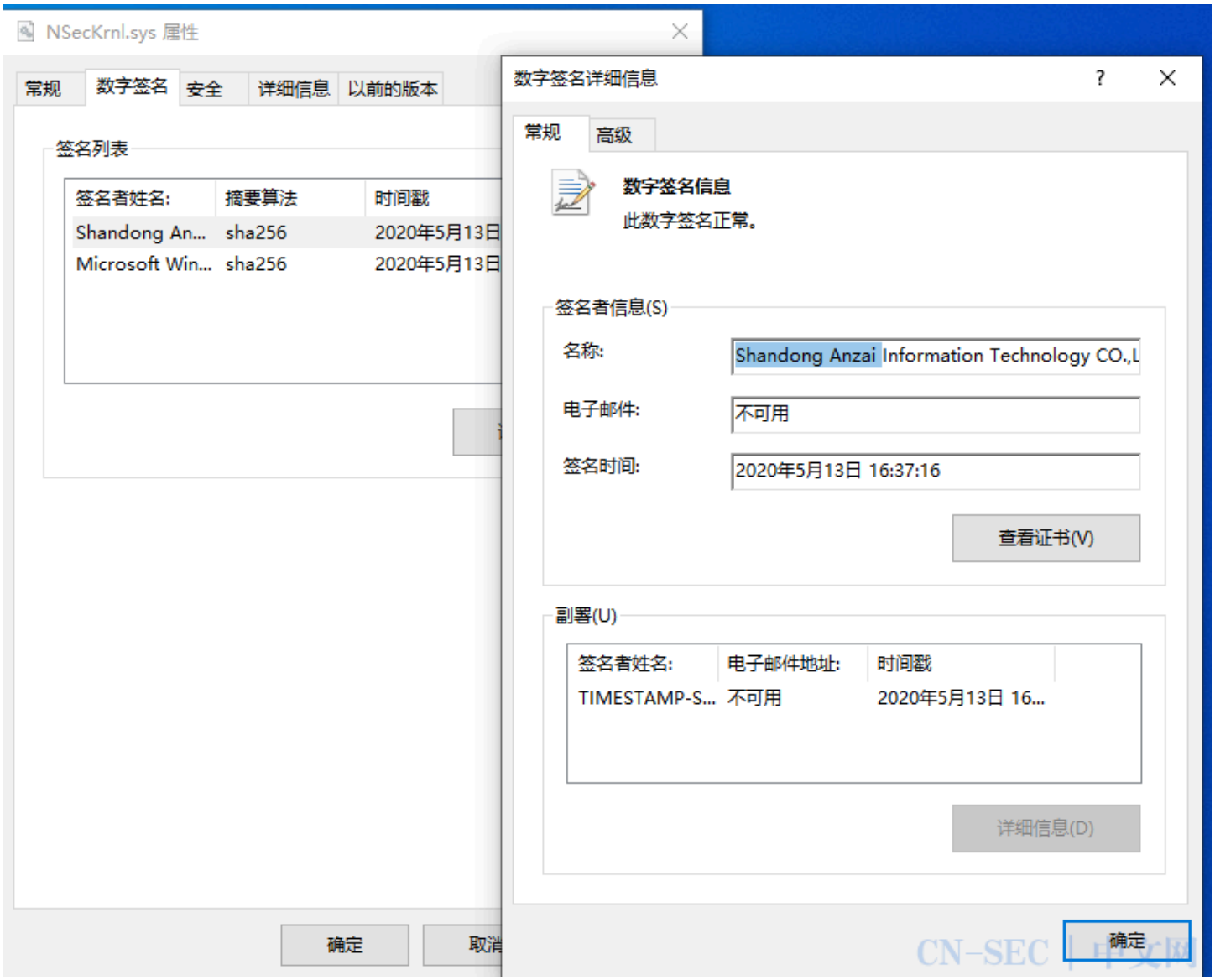
https://github.com/BlackSnufkin/BYOVD/blob/main/BdApiUtil-Killer/src/main.rs的魔改。

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

如果存在这些进程，则发送到驱动程序中进行关闭

```
  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(aIoctlCallFaile, 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

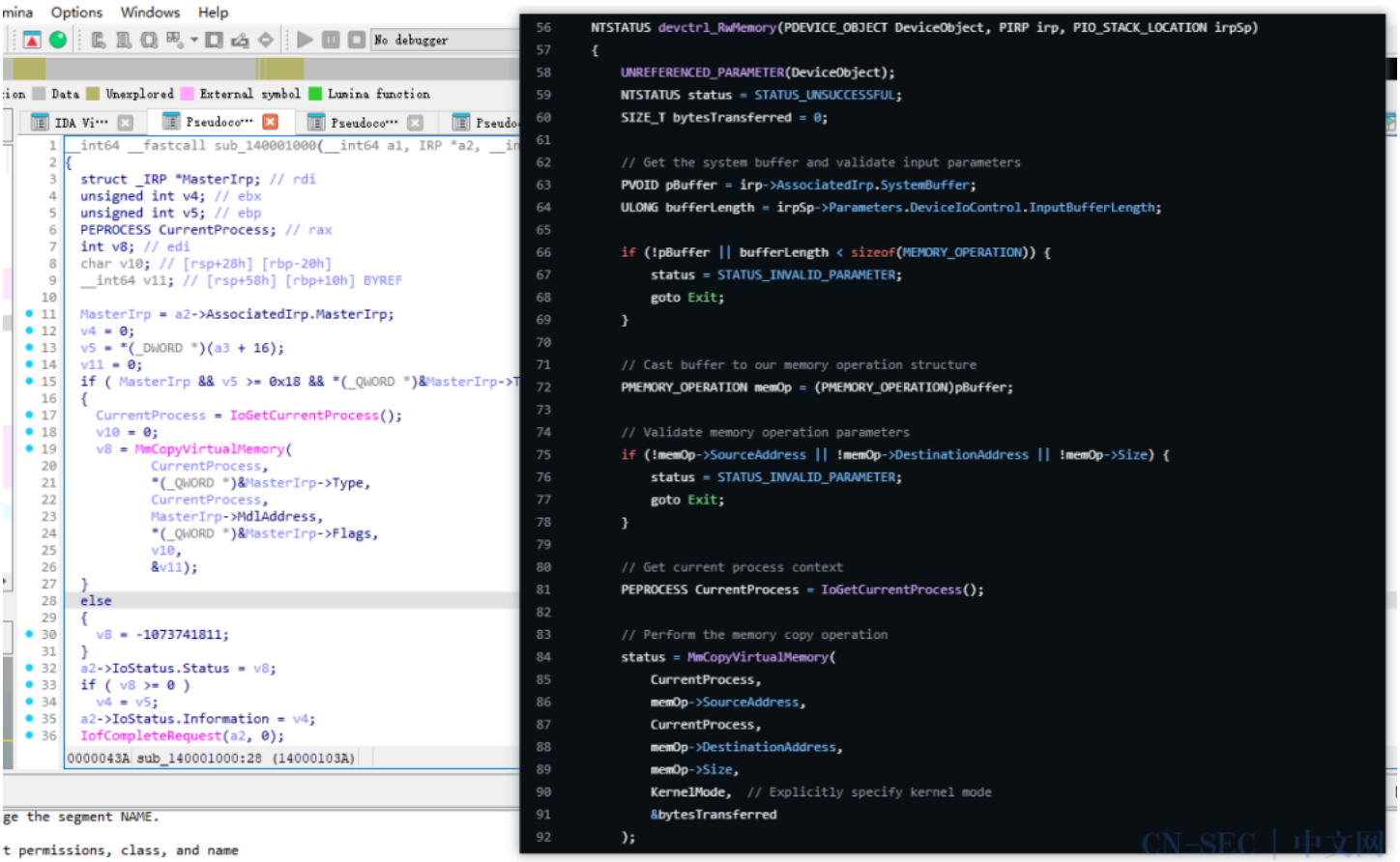


利用过程也是通过遍历所有进程名找到杀毒软件和EDR的进程号发送给驱动程序

- rwdriver.sys

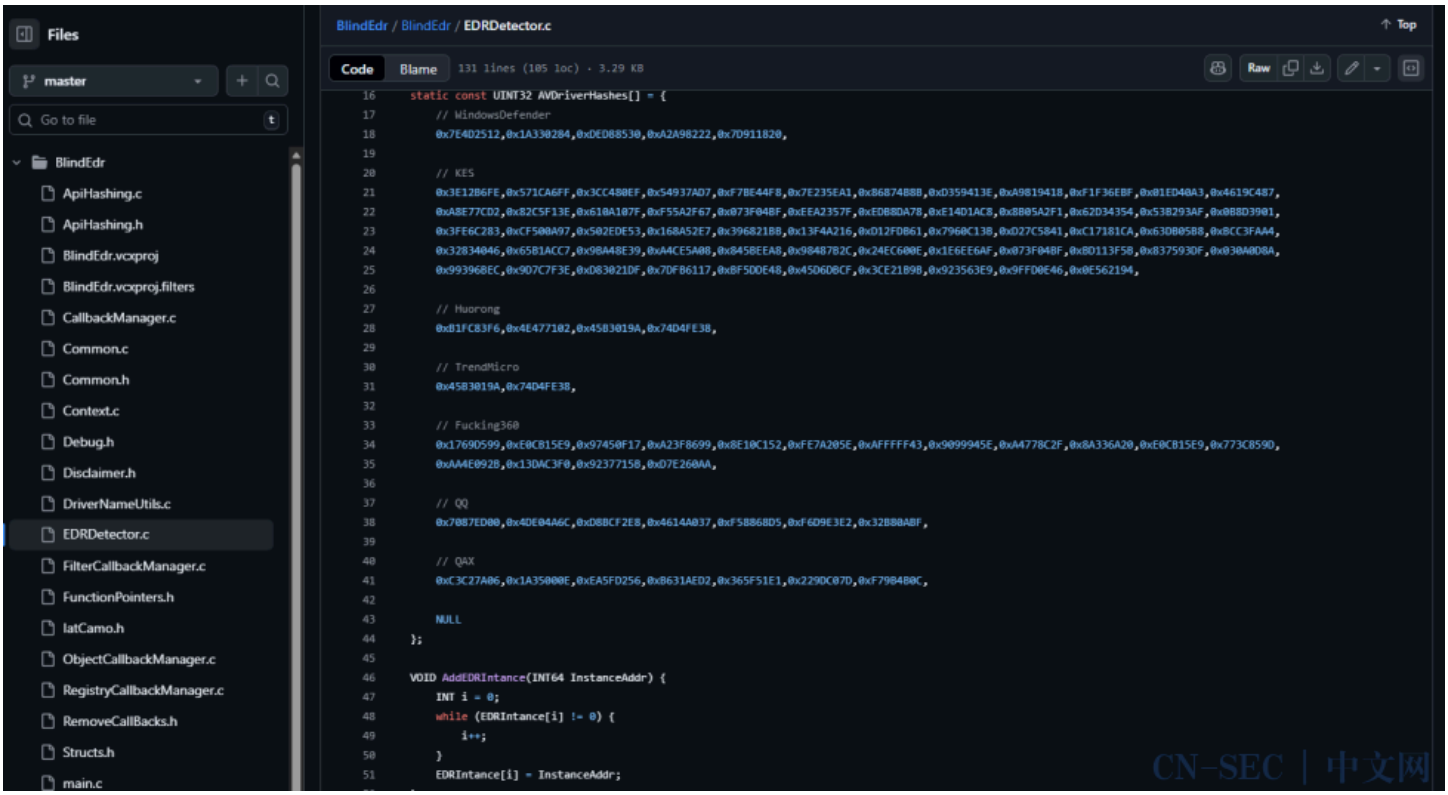
rwdriver.sys使用泄露的“中兴通讯股份有限公司”过期签名

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



这个驱动的使用程序main.exe，为开源项目

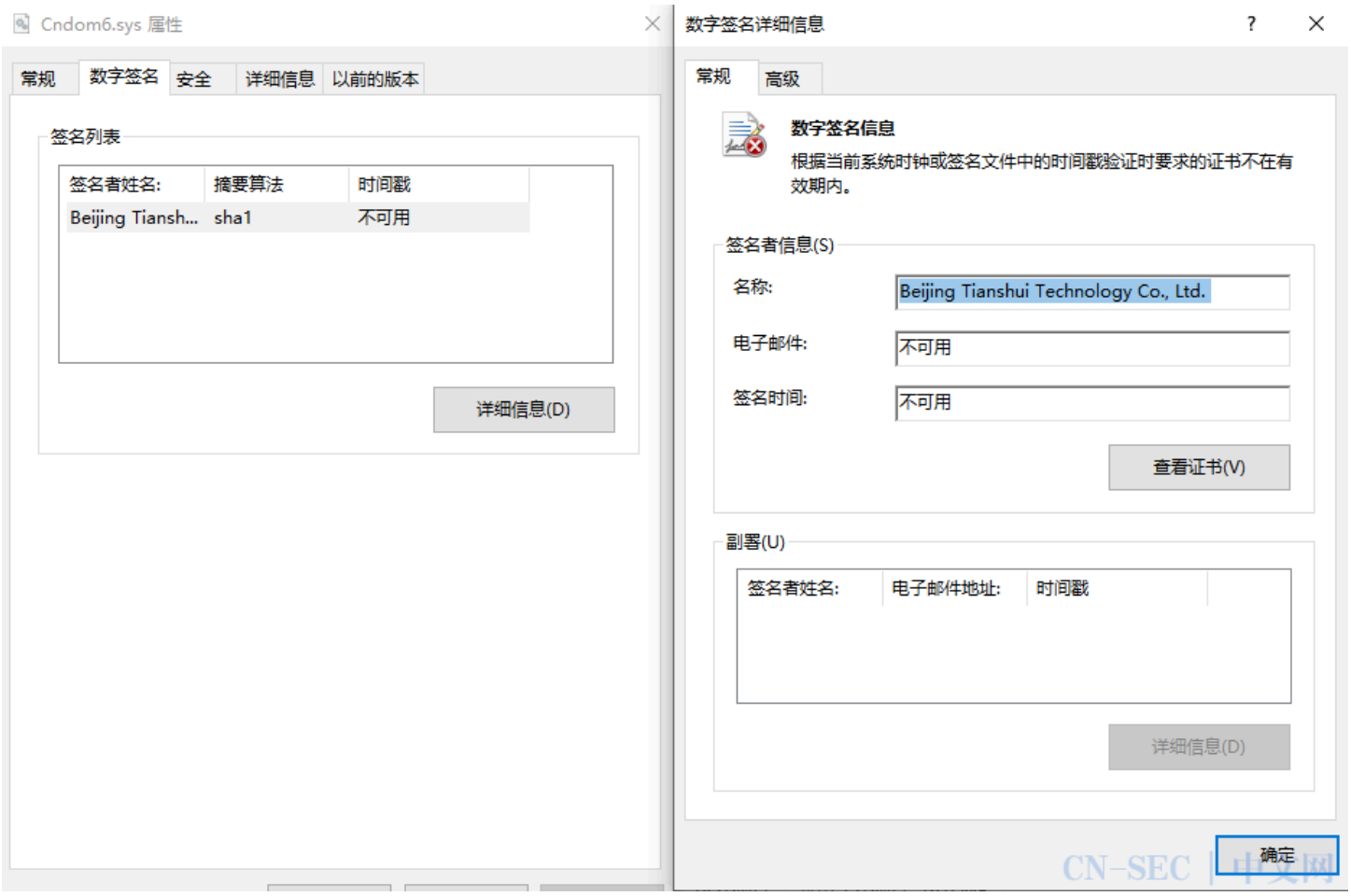
https://github.com/NanoWraith/BlindEdr的二次开发，该项目主要是用于针对一些杀软和EDR，利用内置字节码特征匹配，定位各类内核回调函数的实际地址，并将这些实际地址填充回原本的位置，实现在不终止安全软件进程的前提下，屏蔽其对进程、线程、文件、注册表等行为的监控能力。



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;
              }
```


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

该sys程序可以通过对这五个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。

```
bool sub_140001514()
{
  __int64 v0; // rax
  bool result; // al

  v0 = sub_1400011D8(L"\\Driver\\nsiproxy");
  qword_140003018 = v0;
  result = 0;
  if ( v0 )
  {
    qword_140003020 = *(__int64 (__fastcall **)(_QWORD, _QWORD))(v0 + 224);
    if ( qword_140003020 )
      return 1;
  }
  return result;
}
```

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

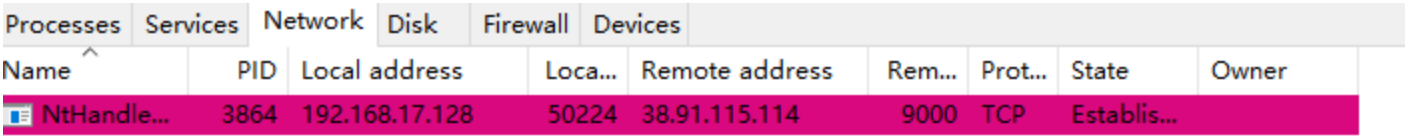
```
CurrentProcessId = (unsigned int)PsGetCurrentProcessId();
if ( !(unsigned __int8)sub_14000161C(CurrentProcessId) )
{
  if ( v6 == 112 )
  {
    if ( v7 == 112 )
    {
      v9 = qword_140003020(a1, a2);
      if ( !v9 && !*(_QWORD *)v4 && !*(_QWORD *)(v4 + 8) && *(_QWORD *)(v4 + 24) == 3 )
      {
        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;
                          *(_WORD *)v13 = 14640;
                          *(_DWORD *)(v13 + 30) = 67305985;
                          *(_WORD *)(v13 + 28) = 0;
                        }
```

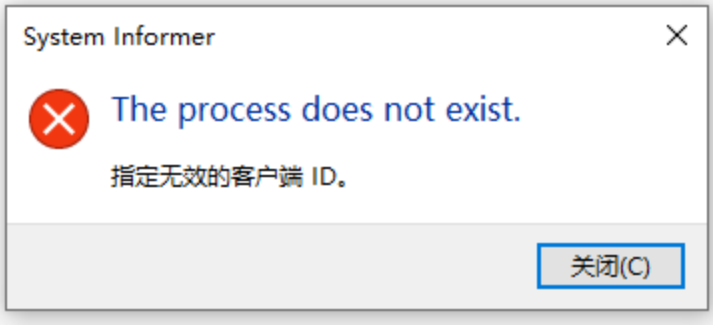
假数据

```
qword_140003010 = PoolWithTag;
if ( P )
{
  if ( PoolWithTag )
  {
    *(_QWORD *)(qword_140003018 + 224) = sub_1400012F4;
    return 0;
  }
  ExFreePoolWithTag(P, 0);
}
if ( qword_140003010 )
  ExFreePoolWithTag(qword_140003010, 0);
IoDeleteSymbolicLink(&SymbolicLinkName);
```


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。





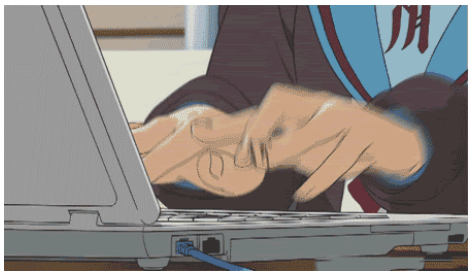
· END ·

推荐阅读

变种月增400+，免杀对抗花式翻新 | 银狐九月总结

模仿APT！银狐寄生政府网站大肆传播 | 银狐八月总结

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

- **左青龙**
- 微信扫一扫
- 

- **右白虎**
- 微信扫一扫
-