



银狐再现：BYOVD与双重“白加黑”攻击链拆解

发布时间：2026年08月17日

类型：公司新闻

分享：

事件概述

近期，公安部网安局等权威部门接连公布了多起打击“银狐”木马病毒的典型案例，再次为企业终端安全敲响警钟。在各地警方破获的真实案件中，涉案团伙的诈骗金额动辄高达数百万甚至上千万元，给中招企业造成了极其惨痛的直接经济损失。在警方侦破的案件中，诈骗分子通过远控木马潜伏，在员工毫无察觉的情况下冒充内部高管，诱导大额转账，全程宛如“透明人”作案，极具隐蔽性。

面对如此狡猾的对手，企业传统安全防线正面临严峻考验。银狐之所以难防，就在于其极快的变种速度和登峰造极的免杀伪装手段。



近期，应急响应中心就捕获到了银狐家族的最新变种。该样本使用了规避技巧：不仅巧妙利用 MSI 安装包获取 SYSTEM 高权限，还连续嵌套双重“白加黑”链路，甚至利用易受攻击驱动（BYOVD）直接在内核层试图瓦解终端安全防护。

为了帮助企业看清敌人的“底牌”，堵住防御漏洞，本文将为您深度拆解银狐变种的攻击全貌，并提供“猎狐”一体化治理方案，助企业化“危”为“安”！

银狐变种概述

该变种初始以 MSI 安装包的形式作为攻击入口，利用 SYSTEM 权限执行自定义动作来下载并释放后续恶意载荷。在运行过程中，样本连续使用了两组“合法签名程序 + 同目录未签名 DLL”的“白加黑”链路来隐蔽执行恶意代码。

根据行为特征分析，该样本具备以下核心威胁能力：

- 内核驱动加载（BYOVD）
- 多重自启动持久化
- 加密载荷下载
- 外部控制（C2）通信能力

综合威胁评级

维度	评级	说明
传播能力	★★★★☆	通过微信、飞书、邮件等 IM 工具和钓鱼链接，进行高精度的社工定向投放。
隐蔽性	★★★★★	核心逻辑隐藏于 MSI 高熵数据流中，连续嵌套双重“白加黑”链路，伪装极强。
持久化	★★★★☆	通过写入 HKLM Run 注册表项，并创建多重伪装的隐藏计划任务实现长期驻留。
破坏性	★★★★☆	具备内核层执行与加密载荷下载能力，可实施高度隐蔽的窃密、双重勒索及精准诈骗。
反检测	★★★★★	大量滥用有效数字签名程序旁加载，并利用 BYOVD 技术在内核层试图强行瓦解 EDR 终端防护。

银狐变种自动化攻击链全景分析

该变种的攻击流程环环相扣，全程自动化且具有极强的隐蔽性。以下为完整攻击链路：

1. 初始触发：释放 app_setup.6653001.msi文件

2. 提权执行：MSI 安装时，Windows Installer 以延迟、

无模拟方式调用其导出函数，使恶意逻辑在 SYSTEM 上下文执行；生成自定义动作 MSI44C9.tmp。

3. 阶段一下载：连接阿里云 OSS (710new[.]oss-cn-beijing[.]aliyuncs[.]com) 下载第一阶段载荷。

4. 第一组“白加黑”与 BYOVD：

释放并运行带腾讯签名的 bJpMzw.exe。

旁加载未签名的 UxEnhance64.dll。

创建并启动内核驱动 TCLService，实现 BYOVD 攻击。

写入 HKLM Run 注册表与隐藏计划任务实现持久化。

5. 阶段二下载与扩散：

从杭州阿里云 OSS (26nn[.]oss-cn-hangzhou[.]aliyuncs[.]com) 下载第二阶段载荷。

运行带 Philips 签名的 KE4qwF.exe，旁加载 XPSPLOG.dll（第二组白加黑）。

复制生成 fJWRN0ft 随机目录变体，形成多副本持久化。

6. C2 通信：连接 8[.]210[.]12[.]210:28300 进行控制通信，并周期性查询 pidjik[.]net。

银狐变种核心威胁技术深度解析

SYSTEM 权限下载与释放

在自然安装阶段，SYSTEM 权限的 MsiExec.exe 会创建远程自定义动作进程，并访问云存储接收约 8.96 MB 的 TLS 数据，随后向公共用户目录和临时目录写入多项恶意载荷。

嵌套双重“白加黑”链路

- **第一组：**落地的 bJpMzw.exe 具有有效腾讯代码签名，启动后立即加载同目录的高熵未签名 DLL (UxEnhance64.dll)，形成 DLL 旁加载（DLL Side-loading）。
- **第二组：**后续创建带有 Philips 签名的 KE4qwF.exe，并同目录加载 XPSPLOG.dll，进一步强化生存能力。

高置信 BYOVD 攻击（引入易受攻击驱动）

样本在运行中创建了名为 TCLService 的自动启动内核驱动。其镜像路径伪装为图片文件，但实际上是一个 28,272 字节的 x64 内核 PE 文件。

- **驱动文件：**该文件具有 Adlice 有效签名，版本信息显示为 TrueSight 2.0.2。
- **攻击目的：**根据研究披露，TrueSight 低于 3.4.0 的版本存在任意进程终止漏洞。攻击者通过 DeviceIoControl 发送特定指令（0x22E044），可在内核层强制结束杀毒软件或 EDR 进程，从而为后续恶意行为“扫清障碍”。

多重伪装持久化

样本在系统中植入了三个维度的持久化机制：

- **Run 键值伪装：**写入 HKLM Run 项 Tencent SecurityHealth，指向恶意文件。
- **隐藏任务：**创建隐藏计划任务，设置为登录和每分钟触发。

- **Edge更新伪装**：创建两条伪装成 Edge Update 的隐藏任务（指向 KE4qwF.exe 及变体），同样包含高频触发机制。

银狐变种信息回传与C2通信网络

目标地址	核心行为	威胁判定
710new[.]oss-cn-beijing[.]aliyuncs[.]com	第一阶段 TLS 下载，约 8.96 MB	载荷分发
26nn[.]oss-cn-hangzhou[.]aliyuncs[.]com	第二阶段 TLS 传输，接收约 11.05 MB	载荷分发
8[.]210[.]12[.]10:28300	建立 TCP 会话并发送 615 字节二进制数据	高可信控制/信标通信
pidjik[.]net	约每 3 秒查询一次	周期域名探测

银狐变种攻击链路 MITRE ATT&CK 战术映射

战术阶段 (Tactic)	技术描述	行为对应
执行 (Execution)	用户执行/系统权限调用	MSI 安装调用 HttpExtensionProc 在 SYSTEM 上下文执行
持久化 (Persistence)	计划任务与注册表 Run 键	写入隐藏计划任务及 Tencent SecurityHealth 启动项
防御规避 (Defense Evasion)	BYOVD 与 白加黑旁加载	利用合法签名文件旁加载恶意 DLL；滥用旧版 TrueSight 驱动试图终止 EDR
命令控制 (C2)	应用程序层协议	与8[.]210[.]12[.]10:28300 建立 TCP 通信传输控制数据

面对银狐变种复杂的多重免杀与内存对抗技术，传统的基于文件特征的杀毒软件往往防不胜防。

基于AI XDR的全链路智能分析与自动化闭环

针对“白加黑”与 BYOVD 的内存级绞杀

阻断恶意 C2 通信与内网横向传播

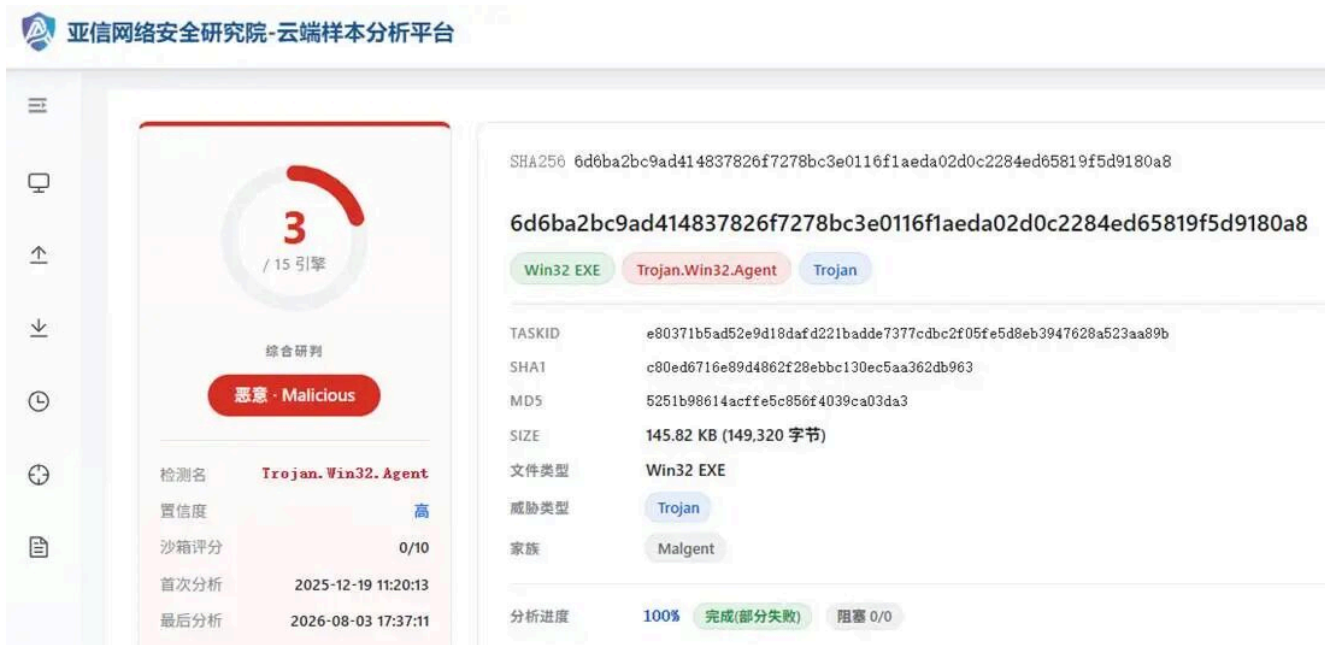
- 痛点应对：该样本会频繁外连云存储下载后续载荷，并与 C2 服务器进行信标通信。
- 解决方案

事前诱饵管控与事后一键溯源

事前防范：银狐常伪装成报税工具或发票，通过飞书、微信等 IM 工具和钓鱼邮件进行投递。TrustOne 提供“社工钓鱼管控”功能，能有效阻止从社工渠道下载各类型的风险文件，直接关上“人为大门”。

核心检测能力

梦蝶增强型病毒扫描特征码版本2.0.0.253已经可以检测该银狐变种文件。



威胁情报云查可以检测报告中提及的IOC。



手动处置方案与防范建议

针对此类高度规避的恶意样本，建议安全运营团队采取以下响应措施：

快速隔离与阻断：

立即隔离命中上述 IOC 的主机，并在网络边界阻断相关恶意域名和 IP/端口通信。

深度清理与复核：

- 终止相关恶意进程，删除三处随机目录及其文件（执行前先校验哈希，避免误删合法程序）。
- 重点处置 BYOVD：停止并删除 TCLService 驱动服务，清理 ranchserv.jpg 文件。驱动已加载的主机建议离线处置并重启复核。
- 清理 Tencent SecurityHealth 注册表项和恶意计划任务。

系统级策略加固：

- 启用并更新 Microsoft Vulnerable Driver Blocklist（微软易受攻击驱动程序阻止列表）。
- 评估并开启 HVCI 及“阻止滥用易受攻击的已签名驱动程序”的 ASR 规则（建议先在审计模式下验证兼容性）。

全网威胁狩猎：

全网排查两组“有效签名宿主 + 同目录未签名高熵 DLL”的组合特征，回溯 MSI 来源确认初始入侵点。

银狐高危变种防御总结

该变种不仅利用了系统高权限执行环境，还通过云端对象存储（OSS）灵活下发载荷，并在终端上交替使用“白加黑”及 BYOVD 技术，对传统终端安全防护体系构成了严重威胁。企业需构建多维度的纵深防御策略，结合驱动拦截策略与威胁情报，方能有效抵御此类高级威胁。

附录 威胁指标（IOC）

文件哈希 (SHA-256)

676a2a7b94ca2f8ec76352ee656e4d075bb342bd7ad6efbc7c19c060001eace7

187f95ab8cd67dc59bd178a59eaa4bac6393e30d9e1c5c45fec5a460d1775ebc

5fdcc68b0b0b2c201835d990acf519dbf49d084cefcdbd6f1fd2d55a1c83a3b0

0d141847f4aef93358d90fd727054496974070990f05bfa3e2ff8fb72fff6f3d

6d6ba2bc9ad414837826f7278bc3e0116f1aeda02d0c2284ed65819f5d9180a8

50cf1db465687d53cf539e7463a2c58069b8c9ef9f099af21136104540af0dcf

52a104cb55ee786810e9eb4d439e961f4ff45db534128cfba615978457eb072d

网络通信地址

710new[.]oss-cn-beijing[.]aliyuncs[.]com

26nn[.]oss-cn-hangzhou[.]aliyuncs[.]com

pidjik[.]net

114[.]1112[.]25[.]211:443

115[.]238[.]6[.]70:443

8[.]210[.]12[.]210:28300