

【天穹】样本专题：典型样本总结与IOC收集（第二期）

 mp.weixin.qq.com/s

星图实验室

一、概述

近日，天穹沙箱团队在例行威胁狩猎过程中发现一款名为 **sofhtaller.3.0.8230002.msi** 的恶意安装包样本。该样本利用 Windows Installer (MSI) 安装包作为攻击载体进行传播，具有高度隐蔽性、持久化驻留以及明显的系统破坏能力，确认为典型的“伪装型恶意安装程序”（Trojan Installer）。此外，该样本具备远程控制能力与数据窃取潜力，经多维研判，确认为“银狐”家族变种样本。

二、样本信息

- 样本名：sofhtaller.3.0.8230002.msi
- SHA1：c21557a97bc0ab7cd75e400aec2a233f27ec2b99
- 文件类型：msi
- 文件大小：5.86 MB (6144000 bytes)
- 家族归属：银狐
- 分析报告链接：<https://sandbox.qianxin.com/tq/report/toNewReport.do?rid=a21f71e6d62b7d06807b225243052a52&index=1&sk=07167123>

三、样本分析

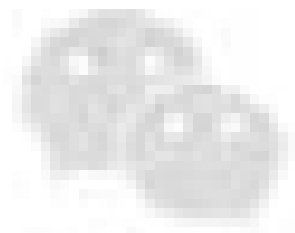
静态分析

该样本采用 MSI 安装包格式作为恶意载荷的封装与传播方式，意图借助这种用户广泛信任的格式降低防御警觉性，实现社会工程学传播。对该安装包内部二进制文件审查发现，样本未携带有效 PE 数字签名，无法验证发布者身份；同时命中“可疑加壳段”Yara 检测规则，表明样本使用混淆或加壳手段规避静态检测，如图 1、2 所示。



此图片来自微信公众平台
未经允许不可引用

图1 签名状态

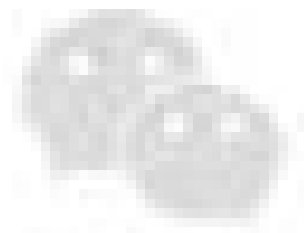


此图片来自微信公众平台
未经允许不可引用

图2 Yara 命中

动态分析

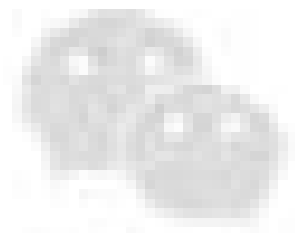
动态分析环境选择 Windows 11 x64 沙箱运行环境，通过 `msiexec.exe` 启动样本安装流程，安装过程中样本驱动 `msiexec.exe` 启动 `vssvc.exe`、`srtasks.exe` 等系统服务组件，利用系统合法进程进行行为伪装，实现权限提升与持久化驻留，如图 3 所示。



此图片来自微信公众平台
未经允许不可引用

图3 多级进程链

样本运行过程中释放 ouipSc.exe、UxEnhance64.dll 等多个恶意文件，写入 C:\Users\Public\下的随机目录。随后，样本将释放文件设置为**隐藏 (Hidden)** 和**只读 (ReadOnly)** 属性，避免用户发现和修改，实现长期驻留，如图 4、5 所示。



此图片来自微信公众平台
未经允许不可引用

图4 释放安装文件



此图片来自微信公众平台
未经允许不可引用

图5 修改文件属性

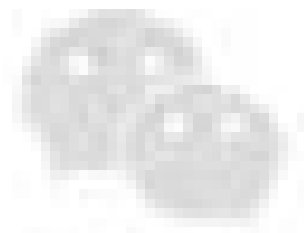
值得关注的是样本采用**隐蔽的云基础设施通信机制**。样本在运行过程中频繁与阿里云 OSS 域名 `zlq2s4[.]oss-cn-beijing.aliyuncs[.]com` 建立 TLS 连接，访问 `tad`、`a.gif`、`s.dat` 等资源，利用云 CDN 服务实现 C2 通信，如图 6 所示。该行为符合“利用云服务通信”的典型特征，通过合法云服务承载恶意流量，提高通信隐蔽性，有效绕过传统网络边界检测。



此图片来自微信公众平台
未经允许不可引用

图6 云服务通信

样本还表现出较强的反分析和痕迹清理能力。在日志记录层面，通过代码覆写技术破坏 `EtwEventWrite` 函数，使 Windows 事件跟踪（ETW）机制失效，以此规避 ETW 日志监控。在进程操控层面，通过调用 `NtResumeThread` 跨进程恢复线程，疑似实现内存注入。此外，为掩盖入侵痕迹，样本利用卷影复制服务（VSS）访问系统备份目录，删除 `SoftwareDistribution` 下的日志与缓存文件，清除系统更新痕迹，降低攻击活动被发现和溯源的风险。



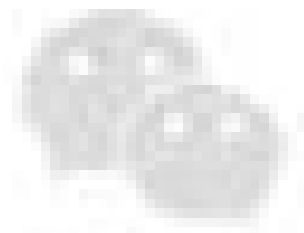
此图片来自微信公众平台
未经允许不可引用

图7 反分析和痕迹清理

该样本属于整个攻击流程的入侵驻留阶段，整体是一个多阶段加载 + 网络下载 + 持久化守护的典型木马框架流程，根据攻击者目的，整体可完成隐私窃密、主机控制等不同目标。

智能体拓线

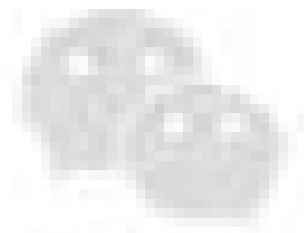
基于天穹团队积累的海量样本数据，天穹智能体通过对提交样本进行深度分析和自动化拓线，构建出了完整的恶意软件攻击网络。报告展示相关同源样本攻击时间跨度超过 5 年，不同阶段展现特点如图 8 所示。



此图片来自微信公众平台
未经允许不可引用

图8 攻击时间轴

智能体通过阿里云 OSS 地址 `zlq2s4[.]oss-cn-beijing.aliyuncs[.]com` 网络拓线发现 9 个新样本，如下表所示：



此图片来自微信公众平台
未经允许不可引用

四、IOC 福利

HVV IOC

204.44.93.88[:]8449123.57.110[.]76cloudproxy[.]link176.53.159[.]222https[:]//app-api.lensstory[.]cc

银狐 IOC

文件



此图片来自微信公众平台
未经允许不可引用

域名/IP

154.12.19.70[:]22011https[:]//dnyk123[.]xyzhttp[:]//zlq2s4[.]oss-cn-beijing.aliyuncs[.]comhttp[:]//710new[.]oss-cn-beijing.aliyuncs[.]comhttp[:]//dd.jiuzhaoren[.]top/orig/douyin-Windows.jpghttps[:]//b6zsrs[.]oss-cn-beijing.aliyuncs.comhttps[:]//z6qz7d[.]oss-cn-

beijing.aliyuncs.comloismfn1.duoshit[.]com103.214.172.16[:]443103.193.173.83[:]9100176
.53.159.222[:]3333176.53.159.222[:]3334

天穹智能分析平台（联系我们申请账号）：<https://sandbox.qianxin.com>

天穹智能分析平台持续迭代升级，致力于为每一位样本分析人员打造更高效、更智能、更易用的分析平台——这始终是我们不变的初心与追求。

如果您希望深入了解平台功能，或在使用过程中遇到任何问题，欢迎随时联系我们。您的反馈，是我们进步的重要动力！