关于“魔盗”窃密木马大规模传播的风险提示

本报告由国家互联网应急中心（CNCERT）与安天科技集团股份有限公司（安天）共同发布。

一、 概述

近期，CNCERT 和安天联合监测到一批伪装成 CorelDraw、Notepad++、IDA Pro、WinHex 等多款实用软件进行传播的窃密木马。通过跟踪监测发现其每日上线境内肉鸡数（以 IP 数计算）最多已超过 1.3 万，由于该窃密木马会收集浏览器书签、邮箱账户等信息，故我们将命名为“魔盗”。

攻击者利用“cdr[.]jyxwlkj.cn”及“cdrnb[.]jyxwlkj.cn”域名建立多个软件下载页面，用于投放伪装成实用软件的“魔盗”窃密木马。窃密木马运行后会收集受害者主机中已安装的软件列表与多款浏览器的历史记录、书签数据和邮件客户端邮箱账户信息，并加密回传至攻击者服务器。由于部分恶意程序具备在线升级能力，因此攻击者可随时更改攻击载荷（如勒索、挖矿、窃密等不同目的的攻击载荷），给受害者造成更大损失。

二、 “魔盗”窃密木马分析

（一）传播方式分析

攻击者利用“cdr[.]jyxwlkj.cn”域名建立软件下载页面，将伪装为“破解版 CorelDraw”绘图工具的压缩包投放至该页面进行大范围传播。用户一旦执行压缩包中的恶意程序便会在主机中创建服务并添加注册表启动项，实现持久化驻留，随后从攻击者服务器中下载窃密组件进行数据窃取并回传。

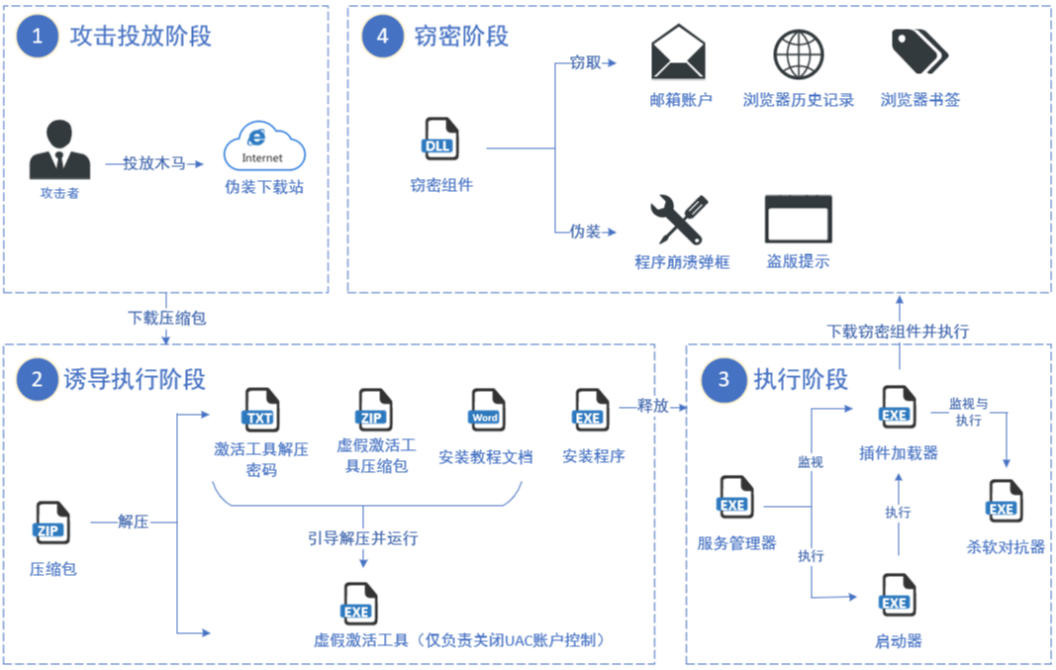

图 1　攻击流程图

（二）相关样本分析

“魔盗”窃密木马整体执行流程可分为 3 个阶段：诱导执行阶段、执行阶段与窃密阶段。组件调用关系图如下：

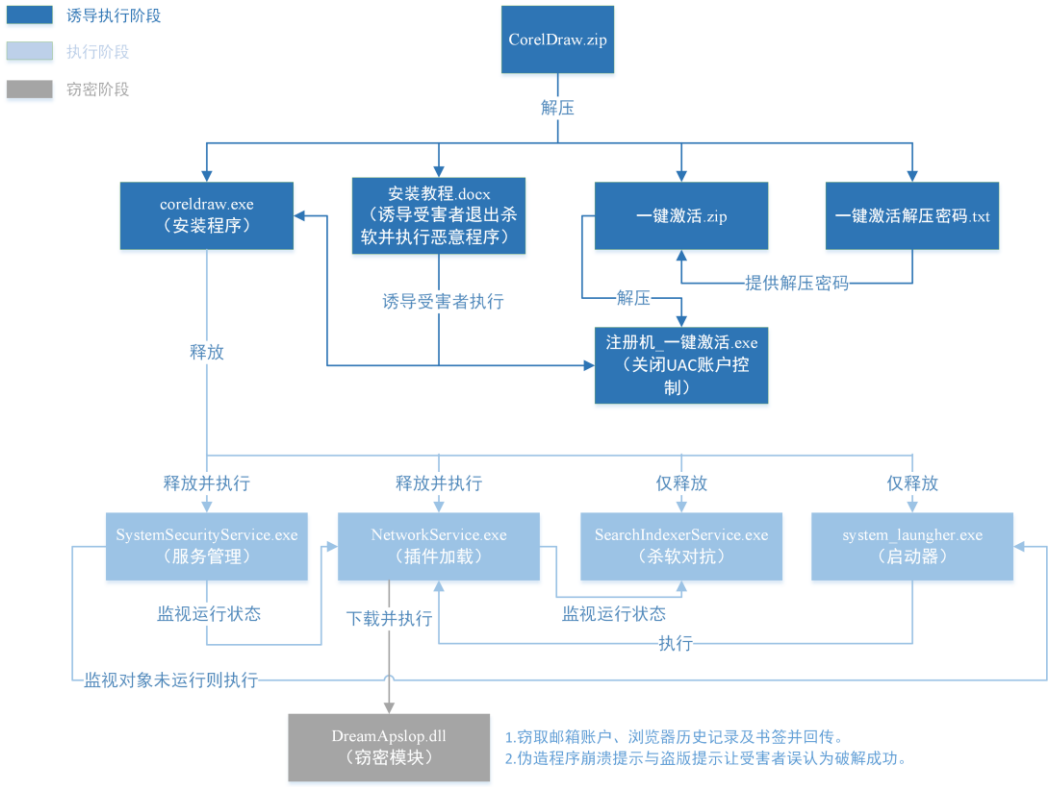

图 2 组件调用关系图

1、诱导阶段

为了诱导受害者执行恶意程序，攻击者在压缩包中提供了4个配套文件，具体文件信息见下表：

文件名	MD5	功能简述
一键激活.zip	0EC96FF955932E185DAA904027B41DF6	激活工具压缩包
coreldraw.exe	CD70268ABEE2F2AFC846E9F1BE6D8AD0	NSIS 安装程序
安装教程.docx	F84AAA3A4A39730994962FFC53F1AECE	安装教程文档
一键激活密码.txt	D6A69EDA56D5CB760C71C32DFD16715F	一键激活.zip 解压密码

其中“安装教程.docx”以“杀毒软件会误报盗版软件”为由，诱导用户关闭杀毒软件，后通过文字+配图的方式诱导受害者执行“安装程序”与“激活工具”。其中，安装程序是包含恶意模块的 NSIS 安装包，激活工具仅用于关闭 UAC 账户控制并无实际激活功能。

图 3 安装教程文档部分内容

2、执行阶段

本阶段以 NSIS 安装程序“coreldraw.exe”作为初始载荷，通过其释放的多个组件间的协同作业保证恶意程序的持续运行。这些组件包括“服务管理组件”、“启动器组件”、“插件加载组件”和“杀软对抗组件”。

2.1 初始载荷

病毒名称	Trojan[Spy]/Win32.APS
原始文件名	coreldraw.exe
MD5	CD70268ABEE2F2AFC846E9F1BE6D8AD0
处理器架构	Intel 386 or later, and compatibles
文件大小	11.4MB(12,041,288 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2012-02-24 19:20:04
数字签名	无
加壳类型	无
编译语言	C++
VT 首次上传时间	无

VT 检测结果	无

压缩包中的“coreldraw.exe”为执行阶段的初始载荷。该程序运行后会创建“%appdata%\Microsoft\Network”、“SysWow64\security”两个目录并向其中释放多个恶意载荷及大量C++运行库文件。释放的恶意载荷信息见下表：

所在目录	主要文件及目录	功能简述
%appdata%\Microsoft\Network	NetworkService.exe	1.回传上线的受控主机基本情况 2.下载并加载窃密插件 3.监视 SearchIndexerService.exe 的运行状态
	SearchIndexerService.exe	对抗杀毒软件
	System_Warning.exe	展示虚假盗版提示
	plugin 目录	包含下载的 DreamApslop.dll 窃密插件
SysWow64\security	SystemSecurityService.exe	1.创建服务实现持久化驻留 2.监视 NetworkService.exe 的运行状态
	system_laungher.exe	启动器组件，仅负责运行“NetworkService.exe”
	NetworkService 目录	%appdata%\Microsoft\Network 目录的完整副本

文件释放完毕后会执行“NetworkService.exe”与“SystemSecurityService.exe”。且分别携带启动参数“nsis winhex.exe”、“start”。

2.2 服务管理

“SystemSecurityService.exe”为服务管理组件，其主要功能为通过创建系统服务实现持久化驻留并确保“NetworkService.exe”进程的持续执行。该组件的样本标签如下：

病毒名称	Trojan[Spy]/Win32.APS
原始文件名	SystemSecurityService.exe
MD5	6ED3E57FDBEF38530385248D2ED7E96B

处理器架构	Intel 386 or later, and compatibles
文件大小	308.0 KB (315,392 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2022-07-19 00:57:49
数字签名	无
加壳类型	无
编译语言	C++
VT 首次上传时间	2022-08-02 08:01:36
VT 检测结果	3/70

该组件执行后会根据创建名为“SystemSecurityService”的服务实现自身的持久化驻留。通过不同的启动参数控制服务的启动与停止。服务的参数如下表：

显示名称	系统安全主动服务+7 位随机数
注册名称	自身文件名（不包括扩展名）
描述内容	管理系统安全程序主机进程。如果此服务被停止，则系统安全服务将无法正确运行，任何依赖它的服务将无法启动。
启动类型	自动

该组件以服务启动后会持续监视“NetworkService.exe”进程是否存在，若不存在则以管理员方式运行“system_laungher.exe”。除此之外，当服务停止或崩溃时还会在自身文件所在目录创建一个自身文件副本并执行，新进程会重复上文操作以实现自身进程的持续运行。

```
result = a1;
if ( a1 == SERVICE_CONTROL_STOP )
{
  ServiceStatus.dwWin32ExitCode = 0;
  ServiceStatus.dwCurrentState = 1;
  SetServiceStatus(hServiceStatus, &ServiceStatus);
  sub_41E924(v2, v3);
  goto LABEL_5;
}
if ( a1 == SERVICE_CONTROL_SHUTDOWN )
{
LABEL_5:
  ServiceStatus.dwWin32ExitCode = 0;
  ServiceStatus.dwCurrentState = 1;
  SetServiceStatus(hServiceStatus, &ServiceStatus);
  return sub_41E924(v2, v3);
}
return result;
```

图 4 崩溃或停止后的再启动

2.3 启动器

“system_laungher.exe”为启动器组件，该组件仅负责运行“NetworkService.exe”。攻击者疑似误将该组件文件名中的“launcher”（发射器）写为“laungher”。该组件的样本标签如下：

病毒名称	Trojan[Stealer]/Win32.APS
原始文件名	system_laungher.exe
MD5	F7CDC25E606FF80B0F72CE6323827374
处理器架构	Intel 386 or later, and compatibles
文件大小	38.0 KB (38,912 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2022-07-19 00:59:21
数字签名	无
加壳类型	无
编译语言	C++
VT 首次上传时间	2022-08-02 08:01:36
VT 检测结果	2/70

该组件运行后会判断“%appdata%\NetworkService\”路径下是否存在“NetworkService.exe”文件，此处与初始载荷释放文件的路径不同，因此在该组件首次运行时文件并不存在。

若文件存在则通过“open”或“rundll32 shell32,OpenAs_RunDLL”命令启动“%appdata%\NetworkService\NetworkService.exe”。

```
if ( !pszPath )
  return -1;
IsDirectoryA = PathIsDirectoryA(pszPath);
v6 = "explore";
if ( !IsDirectoryA )
  v6 = "open";
result = (int)ShellExecuteA(hwnd, v6, pszPath, lpParameters, 0, a4);
if ( result == 0x1F )
{
  sprintf(CmdLine, "rundll32 shell32,OpenAs_RunDLL %s", pszPath);
  result = WinExec(CmdLine, 5u);
}
if ( result > 32 )
  return 0;
return result;
```

图 5 利用命令行启动目标程序

若文件不存在，则会将自身运行目录下的“NetworkService”目录完整复制到“%appdata%”中。随后以上文相同方式启动复制后的“NetworkService”目录下的“NetworkService.exe”。

```
.text:00401F1B                push    eax             ; lpFileOp
.text:00401F1C                mov     [ebp+FileOp.hwnd], 0
.text:00401F23                mov     [ebp+FileOp.fAnyOperationsAborted], 1
.text:00401F2A                mov     [ebp+FileOp.hNameMappings], 0
.text:00401F31                mov     [ebp+FileOp.lpszProgressTitle], offset aMove ; "Move"
.text:00401F38                call    ds:SHFileOperationA
```

图 6 拷贝 NetworkService 目录

2.4 插件加载

“NetworkService.exe”组件用于实现插件加载。该组件根据运行参数的不同分为三个模式：“完整模式”、“简易模式”与“看门狗模式”，三个模式的具体功能见下文。该组件的样本标签如下：

病毒名称	Trojan[Spy]/Win32.APS
原始文件名	NetworkService.exe
MD5	AB4FB51F10548AF01AA8C0829BB723E5
处理器架构	Intel 386 or later, and compatibles
文件大小	311.0 KB (318,464 字节)

文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2022-07-29 14:56:06
数字签名	无
加壳类型	无
编译语言	C++
VT 首次上传时间	2022-08-03 18:05:02
VT 检测结果	4/69

该组件也是所有组件中唯一标注了版本号的组件。

```
.rdata:004405C8 aV113_0         db 'V1.1.3',0
.rdata:004405CF                 align 10h
.rdata:004405D0 aVersion_0      db 'version',0
.rdata:004405D8 aPara_0         db 'para',0
.rdata:004405DD                 align 10h
.rdata:004405E0 aV113_1         db 'V1.1.3',0
.rdata:004405E7                 align 4
.rdata:004405E8 aIndexIni       db 'index.ini',0
.rdata:004405F2                 align 4
.rdata:004405F4 ; const char aSIndexIni_0[]
.rdata:004405F4 aSIndexIni_0    db '%s/index.ini',0
.rdata:00440601                 align 4
.rdata:00440604 aV113_2         db 'V1.1.3',0
```

图 7 样本中标注的版本号

完整模式

当运行参数为“nsis”、随机数或为空时，组件执行该模式。

在该模式下，组件会在注册表“HKCU\Software\Microsoft\Windows\CurrentVersion\Run”及“HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run”两处位置添加名为“NetworkService”的启动项实现自身的持久化驻留。

```
Sub_401C10_GetSelfName(v4);
if ( !RegOpenKeyExA(HKEY_CURRENT_USER, "Software\\Microsoft\\Windows\\CurrentVersion\\Run", 0, 0x20006u, &phkResult) )
{
  memset(Filename, 0, sizeof(Filename));
  ModuleFileNameA = GetModuleFileNameA(0, Filename, 0x104u);
  v0 = (const CHAR *)Sub_403E50_Nothing(v4);
  RegSetValueExA(phkResult, v0, 0, 1u, (const BYTE *)Filename, ModuleFileNameA);
  RegCloseKey(phkResult);
}
if ( !RegOpenKeyExA(
        HKEY_CURRENT_USER,
        "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\StartupApproved\\Run",
        0,
        0x20006u,
        &phkResult) )
{
  v7 = 0;
  v8 = 0;
  v9 = 0;
  v10 = 0;
  Data = 2;
  v1 = (const CHAR *)Sub_403E50_Nothing(v4);
  RegSetValueExA(phkResult, v1, 0, 3u, &Data, 0xCu);
  RegCloseKey(phkResult);
}
std::string::~string((std::string *)v4);
```

图 8 添加注册表启动项

组件使用“dog”加随机数作为运行参数创建看门狗模式下的自身进程。

```
if ( *((_BYTE *)v11 + 56) )
  sprintf(Buffer, "%u", *((_DWORD *)v11 + 13));
else
  sprintf(Buffer, "dog %u", *((_DWORD *)v11 + 13));
v6[8] = v6;
std::string::string((std::string *)v6, Buffer);
v6[7] = v5;
sub_438EC0(v6[0], v6[1], v6[2], v6[3], v6[4], v6[5]);// shell open
```

图 9 启动看门狗模式

随后向攻击者服务器发起 5 次网络请求：

第一次请求：服务器响应数据中会包含 DLL 插件列表及版本号。若插件列表中的文件在“plugin”目录中不存在，或当前版本与响应数据中的版本号不同，则会从攻击者服务器下载列表中的所有插件。随后加载“plugin”目录下的所有 DLL 并执行其导出函数“PlugIn_Create”。

第二次请求：获取受害者主机的 CPUID、处理器签名、系统盘卷号、GUID，将拼接后计算出的 MD5 值，经 AES 加密+Base64 编码后回传至攻击者服务器。

第三次请求：获取注册表“HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall”及“HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall”下保存的所有已安装的程序列表，经 AES 加密+Base64 编码后回传至攻击者服务器。

第四次请求：将初始载荷的文件名（即“coreldraw”）经 AES 加密+Base64 编码后回传至攻击者服务器。

第五次请求：通过执行“whoami”及“netsh wlan show profiles”命令获取受害者主机名、用户名、wifi 列表信息，经 AES 加密+Base64 编码后回传至攻击者服务器。

最后循环判断“SearchIndexerService.exe”进程是否存在，若不存在则运行。

```
while ( 1 )
{
  do
  {
    v38[0] = 1000;
    v19 = sub_42DF10(&v28, v38);
    sub_42DF30((int)v19);
  }
  while ( FindWindowA("MegWnd", "SearchIndexerWnd") );
  v24 = 0;
  v23 = 0;
  v22 = 0;
  v20 = (const CHAR *)Sub_403E50_Nothing(v51);
  ShellExecuteA(0, "open", v20, v22, v23, (INT)v24);
}
```

图 10 监视 SearchIndexerService.exe 进程

简易模式

当运行参数包含“vs”时执行该模式。

该模式相比完整模式仅舍弃了“看门狗创建”与“注册表启动项添加”功能，其余功能均一致。

看门狗模式

当运行参数包含“dog”时执行该模式。

该模式的功能为持续判断“完整模式”下的“NetworkService.exe”进程是否存在。若进程不存在，则以随机数作为运行参数启动自身进程（即“完整模式”）。

```
TickCount = GetTickCount();
v26 = (std::string *)sub_4399D0((int)v17, TickCount);
v27 = (int)v26;
LOBYTE(v50) = 5;
v13 = (BYTE *)v26;
std::string::string((std::string *)v18, "NetworkService");
```

图 11 监视完整模式下的 NetworkService.exe 进程

2.5 杀软对抗

“SearchIndexerService.exe”为杀软对抗组件。该组件通过断开杀毒软件进程的 TCP 连接防止自身样本被上传至云端。该组件的样本标签如下：

病毒名称	Trojan[Spy]/Win32.APS
原始文件名	SearchIndexerService.exe
MD5	9988BF5FF1D0DFDC83B0F880310ACFC9
处理器架构	Intel 386 or later, and compatibles
文件大小	36.5 KB (37,376 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]

时间戳	2022-07-19 14:29:01
数字签名	无
加壳类型	无
编译语言	C++
VT 首次上传时间	2022-08-02 08:01:35
VT 检测结果	1/69

该组件运行后会循环遍历受害者主机上的 TCP 连接，若某个连接的发起进程为“360safe”、“360tray.exe”、“360sd”、“360rp”、“qqpctray.exe”或“hipsmain.exe”则将该 TCP 连接中断。

```
while ( 1 )
{
  sub_4046B0((int)v17);
  v20 = 0;
  v16 = v17;
  sub_403110(
    v17,
    (std::_Deque_unchecked_iterator<std::_Deque_val<std::_Deque_simple_types<std::shared_ptr<LagRecord> >
  sub_4032B0(
    v16,
    (std::_Deque_unchecked_iterator<std::_Deque_val<std::_Deque_simple_types<std::shared_ptr<LagRecord> >
  while ( (unsigned __int8)std::_Tree_const_iterator<std::_Tree_val<std::_Tree_simple_types<std::pair<unsi
  {
    v13 = sub_402CE0(v15);
    v12 = std::string::find((std::string *)(v13 + 68), "360safe", 0) != -1;
    v11 = std::string::find((std::string *)(v13 + 68), "360tray.exe", 0) != -1;
    v10 = std::string::find((std::string *)(v13 + 68), "360sd", 0) != -1;
    v9 = std::string::find((std::string *)(v13 + 68), "360rp", 0) != -1;
    v8 = std::string::find((std::string *)(v13 + 68), "qqpctray.exe", 0) != -1;
    v7 = std::string::find((std::string *)(v13 + 68), "hipsmain.exe", 0) != -1;
    if ( v12 || v11 || v10 || v9 || v8 || v7 )
      sub_404620(*(_DWORD *)v13, *(_DWORD *)(v13 + 32), *(_DWORD *)(v13 + 28), *(_DWORD *)(v13 + 60));
    sub_402D30(v15);
  }
  v5 = 40;
  v4 = sub_401E40(v6, &v5);
  sub_401E60((int)v4);
  v20 = -1;
  sub_402B50(v17);
}
```

图 12 中断杀毒软件 TCP 连接

3、窃密阶段

攻击者在本阶段使用的窃密载荷通过初始载荷释放或插件加载组件进行下载，由插件加载组件负责加载执行。窃密插件加载后会创建三个线程，功能分别为：弹出虚假盗版提示、伪造盗版崩溃及窃取用户数据。窃密插件的样本标签如下：

病毒名称	Trojan[Spy]/Win32.APS
原始文件名	DreamApslop.dll

MD5	652835C8ECFD722950D0F5D8509EA1C2
处理器架构	Intel 386 or later, and compatibles
文件大小	355.0 KB (364,032 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
时间戳	2022-07-29 01:15:31
数字签名	无
加壳类型	无
编译语言	C++
VT 首次上传时间	2022-08-02 02:04:26
VT 检测结果	1/69

窃密插件通过插件加载组件进行下载，且必然包含名为“PlugIn_Create”的导出函数供插件加载组件调用，因此未来攻击者可在不更改执行阶段中的组件的前提下投放不同功能的恶意载荷。

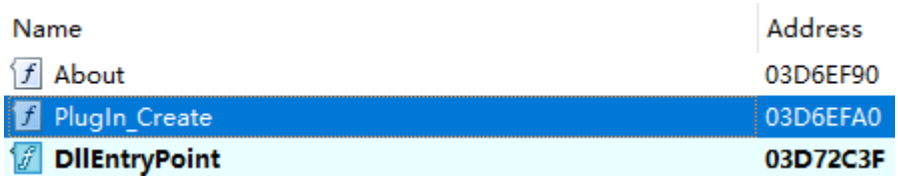

图 13 插件入口

线程 1：虚假盗版提示

线程 1 的主要功能为通过运行“System_Warning.exe”向受害者展示一个包含盗版提示的窗口以此让受害者误认为盗版软件已成功安装。此进程仅用于展示盗版提示，无实质恶意行为。

该线程会访问攻击者服务器获取进程列表，只有当进程列表中的进程正在受害者主机上运行时才会展示盗版提示。盗版提示窗口如下图：

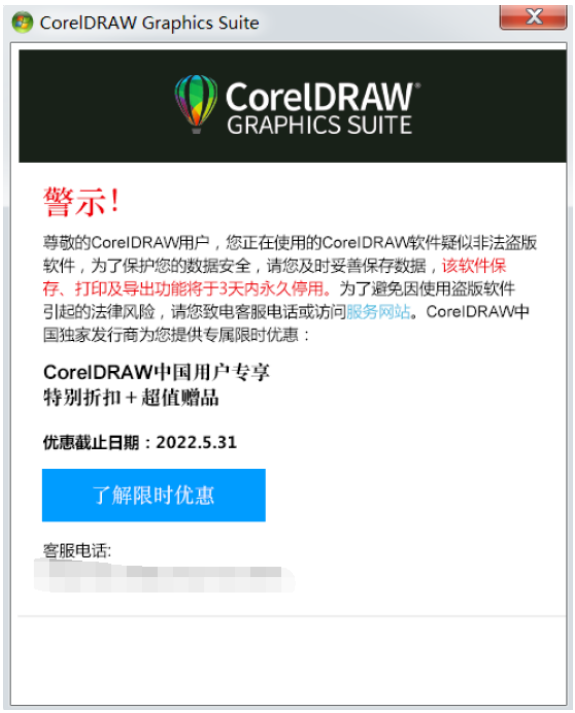

图 14 盗版提示程序界面

线程 2：伪造崩溃提示

为了防止受害者意识到软件并未成功破解，攻击者伪造了进程崩溃的提示。

线程 2 运行后会再次访问攻击者服务器获取另一份进程列表。若进程列表中的进程正在受害者主机运行，则会结束该进程并弹出一个崩溃提示以欺骗受害者。提示内容如下图：

```
std::string::string(
  (std::string *)v2,
  "Try restarting your computer and then restarting the program. If\n"
  " these actions do not resolve the problem, please uninstall and\n"
  " reinstall the program. Error ");
v3 = 0;
Sub_3D3CD50_GetCpuID_Sign_GUID_MD5(v1);
LOBYTE(v3) = 1;
unknown_libname_65(v1);
StrObjBuffer = (const CHAR *)Sub_100030B0_GetStrObjBuffer(v2);
MessageBoxA(0, StrObjBuffer, " ", 0x10u);
```

图 15 伪造进程崩溃提示

为了使崩溃提示看上去更加真实，该线程还会访问攻击者服务器来获取不同进程对应的不同的提示内容。

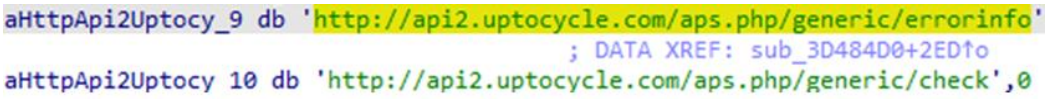

图 16 获取崩溃提示信息的接口地址

线程 3：数据窃取及回传

线程 3 用于窃取受害者主机的系统信息与隐私数据并经 AES 加密+Base64 编码后回传至攻击者服务器。目前攻击者窃取的目标为受害者的网卡信息、网页浏览记录、书签列表及邮箱地址。具体窃取数据及软件信息见下表：

软件名	数据文件	窃取内容
Google 浏览器	%localappdata%\Google\Chrome\User Data\Default\History	历史网址、访问时间
Google 浏览器	%localappdata%\Google\Chrome\User Data\Default\Bookmarks	书签列表
360 浏览器	%localappdata%\360Chrome\Chrome\User Data\Default\Cookies	历史网址、访问时间
360 浏览器	%localappdata%\360Chrome\Chrome\User Data\Default\Bookmarks	书签列表
360 极速浏览器	%localappdata%\360ChromeX\Chrome\User Data\Default\Cookies	历史网址、访问时间
360 极速浏览器	%localappdata%\360Chrome\Chrome\User Data\Default\Bookmarks	书签列表
360 安全浏览器	%localappdata%\secoresdk\360se6\User Data\Default\Cookies	历史网址、访问时间
360 安全浏览器	%localappdata%\secoresdk\360se6\User Data\Default\Bookmarks	书签列表
QQ 浏览器	%localappdata%\Tencent\QQBrowser\User Data\Default\History	历史网址、访问时间
QQ 浏览器	%localappdata%\Tencent\QQBrowser\User Data\Default\BookMarks	书签列表
搜狗浏览器	%localappdata%\SogouExplorer\HistoryUrl3.db	历史网址、访问时间

Edge 浏览器	%localappdata%\Microsoft\Edge\User Data\Default\WebAssistDatabase	历史网址、访问时间
火狐浏览器	%localappdata%\Mozilla\Firefox\Profiles\storage.sqlite	历史网址、访问时间
无	无文件，命令行“ipconfig /all”	MAC 地址
Outlook	%localappdata%\Microsoft\Office 下所有名字包含“@”的文件	历史登录账号
Foxmail	Foxmail 安装路径下所有名字包含“storage”的文件	历史登录账号

（三）样本关联分析

在对上述样本的关联分析中，我们发现攻击者除“CorelDraw”外，还伪装了 IDA Pro、WinHex 等众多热门软件的盗版下载。攻击者正在持续更新木马组件，近一月内国内已有近 65000 台设备受其感染，整体感染量呈上升趋势。

1、攻击者伪装多款软件的盗版下载

攻击者除“CorelDraw”外，还伪造了其他软件的盗版下载。这些伪造的盗版软件均投放到“cdr[.]jyxwlkj.cn”及“cdrnb[.]jyxwlkj.cn”域名中，且传播流程、恶意载荷功能与上文一致。具体伪造的软件列表如下：

软件名	下载页 URL
cdr 格式转换器	*/cdr-zhuanhuanqi.html
cdr 版本转换器	*/cdr-banbenzhuanhuanqi.html
cdr 字体插件	*/cdr-cdrzitichajian.html
cdr 素材	*/cdr-sucai.html
cdr 颜色填充	*/cdr-cdryansetianchong.html
cdr 条形码插件	*/cdr-barcode.html
cdr 不同版本	*/cdr-coreldraw2022.html */cdr-coreldraw2021.html */cdr-coreldraw2020.html */cdr-coreldraw2019.html */cdr-coreldraw2018.html
IDA Pro	*/ida-ida.html

dnSpy	*/ida-dnspy.html
Winhex	*/ue-winhex.html
Typora	*/ue-typora.html
Notepad++	*/ue-notepad.html
Sublime	*/ue-sublime.html
Ultraedit	*/ue-ultraedit.html

这些样本的 PDB 路径中均包含字符串“APS”。

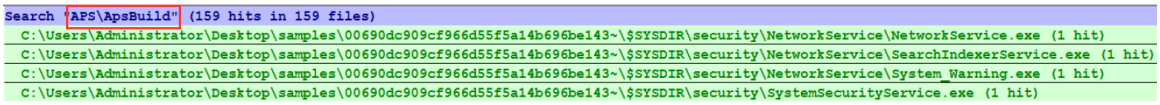

图 17 样本 PDB 中均包含 APS 字符串

2、攻击者正持续更新木马组件

根据样本中标注的版本号及编译时间可知攻击者正在持续更新木马组件。具体信息见下表：

文件名	文件中的版本号	MD5	编译时间
NetworkService.exe	1.1.3	AB4FB51F10548AF01AA8C0829BB723E5	2022-7-29 14:56:06
NetworkService.exe	1.1.2	D8C26A7680916D10406909B41EDC2DBB	2022-7-19 0:58:59
NetworkService.exe	1.1.1	218F439C13442E468BA48CA747CEF66A	2022-5-31 13:58:59

以上三个版本之间并无功能上的差异。通过对比代码结构发现，相比于 1.1.3 版本，1.1.1 和 1.1.2 版本的代码中多出大量无意义且未调用的函数。攻击者在 1.1.3 版本中进行了优化编译，可见攻击者还在持续更新恶意代码。

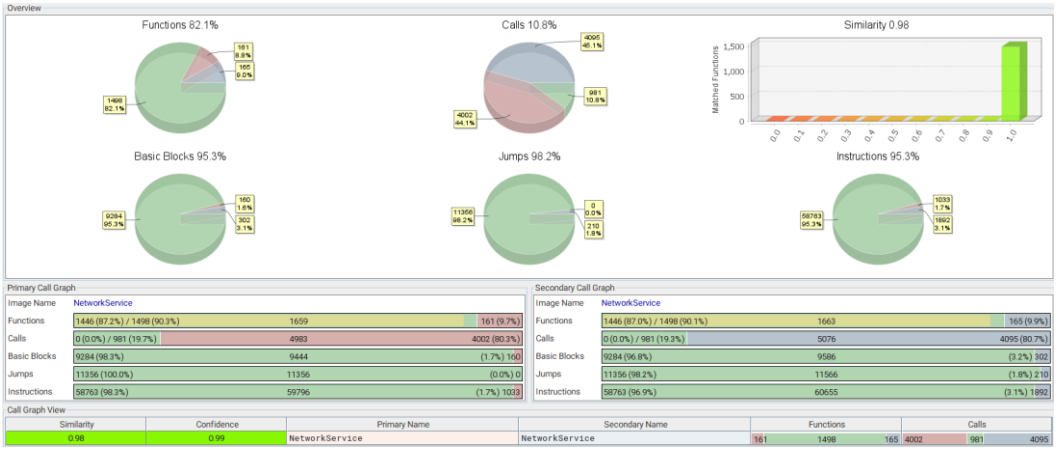

图 18 1.1.2 与 1.1.3 版本对比

三、 感染规模

通过监测分析发现，国内于 2022 年 8 月 3 日至 8 月 23 日期间“魔盗”木马日上线肉鸡数最高达到 1.3 万台，累计已有约 6.5 万台设备受其感染。每日境内上线肉鸡数情况如下。

图 19 每日上线境内肉鸡数

四、 防范建议

请广大网民强化风险意识，加强安全防范，避免不必要的经济损失，主要建议包括：

（1）建议通过官方网站统一采购、下载正版软件。如无官方网站建议使用可信来源进行下载，下载后使用反病毒软件进行扫描并校验文件 HASH。

（2）尽量不打开来历不明的网页链接，不要安装来源不明软件。

（3）加强口令强度，避免使用弱口令，密码设置要符合安全要求，并定期更换。建议使用 16 位或更长的密码，包括

大小写字母、数字和符号在内的组合，同时避免多个服务器使用相同口令。

（4）梳理已有资产列表，及时修复相关系统漏洞。

（5）安装终端防护软件，定期进行全盘杀毒。

（6）当发现主机感染僵尸木马程序后，立即核实主机受控情况和入侵途径，并对受害主机进行清理。

五、 相关 IOC

样本 MD5：

0F977A2D14F24D439FC9ABF7F64D7467

4BCE8BEAEE23770FA49A531DDC42B6CB

DF8F84A5945A218FC494EA25DFB9E730

FABD47AFE7F4E011B5EBD0483C3878D4

19B7EF53432711FA35DF87DFC66779D0

1A144C2394520B16759A4C51C81368E4

A8A626491FDBA630D6C658B1EBBEDF4F

F5D028CAB607319F4BC98CB510E7A642

41522ABC967179AC3E1676C753669F7B

FA36A03682CD077C5C2E2BCB2BD5A4E8

7F0D12C4DD857D1DB8CD641597B1C9D1

4E5C08A01A2BB06EC26A9E54F40400D0

F247621EC45BB5D60A9166C0714058C8

14F02744FEF4AE98BDFF3173185659C0

CD70268ABEE2F2AFC846E9F1BE6D8AD0

B0CDD87C55F266DA7A96AFF914D4208A

F7B7020BF8C2C41720F95F3E09D2C340

59AFEFD4B424A0F27BDEA2EB9E9B3A02

30FBF5D3AF8B2AC7E2490194FA09E55F

DE577D15094E118FB816C13E5C93F76A

6781BFC2B6EFD6FBA59C8862A8AFFD07

C9BF6DB9A46C7450827C714C3EF44066

81DEA5C46E6D67963EA0A3FD2C510563

AE3DD4E31226CC096284921E6F7E26D3

8E2894DADEAA52CD5B55DC03130CCF4D

00690DC909CF966D55F5A14B696BE143

B25E7347C9854E4B408864041D836997

F84AAA3A4A39730994962FFC53F1AECE

3EC9FC9A9D52E1EC78BBA6A4594A86A3

86AF77B5EC9B51F47651611991BBFA9A

45C32D08F20235E11F29DB3082C3AAB7

AB4FB51F10548AF01AA8C0829BB723E5

2F781CDD905FEA6C93A2929B02A7F4F9

218F439C13442E468BA48CA747CEF66A

9988BF5FF1D0DFDC83B0F880310ACFC9

62A5FC2BE6DBA690147CEA052C990276

95387C242C72CCA0E16811B40D46D764

1B5615E90735BE851FDFC556EA2CAE26

652835C8ECFD722950D0F5D8509EA1C2

0CE3A923F6263D877946FFBEB4666DE7

6ED3E57FDBEF38530385248D2ED7E96B

B719599A81D382983DCA526111F2A9D0

E9E3631A3374D7C5E78E6CC769D6326D

F7CDC25E606FF80B0F72CE6323827374

83AE694E25EDE2896A6ABCBB093F8D40

B307431E8122867D00E00FC669932017

IP：

8[.]218.94.162

DOMAIN：

cdr[.]jyxwlkj.cn

cdrnb[.]jyxwlkj.cn

api2[.]uptocycle.com

URL：

hxxp://cdr.jyxwlkj.cn/ida-ida.html

hxxp://cdr.jyxwlkj.cn/download1/ida.zip

hxxp://cdr.jyxwlkj.cn/ida-dnspy.html

hxxp://cdr.jyxwlkj.cn/download1/dnspy.zip

hxxp://cdr.jyxwlkj.cn/cdr-coreldraw.html

hxxp://cdr.jyxwlkj.cn/download1/coreldraw.zip

hxxp://cdr.jyxwlkj.cn/cdr-zhuanhuanqi.html

hxxp://cdr.jyxwlkj.cn/download1/cdr 转换器.zip

hxxp://cdr.jyxwlkj.cn/cdr-banbenzhuanhuanqi.html

hxxp://cdr.jyxwlkj.cn/download1/cdr 版本转换器.zip

hxxp://cdr.jyxwlkj.cn/cdr-cdrzitichajian.html

hxxp://cdr.jyxwlkj.cn/download1/cdr 字体插件.zip

hxxp://cdr.jyxwlkj.cn/cdr-sucai.html

hxxp://cdr.jyxwlkj.cn/download1/cdr 全套素材.zip

hxxp://cdr.jyxwlkj.cn/cdr-cdryansetianchong.html

hxxp://cdr.jyxwlkj.cn/download1/cdr 颜色填充插件.zip

hxxp://cdr.jyxwlkj.cn/cdr-barcode.html

hxxp://cdr.jyxwlkj.cn/download1/barcode.zip

hxxp://cdr.jyxwlkj.cn/cdr-coreldraw2022.html

hxxp://cdr.jyxwlkj.cn/download1/coreldraw2022.zip

hxxp://cdr.jyxwlkj.cn/cdr-coreldraw2021.html

hxxp://cdr.jyxwlkj.cn/download1/coreldraw2021.zip

hxxp://cdr.jyxwlkj.cn/cdr-coreldraw2020.html

hxxp://cdr.jyxwlkj.cn/download1/coreldraw2020.zip

hxxp://cdr.jyxwlkj.cn/cdr-coreldraw2019.html

hxxp://cdr.jyxwlkj.cn/download1/coreldraw2019.zip

hxxp://cdr.jyxwlkj.cn/cdr-coreldraw2018.html

hxxp://cdr.jyxwlkj.cn/download1/coreldraw2018.zip

hxxp://cdr.jyxwlkj.cn/ue-winhex.html

hxxp://cdr.jyxwlkj.cn/download1/winhex.zip

hxxp://cdr.jyxwlkj.cn/ue-typora.html

hxxp://cdr.jyxwlkj.cn/download1/typora.zip

hxxp://cdr.jyxwlkj.cn/ue-notepad.html

hxxp://cdr.jyxwlkj.cn/download1/notepad.zip

hxxp://cdr.jyxwlkj.cn/ue-sublime.html

hxxp://cdr.jyxwlkj.cn/download1/sublime.zip

hxxp://cdr.jyxwlkj.cn/ue-ultraedit.html

hxxp://cdr.jyxwlkj.cn/download1/ultraedit.zip

hxxp://api2.uptocycle.com/update/index.ini

hxxp://api2.uptocycle.com/update/DreamApslop.dll

hxxp://api2.uptocycle.com/aps.php/Isfreed/sanll

hxxp://api2.uptocycle.com/aps.php/udata/comp_info

hxxp://api2.uptocycle.com/aps.php/udata/user_info

hxxp://api2.uptocycle.com/aps.php/udata/install_info

hxxp://api2.uptocycle.com/aps.php/udata/pc_domain_info

hxxp://api2.uptocycle.com/aps.php/checkver/index

hxxp://api2.uptocycle.com/aps.php/window/info

hxxp://api2.uptocycle.com/aps.php/udata/browsing_history

hxxp://api2.uptocycle.com/aps.php/generic/process