关于“银狐”木马“甲蚁（G01）”团伙攻击态势深入分析报告

本报告由 CNCERT 与天融信科技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 联合天融信科技集团股份有限公司共同监测发现，“甲蚁（G01）”团伙近期通过搜索引擎 SEO 投毒与关键词竞价引流，利用 AI 批量复刻高仿真软件下载站传播银狐木马。经专项工作组对该团伙攻击资源与传播控制方式开展关联分析发现：其抢先实名注册“.com.cn\.cn”后缀域名并按统一模板批量命名，仿冒“SafeW”“FinalShell”“NexusDesk”等常用工具软件的官方下载入口，恶意载荷统一托管于云对象存储服务；用户被诱导下载并运行恶意 MSI 安装包与多阶段下载加载器后，样本在显示正常软件安装界面的同时，于后台以“白加黑”侧加载方式分阶段加载后续程序，写入 Windows Defender 排除项、实施进程注入、注册计划任务，并篡改 hosts 阻断安全软件站点访问，随后连接境外 C2 服务器，建立远程控制通道。

专项工作组已核验仿冒域名 1060 个，单日注册峰值 110 个，活跃 C2 地址 2 个。2026 年 9 月 15 日至 22 日，CNCERT 监测发现该团伙共控制境内肉鸡达 8708 个。其中，单日上线

数量峰值 2361 个。此次攻击活动威胁使用开发运维类工具的个人及企业用户，此类用户因工作需要，普遍持有高价值主机权限，其终端一旦被控，攻击者可利用这些权限进一步横向移动，扩大影响范围。

图 1 “甲蚁（G01）”团伙攻击活动总体链路

二、团伙画像与活动特征

该团伙使用单一控制邮箱批量注册数百个域名，借用他人实名信息完成“.com.cn”域名注册，再利用 AI 批量复刻多个品牌官网。各仿冒站点通过统一后台提供恶意载荷，同名压缩包按次打包，哈希值各不相同。站群托管于价格低廉、溯源困难的境外服务，第三方流量统计平台（51.LA）则用于核算投入产出比、调整仿冒主题。其仿冒对象已从大众软件转向开发运维类工具，此类目标用户持有的主机权限具有更高价值。

（一）团伙概况

表 1 “甲蚁（G01）”团伙概况

团伙名称	“甲蚁（G01）”团伙
最早可追溯时间	2026 年 7 月 9 日（现有批次中最早的域名注册时间）

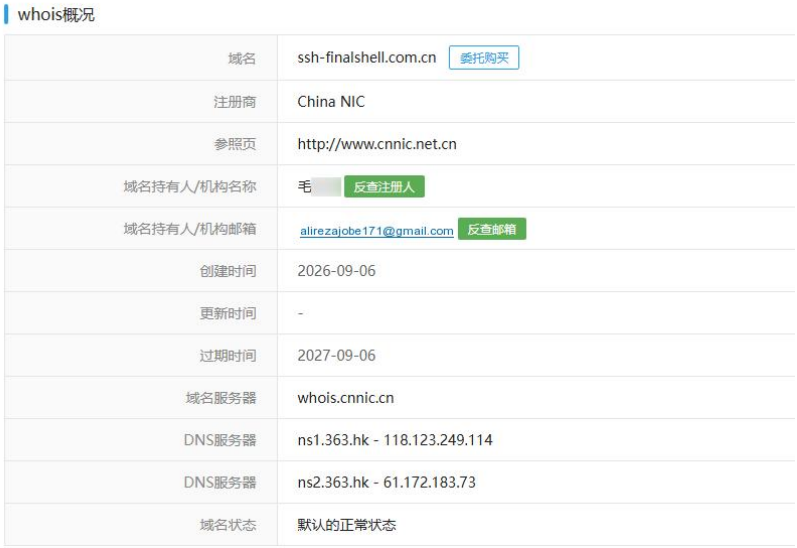
主要攻击目标	使用开发运维类工具（FinalShell、NexusDesk、Xshell、SecureCRT 等）与即时通信类工具（SafeW 等）的个人及企业用户；运维与开发人员为高价值目标
主要传播渠道	搜索引擎 SEO 投毒与关键词竞价引流；AI 批量复刻的高仿真仿冒软件下载站；多层跳转至云对象存储下载
主要恶意功能	多阶段下载与内存加载、白加黑侧加载、进程内存写入、Windows Defender 排除项写入、计划任务持久化、hosts 篡改阻断安全软件、远程控制与双向数据交换
当前活跃情况	活跃。域名注册持续至 2026 年 9 月 9 日。

（二）传播资源与基础设施特征

表 2 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	1060 个	共 1060 个，其中".com.cn”域名 1042 个，占 98.3%;".cn”域名 18 个； 命名模板复用，an-（298）、app-（205）、ah-（203）、ai-（33）、am-（24）等固定前缀，合计占比超 70%; 模式为“字母前缀-品牌关键词.com.cn”与“品牌关键词-功能后缀.com.cn”，并大量采用字母重复、缺字、错拼； 注册周期统一为一年；单日最多注册域名 110 个
解析与托管	集中承载，同一个 IP 多个域名	绝大多数托管于 Cogent 服务商香港节点，带宽廉价、滥用投诉处置缓慢且无需备案；同 IP 反查可见多个仿冒域集中挂靠，形成稳定的批量承载基础设施
下载基础设施	4 个对象存储桶 1 个中转域名	阿里云 OSS（北京、杭州、香港三地域）托管恶意载荷；download.hzx[.]me 承担中转跳转；同一入口多次下载得到同名不同哈希的压缩包，载荷由服务端按次打包
C2 基础设施	2 个	14.128.53[.]194:80 （关联程序 xwizard.exe）； 47.243.152[.]51:18300 （关联程序 VBV4HZ.exe）
证书及其他	签名 2 类 统计服务 1 类	伪造署名“Bytedance Pte. Ltd.”的数字签名； 滥用有效签名 “Speech Processing Solutions GmbH”程序实施白加黑侧加载； 使用 51.LA 等免费流量统计服务，按不同统计 ID 区分仿冒应用并据此核算投资回报率

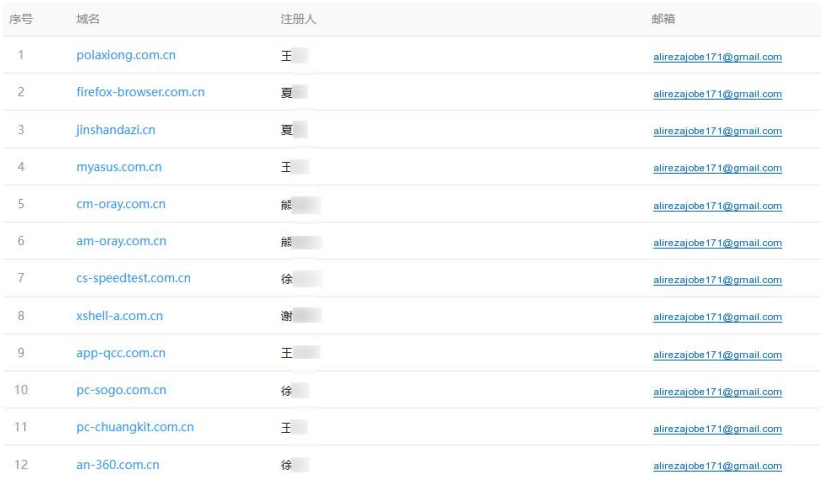
域名注册信息显示，注册人姓名和身份证号对应真实公民，控制邮箱则为境外免费邮箱。反查发现，同一控制邮箱关联多个注册人姓名，并轮换使用。这表明攻击者批量借用他人身份注册域名，注册信息中暴露的是无关公民的身份。



whois概况

域名	ssh-finalshell.com.cn 委托购买
注册商	China NIC
参照页	http://www.cnnic.net.cn
域名持有人/机构名称	毛 反查注册人
域名持有人/机构邮箱	alirezajobe171@gmail.com 反查邮箱
创建时间	2026-09-06
更新时间	-
过期时间	2027-09-06
域名服务器	whois.cnnic.cn
DNS服务器	ns1.363.hk - 118.123.249.114
DNS服务器	ns2.363.hk - 61.172.183.73
域名状态	默认的正常状态

图 2 域名 whois 身份信息与控制邮箱错位



序号	域名	注册人	邮箱
1	polaxiong.com.cn	王	alirezajobe171@gmail.com
2	firefox-browser.com.cn	夏	alirezajobe171@gmail.com
3	jinshandazi.cn	夏	alirezajobe171@gmail.com
4	myasus.com.cn	王	alirezajobe171@gmail.com
5	cm-oray.com.cn	熊	alirezajobe171@gmail.com
6	am-oray.com.cn	熊	alirezajobe171@gmail.com
7	cs-speedtest.com.cn	徐	alirezajobe171@gmail.com
8	xshell-a.com.cn	谢	alirezajobe171@gmail.com
9	app-qcc.com.cn	王	alirezajobe171@gmail.com
10	pc-sogo.com.cn	徐	alirezajobe171@gmail.com
11	pc-chuangkit.com.cn	王	alirezajobe171@gmail.com
12	an-360.com.cn	徐	alirezajobe171@gmail.com

图 3 单邮箱多姓名轮换

ssh-finalshell.com.cn 域名 | 154.19.253.2 IP地址 | 香港 Cogent 地区 | 共有 2 个域名解析

序号	域名	标题
1	nx-nexus.com.cn	Nexus桌面美化官网 - 仿Mac风格Dock栏	内置超80种鼠标悬停特效与丰富小工具
2	ssh-finalshell.com.cn	FinalShell官网 – FinalShell官方平台	国产免费一体化服务器管理工具，替代XShell+WinSCP...

图 4 多个仿冒域名解析至香港 Cogent

三、典型攻击活动分析

（一）传播入口

用户在搜索引擎检索“FinalShell 下载”等关键词后，会被引导至“ssh-finalshell.com[.]cn”等仿冒站点。该站点冒充 FinalShell 官方正版下载入口，提供携带银狐木马的恶意压缩包。该团伙还批量注册并运营“apps-finalshell.com[.]cn”“www.ch-finalshell.com[.]cn”“web-finalshell.com[.]cn”等域名，均沿用“前缀-finalshell.com.cn”的命名模板。

图 5 由 AI 批量复刻生成的高仿真 FinalShell 仿冒下载页面

本次活动主要仿冒开发运维类工具，早期活动则集中仿冒 Chrome、WPS、Telegram 等大众软件。FinalShell 是常用的远程连接（SSH/SFTP）客户端，用户中有大量持有高价值主机权限的运维与开发人员。此类用户的主机一旦被控，攻击者可利用其权限进一步横向移动。

仿冒页面采用高度标准化的前端结构、规整的 HTML 注释和通用前端技术栈，与官方网站的文字并非逐句对应。同一仿冒主题下，不同时间注册站点的页面布局和内容也趋于

一致。综合这些特征，研判认为，此类页面由 AI 爬取原官网后批量复刻生成，可同时用于仿冒多个品牌。

该团伙还大量选用需强实名的“.com.cn”后缀，通过前期泄露数据中的“姓名、身份证号”组合完成注册，借用他人身份规避溯源。

（二）跳转与下载链

传播链路为“搜索结果->仿冒域名入口->云对象存储->恶意样本”。恶意资源多托管于阿里云 OSS 等云对象存储服务，下载过程中设置多层跳转，以迷惑用户并降低早期被检测拦截的概率。

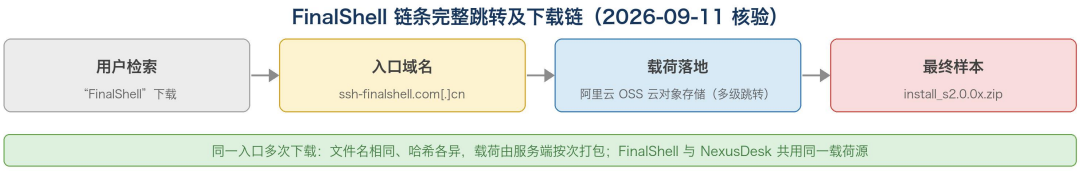


图 6 “FinalShell”传播链完整跳转及下载链

表 3 传播链各环节

环节	URL/域名	作用
入口	ssh-finalshell.com[.]cn	仿冒 FinalShell 下载页，伪装为官方正版下载入口
跳转	apps-finalshell.com[.]cn 等域名	关联仿冒域名，与 NexusDesk 主题站共用同一载荷供给后台
下载	阿里云 OSS（多层跳转）	云对象存储托管，落地携带银狐木马的 instell_s2.0.0x.zip

对同一入口多次下载的样本进行校验发现，文件名相同，哈希值却不同，表明服务端按次打包并持续更新恶意程序，以规避哈希特征检测。FinalShell 传播链中的 instell_s2.0.0x.zip 存在这一现象，例如，FinalShell 与 NexusDesk 仿冒站点提供的压缩包名称也完全一致。

表 4 同一下载入口多次下载所得样本的哈希

样本文件名	MD5
instell_s2.0.04.zip	cb03bffe8eb990a4071cb9c82dff8c94
instell_s2.0.04 (1).zip	21a495caeba6efdcd16e54ce7ce26e41
instell_s2.0.03.zip	ea2eaf5b853fd93b4771f641c98639d8
instell_s2.0.03.zip	6ac53bdfa55e9e417b2688804658664d
instell_s2.0.03.zip	95cfcfa1a4bbf679faea0a5abff8e6ac

（三）样本落地与执行

钓鱼站点提供的压缩包仅包含一个伪装成安装程序的 Windows 64 位可执行文件，大小为 35,473,200 字节。不同入口提供的同名文件哈希值不同，表明服务端按次打包并持续更新载荷，以规避哈希特征检测。样本携带的第三方签名与文件实际摘要不符，属于伪造签名。入口程序在公共用户目录释放组件、注册计划任务后退出，后续组件由计划任务逐级启动。各阶段的存放位置、命名方式和触发机制相互独立，部分组件利用带有效签名的第三方程序侧加载恶意模块，形成“白加黑”结构，并通过随机命名和伪装扩展名规避文件名与类型检测。

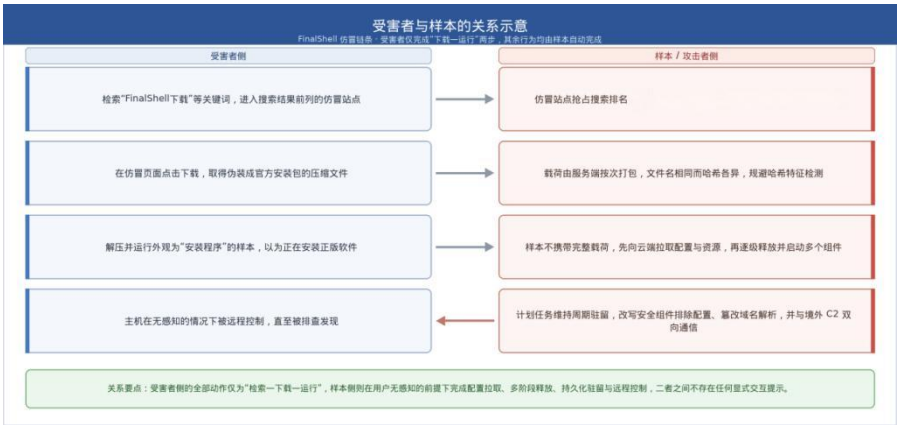


图 7 受害者与样本关系

（四）远程控制与恶意功能

样本本体负责从远端下载载荷，自身不直接实施窃密，而是通过释放中间态 EXE 文件，再由中间态 EXE 释放最终载荷的分阶段投放方式实施攻击。

各阶段组件的存放位置、命名方式和触发机制相互独立，清除单个环节后，其余载荷仍可运行。执行链共设置 6 个计划任务，采用登录触发和周期触发，部分任务冒用系统更新名称并设为隐藏，使原始样本退出后仍可定时启动后续载荷。样本还以较高系统权限改写安全组件排除配置，将安全厂商域名指向回环地址。远控组件与境外 C2 地址保持 TCP 双向通信；配置和资源托管于云对象存储，可随检测情况替换，控制通道则通过非标端口直连并长期保持稳定。这种分开部署方式便于批量运营，也增加了封堵和溯源难度。

四、典型恶意样本分析

表 5 样本基本信息

样本标签	内容
SHA-256	285b3bc94b18ac314c6a4e9d2fc39383a46a459b5e5db8d627dd8b8db6b79743
MD5	3478c09e3c39ebaba0a8c7872aad3653
文件名称	instell_s2.0.03.exe
文件大小	35,473,200 字节
文件类型	Windows 64 位可执行程序（PE32+）
数字签名	样本内嵌署名“Bytedance Pte. Ltd.”的签名记录，但摘要校验未通过，签名无效。
特征	多阶段下载加载器；释放程序与目录使用随机化命名，部分文件使用.png、.jpg、.dat、.db 等迷惑性扩展名
投递来源	ssh-finalshell.com[.]cn 等仿冒站 → instell_s2.0.0x.zip（同名不同哈希）

（一）初始载荷与解密加载

样本伪装成安装程序，实际为 Windows 64 位多阶段下载加载器。加载过程分为两层，依次获取配置、解码资源并加载后续程序。配置地址为“https://02bbe6.oss-cn-beijing.aliyuncs[.]com/tad”，程序还内置同站点下的 /s.dat 与 /s.jpg 资源地址。

原始程序首先在“C:\Users\Public\SXRh6d”目录释放 bcCfOw.exe、UxEnhance64.dll 及配套数据文件，并注册计划任务“fX8Ia”。原始进程退出后，任务计划服务启动 bcCfOw.exe，由其加载同目录的 UxEnhance64.dll，继续释放并启动 VBV4HZ.exe。随后，VBV4HZ.exe 加载同目录的 XPSPLOG.dll 连接远端服务器，同时释放 XsOewfN.exe、Pl6VgrWG.exe 与 O02PwqGh.exe；O02PwqGh.exe 再释放 DnsrvKyi.exe。部分程序和目录采用随机命名：aLpkwp.exe 与 bcCfOw.exe 内容完全相同，baKv9z.exe、PnA1azgv.exe 分别与 VBV4HZ.exe、XsOewfN.exe 内容一致。

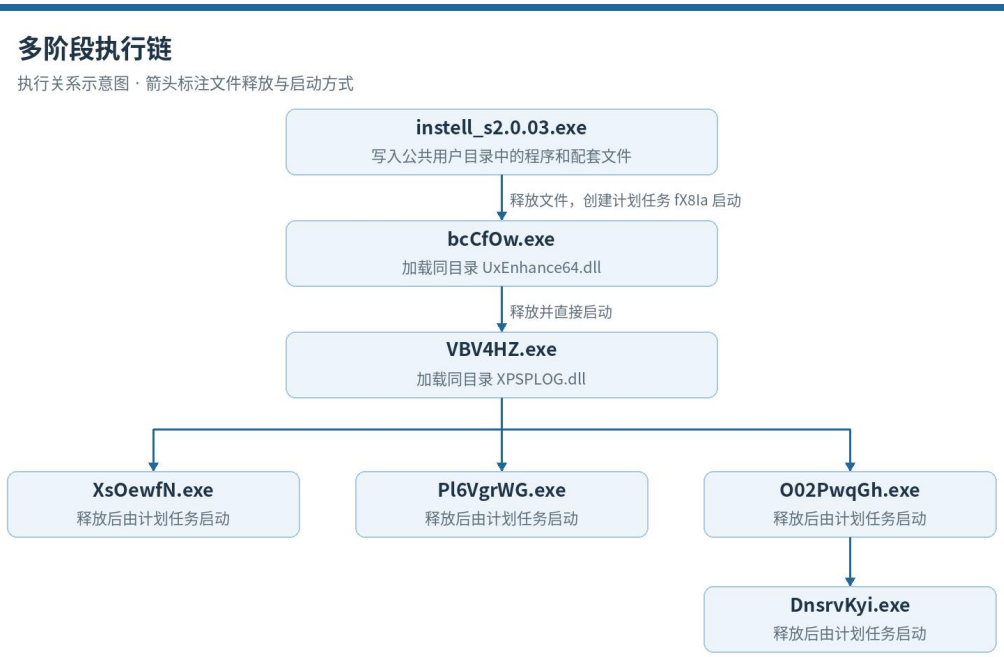


图 8 样本多阶段执行关系图

表 6 样本释放文件及位置

存放位置	文件
C:\Users\Public\SXRh6d	bcCfOw.exe、UxEnhance64.dll、msadox.tb、adoresd.dat
C:\Program Files (x86)\VBV4HZ	VBV4HZ.exe、XPSPLOG.dll、image.png、thumbs.db
C:\Program Files (x86)\S7UA99K	XsOewfN.exe、XPSPLOG.dll、image.png、thumbs.db
C:\ProgramData\cgL18U72	O02PwqGh.exe、O02PwqGh.dat、O02PwqGh.png
C:\ProgramData	Pl6VgrWG.exe
C:\ProgramData\cpLjQb7s	DnsrvKyi.exe
C:\Windows\Temp	ranchserv.jpg

（二）持久化与规避检测

样本共注册六个计划任务，分别通过用户登录和周期执行启动载荷。其中两个任务冒用 MicrosoftEdgeUpdateTaskUA 名称，伪装成浏览器更新任务并设为隐藏，每隔 1 分钟执

行一次，且无限期重复。原始样本退出后，这些任务仍会定时启动各阶段载荷。

表 7 样本注册的计划任务

计划任务名称	执行程序	重复间隔
fX8Ia	bcCfOw.exe	1 分钟
MicrosoftEdgeUpdateTaskUA Task-S-1-5-18 9Gkjk	VBV4HZ.exe	1 分钟
MicrosoftEdgeUpdateTaskUA Task-S-1-5-18 gsWzP	XsOewfN.exe	1 分钟
Our Empowering Procedure Standardization And	O02PwqGh.exe	10 分钟
Software Business Prioritization	Pl6VgrWG.exe	30 分钟
Assessment Intelligent Data Objective Seamlessly	DnsrvKyi.exe	5 分钟

样本通过 PowerShell 批量添加 Windows Defender 排除路径，将系统目录、用户目录和程序目录等位置排除在检测范围之外。运行期间，后续程序又以 SYSTEM 权限修改注册表键“HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths”，写入 C:\Users\Public\SXRh6d、C:\ProgramData、C:\Users、C:\Program Files (x86)及用户文档目录等路径。

VBV4HZ.exe 还会修改系统 hosts 文件，将 weishi.360[.]cn、www.360[.]cn、sd.360[.]cn 三个域名指向回环地址 127.0.0.1，阻断用户访问相关安全软件站点。

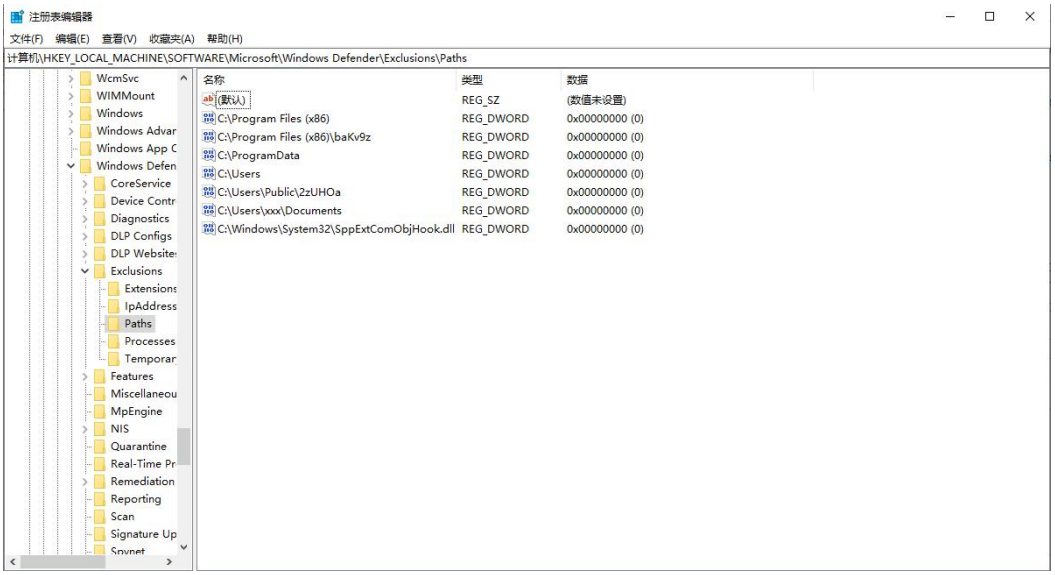


图 9 注册表中被写入的 Windows Defender 排除路径

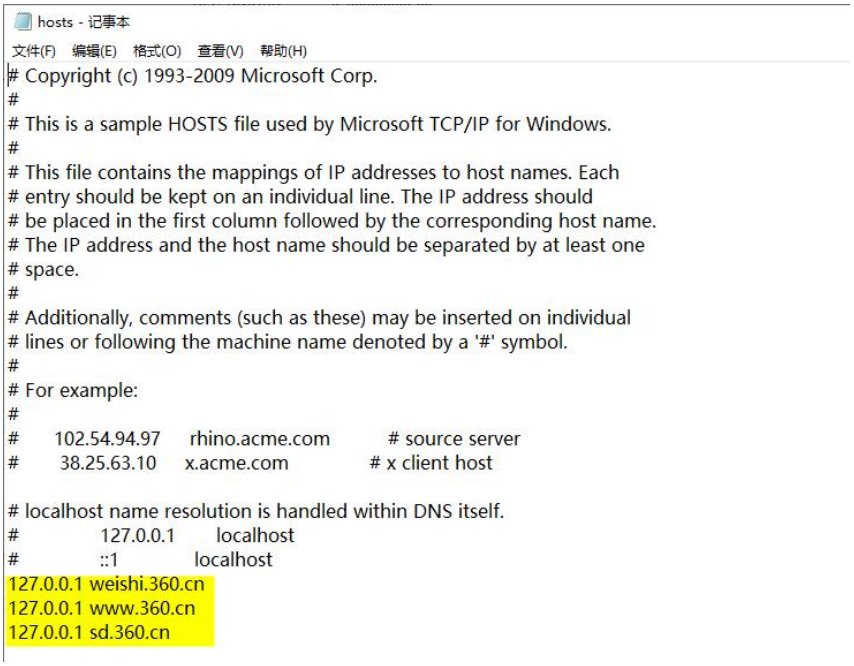


图 10 hosts 文件中安全软件网站域名被指向回环地址

（三）窃密与远控功能

样本自身负责多阶段下载加载和持久化，不直接实施窃密，远程控制由后续载荷完成。VBV4HZ.exe 侧加载 XPSPLOG.dll 后，与远端服务器建立连接并双向交换数据，具备接受远程指令的条件。各阶段功能相互独立，清除单个环节后，其余载荷仍可运行。

（四）通信协议与配置特征

样本分别访问 OSS 资源和远端服务器。bcCfOw.exe、VBV4HZ.exe 与 O02PwqGh.exe 解析相关域名后连接对应地址，其中 VBV4HZ.exe 与 47.243.152[.]51:18300 双向交换数据。配置和资源统一托管于阿里云 OSS，专用 C2 通过自定义大端口直连，二者独立部署，配置与资源可单独替换。

表 8 样本程序内置地址与实际通信目标

地址	用途或行为
https://02bbe6.oss-cn-beijing.aliyuncs[.]com/tad	获取配置
https://02bbe6.oss-cn-beijing.aliyuncs[.]com/s.dat	程序内置资源地址
https://02bbe6.oss-cn-beijing.aliyuncs[.]com/s.jpg	程序内置资源地址
mm2027.oss-cn-hangzhou.aliyuncs[.]com	后续程序访问的 OSS 地址，由 bcCfOw.exe 连接
new2027.oss-cn-hongkong.aliyuncs[.]com	后续程序访问的 OSS 地址，由 VBV4HZ.exe、O02PwqGh.exe 连接
47.243.152[.]51:18300	远端通信地址，与 VBV4HZ.exe 双向交换数据

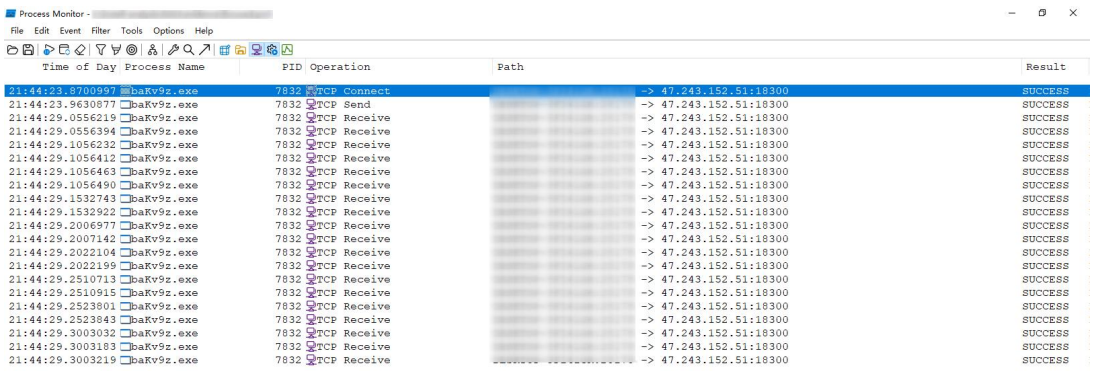


图 11 后续程序与 47.243.152[.]51:18300 的连接及双向通信

五、团伙关联与同源性分析

此次攻击行动在仿冒品牌、注册人身份和控制邮箱上存在差异，但域名命名、建站方式、引流分发和托管选择具有一致性。

专项工作组综合“钓鱼模板与下载链”和“注册要素”两类独立强证据，以及上述特征在两个时间上不相邻的批次中稳定复现等特点，研判确认属于同一团伙的攻击行为。对本次团伙利用的域名进行统计，其中 83.5%以字母 a 开头，并大量采用 an-、app-、ah-等前缀与仿冒品牌关键词组合，形成较为稳定的域名命名特征，专项工作组将该团伙命名为“甲蚁（G01）”。

表 9 团伙关联证据与专属性评估

证据类别	本次活动特征	历史团伙特征	关联性
样本代码与加密	多阶段下载加载、白加黑侧加载、以大体积数据段承载载荷	历史风险提示中同类载荷结构	弱关联。
配置及通信协议	阿里云 OSS 拉取配置（/tad、/s.dat、/s.jpg）；专用 C2 使用非标端口直连	同为公有云对象存储托管 + 独立 C2 直连	中等关联。
C2 与历史	14.128.53[.]194:80、47.243.152[.]51:18300；钓鱼网站群集中托管于香港 Cogent	历史批次同样选择境外廉价、免备案托管	中等关联。

解析			
钓鱼模板与下载链	“字母前缀-品牌关键词.com.cn”命名模板；AI 批量复刻页面；51.LA 统计区分主题；多层跳转至云存储	历史 IOC 中“wps-office-wps-xlsx.com[.]cn”等采用同类关键词堆叠命名，页面同为 AI 批量生成	强关联。
活动时间与目标	2026-07-09 至 2026-09-09 集中注册，注册周期统一为一年；目标转向代理加速类与开发运维类工具	历史批次时间更早，目标以大众办公与浏览器软件为主	辅助证据
注册要素	单一 Gmail 邮箱统辖数百域名；单邮箱多姓名轮换；盗用真实公民身份满足“.com.cn”强实名要求	历史批次经 duck.com 邮箱批量注册同格式仿冒域，注册行为模式一致	强关联。

图 12 钓鱼页面比对（左：历史风险提示所述页面；右：本次捕获页面）

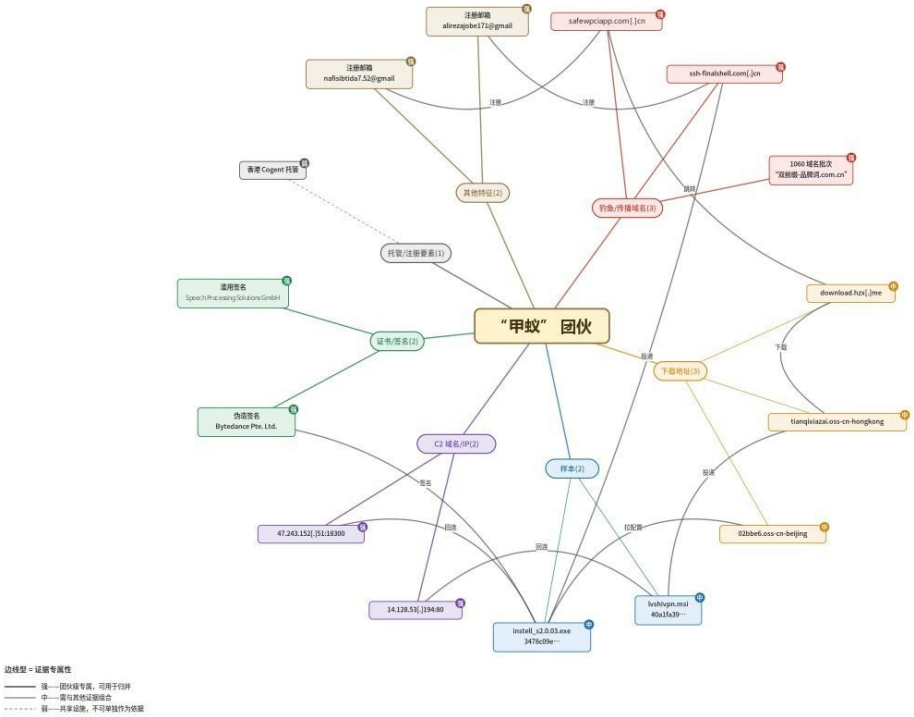


图 13 “甲蚁（G01）”团伙：“域名—IP—样本—证书”点边关系图谱

六、活动与控制规模

2026 年 9 月 15 日至 22 日，CNCERT 监测发现该团伙共控制境内肉鸡达 8708 个。其中，单日上线数量峰值 2361 个。相关变化情况如下图所示。

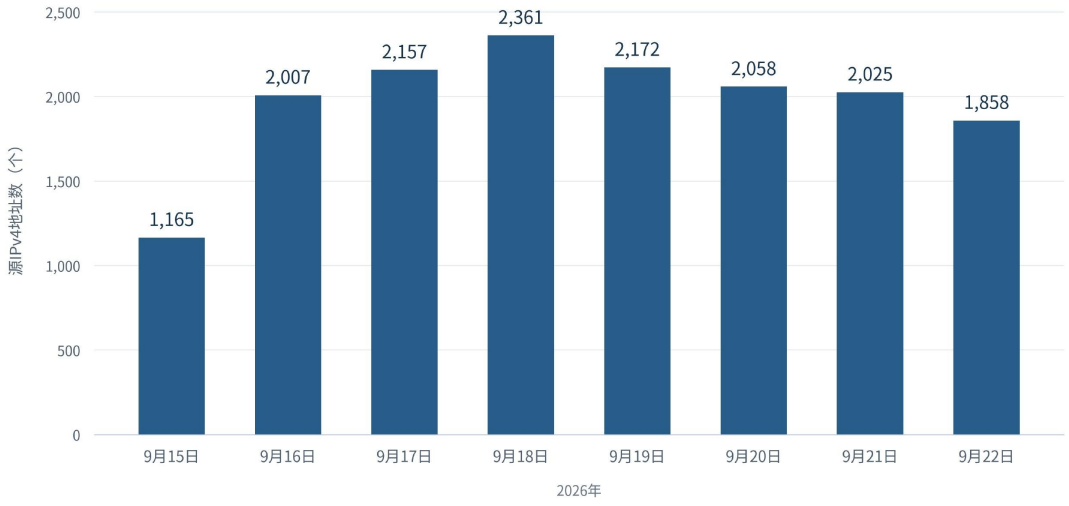


图 14 每日上线肉鸡数

七、防范建议

针对“甲蚁（G01）”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。

（2）不要将“.com.cn\.cn”后缀等同于官方站点。该团伙大量抢注强实名“.com.cn\.cn”域名以制造可信假象，并伴有字母重复、缺字、错拼等特征，下载前应逐字核对域名。

（3）重点保护运维与开发人员终端。该团伙已转向仿冒 FinalShell、Xshell、SecureCRT、NexusDesk 等远程连接和运维工具。此类终端普遍持有高价值主机凭据，被控后极易成为横向移动的跳板。建议企业统一分发此类软件，并禁止员工自行下载。

（4）对 Windows Defender 排除项变更建立告警。监测注册表键“HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths”的修改，以及 PowerShell 调用 Add-MpPreference 的行为，重点检查将 C:\Users、C:\ProgramData、C:\Windows\System32 等大范围目录加入排除项的操作。

（5）排查冒用系统更新名称的隐藏计划任务。重点检查名称包含“MicrosoftEdgeUpdateTaskUA”、执行目标却位于 C:\Users\Public、C:\ProgramData 等非常规目录的任务，以

及每隔 1 至 30 分钟重复执行、设为隐藏且无限期运行的任务。

（6）检查 hosts 文件与安全软件可达性。若发现安全厂商域名被解析至 127.0.0.1，应结合修改来源、关联进程和其他恶意行为开展排查；确认感染后立即隔离处置。

（7）启用终端行为检测，并对报告所列 IOC 中的域名与 C2 地址实施网络层阻断。该团伙在服务端按次打包载荷，同名文件的哈希值不同，基于文件哈希的黑名单拦截基本失效，下载时应警惕此类文件。

八、相关 IOC

受篇幅所限，钓鱼及传播域名表仅抽样列出 50 条代表性条目，全量 IOC 清单见附件《“银狐”木马“甲蚁（G01）”团伙全量仿冒网站清单》。

（一）钓鱼域名

域名	仿冒对象	域名	仿冒对象
114-best.com[.]cn	114 查号/号码查询	114-phone[.]cn	114 查号/号码查询
2345browser-pc.com[.]cn	2345 浏览器/导航	2345browser-web.com[.]cn	2345 浏览器/导航
360scdn.com[.]cn	360 系软件	360tool.com[.]cn	360 系软件
app-aisizhushou.com[.]cn	爱思助手	aida66-ai.com[.]cn	AIDA64
app-aulacn.com[.]cn	Aula	ah-autocad.com[.]cn	AutoCAD
ah-dism.com[.]cn	Dism++	an-dism.com[.]cn	Dism++
ah-kook.com[.]cn	KOOK	an-kook.com[.]cn	KOOK
ai-photosir.com[.]cn	PhotoSir	ah-photopea.com[.]cn	Photopea
an-libreoffice.com[.]cn	libre Office	an-pdf24.com[.]cn	PDF
app-colorful.com[.]cn	七彩虹	app-colorfuldrdrive.com[.]cn	七彩虹

域名	仿冒对象	域名	仿冒对象
an-quanlishi.com[.]cn	全历史	51-cxsoft.com[.]cn	其他(51cxsoft)
an-yuanzheng.com[.]cn	其他(yuanzheng)	ah-fenghuangwang.com[.]cn	凤凰网
7-zip-am.com[.]cn	压缩工具(7-Zip/好压/Bandizip)	7-zip-en.com[.]cn	压缩工具(7-Zip/好压/Bandizip)
ai-ximalaya.com[.]cn	喜马拉雅	an-tuba.com[.]cn	图吧工具箱
an-xueersi.com[.]cn	学而思	antutu-app.com[.]cn	安兔兔
app-eggrj.com[.]cn	小众工具类	app-huijiwiki.com[.]cn	小众工具类
app-buyinjinritemai.com[.]cn	抖音电商	an-qiangpiaowang.com[.]cn	抢票类
ah-huilv.com[.]cn	汇率查询类	an-hanhuahezi.com[.]cn	汉化盒子
ab-huorong.com[.]cn	火绒安全	an-huorong.com[.]cn	火绒安全
ai-yuanfudao.com[.]cn	猿辅导	antivirus-rising.com[.]cn	瑞星杀毒
ah-uujiasu.com[.]cn	网易 UU 加速器	163-wyyun.com[.]cn	网易云音乐
ah-tengxunhuiyi.com[.]cn	腾讯会议	an-qqweiyun.com[.]cn	腾讯微云
an-yuque.com[.]cn	语雀	ah-doubao.com[.]cn	豆包
an-jinshanwd.com[.]cn	金山系	app-jinshandazi.com[.]cn	金山系
an-leidian.com[.]cn	雷电模拟器	ah-razer.com[.]cn	雷蛇

（二）传播地址

地址	说明
download.hzx[.]me	中转跳转域
tianqixiazai.oss-cn-hongkong.aliyuncs[.]com	载荷托管（SafeW2.5.zip）
https://02bbe6.oss-cn-beijing.aliyuncs[.]com/tad	配置地址
https://02bbe6.oss-cn-beijing.aliyuncs[.]com/s.dat	内置资源地址
https://02bbe6.oss-cn-beijing.aliyuncs[.]com/s.jpg	内置资源地址
mm2027.oss-cn-hangzhou.aliyuncs[.]com	后续程序访问的 OSS 地址

new2027.oss-cn-hongkong.aliyuncs[.]com	后续程序访问的 OSS 地址

（三）C2 地址

地址
14.128.53[.]194:80
47.243.152[.]51:18300

（四）样本名称及 hash

文件名	类型	SHA-256 / MD5
instell_s2.0.03.exe	PE32+下载加载器	SHA-256：285b3bc94b18ac314c6a4e9d2fc39383a46a459b5e5db8d627dd8b8db6b79743 MD5：3478c09e3c39ebaba0a8c7872aad3653
instell_s2.0.04.zip	投递压缩包	MD5：cb03bffe8eb990a4071cb9c82dff8c94
instell_s2.0.04 (1).zip	投递压缩包	MD5：21a495caeba6efdcd16e54ce7ce26e41
instell_s2.0.03.zip	投递压缩包	MD5：ea2eaf5b853fd93b4771f641c98639d8
instell_s2.0.03.zip	投递压缩包	MD5：6ac53bdfa55e9e417b2688804658664d
instell_s2.0.03.zip	投递压缩包	MD5：95cfcfa1a4bbf679faea0a5abff8e6ac

（五）签名特征

特征	说明
Bytedance Pte. Ltd.	样本内嵌署名“Bytedance Pte. Ltd.”的签名记录，但摘要校验未通过，签名无效。
Speech Processing Solutions GmbH	被滥用的有效签名主体。签名文件描述为 Philips Speech Driver Client Configuration，被用作白加黑侧加载的白文件

（六）主机及流量特征

类型	特征
文件路径	C:\Program Files (x86)\lnte\lnte\scuttled.dll；%APPDATA%\Adobe\h114915286

	36771541391.ini；C:\Users\Public\venwin.lock
文件路径	C:\Users\Public\SXRh6d\（bcCfOw.exe、UxEnhance64.dll、msadox.tb、adoresd.dat）；C:\ProgramData\cgL18U72\；C:\ProgramData\cpLjQb7s\；C:\Windows\Temp\ranchserv.jpg
注册表	HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths 下写入 C:\Users\Public\SXRh6d、C:\ProgramData、C:\Users、C:\Program Files (x86) 及用户文档目录
计划任务	fX8Ia；MicrosoftEdgeUpdateTaskUA Task-S-1-5-18 9Gkjk；MicrosoftEdgeUpdateTaskUA Task-S-1-5-18 gsWzP；Our Empowering Procedure Standardization And；Software Business Prioritization；Assessment Intelligent Data Objective Seamlessly
hosts 劫持	weishi.360[.]cn、www.360[.]cn、sd.360[.]cn 被指向 127.0.0.1
Defender 排除	PowerShell 以 -NoProfile -ExecutionPolicy Bypass 调用 Add-MpPreference，排除 C:\Users、C:\ProgramData、C:\Windows\System32 及进程 xwizard.exe、wuauclt.exe
注册邮箱	nafisibtida7.52@gmail[.]com；alirezajobe171@gmail[.]com
流量特征	与 14.128.53[.]194:80 高频小包通信，44 字节与 136 字节数据块反复出现

附件：“银狐”木马“甲蚁（G01）”团伙全量仿冒网站清单