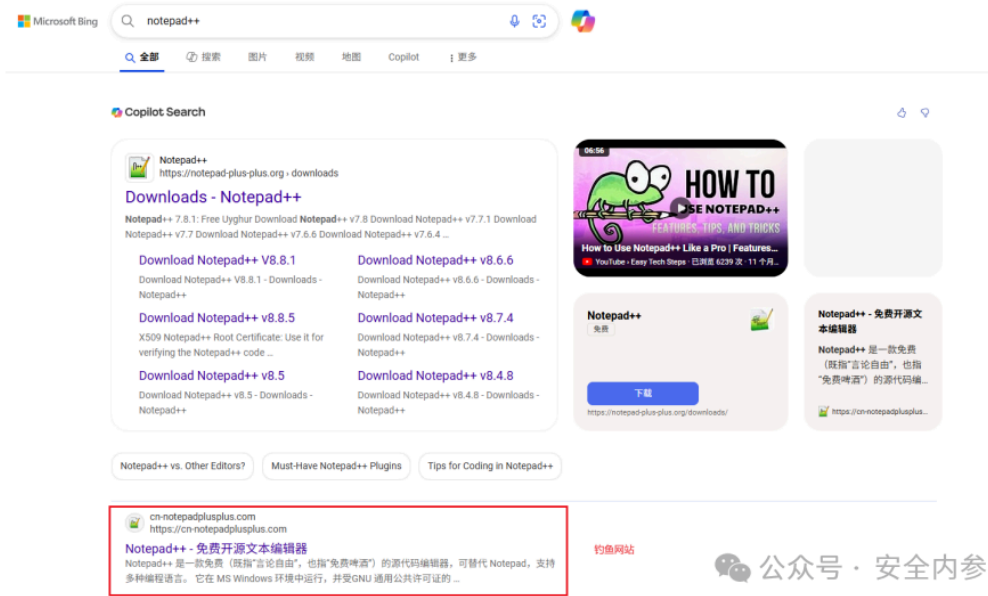


CNCERT：关于“黑猫”团伙利用搜索引擎传播仿冒Notepad++下载远控后门的风险提示

mp.weixin.qq.com/s

CNCERT



2026年1月5日 04:17

Editor's Note

仿冒Notepad++下载远控后门会在用户不知情的情况下植入后门木马，导致主机敏感数据被攻击者窃取。

国家互联网应急中心CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称CNCERT或CNCERT/CC），成立于2001年8月，为非政府非盈利的网络安全技术中心，是中国计算机网络应急处理体系中的牵头单位。

一、概述

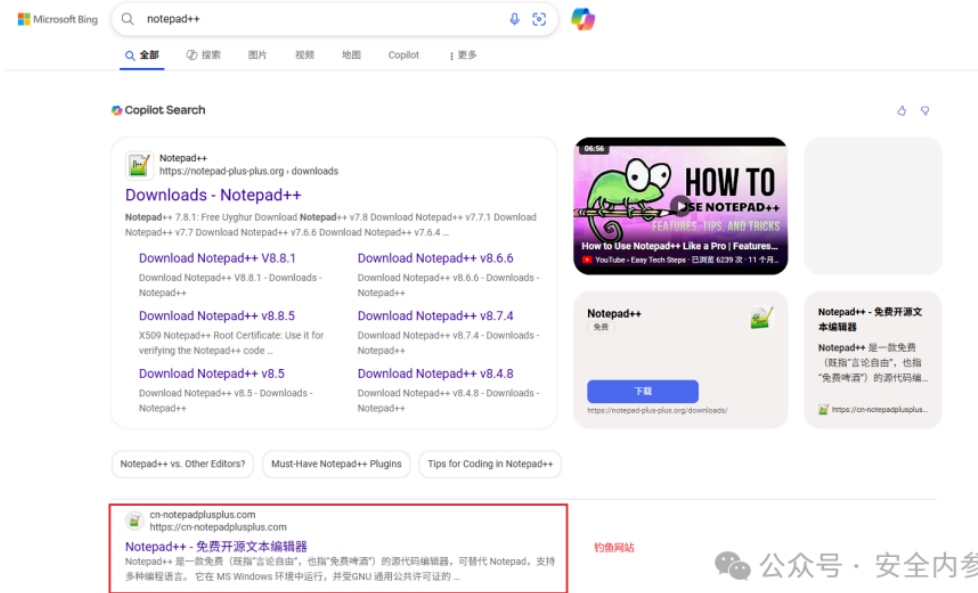


图1 钓鱼网站在搜索引擎结果排行

“黑猫”黑产团伙最早攻击活动能追溯至22年，是一个主要目标为窃密远控的黑产团伙。该团伙的常见手法就是通过部署钓鱼网站，并在搜索引擎进行投递，向用户传播窃密木马以窃取用户主机信息。23年该团伙通过仿冒AICoin（虚拟货币行情交易平台）虚假下载网站，窃取了价值不低于16万美金的虚拟货币。24年该团伙通过搜索引擎SEO技术在Bing搜索引擎投递了仿冒Chrome浏览器钓鱼页面诱导用户点击安装，在受害者主机上释放了窃密程序，并一同释放挖矿程序进行挖矿。25年6月该团伙利用国内某知名搜索引擎投递了QQ国际版、爱思助手等软件的仿冒程序，诱导用户安装传播窃密程序。

近期，“黑猫”团伙的攻击活动依旧猖獗，并进一步向普通网民进行传播。

二、案例分析

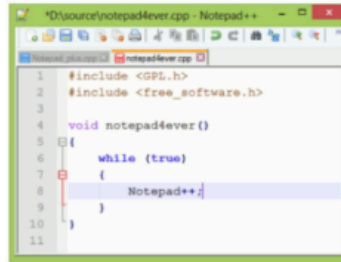
“黑猫”团伙将精心构造的钓鱼网站的在搜索引擎排名进行优化，用户通过在搜索引擎搜索关键词Notepad++后，访问了搜索引擎排行第二的搜索结果，实际为“黑猫”团伙构造的钓鱼网站，经过诱导下载后，用户下载了含有后门程序的软件安装包，安装后会释放后门文件，从而被攻击者远控。

在本次钓鱼攻击活动中，“黑猫”团伙构造了非常拟真的钓鱼网站，而不是从官网进行复制，在钓鱼网站的内容中，除了包含下载链接外，还有很多教程文章来增强钓鱼网站的可信度：



什么是 Notepad++ ?

Notepad++ 是一款免费（既指“言论自由”，也指“免费啤酒”）的源代码编辑器，可替代 Notepad，支持多种编程语言。它在 MS Windows 环境中运行，并受GNU 通用公共许可证的约束。



Notepad++ 基于强大的编辑组件 Scintilla，采用 C++ 编写，并使用纯 Win32 API 和 STL，从而确保更高的执行速度和更小的程序大小。通过在不牺牲用户友好性的前提下尽可能地优化例程，Notepad++ 致力于减少全球二氧化碳排放量。当 CPU 功耗较低时，PC 可以降低运行速度并降低功耗，从而创造更环保的环境。

Notepad++ 下载:

立即下载

近期

- 1: notepad plus是什么软件
- 2: linux notepadqq怎么安装
- 3: ise如何关联notepad++
- 4: IAR怎么调用Notepad++
- 5: linux下类似notepad++好用的文本
- 6: notepad plus是什么

往期

- 1: notepad plus是什么软件
- 2: ise如何关联notepad++
- 3: linux notepadqq怎么安装
- 4: notepad plus是什么
- 5: linux下类似notepad++好用的文本
- 6: IAR怎么调用Notepad++
- 7: Notepad++ 7.6.5开始使用GPG签名认证
- 8: Notepad Plus 32位是什么软件
- 9: Notepad++ 在开头和结尾添加内容
- 10: linux如何安装notepad++

公众号 · 安全内参

图2 钓鱼网站页面

用户后续点击页面的立即下载按钮并不直接跳转下载文件链接，而是一个常见下载页面，选择下载方式或者下载文件内容，但实际这些链接都指向一个地址：



Notepad++ 最新下载

Notepad++ 是一款功能强大的文本编辑器，支持正则表达式和插件扩展。如果您需要替代软件，可以考虑 Notepad 或 Notepad3。

从第三方下载 Notepad++ :

设备	下载
Win 64位安装包 v8.8.5	下载ZIP
Win 32位安装包 v8.8.5	下载ZIP
ARM 安装包 v8.8.5	点击下载

最新版本: v8.8.5
更新时间: 2025-08-14
软件大小: 6.5MB

更新说明:
安全与基础优化

1. 二进制文件自签名，修复卸载/安装程序安全问题 (CVE-2025-49144)，增强 DLL 加载安全
2. 更新 WinGUp 的 cURL 至 8.13.0，修复其安全漏洞 (CVE-2025-0167)
3. 升级至 scintilla 5.5.7 和 Lexilla 5.4.5

问题修复

公众号 · 安全内参

图3 钓鱼网站下载跳转页面

点击再次跳转到仿冒的下载地址，这个下载地址和页面伪装为了知名开源网站Github的风格来迷惑用户，实际为“黑猫”团伙精心构造的下载钓鱼页面：

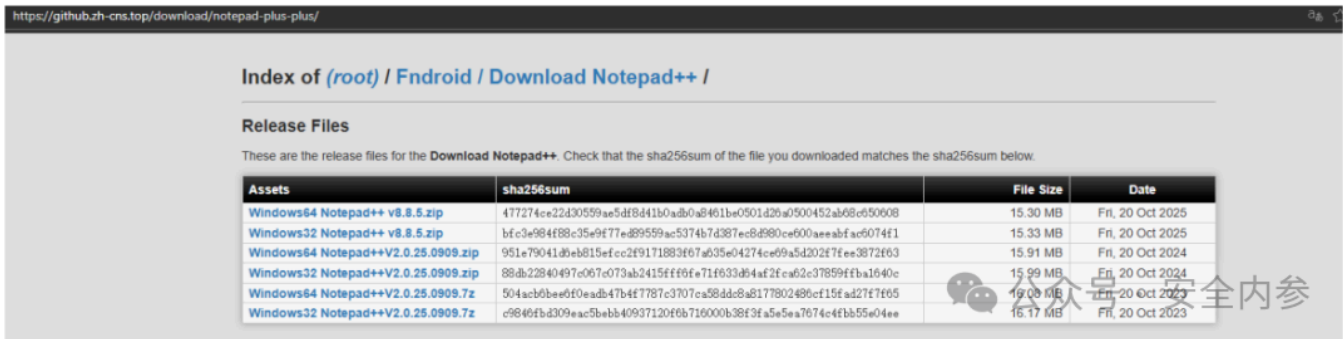


图4 钓鱼网站仿冒下载页面

此时点击才会下载携带后门文件的软件安装程序，经过多次跳转和部署的拟真钓鱼页面，受害者已经降低对该网站的怀疑，黑猫团伙也在此过程中使用了高度相似的钓鱼网站域名：

域名	属性
notepadplusplus. cn	钓鱼域名，仿冒 Notepad++软件
clash. net. cn	钓鱼域名，仿冒 clash 软件
clash. ac. cn	钓鱼域名，仿冒 clash 软件
cn-notepadplusplus. com	钓鱼域名，仿冒 Notepad++软件
zh-clash. com	钓鱼域名，仿冒 Clash 软件
clashforwindows. org. cn	中间跳转页面钓鱼域名
github. zh-cns. top	中间下载页面钓鱼域名
*. cdn-ccdwn. com	下载文件链接域名

表1 “黑猫”团伙本次钓鱼相关网站

从钓鱼网站下载的样本信息如下：

Sha256	b94c54290015ed751c84d0a9bfa6e63481c72c0d7528b4b65a2816f72ea5c994
文件名称	Notepad++. zip
文件大小	16. 17MB
文件类型	ZIP 压缩文件
文件来源	https://cn-notepadplusplus.com/
文件下载链接	https://m76.cdn-ccdown.com/Notepad++. zip
文件功能描述	伪装 Notepad++ 安装程序，在安装目录下存在白加黑恶意组件，在桌面释放快捷方式指向白加黑恶意组件，组件运行后加载解密后续恶意 DLL，连接 C2 并传输主机剪切板数据，键盘记录数据，浏览器数据，然后运行 Notepad++ 正常软件程序。

表2 “黑猫”团伙投递样本信息

样本初始载荷伪装为Notepad++安装包：

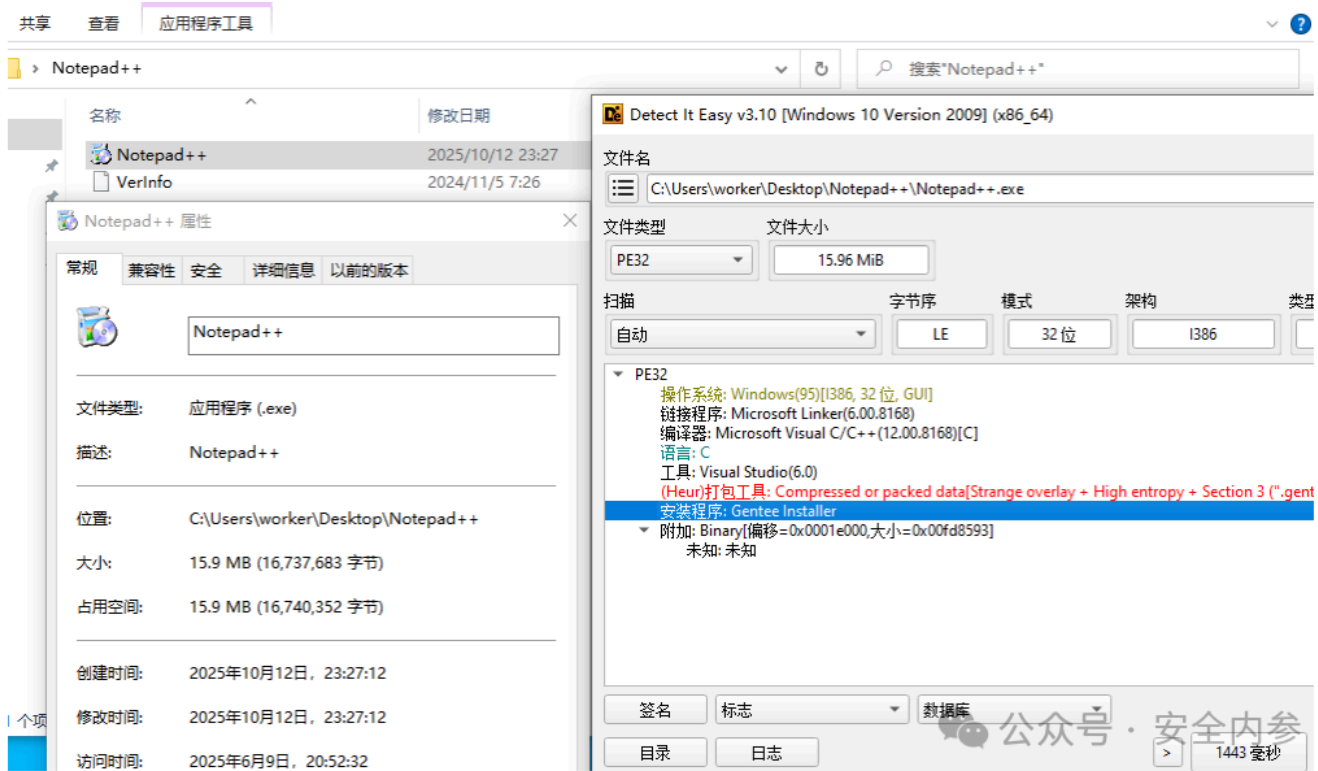


图5 软件初始安装程序

程序安装完成后，后门组件不会直接执行，而是通过在桌面生成快捷方式，而快捷方式指向后门组件入口：

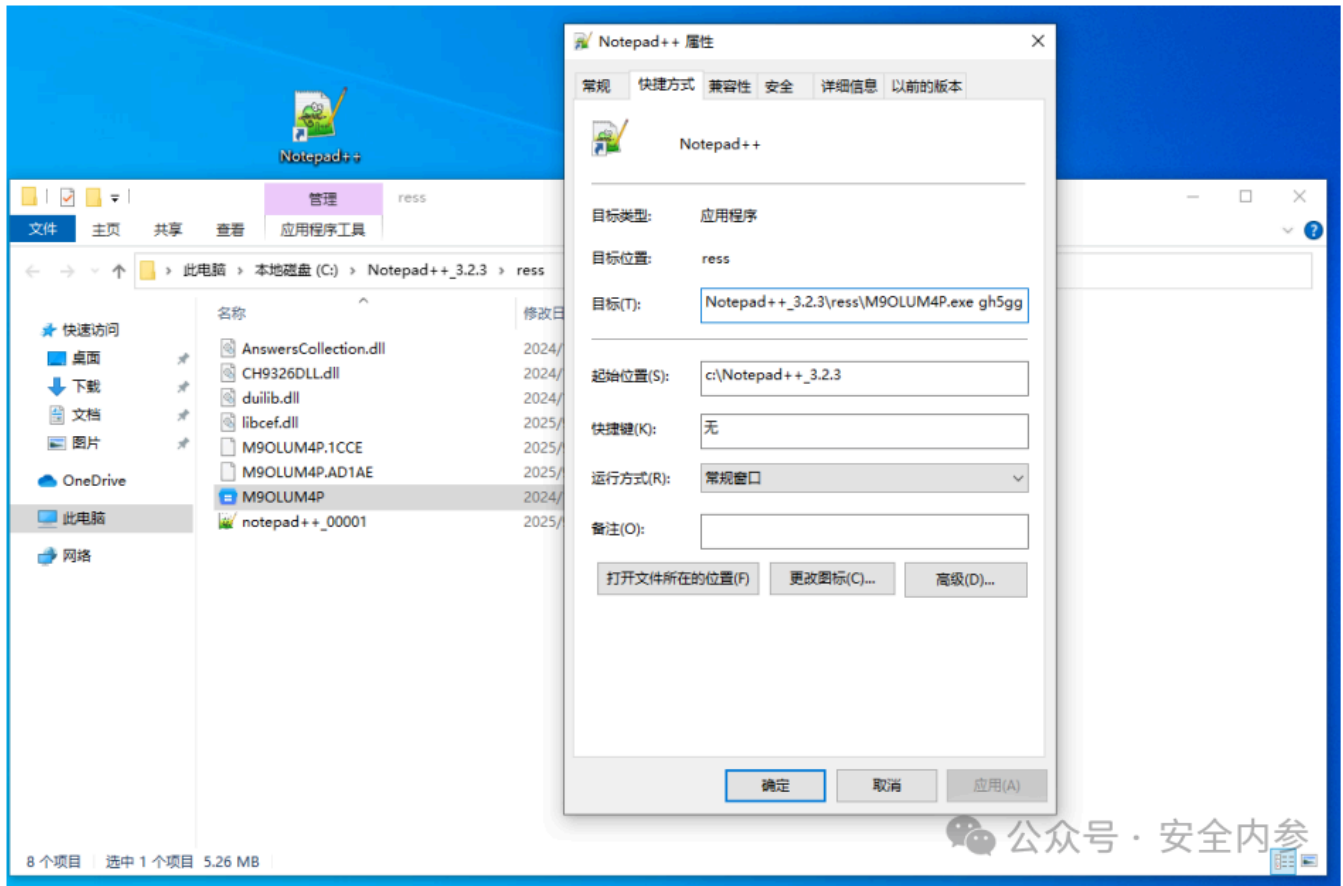


图6 安装后桌面生成快捷方式

该后门程序通过白加黑执行恶意dll：



图7 后门白加黑组件

通过读取M9OLUM4P.1CCE文件进行解密：

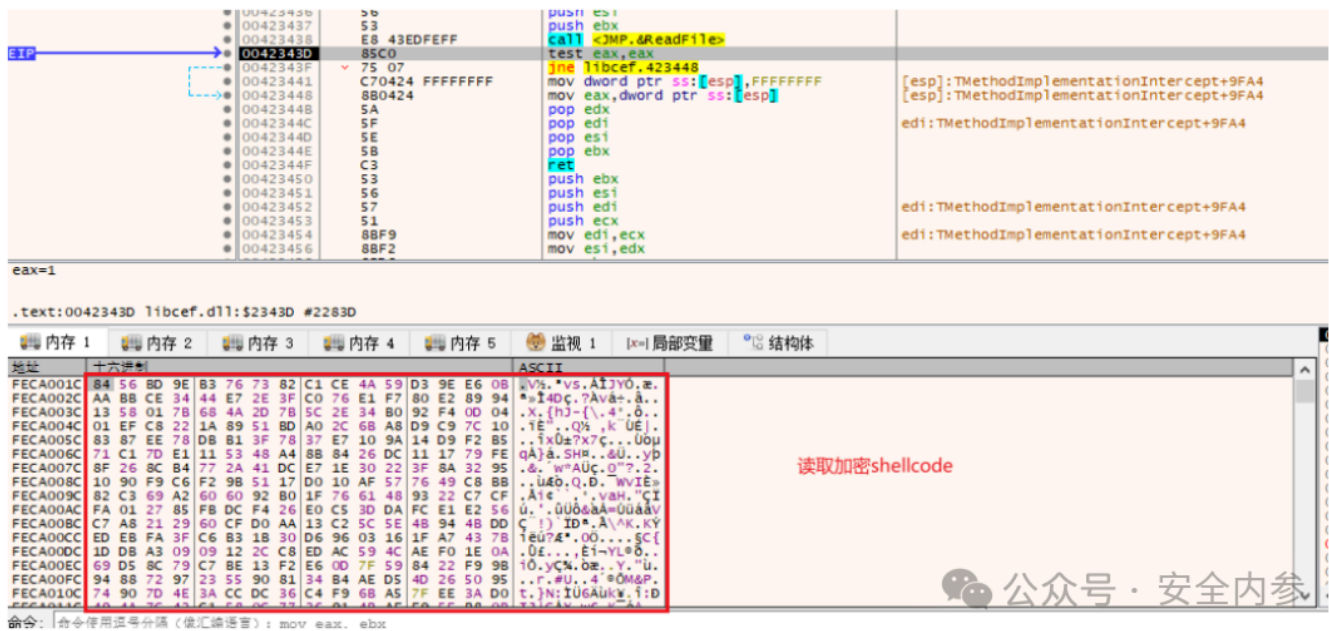


图8 恶意DLL文件尝试读取加密文件

解密后实际为PE文件，后门通过反射加载该PE文件执行：



图9 恶意DLL文件对加密文件进行解密执行

对解密文件进行分析，文件首先查看注册表是否存在相关配置：

```

Get_Config_From_HKEY(
    HKEY_CURRENT_USER,
    *(_DWORD *)SOFTWARE_FGHGE2E61DDSF,
    (int)L"InjectProcess",
    (int *)&v46,
    (int)L"No");
v2 = drg_check_contain_Yes(v46, a1);
Get_Config_From_HKEY(HKEY_CURRENT_USER, *(_DWORD *)SOFTWARE_FGHGE2E61DDSF, (int)L"OffKeyLog", (int *)&v45, (int)L"No");
v51 = drg_check_contain_Yes(v45, v2);
Get_Config_From_HKEY(
    HKEY_CURRENT_USER,
    *(_DWORD *)SOFTWARE_FGHGE2E61DDSF,
    (int)L"CopyUSBDeviceFiles",
    (int *)&v44,
    (int)L"No");
v48 = drg_check_contain_Yes(v44, v2);
Get_Config_From_HKEY(
    HKEY_CURRENT_USER,
    *(_DWORD *)SOFTWARE_FGHGE2E61DDSF,
    (int)L"ShareExclusive",

```

公众号 · 安全内参

图10 恶意程序读取注册表内预设的配置信息

创建相关字符串：

```

idr619347__UStrCat3((int)L"\\klogs", *(void **)off_2D568F8, v27);
idr619347__UStrCat3((int)L"\\slogs", *(void **)off_2D568F8, v28);
idr619347__UStrCat3((int)L"\\plugins", *(void **)off_2D568F8, v29);
idr619347__UStrCat3((int)L"\\usbfiles", *(void **)off_2D568F8, v30);
idr619347__UStrCat3((int)L"\\MnemonicWord", *(void **)off_2D568F8, v31);

```

图11 恶意程序设置存储窃密数据目录

创建相关目录：

<< 用户 > worker > AppData > Roaming > M9OLUM4P > Default >				
名称	修改日期	类型	大小	
klogs	2025/6/9 21:14	文件夹		
plugins	2025/6/9 21:14	文件夹		
slogs	2025/6/9 21:14	文件夹		

公众号 · 安全内参

图12 恶意程序创建窃密数据存储目录

通过注册表创建自启动项：

```
Get_Config_From_HKEY(HKEY_CURRENT_USER, (int)L"Software\\Microsoft\\Windows\\CurrentVersion\\Run", v16, &v15, 0);
v5 = v15;
if ( v15 )
    v5 = *(DWORD *)(v15 - 4);
if ( !v5 )
{
    idr619347__UStrCat3(v18, v17, v10[0]);
    v9 = (BYTE *)sub_29A9B64(v14);
    v6 = (const WCHAR *)sub_29A9B64(v16);
    Set_HKEY(v6, L"Software\\Microsoft\\Windows\\CurrentVersion\\Run", v9);
}
```

公众号 · 安全内参

图13 恶意程序通过自启动设置来保证持久化驻留

其C2硬编码到代码中，为 sbido.com:2869，远程连接该域名，进行数据传输

图14 恶意程序连接远程地址上传窃密数据

样本使用硬编码的域名作为C2，域名解析IP不定期进行更新，域名sbido.com 在2025-09-0508:13:32被注册使用，通过历史解析IP进行查询从2025-09-12后，解析的IP地址都为“黑猫”团伙所使用：

sbido.com 2025-09-25 情报更新 Umbrella 100w+ · Alexa 100w+ · 查看历史排名

远控 黑产团伙 黑猫

相关URL 0 解析IP数 18 注册时间 2025-09-05 08:13:32 域名服务商 WEBCC
相关样本 36 子域名数 18 过期时间 2026-09-05 08:13:32 域名注册邮箱 reg_22060805@whoisprotection.cc
ICP 备案 -

历史解析记录 (17)

时间	IP
2025-12-13	223.26.63.103
2025-11-19	27.50.63.118
2025-11-18	27.50.54.144 27.50.63.118
2025-11-07	27.50.54.144
2025-11-05	137.220.252.82
2025-10-18	206.119.64.108
2025-10-04	38.55.16.61
2025-09-12	154.213.190.46
2024-11-03	172.65.190.172
2023-10-30	104.140.98.208

154.213.190.46 远控 黑产团伙 黑猫
日本 东京都 千代田区

公众号 · 安全内参

图15 恶意域名sbido.com历史更新的解析IP

该木马主要功能为窃密，主要窃取受害主机浏览器数据：

```

14         dd 20480h, 0FFFFFFFFh, 18h
10 aGoogleChromeUs_0:                ; DATA XREF: sub_2BB47A8+19E4fo
10         text "UTF-16LE", 'Google\Chrome\User Data\','0
12         align 4
14         dd 20480h, 0FFFFFFFFh, 19h
10 aMicrosoftEdgeU:                ; DATA XREF: sub_2BB47A8+19F7fo
10         text "UTF-16LE", 'Microsoft\Edge\User Data\','0
14         dd 20480h, 0FFFFFFFFh, 26h
10 aBravesoftwareB:                ; DATA XREF: sub_2BB47A8+1A0Afo
10         text "UTF-16LE", 'BraveSoftware\Brave-Browser\User Data\','0
1E         align 10h
10         dd 20480h, 0FFFFFFFFh, 1Ch
1C aTencentQqbrows:                ; DATA XREF: sub_2BB47A8+1A1Dfo
1C         text "UTF-16LE", 'Tencent\QQBrowser\User Data\','0
16         align 4
18         dd 20480h, 0FFFFFFFFh, 11h
14 a360se6UserData:                ; DATA XREF: sub_2BB47A8+1A46fo

```

公众号 · 安全内参

图16 恶意程序会窃取浏览器用户数据

监控键盘，记录键盘输入数据：

```

v7 = sub_2CAF600(a3, &aForeignKey[8]);
v8 = v7;
if ( v7 )
{
    v9 = sub_2C34814(v7);
    sub_2CF5B68(a1, a2, v8, v9);
}
else
{
    v10 = sub_2CAF600(a3, aTextkey);
    if ( v10 )
        sub_2CF5B68(a1, a2, v10, -1);
    else
        return 0;
}

```

公众号 · 安全内参

图17 恶意程序会记录保存键盘敲击数据

监控剪切板，获取剪切板内复制的数据：

```

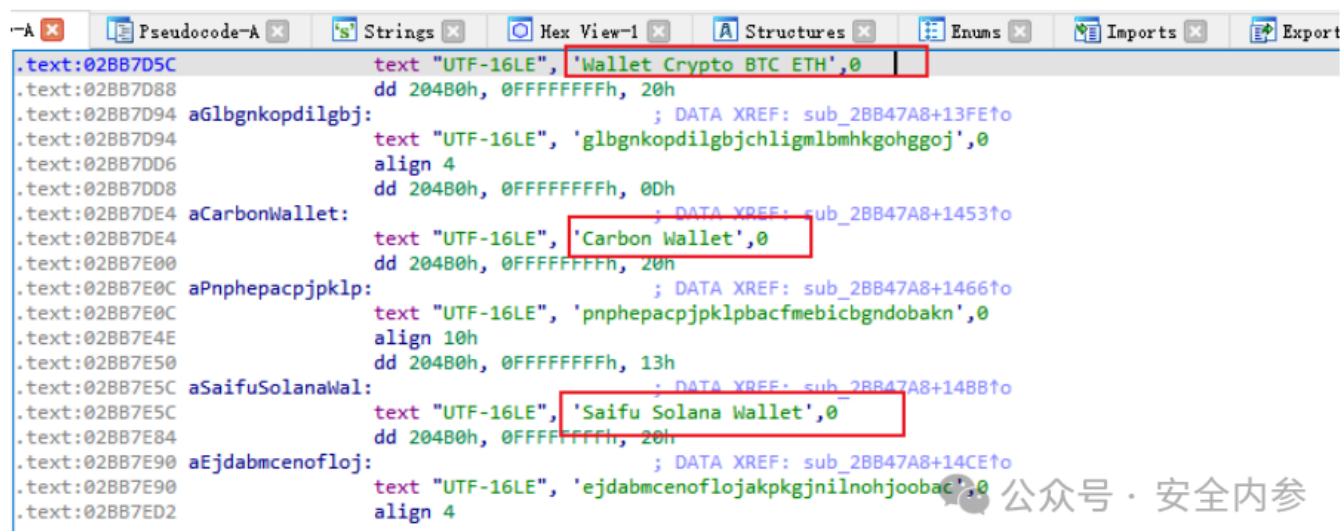
    _writefsdword(0, (unsigned int)v6);
    hMem = GetClipboardData(0xDu);
    if ( hMem )
    {
        v5 = &savedregs;
        v4[1] = (int)&loc_2BD0DC3;
        v4[0] = (int)NtCurrentTeb()->NtTib.ExceptionList;
        _writefsdword(0, (unsigned int)v4);
        GlobalLock(hMem);
        v9 = (void *)GlobalSize(hMem);
        v10 = 0;
        sub_29AB190(v9);
        System::Move(v9, v13, v4[0]);
        System::_linkproc__ WStrAsg(v2, v13);
        _writefsdword(0, v4[0]);
        v5 = (int *)&loc_2BD0DCE;
        GlobalUnlock(hMem);
    }
}

```

公众号 · 安全内参

图18 恶意程序会记录保存剪切板数据

以及主机内其他敏感信息数据：



公众号 · 安全内参

图19 恶意程序会窃取其他敏感数据

三、关联分析

通过对窃密样本中硬编码的C2域名sbido.com进行关联分析，域名解析IP上关联了其他“黑猫”C2的域名：

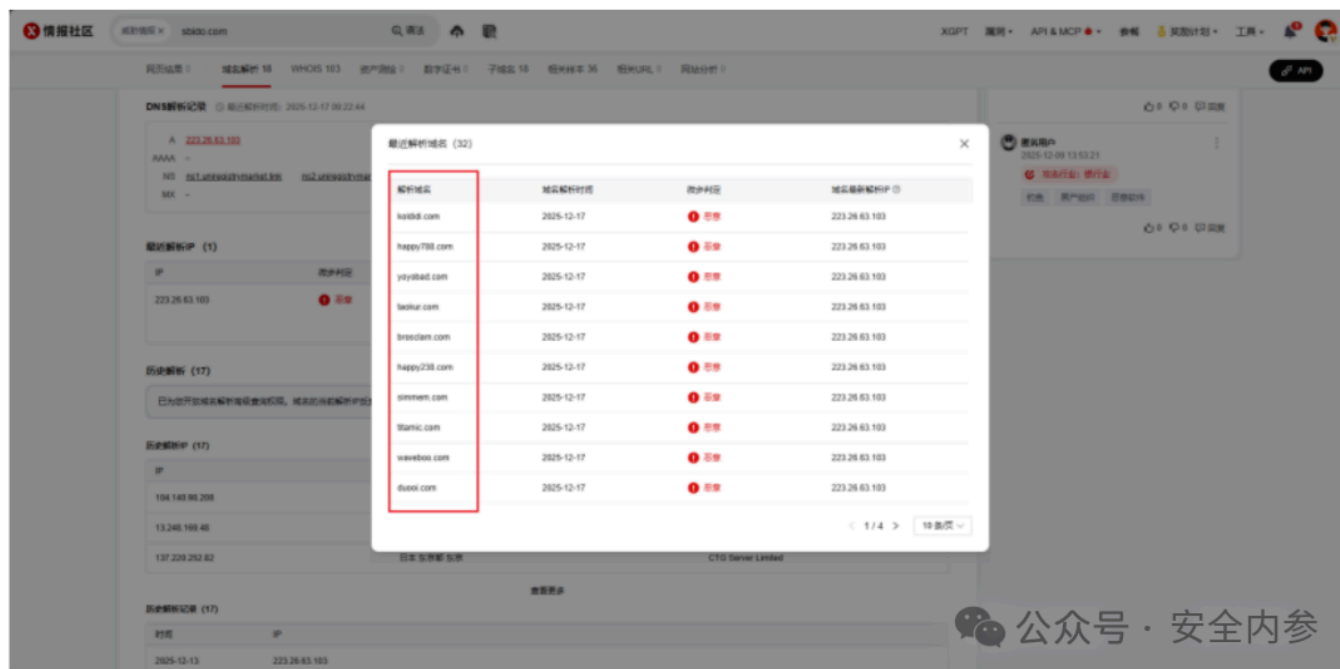


图20 恶意域名解析IP关联其他域名

且部分解析域名为微步情报局在24年10月披露的黑猫C2域名：



图21 关联历史披露“黑猫”资产

这表明“黑猫”团伙在C2资产上的增量更新，“黑猫”仍会使用旧的C2资产。同时，通过对24年10月“黑猫”样本和本次发现样本对比发现：

ToDesk > {app} > dev				搜索“dev”
名称	修改日期	类型	大小	
chrome_elf.dll	2022/6/24 10:10	应用程序扩展	571 KB	
libcef.dll	2024/10/6 11:30	应用程序扩展	4,332 KB	黑文件
msvcp140.dll	2023/2/20 11:45	应用程序扩展	439 KB	
PerfSringup.exe	2024/2/20 11:19	应用程序	215 KB	白文件
PerfSringup.fh6acv	2024/10/6 11:26	FH6ACV 文件	1 KB	
PerfSringup.gh6u	2024/10/6 11:32	GH6U 文件	4,119 KB	加密载荷
vcruntime140.dll	2023/2/20 11:46	应用程序扩展	89 KB	

图22 早期“黑猫”样本释放白加黑组件

主要迭代更新不大，只是优化了释放的白加黑组件，该类型窃密木马属于“黑猫”独有自研的窃密木马，目前暂未在其他黑产团伙攻击活动中出现。

除了对C2资产进行拓线发现，对“黑猫”团伙近期使用的钓鱼网站进一步进行拓线：

钓鱼网站	仿冒软件	历史搜索引擎排名
cn-obsidian. com	Obsidian 科研笔记软件	第二
cn-winscp. com	WinSCP 远程文件管理软件	第四
notepadplusplus. cn	Notepad++ 笔记本	第一

表3 近期“黑猫”团伙新增钓鱼网站类型

这三类钓鱼网站属于“黑猫”团伙近期新增的仿冒软件类型。结合其早期曝光的仿冒网站特征进行对比可以看出，该团伙的窃密对象已不再局限于特定用户群体，而是明显向普通网民扩散，风险覆盖面进一步扩大。

四、感染规模

通过监测分析发现，我国境内于2025年12月7日至20 日期间，“黑猫”黑灰产团伙通过案例木马投放导致主机被控数量约 27.78万台，境内日上线肉鸡数量最高达62167台，肉鸡C2日访问量最高达 43.77万次。境内日上线肉鸡数量情况如下图所示。

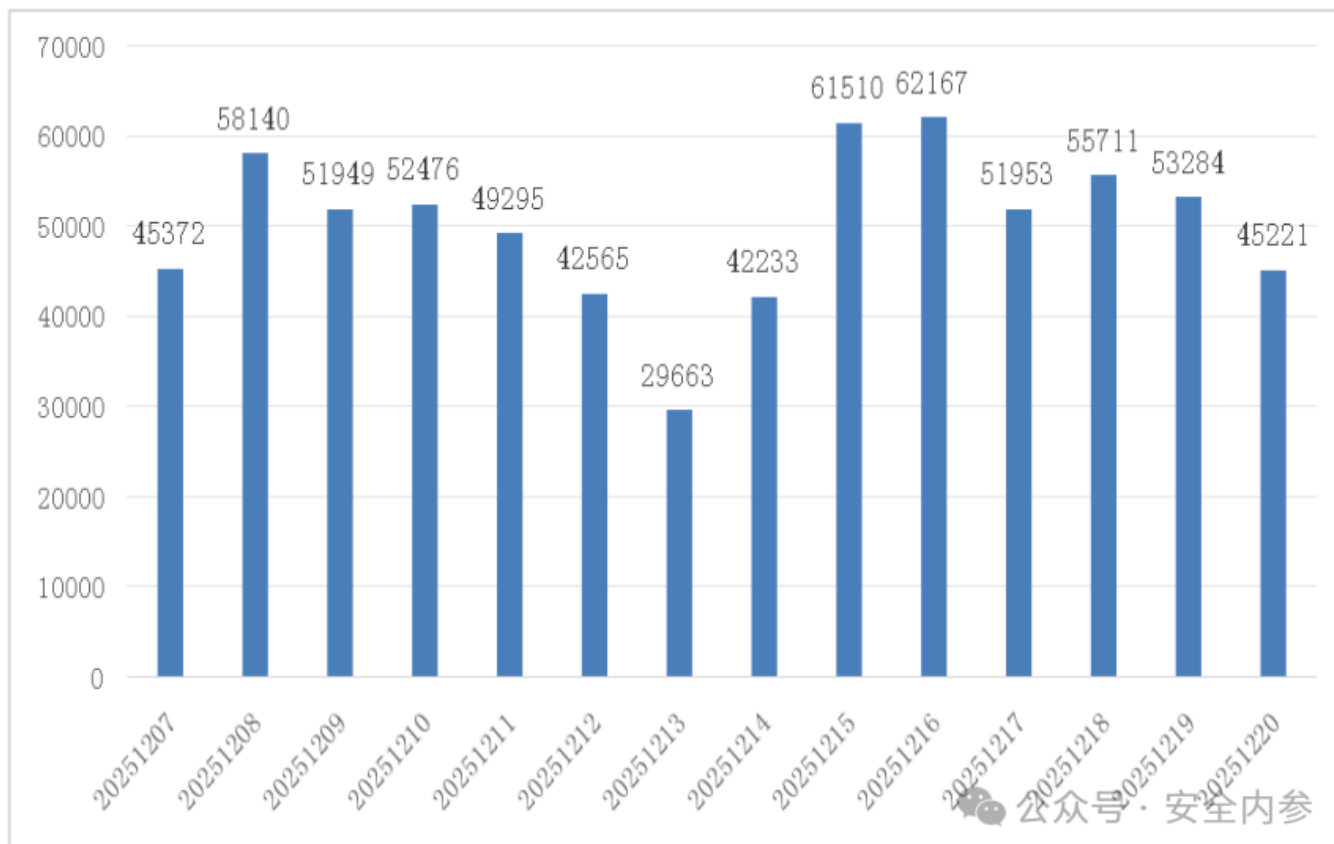


图23 境内日上线肉鸡数量分布情况

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：

notepadplusplus[.]cn

clash.net[.]cn

clash.ac[.]cn

cn-notepadplusplus[.]com

zh-clash[.]com

钓鱼软件下载相关地址：

clashforwindows.org[.]cn

github.zh-cns[.]top

cdn-ccdwn[.]com

C2地址：

223.26.63.103:2869

27.50.63.118:2869

27.50.54.144:2869

27.50.63.118:2869

137.220.252.82:2869

206.119.64.108:2869

38.55.16.61:2869

154.213.190.46:2869

jiaweo[.]com

taokur[.]com

jouloi[.]com

duooi[.]com

golomee[.]com

titamic[.]com

sadliu[.]com

olabb[.]com

vlumu[.]com

jokewick[.]com

alonesad[.]com

lovemeb[.]com

theaigaming[.]com

hiluxo[.]com

sbido[.]com

kimhate[.]com

样本HASH：

b94c54290015ed751c84d0a9bfa6e63481c72c0d7528b4b65a2816f72ea5c994
aa8e535d8576f0471a98865eb44e5e5ae3c3a279f15807e9a8317adb80bf8c9d
46c9e9e2003f92ea1aa06984b02d4827deae71631c5ecf2bed5e4f7f8d5d16c8
087ce894e139f281bd9ebd4b78d4451e458357cef38807e5b4b98ef3ba2fd35c
9868a6e020f35b8e55f6e2366feea72e617648ab7ebad1972d093642f3058f70
3fe9868b56cfbb4de67f65afece0ac95a16267e44d2f555c25263fd641ed7374
267f5bcd5b1ebaa855b9b041351892868d0b4a9153517178ef02a55a6f17bd
8c6e135ea743c82d6f36facd293f5ddc01973ab0c5c52f42ed70e2885e838c4c
b0fcdb33e486ddbc0553f201cf6b9255ec22a12cb85dc9d12ebceb9c7308e51d
c4c1b6d2608b9dd09cddc2f4a040043c590301d3b6ce9bf479c4803b1f679bd5

推荐阅读

- [网安智库平台长期招聘兼职研究员](#)
- [欢迎加入“安全内参热点讨论群”](#)

点击下方卡片关注我们，
带你一起读懂网络安全 ↓