奇安信 威胁情报中心

RESEARCH
数 据 驱 动 安 全

Latest Target Attack of DarkHydruns Group Against Middle East

2019-01-16 By 奇安信威胁情报中心 | 事件追踪

Background

QiAnXin Threat Intelligence Center captured several lure Excel documents written in Arabic in January 9, 2019. A backdoor dropped by macro in the lure documents can communicate with C2 server through DNS tunnel, as well as Google Drive API.

We confirmed that this is a DarkHydrus Group's new attack targeting Middle East region. In July 2018, Palo Alto disclosed DarkHydrus Group which showed its special interest to governments in Middle East[1]. Prior to that report, we published detail analysis on malware exploiting CVE-2018-8414 vulnerability (remote code execution in SettingContent-ms), which is believed a work of DarkHydrus[2].

Timeline

Timeline of activities of DarkHydrus Group:

Kaspersky named "LazyMeerkat" to this APT group. [4]

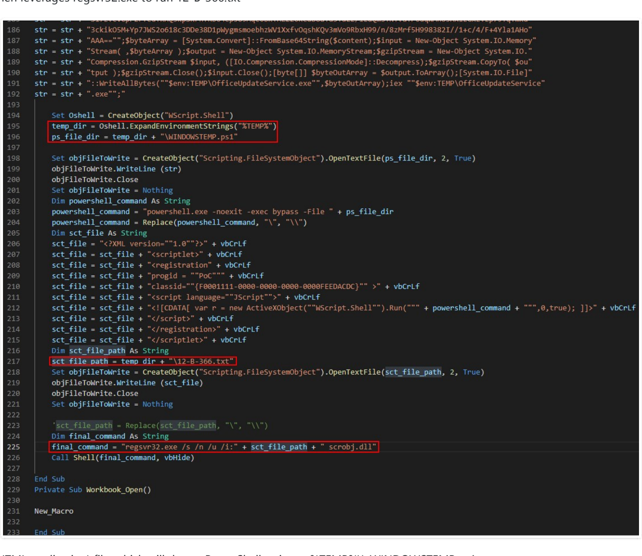
Sample Analysis

Dropper（Macros）

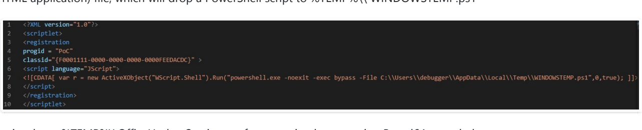
MD5	5c3f96ade0ea67eef9d25161c64e6f3e
Filename	الفهارس.xlsm（indexes. xlsm）

MD5	8dc9f5450402ae799f5f8afd5c0a8352
Filename	الاطلاع.xlsm（viewing. xlsm）

This malware is a lure Excel document with name 'الفهارس.xlsm'. When it is opened, embedded VBA macro is trigged to run. That macro drops 12-B-366.txt to '%TEMP%' directory first, then leverages regsvr32.exe to run 12-B-366.txt



12-B-366.txt is a HTA (HTML application) file, which will drop a PowerShell script to %TEMP%\\ WINDOWSTEMP.ps1

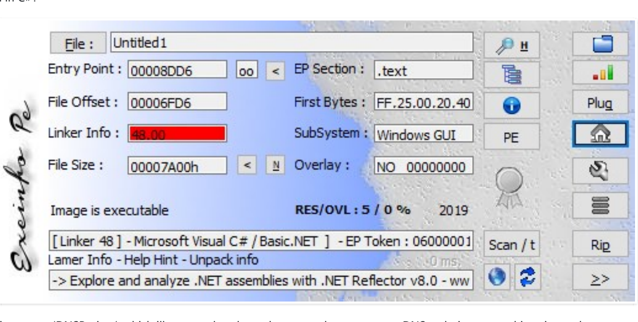


Finally, the PowerShell script drops %TEMP%\\OfficeUpdateService.exe for execution by extracting Based64-encoded content.

Backdoor（OfficeUpdateService.exe）

MD5	b108412f1cdc0602d82d3e6b318dc634
Filename	OfficeUpdateService.exe
PDB path	C:\Users\william\Documents\Visual Studio 2015\Projects\DNSProject\DNSProject\obj\Release\DNSProject.pdb

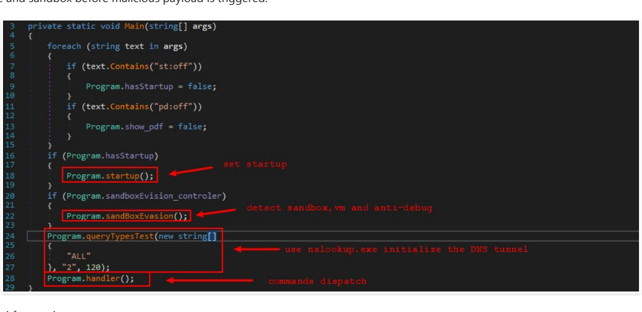
This backdoor is written in C#：



The PDB path has a project name 'DNSProject', which illustrates that the malware may leverage some DNS techniques to achieve its goal.

C:\Users\william\Documents\Visual Studio 2015\Projects\DNSProject\DNSProject\obj\Release\DNSProject.pdb

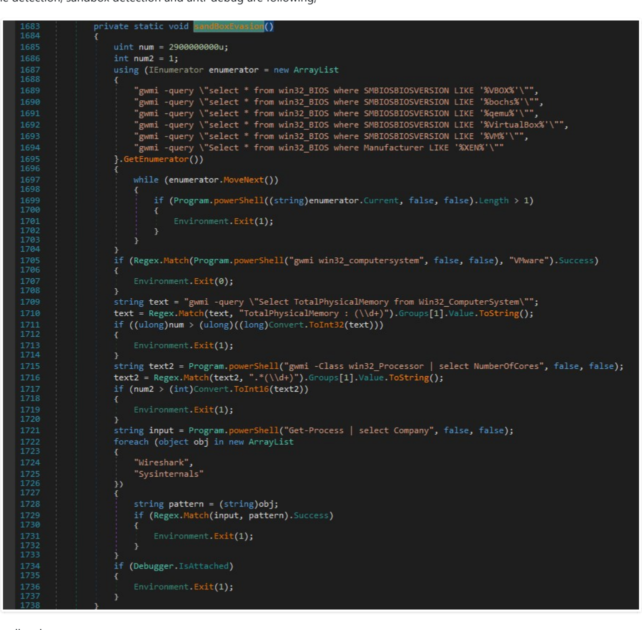
The backdoor checks if 'st:off' and 'pd:off' is given as paramters. If 'st:off' presents, no persistence entry is added; PDF file is not dropped if 'pd:off' exists. Then it detects existence of virtual machine and sandbox before malicious payload is triggered.



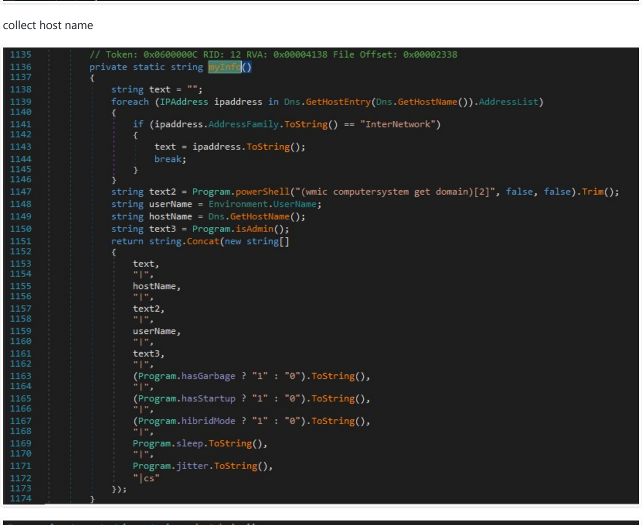
A registry entry is added for persistence：

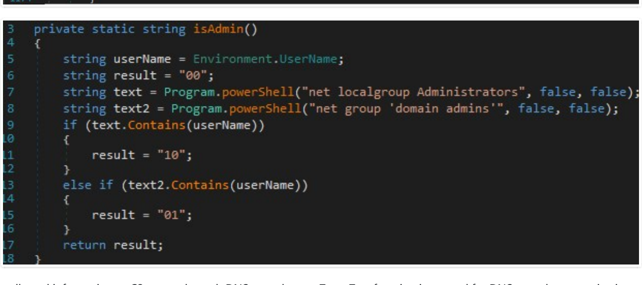
It can drop a PDF file：

Codes of virtual machine detection, sandbox detection and anti-debug are following,

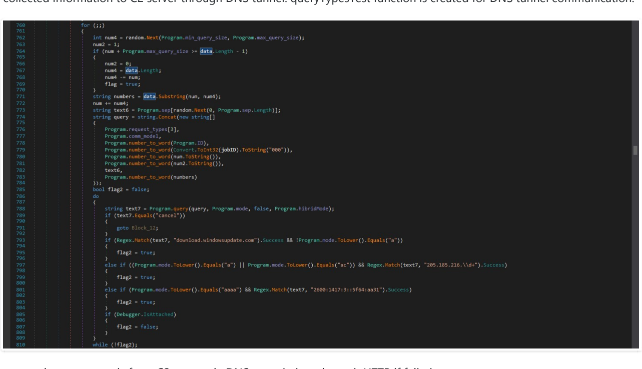


Next, the backdoor will collect host name

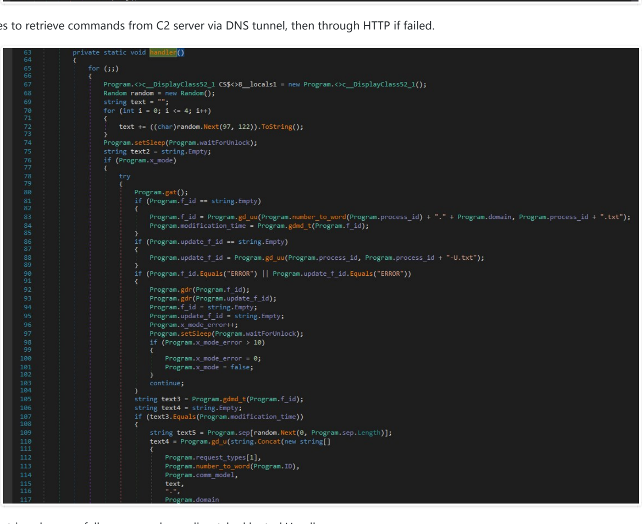




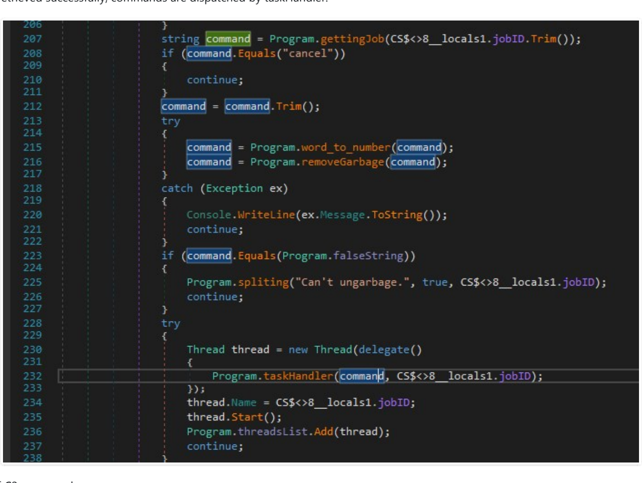
The backdoor will send collected information to C2 server through DNS tunnel. queryTypesTest function is created for DNS tunnel communication.



Then, the backdoor tries to retrieve commands from C2 server via DNS tunnel, then through HTTP if failed.



After C2 commands is retrieved successfully, commands are dispatched by taskHandler.



Screenshot of a part of C2 commands

"^\\$x_mode" command sets file server address which is sent in DNS tunnel.

One file server is Google Drive

https://www.googleapis.com/upload/drive/v3/files/" + file_id + "?supportsTeamDrive=true&uploadType=resumable&fields=kind,id,name,mimeType,parents

All command lists are following：

Command	Feature
^kill	Kill thread or process
^\$fileDownload	Download file
^\$importModule	Import module
^\$x_mode	In x_mode，configure C2 address，then send RAT data to C2 by HTTP protocol
^\$ClearModules	Remove module
^\$fileUpload	Upload file
^testmode	Test module
^showconfig	Show configuration
^changeConfig	Change configuration
^slp	Sleep
^exit	Exit process

DNS Tunnel

DNS tunnel is a C2 communication technique in which malware send data and retrieve commands by DNS query packets. This technique is very effective since most gateways or firewalls allow both ingress and egress DNS traffic.

If C2 server is assigned in the format of IP address in malware body, malware can contact C2 directly. But OfficeUpdateService.exe backdoor has C2 server in the format of DNS name, which requires a DNS resolution to C2 domain name first. To do that, the backdoor queries C2 domain in specific name server. Then the backdoor communicates C2 server in DNS tunnel.

C2 domain names are following：

Name Server

Malware sends DNS queries to these two name servers for C2 domain name resolution: 'tvs1.trafficmanager.live' and 'tvs2.trafficmanager.live'

Malware uses nslookup to send out DNS query, with following parameters: 'timeout' and 'q' for DNS record type

C&C Commands

To parse C2 commands from above types of DNS records, the malware uses different regular expressions. For example, if commands are sent back in DNS A record, the malware will use following regular expression:

Malware will retrieve a process ID as victim ID, then treats victim ID as subdomain name in C2 communication.

C2 commands are parsed out by regular expressions based on DNS record types.

We manually send out a DNS TXT query with victim ID as illustration.

A domain name 'ajpinc.akamaiedge.live' is created. In subdomain 'ajpinc', 'a' means this is the first request, and 'c' is the character for string end, while 'jpin' is process ID. Then, we send DNS query by using nslookup command as following

The malware will use following regular expression to parse out command, ([\\w+).(akdns.live|akamaiedge.live|edgekey.live|akamaized.live](file://w+).(akdns.live|akamaiedge.live|edgekey.live|akamaized.live)).

Finally, system configuration is sent to C2 server in DNS protocol.

Communication Rule

This malware uses following types of DNS record

A
AAAA
AC
CNAME
TXT
SRV
SOA
MX

To parse C2 commands from above types of DNS records, the malware uses different regular expressions. For example, if commands are sent back in DNS AC record, the malware will use following regular expression:

Following regular expression is for commands in DNS AAAA records,

And there is one regular expression for several DNS record types, including CNAME, SRV, SOA,

Breakdown of regular expressions are as following,

Types of DNS record	Regular expressions
A	`Address:\\s+(\\d+.\\d+.\\d+.\\d+)`
AC	`([^r-v\\s]+)[r-v]([\\w\\d+\\/=]+)-\\w+.(<C2DOMIAN>)`
AAAA	`Address:\\s+(([a-fA-F0-9]{0,4}:{1,4}[\\w|:]+){1,8})`
CNAME、TXT、SRV、SOA、MX	`([^r-v\\s]+)[r-v]([\\w\\d+\\/=]+)-\\w+.(<C2DOMIAN>)` and `(\\w+).(<C2DOMIAN>)`

However, the malware will cancel operation if commands is matched by following regular expression: "216.58.192.174|2a00:1450:4001:81a::200e|2200::|download.microsoft.com|ntservicepack.microsoft.com|windowsupdate.microsoft.com|update.microsoft.com"

Attribution

We found some traces which lead us to believe that DarkHydrus is behind this attack.

Samples with DNS Tunnel Function

Similar to the malware disclosed by Palo Alto[2], both malware use DNS tunnel technique:

Sandbox detection and Backdoor Capability

The new malware has very similar code of detection to sandbox and virtual machine as previous DarkHydrus samples

Both samples have very similar code and functionality:

Pivot

One interesting finding is that, there is one Twitter user Steve Williams with handle name @darkhydrus2. It's coincident that both 'darkhydrus' (APT group name) and 'Williams' (user name in PDB path) found in this Twitter user.

Summary

In recent APT incidents, more and more threat actors tend to adopt Office VBA macro instead of Office 0day vulnerability in the consideration of cost reduction. It is recommended that users avoid to open documents from untrusted sources. And Office macro should be disabled by default.

Products of 360 ESG can protect users from this new malware, including QiAnXin Threat Intelligence Platform, SkyEye APT Detection, NGSOC.

IOC

MD5
5c3f96ade0ea67eef9d25161c64e6f3e
8dc9f5450402ae799f5f8afd5c0a8352
b108412f1cdc0602d82d3e6b318dc634
039bd47f0fdb6bb7d68a2428c71f317d
PDB PATH
C:\Users\william\Documents\Visual Studio 2015\Projects\DNSProject\DNSProject\obj\Release\DNSProject.pdb
C2
0ffice365.life
0ffice365.services
0nedrive.agency
akamai.agency
akamaiedge.live
akamaiedge.services
akamaized.live
akdns.live
azureedge.today
cloudfronts.services
corewindows.agency
edgekey.live
microsoftonline.agency
nsatc.agency
onedrive.agency
phicdn.world
sharepoint.agency
skydrive.agency
skydrive.services
t-msedge.world
trafficmanager.live

References

[1]. https://ti.qianxin.com/blog/articles/analysis-of-settingcontent-ms-file/

[2]. https://unit42.paloaltonetworks.com/unit42-new-threat-actor-group-darkhydrus-targets-middle-east-government/

[3]. https://ti.qianxin.com/

[4]. https://twitter.com/craiu/status/1083305994652917760

APT DARKHYDRUNS LAZYMEERKA

分享到：