

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 密钥。
- (3) 将密钥后 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。

57 D2 1C 5F EA 50 6D 40 00 00 20 00	49 44 41 54	W0. ePm@... IDAT	
12 03 10 BF 3D 3E 81 E0 42 67 27 56 37 B9 03 04		... ?= aBg'v7^..	
8B E1 35 1D 74 BB 2B 84 B7 F3 FD 99 5E CD B1 B1		< a5.t>+,, 'dy'af++	
EB 3F 19 DF 3D B5 64 37 F2 94 68 D7 BB 9C 1F D7		è?. ß=ad7ò"hx»æ. x	
87 C4 21 D2 0B C3 4B 94 D1 88 82 3C E2 08 F0 F6		†A!Ò.ÄK'N<, <a.ðö	
9D B2 35 EA AD B7 76 31 16 51 4B 22 2D 1A 71 19		.²5è- vl.QK' .q.	
AA F2 C3 60 65 8F 5B 5C 26 D9 D9 86 18 4E 21 8C		ªðÄ`e. [\&ÜÜ†.N!E	
02 47 71 7C 32 15 12 36 CE AA 7A 28 4A 06 0D 03		.Gq 2..6îªz (J...	
0D B9 80 27 40 20 B8 78 C8 6B 47 7D 8F C5 D3 B8		.¹e'@ ,xEkG}.ÄÖ,	
09 A1 32 34 F5 21 F3 A7 B1 5D 03 2E 11 99 3A 15		.;24ö!óS±]...™:.	
7B 05 BF B2 81 82 30 0D 89 6F F5 83 74 7C AB 52		{.¿. 0. %oöft «R	
EE F3 E8 5A 47 49 5C CD BC 65 25 FA A0 7D 9F 9C		îóèZGI\Iæ&ú }ÿœ	
71 7B C4 EA D0 0B 07 23 6B 58 CE BE 5A 8E D1 21		q{ÄèÐ...#kXîªZzÑ!	
80 57 4A 41 3D 6B 06 14 68 4D CF 22 D0 E0 C6 06		EWJA=k...hMÍ"DaE.	
54 6D D9 25 02 1A 00 E0 07 EA AF 28 25 02 08 7E		TmÜ%...à.è~ (%...~	
38 6A 75 1C 30 8A 41 F6 47 49 1F 8D 03 73 BE DA		8ju.0ŠAöGI...s³ú	
3A 6F A8 A9 AA 4B 04 23 EF 5C D4 8A CC 49 E9 35		:o"®ªK.#ÿ\ÖŠÏIé5	
74 0A 57 04 9B 3F AC 65 0D 0A E4 28 78 96 47 B5		t.W. >?-e...ä (x-Gp	

IDAT标志
RC4密钥
密文

B6 88 86 38 5F 33 BD 0E 27 07 42 E5 17 0A 12 E8	¶†8 3½.'.Bá...è	
D2 BC 30 CE 88 9F CF 00 00 35 32 00 16 98 5D 5B	Ö¼0î~ÿÏ...52...~][
EF 70 2E 07 00 00 20 00 49 44 41 54 26 1B 7A 4B	ÿp.... IDAT&.zK	
C9 CA 9F EE 87 12 F7 92 FD 65 73 A1 55 A8 0A 48	EEÿ†.ª=ÿes Ü`H	
F8 88 32 B3 AF 00 F0 5D F0 BE 6E 97 F5 F8 C1 A4	ø^2³~.ð]ð³m-öøÄª	
EF 5F 30 F1 8F 3E 9D 12 9A 18 C1 3E 6B 7D A3 E5	ÿ_öñ.>...š.Ä>k}fâ	
72 11 18 F4 79 8D C6 D5 8B 65 72 23 6E 3C FE 81	r...öy.ÈÖ<er#n<p.	

密文结束

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。

122 18.118854	192.168.220.140	192.168.220.2	DNS	79 Standard query 0x40d5 A fyat.mlcrosoft.cyou
123 18.132105	192.168.220.2	192.168.220.140	DNS	95 Standard query response 0x40d5 A fyat.mlcrosoft.cyou A 114.114.114.114
124 19.409225	192.168.220.140	192.168.220.2	DNS	74 Standard query 0xde0a A xat.tk9885.com
125 19.416353	192.168.220.2	192.168.220.140	DNS	90 Standard query response 0xde0a A xat.tk9885.com A 202.79.175.117
136 19.852774	192.168.220.140	192.168.220.2	DNS	83 Standard query 0x217c A www.msftconnecttest.com
137 19.859980	192.168.220.2	192.168.220.140	DNS	233 Standard query response 0x217c A www.msftconnecttest.com CNAME ncsi-geo.tra
149 20.026937	192.168.220.140	192.168.220.2	DNS	76 Standard query 0xe006 A wpad.localdomain
160 21.030909	192.168.220.140	192.168.220.2	DNS	76 Standard query 0xe006 A wpad.localdomain
167 21.553511	192.168.220.140	192.168.220.2	DNS	82 Standard query 0x2b98 A client.wms.windows.com

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。

```
Whois Lookup ⓘ  
Administrative city: Redacted for privacy  
Administrative country: Redacted for privacy  
Administrative state: Redacted for privacy  
Create date: 2025-04-03 00:00:00  
Domain name: tk9885.com  
Domain registrar id: 1923  
Domain registrar url: www.gname.com  
Expiry date: 2026-04-03 00:00:00  
Query time: 2025-04-04 12:48:54  
Registrant city: ddb75a553547a419  
Registrant company: ddb75a553547a419  
Registrant country: Cambodia  
Registrant email: 6d57077302b2b258s@  
Registrant fax: 224ebce19c8a675a  
Registrant name: ddb75a553547a419  
Registrant phone: 224ebce19c8a675a  
Registrant state: 2fab5197227e3205  
Registrant zip: ddb75a553547a419  
Technical city: Redacted for privacy
```

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 密钥。
- (3) 将密钥后 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。

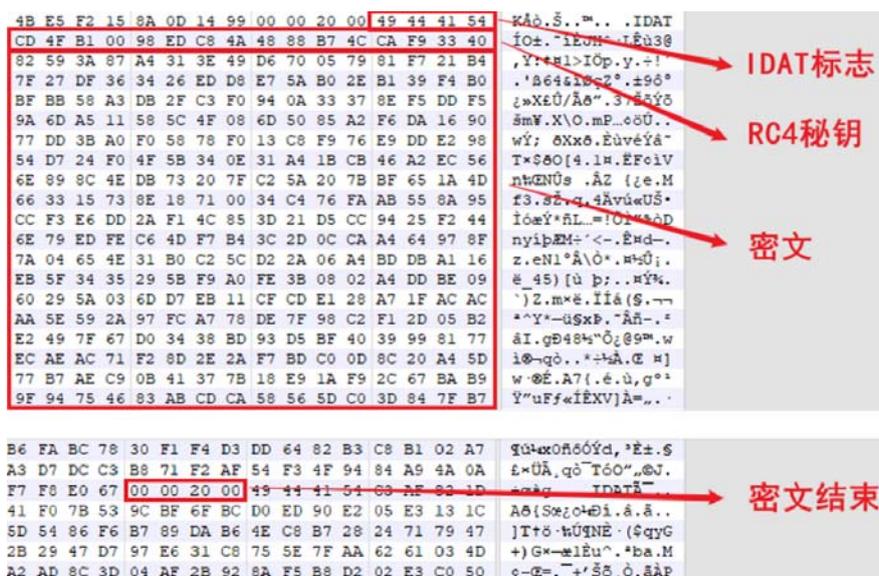


图 4 某载荷加密方式图解

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。

```
3552 74.581245 192.168.220.2 192.168.220.140 DNS 99 Standard query response 0x84ea A fymaimi.microsoft.asia A 114.114.114.114
3566 74.793582 192.168.220.2 192.168.220.140 DNS 99 Standard query response 0x84ea A fymaimi.microsoft.asia A 114.114.114.114
3589 75.487249 192.168.220.140 192.168.220.2 DNS 76 Standard query 0x4a32 A upad.localdomain
3679 77.498384 192.168.220.140 192.168.220.2 DNS 76 Standard query 0x4a32 A upad.localdomain
3712 78.426453 192.168.220.140 192.168.220.2 DNS 82 Standard query 0x4db1 A client.wms.windows.com
3713 78.444464 192.168.220.2 192.168.220.140 DNS 141 Standard query response 0x4db1 A client.wms.windows.com CNAME wms.notify.trafficmanager.net A 4.213.25.2...
3891 81.724016 192.168.220.140 192.168.220.2 DNS 75 Standard query 0x38c2 A mm.opi6qi5k.com
3892 81.742893 192.168.220.2 192.168.220.140 DNS 91 Standard query response 0x38c2 A mm.opi6qi5k.com A 143.92.60.214
4477 96.533324 192.168.220.140 192.168.220.2 DNS 76 Standard query 0x40eb A upad.localdomain
```

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。

Whois Lookup

```
Create date: 2025-02-02 00:00:00
Domain name: opi6qi5k.com
Domain registrar id: 1923
Domain registrar url: http://www.gname.com
Expiry date: 2026-02-02 00:00:00
Name server 1: gabriella.ns.cloudflare.com
Name server 2: johnathan.ns.cloudflare.com
Query time: 2025-02-03 12:49:51
Update date: 2025-02-03 00:00:00
```

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。

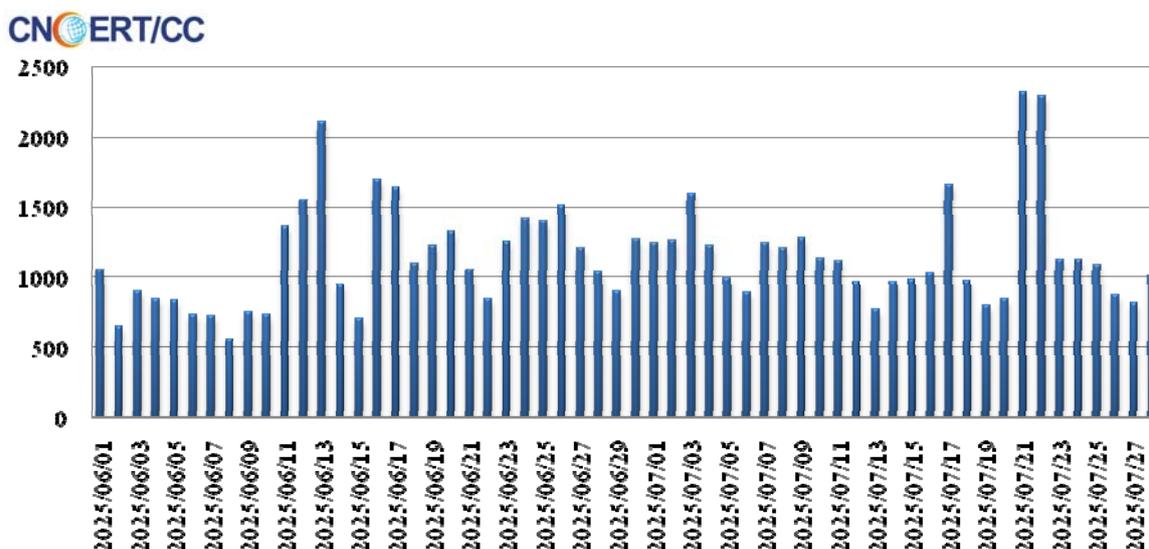


图 7 境内日上线肉鸡数量分布情况

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

[https://windqq.oss-ap-southeast-1.aliyuncs\[.\]com/windo-qq64.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://kuaianlest.oss-ap-southeast-1.aliyuncs[.]com/qq_9.9.025311.zip)

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

回连地址:

fyat.mlicrosoft[.]cyou

fymaimai.mlicrosoft[.]asia

C2 地址:

xat.tk9885[.]com

202.79.175[.]117

mm. opi6qi5k[.]com

143.92.60[.]214

样本 **HASH:**

f86ecc767faa13fd8dc55d51878d3cc6

9d32902ad0d9f44e7f594d97d0fb88ab