关于“黑猫”团伙利用搜索引擎传播捆绑远控木马的知名应用程序安装包的风险提示

本报告由国家互联网应急中心（CNCERT）与杭州安恒信息技术股份有限公司（安恒信息）共同发布。

一、 概述

近期，CNCERT 和安恒信息联合监测到由“黑猫”黑灰产团伙发起的针对性攻击。该团伙将包含钓鱼软件的恶意网站推送到搜索结果前列，并诱导搜索引擎错误地将部分钓鱼网站标注为“官方”，极大地增强了其欺骗性。用户在访问这些高排名或带有“官方”标签的钓鱼页面后，极有可能会下载捆绑恶意程序的安装包。一旦运行安装，该程序会在用户不知情的情况下植入远程控制木马，导致设备被攻击者控制。CNCERT 已协调搜索引擎厂商对部分钓鱼网站搜索结果进行处置。

二、 案例分析一

团伙将钓鱼网站的搜索引擎排名进行优化，通过国内某搜索引擎搜索关键词后，钓鱼网站排在第一位，且被打上了“官方”的标签。攻击者刻意使用与正版软件官网域名非常相似的域名，从而迷惑用户。进入钓鱼网站页面，能够发现网站内容与官网无异，通过详细比对发现攻击者直接对正版软件官方网站的主要页面进行了复制，并将下载地址按钮对应的链接修改为钓鱼软件链接。

钓鱼网站地址及恶意安装包下载地址如下表所示。

表 1 某钓鱼网站地址及恶意安装包下载地址

钓鱼网站	https://www.imqqd[.]com
恶意安装包下载链接	https://www.imqqd[.]com/qq_9.9.025311.zip（网页中央按钮）
	https://windqq.oss-ap-southeast-1.aliyuncs[.]com/windo-qq64.zip（网页其它位置按钮）
	https://kuaianlest.oss-ap-southeast-1.aliyuncs[.]com/qq_9.9.025311.zip（网页其它位置按钮）

从钓鱼网站首页下载的样本解压后信息如下:

表 2 某样本信息

文件名	qqdslgj.exe（解压后）
md5	f86ecc767faa13fd8dc55d51878d3cc6
文件格式	Inno Setup Module(6.0.0)
语言	Delphi

样本使用 Inno Setup 打包，解包后文件目录如下:

```
|   install_script.iss（Inno Setup 安装脚本）
├──dev-confi
|       QQ_9.9.17.31.exe
└──raw-j
        fgUSymqzvm.exe（加载 Y6vv.dll）
        rR40b.kw（加密的远控程序）
        Y6vv.dll（解密加载 rR40b.kw）
```

双击钓鱼软件后，在安装正版软件的同时，后台会运行 fgUSymqzvm.exe，该文件在运行时会加载 Y6vv.dll 文件，Y6vv.dll 文件使用 vmp 加壳。运行时首先会访问 fyat.mlcrosoft[.]cyou，该域名解析地址为 114.114.114[.]114，但该域名用途非远控地址，可能用于运行环境判定。随后会读取 rR40b.kw 文件并解密，解密过程如下:

（1） 文件中查找“IDAT”字符串。

（2） 将该字符串后 16 字节作为 RC4 秘钥。

（3） 将秘钥后 0x1ff0 个字节作为密文进行解密。

（4） 查找下一“IDAT”字符串，再次循环（2）（3）步骤。

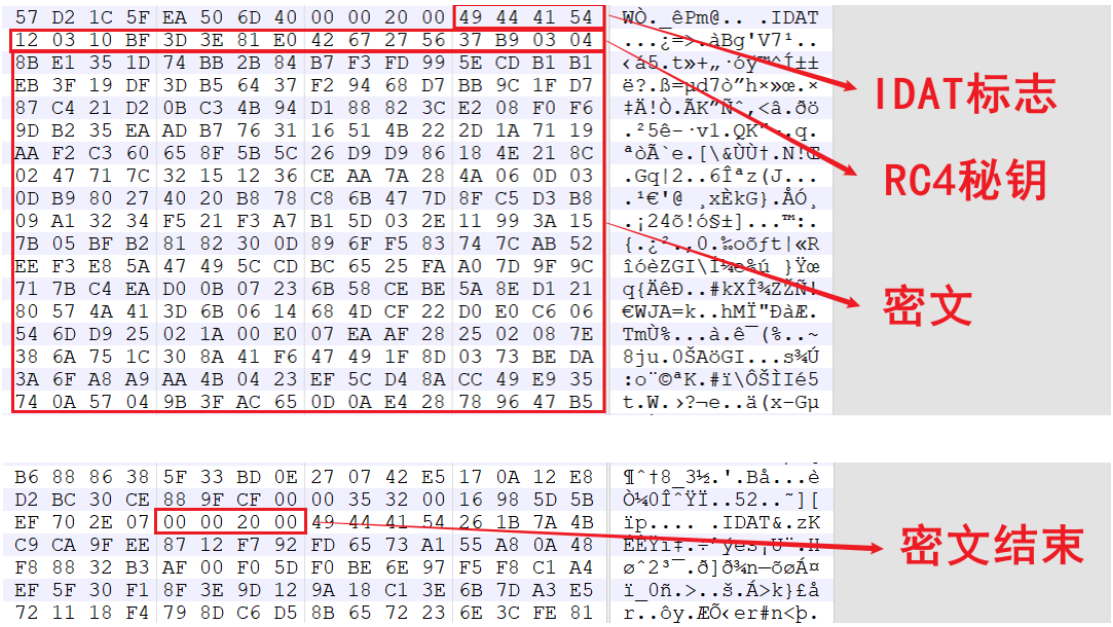

图 1 某加密载荷文件内容

rR40b.kw 文件解密后为远控木马。该恶意软件运行时会访问远控地址 xat.tk9885[.]com:45（域名解析 IP 地址为 202.79.175[.]117），实现后续恶意行为。

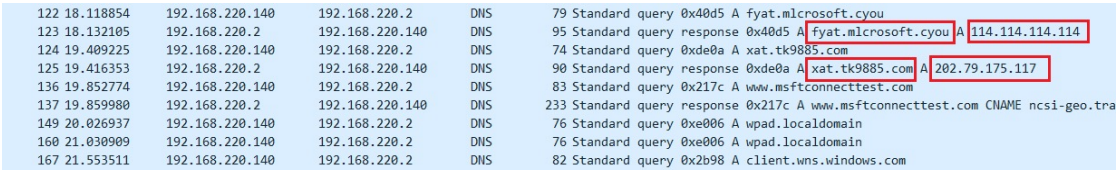

图 2 运行后远控木马回连 xat.tk9885[.]com

xat.tk9885[.]com 注册时间为 2025 年 4 月 3 日，有效期至 2026 年 4 月 3 日。经过检测，并未发现该域名有正常服务业务运行，判断其为攻击者注册的用于远控木马回连服务的恶意

域名。

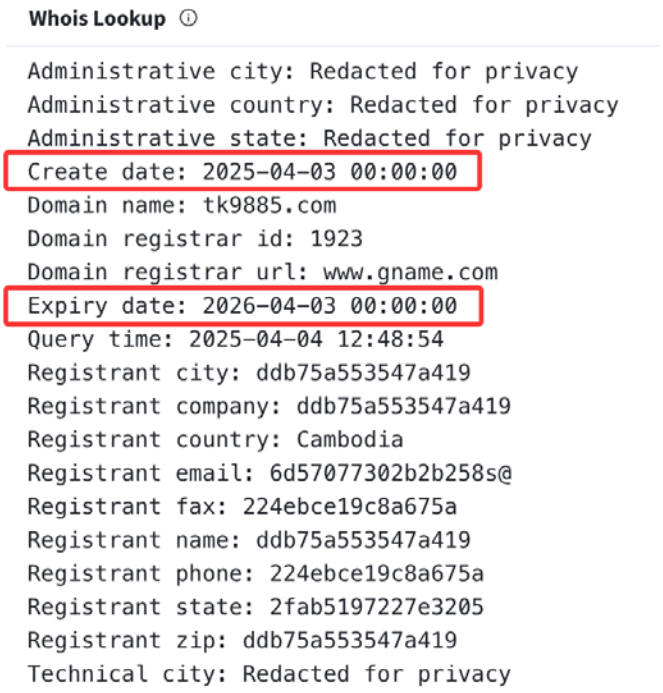

图 3 xat.tk9885[.]com 域名 Whois 查询结果

三、 案例分析二

类似的，团伙将仿冒网站的搜索引擎排名进行优化，在钓鱼网站中嵌入捆绑对应恶意程序的软件安装包下载地址。

表 3 某钓鱼网站地址及恶意安装包下载地址

钓鱼网站	i4.com[.]vn
恶意安装包下载链接	https://oss12318.oss-cn-hongkong.aliyuncs[.]com/i4aisizshou06.23.09.zip（“Win 版 64 位”、“Win 版 32 位”按钮）

从钓鱼网站首页下载的样本解压后信息如下:

表 4 某恶意样本信息

文件名	i4aisizshou06.23.09.exe（解压后）
md5	9d32902ad0d9f44e7f594d97d0fb88ab
文件格式	Inno Setup Module(6.4.3)

语言	Delphi

样本使用 Inno Setup 打包，解包后文件目录如下:

```
├─external
|        i4Tox64. exe
└─exter
stQkSAAC. exe（加载 KpKUt8. dll）
osZswz6. T0（加密的远控程序）
KpKUt8. dll（解密加载 osZswz6. T0）
```

双击钓鱼软件后，在安装正版软件的同时，后台会运行 stQkSAAC.exe，该文件在运行时会加载 KpKUt8.dll 文件。运行时首先访问 fymaimai.mlcrosoft[.]asia，该域名解析地址为 114.114.114[.]114，但域名用途非远控地址，可能用于运行环境判断。随后会读取 osZswz6.T0 文件并解密，解密过程如下:

（1） 文件中查找“IDAT”字符串。

（2） 将该字符串后 16 字节作为 RC4 秘钥。

（3） 将秘钥后 0x1ff0 个字节作为密文进行解密。

（4） 查找下一“IDAT”字符串，再次循环（2）（3）步骤。

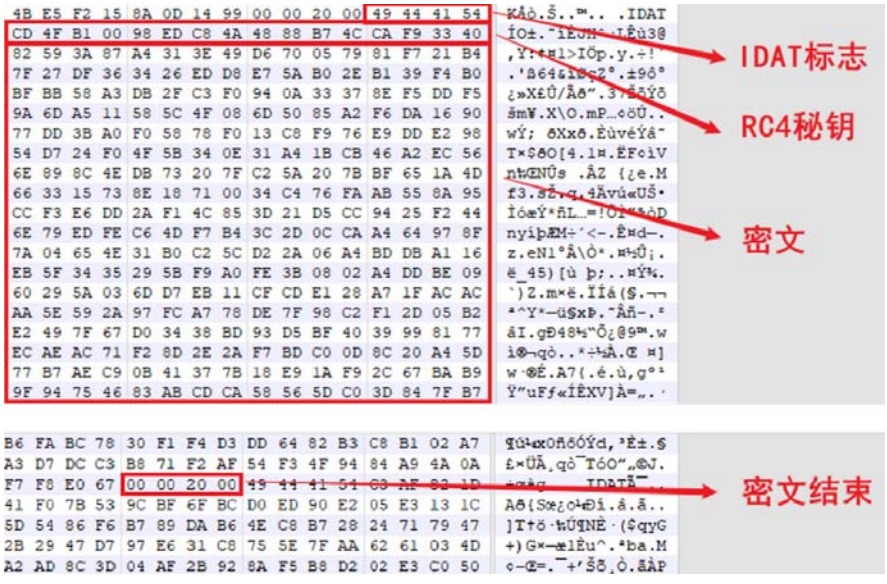

图 4 某载荷加密方式图解

osZswz6.T0 文件解密后为远控木马。该恶意软件运行时会访问远控地址 mm.opi6qi5k[.]com（域名解析 IP 地址为 143.92.60[.]214），实现后续恶意行为。

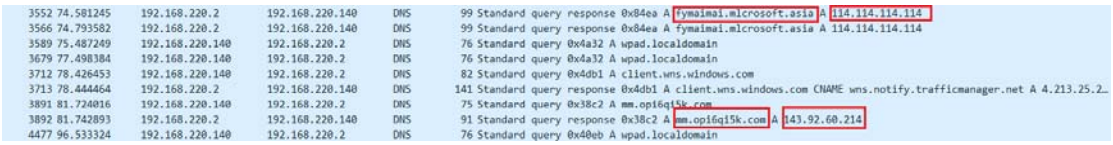

图 5 运行后远控木马回连 mm.opi6qi5k[.]com

mm.opi6qi5k[.]com 注册时间为 2025 年 2 月 2 日，有效期至 2026 年 2 月 2 日。经过检测，并未发现该域名有正常服务业务运行，判断其为攻击者注册的用于远控木马回连服务的恶意域名。

图 6 mm.opi6qi5k[.]com 域名 Whois 查询结果

四、 感染规模

通过监测分析发现，我国境内于 2025 年 6 月 1 日至 7 月 28 日期间，“黑猫”黑灰产团伙通过案例一木马投放导致主机被控数量约 2.88 万台，境内日上线肉鸡数量最高达 2328 台，肉鸡 C2 日访问量最高达 18913 次。境内日上线肉鸡数量

情况如下图所示。

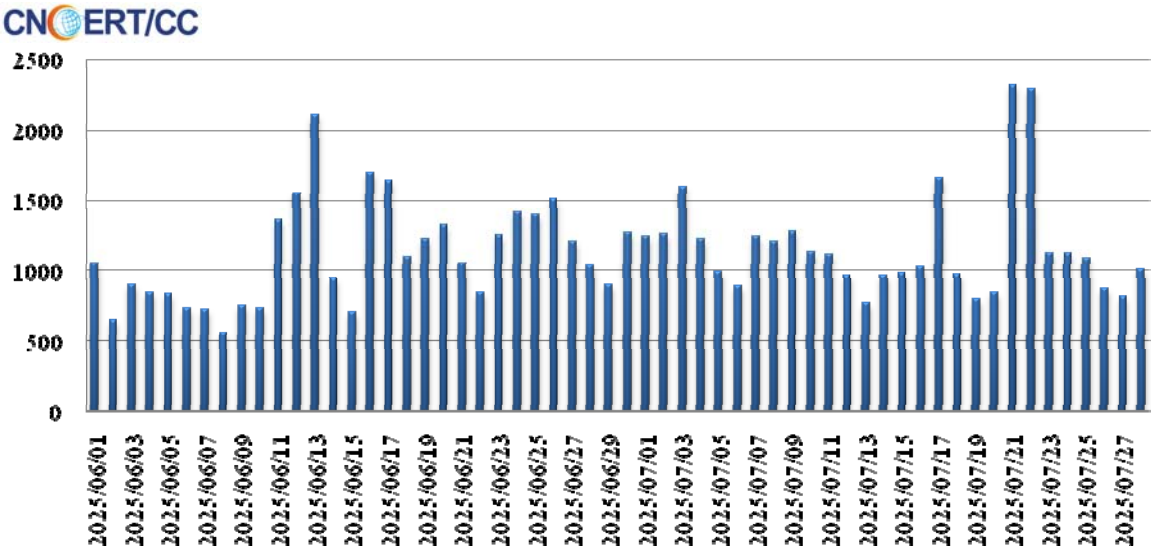

图 7 境内日上线肉鸡数量分布情况

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）安装终端防护软件，定期进行全盘杀毒。

（4）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

钓鱼网站地址:

www.imqqd[.]com

i4.com[.]vn

钓鱼软件下载地址:

https://www.imqqd[.]com/qq_9.9.025311.zip

https://windqq.oss-ap-southeast-1.aliyuncs[.]com/windo-qq64.zip

https://kuaianlest.oss-ap-southeast-1.aliyuncs[.]com/qq_9.9.025311.zip

https://oss12318.oss-cn-hongkong.aliyuncs[.]com/i4aisizshou06.23.09.zip

回连地址:

fyat.mlcrosoft[.]cyou

fymaimai.mlcrosoft[.]asia

C2 地址:

xat.tk9885[.]com

202.79.175[.]117

mm. opi6qi5k[.]com

143.92.60[.]214

样本 **HASH**:

f86ecc767faa13fd8dc55d51878d3cc6

9d32902ad0d9f44e7f594d97d0fb88ab