

关于“银狐”木马“镜昙（G02）”团伙攻击态势深入分析报告

本报告由 CNCERT 与启明星辰信息技术集团股份有限公司共同发布。

一、事件概述

在“银狐”木马专项工作中，CNCERT 监测发现，银狐新团伙“镜昙”近期利用搜索引擎 SEO/仿冒软件下载站/其他渠道传播银狐木马。该团伙依托镜像文件投毒，且恶意程序可按预设时间自动终止，攻击呈现“昙花一现”的特征。相比银狐历史分支，镜昙完成多维度技术升级：改用 IMG/ISO/VHD 镜像载体规避静态检测、采用三重混淆加密保护木马配置、重构配置存储加载架构，并新增可定制的攻击失活时间机制，隐蔽性与可控性显著增强。

专项工作组围绕该团伙的域名、下载链、样本、C2 及通信行为开展关联分析，研判发现其具有载荷类型新、批量注册、模板复用、白加黑、持久化、反分析、攻击时间定制化等特征。2026 年 7 月 17 日至 10 月 20 日累计被控设备 5834 台，单日上线被控客户端最高 252 台，C2 日访问峰值为 727802 次。

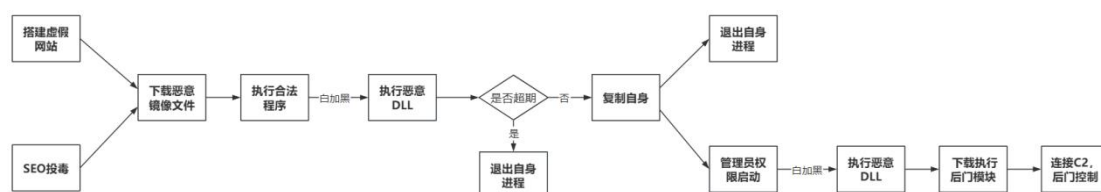


图 1 “镜昙”团伙攻击活动总体链路

二、团伙画像与活动特征

“镜昙” 银狐团伙是银狐攻击生态下独立运营的全新攻击分支，目标聚焦金融财务、银行、税务领域，攻击对象覆盖简体、繁体中文用户群体。该分支最早于 2026 年 7 月中下旬至 8 月开始活动，9 月进入集中爆发阶段，活跃时间窗口显著晚于银狐历史分支。

团伙代号“镜昙”来源于两大攻击特征：一是以镜像类文件作为初始攻击载体；二是攻击时间支持定制，到达设定日期后停止执行恶意行为，呈现“昙花一现”的攻击特点。相较于银狐既往攻击分支，镜昙分支在载荷模式、加解密特征、配置存储加载机制、攻击时间可控能力等方面完成全面技术迭代升级，核心差异与技术更新如下：

1) 恶意载荷投递方式全面革新：区别于银狐传统分支惯用的 MSI 安装包、NSIS/Inno Setup 封装 EXE 可执行文件的投递形式，镜昙分支团伙采用 IMG、ISO、VHD 镜像文件作为核心恶意载荷载体。攻击者借助合法第三方对象存储桶或搭建钓鱼页面诱导用户下载仿冒软件，利用镜像文件的特殊属性规避主流静态检测手段，大幅丰富攻击投递链路，提升载荷落地成功率。

2) 配置信息加密强度大幅提升：传统银狐木马仅对配置信息进行简单逆序处理后硬编码嵌入样本，对抗能力较弱。

镜昙分支团伙对配置混淆机制完成全面升级，采用逆序→加密→逆序三重混淆处理逻辑，极大提升了配置信息的隐藏效果，显著增加安全分析人员提取、解密、解析木马配置信息的难度。

3) 配置信息存储与加载模式重构优化：该分支团伙彻底摒弃银狐传统的硬编码配置存储方式，重构了配置存储与加载架构。攻击者将木马配置信息与 **shellcode** 代码合并后整体加密，独立存放于专属文件中，后续通过独立解密模块完成解密、执行 **shellcode**，再将有效配置参数传递至 **winos** 木马主体，以规避常规特征检测与静态 **IOC** 提取手段，提升攻击隐蔽性。

4) 新增攻击时间定制化可控机制：银狐既往分支的木马样本均无失活时间等限制条件，攻击生命周期不可控。而分支团伙新增精细化时间对抗机制，在木马配置模块中内置专属失活时间，可自主控制恶意程序的有效存活与攻击周期，既提升了攻击者对整体攻击活动的可控性，也进一步规避长期驻留带来的溯源与检测风险，强化整体对抗能力。

(一) 团伙概况

项目	内容
团伙名称	“镜昙”团伙
最早可追溯时间	2026 年 7 月下旬（2026.7.22 日）
主要攻击目标	中文背景用户（简体/繁体并存）；行业聚焦金融财务/银行/税务方向
主要传播渠道	搜索引擎检索引流+仿冒软件下载站、第三方对象存储桶资源直链下发镜像（仿冒企业办公软件/税务/银行对账等）
主要恶意功能	远控与信息窃取

当前活跃情况	持续活跃中：截至分析时间（2026.10.14）部分钓鱼页面仍可访问下载，最新下载样本远控配置 CC 持续有效；
--------	--

（二）传播资源与基础设施特征

观察维度	统计结果	主要特征
域名与注册	自有 C2 / 中转域名池 28 个（19 个 .club + 9 个 .cc）	后缀集中于 .club、.cc；该批域名呈 字母+数字 或纯字母 规律命名（acms555、taku788、moik77a、qzqy688 fshsjlk、hscdmnz、Hdfn xzn、hxnxcn），疑批量注册。注册商均为 为 22net, Inc. 是一家位于中国的 ICANN 认证域名注册商，总部在杭州
解析与托管	钓鱼侧承载 IP 64.81.30.137 单点承载 16 个域；C2 侧非标端口直连 IP	钓鱼侧域名多为“tax”前缀，仿冒税务相关软件/文档（tax-documentsXX、company-tool）；网站通过“企业软件安全下载中心”标题仿冒企业安全软件
下载基础设施	阿里云 OSS 6 bucket（东京 / 雅加达 / 香港）+ 腾讯云 COS 6 bucket（新加坡 / 香港 / 雅加达）+ AWS S3（yingxiang.s3.ap-northeast-1.amazonaws.com）	三家云厂商分池托管；载荷名 setup.exe、<随机>.exe、DMRootCA.zip、202609013823.img

三、典型攻击活动分析

（一）传播入口

攻击者通过发送钓鱼链接或钓鱼跳转诱导用户访问钓鱼网站下载恶意文件。攻击者注册钓鱼域名，搭建名为“星河科技软件下载中心”的银狐仿冒网站，提供伪装的“企业官方软件安装包”下载功能。攻击者实施 SEO 污染与钓鱼投递，以此确保必应搜索“星河科技软件下载中心”，搜索页面排名靠前的搜索结果大多为银狐组织仿冒网站，搜索结果如下图所示。推测其可能在发送信息中使用跳转页面、下载

提示或话术中使用“星河科技软件下载中心”等字样，以使部分用户查找、访问钓鱼网站。



图 2 传播入口或仿冒页面

打开后页面如下图所示，页面以“安全、稳定、快速的软件分发中心”为话术，落地页标题统一为“星河科技软件下载中心”。

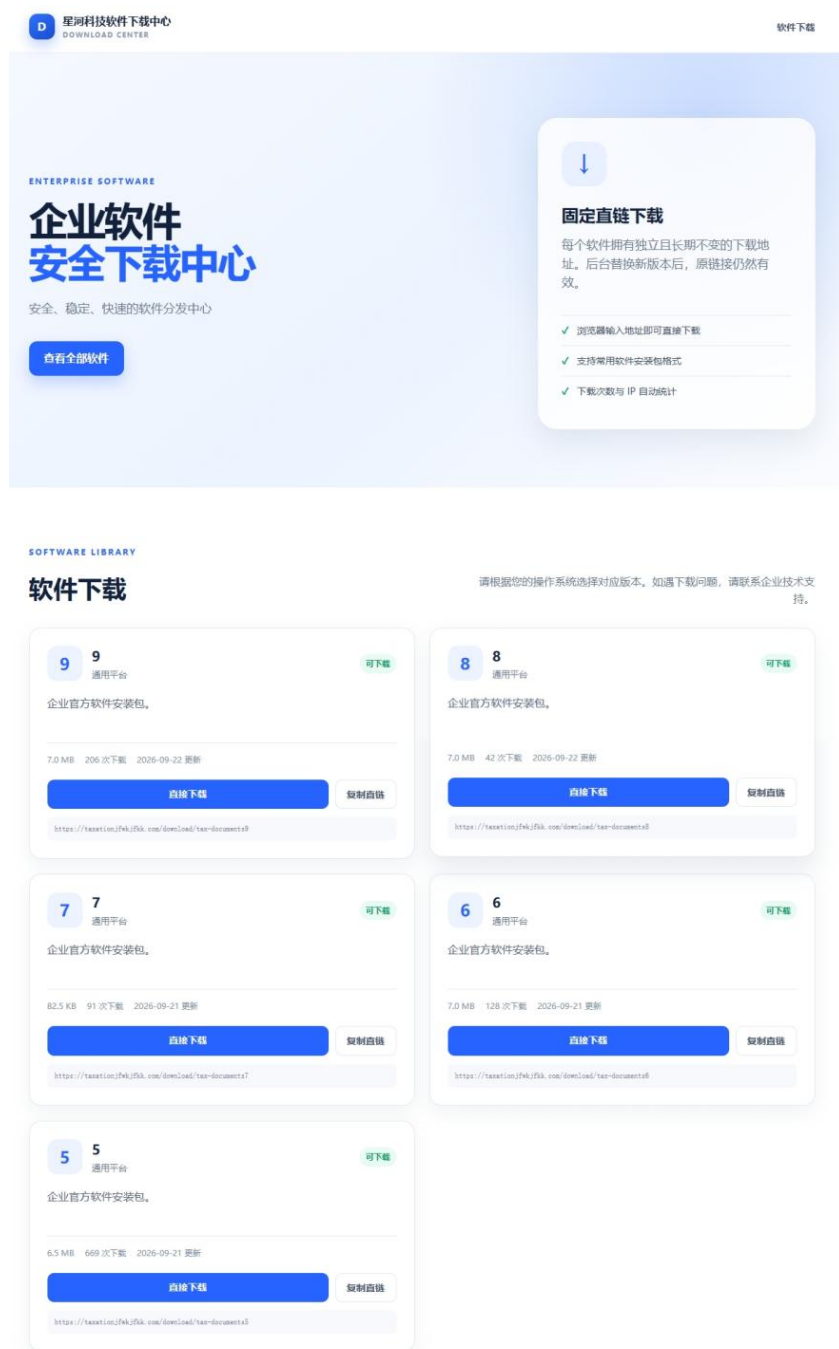


图 3 仿冒钓鱼页面

（二）跳转与下载链接

钓鱼页面包含多个下载链接，分别对应恶意文件的不同版本（如链接格式为 <https://taxationjfwk.com/download/tax-documentsXX>，XX 为数字后缀）；攻击者只需修改该数字后缀，即可实现恶意文件的版本更新。点击即可下载诱

饵文件，这些诱饵文件采用税务文件、对账单据、采购订单、逾期账户对账单等财税业务主题构建或直接以时间命名，如“tax-documents1.zip”、“Reconcile an account.zip”、“Statement of Outstanding Account.zip”、“Bank Statement.zip”等。下载的 ZIP 文件解压即得到恶意 IMG/ISO/VHD 文件，以此规避杀毒软件对 EXE 等常用格式文件的静态检测。

环节	URL/域名	作用	核验时间
入口	taxationjfwk.com（解析 ip:64.81.30.137）	仿冒网站	2026.9.12
跳转	https://taxationjfwk.com/download/tax-documentsXX	下载链接（XX 为数字，支持通过数字进行更新及多个版本链接下载）	2026.9.12
下载	https://taxationjfwk.com/download/tax-documents42	当前分析文件下载链接	2026.9.12
最新链接	https://taxationjfwkjfkk.com/download/tax-documents9	同 ip 解析的域名对应的最新链接；持续更新生成不同批次的仿冒链接。	2026.9.23

（三）样本落地与执行

以样本 1886e9fb95c4b1a62ae192e688f583f9d4c444f02082a7768041603517f52f52 为例，该样本为 IMG 文件，其中包含名为“AMD.0903002123.EXE”的合法程序和名为“xwEB_eLF.dll”的恶意 DLL 文件，用户执行“AMD.0903002123.exe”时，以白加黑方式启动“xwEB_eLF.dll”。该恶意 DLL 首先解密配置信息，检测当前的系统时间是否晚于有效期限。如果已超期，则弹出提示框并退出进程；否则执行后

续恶意功能。在“%public%”下创建名为“NVTELEMETRY”的文件夹及随机名称的子文件夹，并将上述合法程序复制为“NvTelemetryBridge64.exe”，复制恶意 DLL 文件，然后创建新进程，执行该合法程序。

新进程启动后，以白加黑方式启动恶意模块“xwEB_eLF.dll”，执行恶意行为。



图 4 样本执行链

（四）远程控制与恶意功能

恶意 DLL 模块启动后，解密出配置信息并解析各个字段，向 C2（acms555.club）发起连接，下载执行具有后门功能的“登录模块”。该后门具备文件管理、键盘记录、插件动态加载、系统重启/关机等多种控制能力。

Source	Destination	Protocol	Leng	Info
192.168.64.131	192.168.64.2	DNS	72	Standard query 0xf63b A acms555.club
192.168.64.2	192.168.64.131	DNS	88	Standard query response 0xf63b A acms555.club A 192.252.178.137

图 5 通信或恶意功能证据

四、典型恶意样本分析

如下为该团伙使用恶意样本的分析结果，该样本详细信息如下表所示。

样本标签	内容
SHA-256	1886e9fb95c4b1a62ae192e688f583f9d4c444f02082a7768041603517f52f52
文件名称	AMD.0903002123.img
文件大小	9.98 MB (10469376 bytes)
文件类型	IMG 镜像文件
数字签名	无
编译/时间特征	2026.09.03

投递来源	钓鱼网站
主要功能	银狐木马的上线模块（即下载器）

（一）初始载荷与解密加载

前置攻击载荷通过钓鱼网站诱骗用户下载相关仿冒软件类的恶意文件。下载关键词多与税务、财务、企业办公相关。

关键词	攻击指向
tax-documents	税务
Reconcile an account、Statement of Outstanding Account、Bank Statement	银行对账/财务
Purchase Order	企业采购
company-XX、软件下载	企业/办公软件

本次分析中下载的母体压缩包文件名为 “tax-documentsXX” (XX 为数字)，内嵌文件为主体分析文件：“AMD.0903002123.img”



图 6 初始载荷

该 IMG 文件中包含白文件 “AMD.0903002123.exe” 和恶意文件 “xwEB_eLF.dlI”，通过白加黑方式启动该恶意文件。如下图所示：

Name	Date modified	Type	Size
AMD.0903002123.EXE	9/3/2026 4:56 PM	Application	2,203 KB
xwEB_eLF.dlI	9/3/2026 4:56 PM	Application extens...	7,395 KB

图 7 内嵌文件载荷

恶意文件 “xwEB_eLF.dlI” 中硬编码了经过加密的配置

信息，如下图所示：

```
.data:000000001804BB0F0 a38ca425b61f957: ; DATA XREF: sub_18001D090+1Df0
.data:000000001804BB0F0 text "UTF-16LE", '38CA425B61F95775D1D923B1DFC220B828C73BA7EB65A384640'
.data:000000001804BB0F0 text "UTF-16LE", 'D8466A9270BA3E6497989C458F827038E540A382529FE0CD4D6'
.data:000000001804BB0F0 text "UTF-16LE", '109471CB4194134D72C15A00E0E88605625E841DE7F534BC56F'
.data:000000001804BB0F0 text "UTF-16LE", 'CA670CDC19802849B73B9E0764C79F83A6362891694D65FB05A'
.data:000000001804BB0F0 text "UTF-16LE", '0606C262C19BBC922FC20151DE631CA1421A02A3AC5ADB9A63E'
.data:000000001804BB0F0 text "UTF-16LE", '59BE68EE06A6FAA5456A7F30995BA6EAAE625BB1E497327E922'
.data:000000001804BB0F0 text "UTF-16LE", 'FAFC10FA4043B2F46312924FD8E8204CA6EBF4C7D78F079F508'
.data:000000001804BB0F0 text "UTF-16LE", '8A0A9AA9E8A3A845872E0CD92A07E723E91069530900BB7B1C1'
.data:000000001804BB0F0 text "UTF-16LE", '6F8A62E42F46CA0',0
```

图 8 加密的配置信息

该 DLL 启动后，首先将该配置信息进行逆序+rc4 解密+逆序处理，以得到明文。如下图所示：

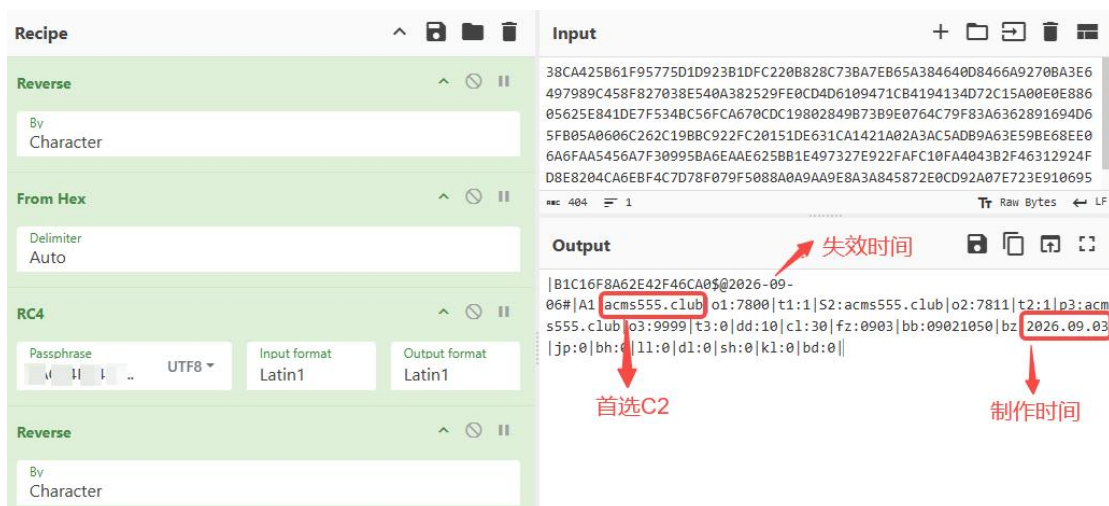


图 9 配置信息解密过程

从明文配置信息可知，C2 为“acms555.club”，该恶意指程序的制作时间为 2026.09.03，失效时间为 2026.09.06。

判断当前系统时间是否晚于失效时间，如果是，则弹出提示框并退出当前进程。如下图所示：

```
if ( *v126 > v127 && *v126 - v127 > 864000000000i64 )// 比失效时间晚1天
{
    MessageBoxW(0i64, &word_1803A8D38, &word_1803A8D2C, 0x10u);// 弹出超期提示框
    ExitProcess(0); // 退出进程
}
```

图 10 检测是否在有效期内

弹出的超期提示框如下图所示，如果在有效时间内，继续执行后续恶意功能。

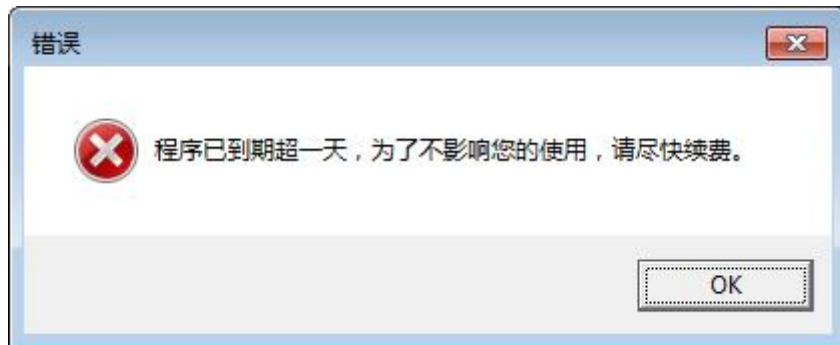


图 11 超期提示框

按照各字段解析配置信息，如下图所示：

```
memset_18037F660(&stru_1804CB270, 0, 0x12A0ui64);
sub_18001D5D0(Data, L"A1:", &unk_1804CB28E, 0i64);// 解析首选C2的域名/IP
sub_18001D5D0(Data, L"o1:", &unk_1804CB48C, 0i64);// 解析首选C2的端口
sub_18001D5D0(Data, L"t1:", 0i64, &dword_1804CB4C8);// 解析与首选C2通信采用的协议
sub_18001D5D0(Data, L"S2:", &unk_1804CB4CC, 0i64);// 解析第二个C2的域名/IP
sub_18001D5D0(Data, L"o2:", &unk_1804CB6CA, 0i64);// 解析第二个C2的端口
sub_18001D5D0(Data, L"t2:", 0i64, &dword_1804CB708);// 解析与第二个C2通信采用的协议
sub_18001D5D0(Data, L"p3:", &unk_1804CB70C, 0i64);// 解析第三个C2的域名/IP
sub_18001D5D0(Data, L"o3:", &unk_1804CB90A, 0i64);// 解析第三个C2的端口
sub_18001D5D0(Data, L"t3:", 0i64, &dword_1804CB948);// 解析与第三个C2通信采用的协议
sub_18001D5D0(Data, L"fz:", &unk_1804CB9C4, 0i64);// 解析分组信息
sub_18001D5D0(Data, L"bb:", &unk_1804CBA28, 0i64);// 解析版本信息
sub_18001D5D0(Data, L"bz:", &unk_1804CBA8C, 0i64);// 解析编译制作时间
```

图 12 解析配置各字段

如果当前进程文件路径不包含“%public%\NVTELEMETRY”，在“%public%”下创建名为“NVTELEMETRY”的文件夹，在该文件夹中创建一个“【32 个随机数字】.【3 个随机字母】”命名的子文件夹，将“AMD.0903002123.EXE”复制为该子文件夹下的“NvTelemetryBridge64.exe”，将“xwEB_eLF.dll”复制为“xwEB_eLF.dll”，如下图所示：

```

sub_180008840(v189, 260i64, L"%sLibraries\\NVTELEMETRY\\%s", v110, v157);
sub_18002D180(L"%s\n", v189);
memset_18037F660(v193, 0, 0x208ui64);
sub_180008840(v193, 260i64, L"%s\\%s", v189, v44);
memset_18037F660(v194, 0, 0x208ui64);
sub_180008840(v194, 260i64, L"%s\\xwEB_eLF.dll", v189);
memset_18037F660(v192, 0, 0x208ui64);
__asm { rcr dx, 0Dh }
GetModuleFileNameW(0i64, v192, 0x104u);
v124 = sub_1802F86F4(v192, 92i64);
v116 = 0i64;
if ( v124 )
    *(v124 + 2) = 0;
lstrcatW(v192, L"XWEB_ELF.DLL");
if ( CopyFileW(v190, v193, 0) && CopyFileW(v192, v194, 0) )// 复制文件

```

图 13 复制载荷文件

复制完成的文件如下图所示：

Name	Date modified	Type	Size
NvTelemetryBridge64.EXE	9/3/2026 4:56 PM	Application	2,203 KB
xwEB_eLF.dll	9/3/2026 4:56 PM	Application extens...	7,395 KB

图 14 复制完成图

以管理员权限执行合法程序“NvTelemetryBridge64.exe”，退出当前进程。如下图所示：

```

hNtdll = GetModuleHandleW(L"ntdll.dll");
if ( !hNtdll
    || (RtlGetVersion = GetProcAddress(hNtdll, "RtlGetVersion")) == 0i64
    || (osv.dwOSVersionInfoSize = 0x11C, memset_18037F660(&osv.dwMajorVersion, 0, 0x118ui64), (RtlGetVersion)(&osv)
    || osv.dwMajorVersion < 0xA // Windows 10以前版本
    || !sub_180508000(v194) )
{
    pExecInfo.cbSize = 0x70;
    *(&pExecInfo.lpVerb + 4) = 0i64;
    *(&pExecInfo.lpParameters + 4) = 0i64;
    *(&pExecInfo.nShow + 1) = 0i64;
    *(&pExecInfo.lpIDList + 4) = 0i64;
    *(&pExecInfo.hkeyClass + 4) = 0i64;
    *(&pExecInfo.hMonitor + 4) = 0i64;
    HIDWORD(pExecInfo.hProcess) = 0;
    pExecInfo.fMask = SEE_MASK_NOCLOSEPROCESS;
    pExecInfo.lpVerb = L"runas"; // 管理员权限
    pExecInfo.lpFile = v192;
    pExecInfo.hwnd = 0i64;
    pExecInfo.nShow = 1;
    ShellExecuteExW(&pExecInfo); // 以管理员权限执行NvTelemetryBridge64.exe
}
ExitProcess(0); // 退出当前进程

```

图 15 载荷执行过程图

新进程 “NvTelemetryBridge64.exe” 执行后，以白加黑方式启动恶意模块 “xwEB_eLF.dll”。

解密出配置信息并解析各字段，向 C2 发起网络连接，发送随机生成的密钥，发送数据的格式如下表所示：

偏移（字节）	长度（字节）	含义
0	4	数据总长度
4	10	原始密钥，与 0x36 相加后作为真正异或密钥
14	不固定	有效通信数据

对 C2 回复的数据进行验证，通过验证后，请求下一阶段的载荷并执行，即 winos 木马的“登录模块”，主要功能是远程后门，如下图所示：

```
qmemcpy(v13, "{vU_!jWW", 8); // "登录模块.dll_bin"
v13[2] = 'd\0.';
v13[3] = 'l\0l';
v13[4] = 'b\0_';
v13[5] = 'n\0i';
v14 = 0;
memset_18037F660(v15, 0, 0x1E6ui64);
```

图 16 构造请求数据

（二）持久化与规避检测

- 1) 注册表存储：远控模块将插件数据存放于“HKCU\Console\0”（32 位）或“HKCU\Console\1”（64 位），减少磁盘取证痕迹；
- 2) VMP 加壳：核心 DLL 经 VMProtect 加壳保护，增加逆向分析难度；
- 3) 配置加密处理：C2 配置字符串以逆序+rc4 加密+逆序的方式存储在样本中，运行时解密，规避静态字符串匹配。

（三）通信协议与配置特征

配置特征：配置经解密后，包括 C2、端口、协议、版本、编译制作时间、失效时间等信息。

各字段及含义见下表：

字段名	含义
\$@	样本失效时间
A1 / S2 / p3	首选 / 第二 / 第三 C2 域名或 IP
o1 / o2 / o3	对应 C2 端口
t1 / t2 / t3	对应 C2 通信协议
dd	执行延迟
cl	通信间隔
fz	分组标识
bb	版本号
bz	编译制作时间
jp	键盘记录器开关
bh	结束蓝屏开关
ll	反流量监控开关
dl	入口点
sh	创建守护进程
kl	进程镂空
字段名	含义

通信协议特征：上线模块采用 TCP 协议与 C2 建立连接，发送数据结构为“4 字节总长度 + 10 字节密钥（与 0x36 异或） + 有效载荷”。C2 返回数据为下一阶段的恶意模块。

网络流量如下图所示：

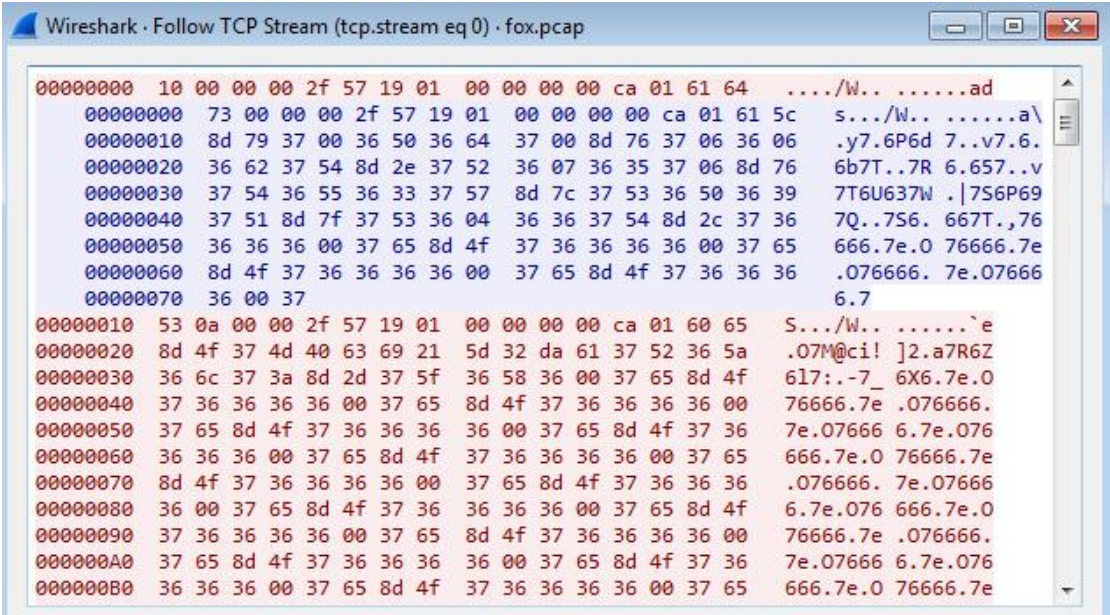


图 17 网络流量图

向 C2 发送的请求数据解密前后如下图所示，可知请求内容为“登录模块.dll.bin”。登录模块执行后，可以下载其它插件或远控软件，执行更多恶意功能。

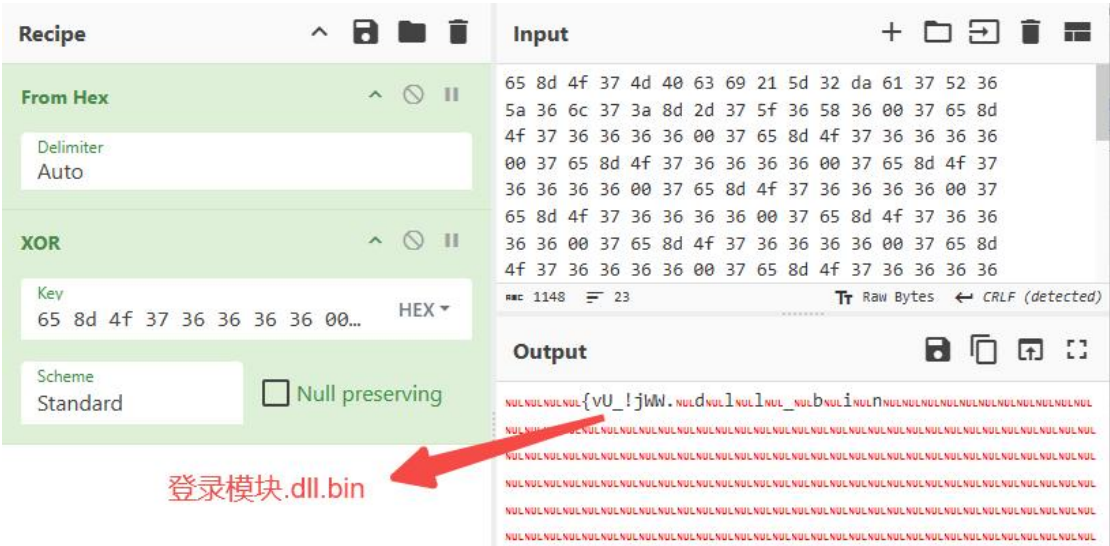


图 18 通信数据解密图

五、团伙关联与同源性分析

团伙分析结果如下表所示。

证据	本次活动特征	历史团伙特征	一	专属性/局限
----	--------	--------	---	--------

类别			致性	
初始 载荷	IMG/ISO/VHD 镜像类文件	MSI 安装包、N SIS/Inno Setup 等封装的 EXE 可执行文件	低	本分支团伙的专属特 征：使用镜像类新型 载荷模式攻击
样本 代码 与加 密	三层配置解密	直接硬编码在 文件中	中	配置加密存储，同时 基于关联也发现有部 分攻击将配置部分及 shellcode 单独放置在 独立文件中进行加载 的情况，这是本次攻 击的专属特征，增强 了检测对抗能力
配置 及通 信协 议	XXXXXXXXXXXXXXXXX XXX\$@YYYY-MM-DD# A 1:X.X.X.X o1:XX t1:1 S 2:X.X.X.X o2:XX t2:1 p 3:X.X.X.X o3:XX t3:0 d d:10 cl:30 fz:XX bb:YYD DNNNN bz:YYYY.MM.DD jp:0 bh:0 ll:0 dl:0 sh:0 k l:0 bd:0	p1:X.X.X.X o1:XX t1:1 p 2:X.X.X.X o 2:XX t2:1 p3: X.X.X.X o3: XX t3:0 dd:1 cl:1 fz:默认 b b:1.0 bz:YYY Y.MM.DD jp: 0 bh:0 ll:0 d l:0 sh:0 kl:0 bd:0	高	三组 C2 字段 A1/o 1/t1...、内置 bz 时 间、功能开关位；非 标端口 TCP 与以往 高度重合部分，但也 具备自身专属特征： 针对有效攻击的失效 时间做了限定，保证 攻击时间可控
失活 机制 判断	内置在配置中的失效时间， 当程序判断当前时间高于失 效时间会弹窗迷惑用户同时 不再执行后续核心行为	无相关判断机 制	低	本分支团伙专属特征
C2 与历 史解 析	多个 tax 前缀系列域名（taxa tionjfwkjfkf.com, www.taxa tionjfwkjfkf.com, taxationjfwk jfkf.com, www.taxationjfwkj f.com, taxationjfwkf.com, w ww.taxationjfwkj.com, taxati onjfwkj.com, www.taxationjfw wk.com, taxationjfwk.com, hz -bopen.com, www.taxationjfw wk.com, taxationjfw.com, www.tax ation01jf.com, www.amgttot t.com, taxation01jf.com, amgt tott.com），解析至同一 I P: 64.81.30.137;	存在同一 IP 域 名绑定多个域 名资产的情况	高	与银狐组织高度重合

钓鱼模板与下载链	仿冒软件下载站；“安全、稳定、快速的软件分发中心”；页面标题“星河科技软件下载中心”，关联多个域名钓鱼页面高度复用，属模板复用特征；关联也发现存在通过第三方对象存储载荷分发 URL 的攻击（如： https://fafafa-1330906210.com/ap-singapore.myqcloud.com/20260830215344-FD6BBE EACCF3.zip https://yingxiang.s3.ap-northeast-1.amazonaws.com/202609013823.img ）	利用搜索引擎 SEO/仿冒软件下载站为该组织常用入口手法	高	银狐常用手法
活动时间与目标	2026.7 月底开始出现,持续活跃中,目标为金融财务（简繁中文并存）	攻击窗口在此之前；攻击目标行业与银狐多个历史团伙重合	高	专属时间，目标一致

综合镜像型载荷类型、配置信息（含银狐固定的配置参数及本团伙专有的加解密特征及时间控制参数）、攻击目标（符合银狐组织特征）、流量特征等，专项工作组研判认为，本次攻击活动可确认为银狐“镜昙”团伙。

六、控制规模

指标	统计时段	数值
关联域名数	2026/07/17-2026/10/12	29
活跃 C2 数	2026/07/17-2026/10/12	25
日上线被控 IP 峰值	2026/07/17-2026/10/12	252
C2 日访问量峰值	2026/07/17-2026/10/12	727802
累计被控设备数	2026/07/17-2026/10/12	5834

通过监测分析发现 2026 年 7 月 17 日至 10 月 20 日累计控制规模 5834 台，其中，2026 年 8 月 20 日上线 252 台被控端。相关变化情况如下图所示。经银狐专项打击，近期该组

织控制规模整体明显下降。



图 19 每日上线被控 IP 数

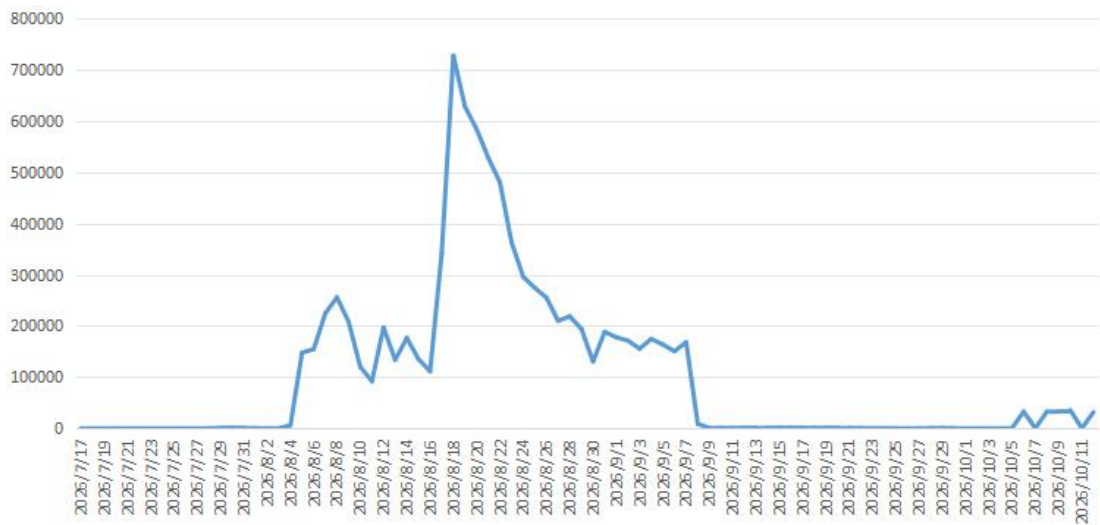


图 20 每日 C2 访问量

七、防范措施

针对银狐“镜昙”团伙的传播方式和样本行为，建议个人用户及有关单位采取以下防范措施：

- (1) 通过软件官方渠道或可信应用商店下载软件。该团伙利用 SEO 投毒与关键词竞价，使仿冒站点出现在搜索结果

前列。使用搜索引擎时，应核实下载来源，尤其注意标注“广告”“推广”的结果。请勿通过非正规渠道下载或安装软件，警惕仿冒网站及恶意跳转链接，务必认准官方渠道获取安装程序。

(2) 企业应面向全体员工开展专项安全意识培训，重点覆盖财务、业务对接、行政等岗位；同时，在邮件网关、网页代理、即时通信网关预置仿冒软件类钓鱼链接的拦截规则，从投递端阻断钓鱼下载路径。

(3) 对伪装注册表持久化及载荷目录落地建立告警。监测注册表键“HKCU\Console\0”（32 位）或“HKCU\Console\1”（64 位）的创建与写入，以及“C:\Users\Public\NVTELEMETRY”目录的生成行为，重点检查将 C:\Users\Public、C:\Users\Public\NVTELEMETRY 等大范围目录加入排除项的操作

(4) 定期检查终端自启动项、系统服务、运行进程及网络连接情况，妥善留存终端与边界网络日志，为后续影响范围认定、溯源分析和处置工作提供依据。

(5) 金融、银行、集团财务类单位应回溯近 3 个月的邮件附件、即时通信文件、网页下载全链路日志，逐笔排查是否存在点击下载、执行该团伙恶意载荷的行为，及时清除存量失陷节点。

(6) 在网络出口侧全量封堵本次披露的相关 IOC（C2

域名、IP、样本哈希)；同步在全网终端基于 IOC 特征开展全盘扫描，清除已落地的恶意样本。

八、相关 IOC

控制端 IP 地址

156[.]251[.]11[.]58	156[.]234[.]7[.]46:443
192[.]252[.]187[.]52	112[.]213[.]110[.]210:441
103[.]199[.]102[.]28:441	202[.]162[.]99[.]165:441
202[.]61[.]160[.]183:446	202[.]61[.]140[.]222:448

控制端域名

acms555[.]club	usdt888[.]club	hscdbjx[.]cc
acuf444[.]club	msms818[.]club	hcvsdcax1[.]cc
aeyh688[.]club	nipao817[.]club	bscscaxas2[.]cc
atyv788[.]club	weqt588[.]club	hxsajns1[.]cc
caiyun1[.]club	qzqy688[.]club	rezmv3s[.]club
geco249[.]club	fshsjlk[.]cc	geco249[.]club
hevk66b[.]club	hscdmnz[.]cc	oswin[.]club
juea802[.]club	hdfnxzn[.]cc	qztt688[.]club
moik77a[.]club	hxnxcn[.]cc	evubt8z[.]club
taku788[.]club	asiodjxxz[.]cc	

钓鱼网站

taxationjfwkjfk[.]com	taxationjfwkj[.]com
www[.]taxationjfwkjfk[.]com	smsqlcx[.]com
64[.]81[.]30[.]137	www[.]taxationjf[.]com
45[.]197[.]239[.]23	www[.]ycjjhx[.]com
www[.]taxationjfwkjf[.]com	www[.]amgttott[.]com
taxationjfwkjf[.]com	www[.]jfbcea[.]com
mpaceart[.]com	www[.]taxationjfwk[.]com
dsagstyopn[.]com	taxationjfwk[.]com
amgttott[.]com	taxationjf[.]com
www[.]taxation01jf[.]com	ltingzx[.]com
taxation01jf[.]com	hz-bopen[.]com
chinalookup[.]com	vansalonu[.]com
www[.]taxationjfwkj[.]com	

恶意样本下载地址

[https://fafafa-1330906210\[.\]cos\[.\]ap-](https://fafafa-1330906210[.]cos[.]ap-)

singapore[.]myqcloud[.]com/20260830215344-FD6BBEEACCF3[.]zip
https://yingxiang[.]s3[.]ap-northeast-1[.]amazonaws[.]com/202609013823[.]img
https://taxationjfwk[.]com/download/tax-documentsXX

第三方对象存储载荷域名

hxnamz.oss-ap-northeast-1[.]aliyuncs[.]com
hsdfnj8.oss-ap-northeast-1[.]aliyuncs[.]com
hjkdhfi.oss-ap-southeast-5[.]aliyuncs[.]com
jsdcnkjnasdn.oss-ap-southeast-5[.]aliyuncs[.]com
hjsdkcfjnk.oss-ap-southeast-5[.]aliyuncs[.]com
zhuohao2.oss-cn-hongkong[.]aliyuncs[.]com
yxz-1469461062.cos.ap-singapore[.]myqcloud[.]com
xzy-1469461515.cos.ap-singapore[.]myqcloud[.]com
xzy-1469463437.cos.ap-singapore[.]myqcloud[.]com
xiazai-1463565404.cos.ap-singapore[.]myqcloud[.]com
xz-1363546456.cos.ap-hongkong[.]myqcloud[.]com
abcdlouj20000-1487618693.cos.ap-jakarta[.]myqcloud[.]com
yingxiang.s3.ap-northeast-1[.]amazonaws[.]com

样本 SHA-256

1886e9fb95c4b1a62ae192e688f583f9d4c444f02082a7768041603517f52f52
ca93c311598960dedd81d7ab9d1a72bbece32403a956808270b17fa02a3f4bf
cb6ad72d122b7d7bb5b391403eb960b54ba3e6c6869f9998c103c3bccbddd96
3c253d2d70c27823e34b457f786443e40053bed57873f6cacca10ca331462acf
6eea260ad32653938205496fdb8fc4e50a0fd05bf70d9aed44b6492987640c1e
2f4793b471255e32636b30f94b4349cda4957e178fc9349966120339103d4d4c
d497d45f9a43cc6c73528e158706b3cd8a94a9f4c3f89b4b4ba248dc93babff0
7078c4b11e8f45107c5e04b1ea4476b95c9b85c470a3e14ff8b2539b7b7567
473d617f4e89c0c31ee5e66a4477867b000bcfaacf4b68e0df77f048db54145e
45be73ea603f80127d15e1f64fd08ddef545c1ac160bc5d88c79ef104e5969d2
5457fd9a14d28a902b672d33340711fdc281ce32e0957e79643bcddffeabf235
bb3ce0f1113ddecf3f2daf58798ffb8a3b2894209db83624ae965722e70dda67
cb04a85a2683872a9d46065320438db1314759a0a8dd923119f08af54e8f8de7
5a91497a93d0c0d6befcef7c9b66fb4c90896bdb28559ba9b041658305e4716d
c477605cf3cb21b07312d2a344a57c8d09e9ca21213b47445f359bbe08b30289
2012d9b8d03a4350c9c4bad6997eb74b3ebb278fla2dec4f847091ef22b4757
bc6da4483a9d7f4c2f10270e5d10f86f4da8414a8a12af0c1cb840c1b7da0a69
40b628b6c2da5be954af8079994082c5185928a7651e7d1794fb9855438d0bcb
e727a1645f8075cc6146f1a9f935a2152f8300a84af4da0c40fb2b9d07cb597b