关于“游蛇”黑产攻击活动的风险提示

本报告由国家互联网应急中心（CNCERT）与安天科技集团股份有限公司（安天）共同发布。

一、 概述

近期，CNCERT 和安天联合监测到“游蛇”黑产团伙（又名“银狐”、“谷堕大盗”、“UTG-Q-1000”等）组织活动频繁，攻击者采用搜索引擎 SEO 推广手段，伪造 Chrome 浏览器下载站。伪造站与正版官网高度相似，极具迷惑性。用户一旦误信并下载恶意安装包，游蛇远控木马便会植入系统。实现对目标设备的远程操控，盗取敏感数据等操作。通过跟踪监测发现其每日上线境内肉鸡数（以 IP 数计算）最多已超过 1.7 万。

“游蛇”自 2022 年下半年开始频繁活跃至今，针对国内用户发起了大量攻击活动，以图窃密和诈骗。该黑产团伙主要通过即时通讯软件（微信、企业微信等）、搜索引擎 SEO 推广、钓鱼邮件等途径传播恶意文件，其传播的恶意文件变种多、免杀手段更换频繁且攻击目标所涉及的行业广泛。

二、 攻击活动分析

攻击者搭建以“Chrome 浏览器”为诱饵的钓鱼网站，诱导受害者从网站下载恶意安装包。

图 1 钓鱼网站示例 1

图 2 钓鱼网站示例 2

攻击者搭建了多个钓鱼网站，下载时又跳转至多个下载链接，具体如下表所示。

表 1 钓鱼网络地址及恶意安装包下载地址

钓鱼网站	https[:]//google-chrom.cn（目前下载按钮失效）
	http[:]//google-chrom.cn（目前下载按钮失效）
	https[:]//chrome-html.com（目前下载按钮存活）
	https[:]//am-666.com（目前已无法访问）
	https[:]//chrome-admin.com/（目前下载按钮存活）

恶意安装包下载链接	https[:]//zhcn.down-cdn.com/chromex64.zip（目前失效）
	https[:]//cdn.downoss.com/chromex64.zip（目前存活）
	https[:]//oss.downncdn.com/chromex64.zip（目前存活）
	https[:]//cdn-kkdown.com/chromex64.zip（目前存活）

下载的恶意安装包是以“chromex64.zip”命名的压缩包文件。

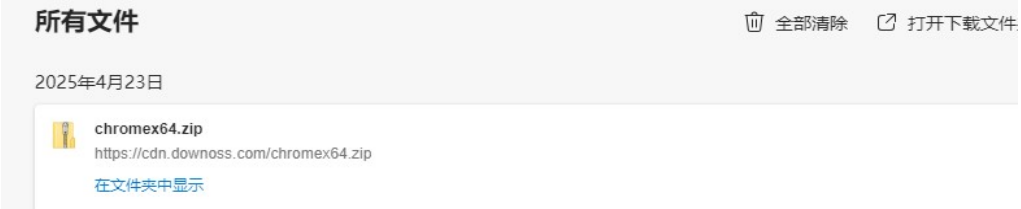

图 3 下载的恶意安装包

压缩包存在两个文件，其中 chromex64.exe 是一个文件解压程序，另一个是正常的 dll 文件，但文件名以日月年格式命名，疑似恶意程序更新日期。

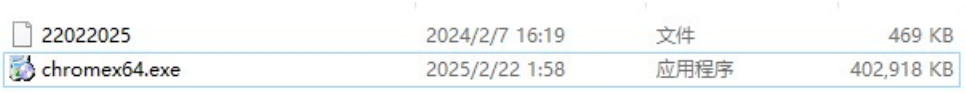

图 4 恶意安装包中的文件

chromex64.exe 运行后将默认在 C:\Chr0me_12.1.2 释放文件。其中包含旧版本 Chrome 浏览器相关文件，由于该软件不是正常安装，导致浏览器无法正常更新。

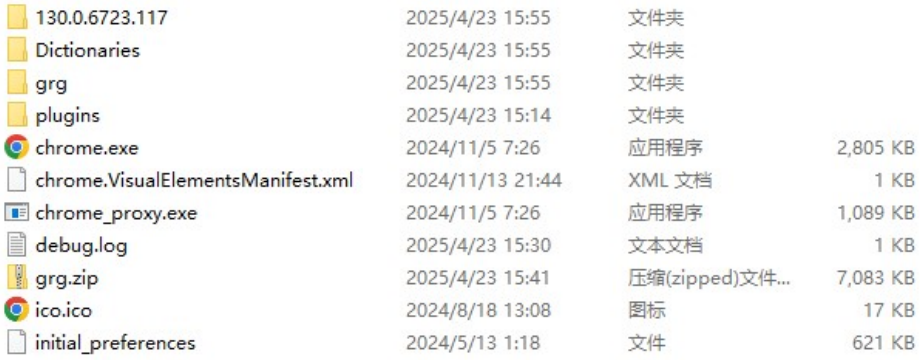

图 5 安装程序释放的文件

同时会解压程序在桌面创建快捷方式，但快捷方式中实际初始运行的是本次活动投放的恶意文件，携带参数运行，不仅启动自身，还启动 Chrome 浏览器进程，以掩盖该恶意快捷方式功能。

图 6 伪装的 Chrome 快捷方式

对应路径文件如下，采用 dll 侧加载（白+黑）形式执行。

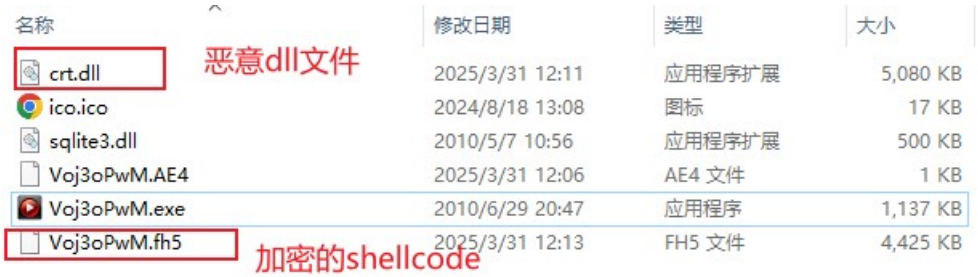

图 7 实际投放的恶意文件

在内存中解密并执行 shellcode，该 shellcode 实质为 dll 格式的 Gh0st 远控木马家族变种。

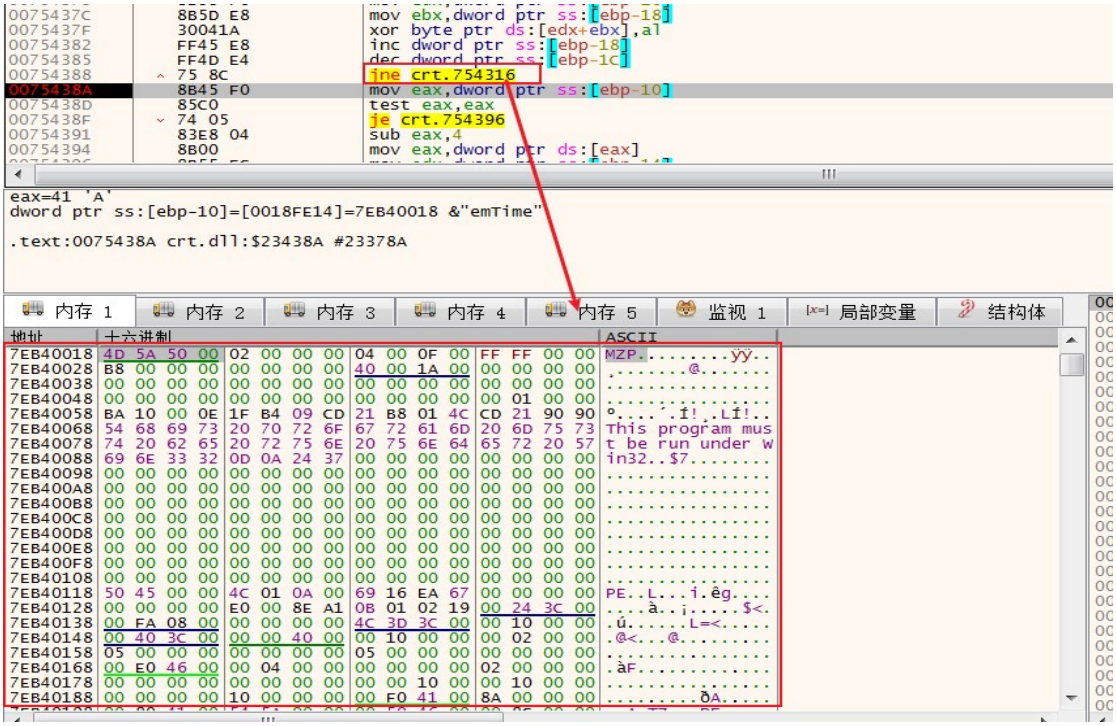

图 8 内存中的 Gh0st 运控木马

该 dll 加载后，连接 C2 地址 duooi.com:2869，其中的域名是 2025 年 2 月 19 日注册的，目前最新样本主要请求该域名。

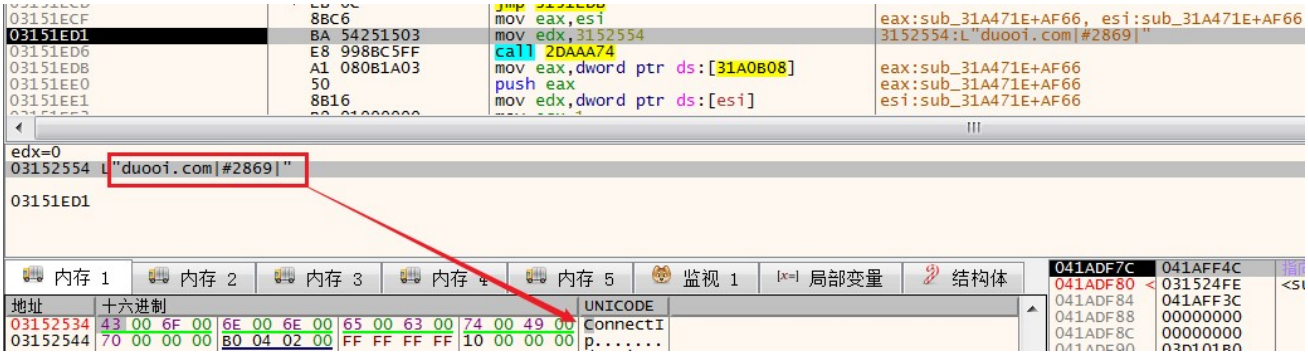

图 9 连接 C2 地址

基于情报关联域名解析的 IP 地址，发现攻击者基于任务持续注册域名，并硬编码至加密的 shellcode 文件中，部分旧有域名也更换 IP 地址，样本分析期间所有域名又更换了两次解析 IP 地址。

表 2 C2 域名变化

域名	注册时间	状态	解析 IP	解析 IP	解析 IP
hiluxo.com	2024 年 01 月 10 日	存活	104.233.164.131	61.110.5.21	137.220.131.139
titamic.com	2024 年 03 月 05 日	存活	104.233.164.131	61.110.5.21	137.220.131.140
golomee.com	2024 年 05 月 05 日	存活	104.233.164.131	61.110.5.21	137.220.131.140
simmem.com	2024 年 08 月 03 日	存活	104.233.164.131	61.110.5.21	137.220.131.139
duooi.com	2025 年 02 月 19 日	存活	104.233.164.131	61.110.5.21	137.220.131.139
sadliu.com	2025 年 03 月 03 日	存活	104.233.164.131	61.110.5.21	137.220.131.139

三、 样本对应的 ATT&CK 映射图谱

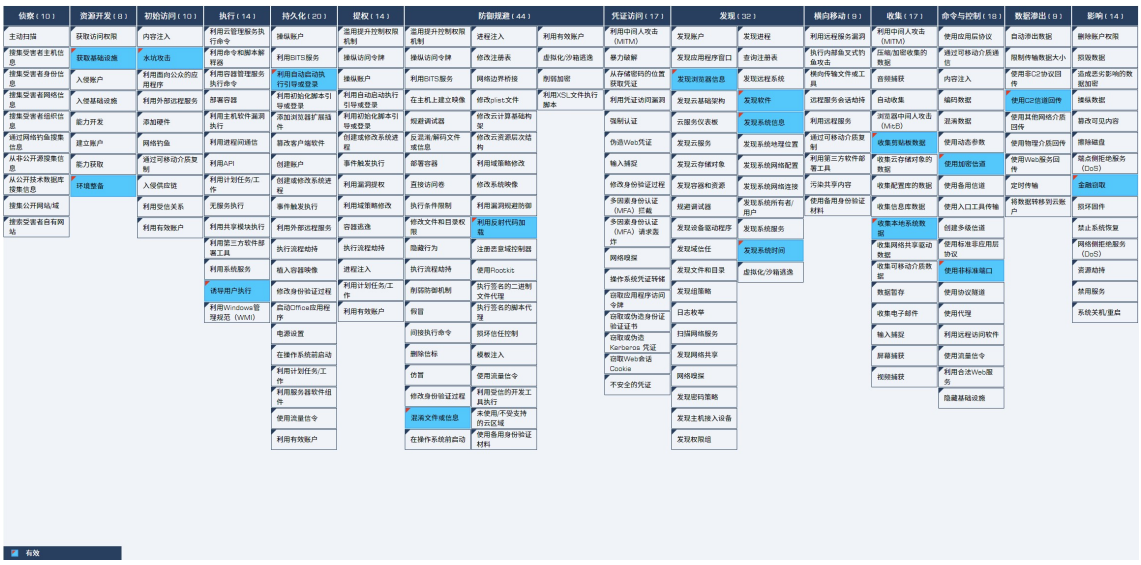

图 10 技术特点对应 ATT&CK 的映射

ATT&CK 技术行为描述表如下。

表 3 ATT&CK 技术行为描述表

ATT&CK 阶段/类别	具体行为	注释
资源开发	获取基础设施	获取服务器、注册域名
资源开发	环境整备	搭建钓鱼网站
初始访问	水坑攻击	构造钓鱼网站，诱导用户访问
执行	诱导用户执行	结合钓鱼网站诱导用户安装，并诱导用户执行恶意快捷方式
持久化	利用自动启动执行引导或登录	创建自启动项
防御规避	利用反射代码家族	动态内存加载恶意文件
	混淆文件或信息	加密 shellcode
发现	发现浏览器信息	遍历多种浏览器路径
	发现软件	探测反病毒软件
	发现系统时间	查看系统时间

	发现系统信息	获取系统信息
收集	收集剪贴板数据	窃取剪贴板数据
	收集本地系统数据	收集系统版本、时间、语言等信息
命令与控制	使用加密信道	与 C2 通信的内容加密
	使用非标准端口	远控木马使用 TCP 协议 2869 端口进行 C2 通信
数据渗出	使用 C2 信道回传	上线后回传系统信息
影响	金融窃取	修改数字货币转账的目的钱包地址，窃取数字货币

四、 感染规模

通过监测分析发现，于 2025 年 4 月 23 日至 5 月 12 日期间，“游蛇”黑产团伙使用的 Gh0st 远控木马日上线境内肉鸡数最高达到 1.7 万余台，C2 日访问量最高达到 4.4 万条，累计已有约 12.7 万台设备受其感染。每日境内上线肉鸡数情况如下。

图 11 每日上线境内肉鸡数

五、 防范建议

请广大网民强化风险意识，加强安全防范，避免不必要的经济损失，主要建议包括:

（1）建议通过官方网站统一采购、下载正版软件。如无

官方网站建议使用可信来源进行下载，下载后使用反病毒软件进行扫描并校验文件 HASH。

（2）尽量不打开来历不明的网页链接，不要安装来源不明软件。

（3）加强口令强度，避免使用弱口令，密码设置要符合安全要求，并定期更换。建议使用 16 位或更长的密码，包括大小写字母、数字和符号在内的组合，同时避免多个服务器使用相同口令。

（4）梳理已有资产列表，及时修复相关系统漏洞。

（5）安装终端防护软件，定期进行全盘杀毒。

（6）当发现主机感染僵尸木马程序后，立即核实主机受控情况和入侵途径，并对受害主机进行清理。

六、 相关 IOC

样本 MD5:

A1EAD0908ED763AB133677010F3B9BD7

ED74A6765F2FFEE35565395142D8B8B4

10FAC344D2F74D47FF79FE4A6D19765E

IP:

104[.]233.164.131

61[.]110.5.21

137[.]220.131.139

137[.]220.131.140

DOMAIN:

hiluxo[.]com

titamic[.]com

simmem[.]com

golomee[.]com

duooi[.]com

sadliu[.].com

URL:

http[:]//google-chrom.cn

https[:]//google-chrom.cn

https[:]//chrome-html.com

https[:]//am-666.com

https[:]//chrome-admin.com/

https[:]//zhcn.down-cdn.com/chromex64.zip

https[:]//cdn.downoss.com/chromex64.zip

https[:]//oss.downncdn.com/chromex64.zip

https[:]//cdn-kkdown.com/chromex64.zip