Iranian APT group 'MuddyWater' Adds Exploits to Their Arsenal

Overview and Analysis of MuddyWater New Infrastructures and TTPs

June 2019

Table of Contents

Executive Summary

In recent months, there has been considerable unrest in the Iranian cyber sphere. Highly sensitive data about Iranian APT groups was leaked, exposing abilities, strategies, and attack tools. The main medium for this leak was a telegram channel.

The first leak uncovered attack frameworks and webshells of APT-34[1] (Known as OilRig group). This was followed by another leak that that exposed previously unknown details (such as compromised C2 servers) regarding the operation of MuddyWater[2]. Further, it detailed the modus operandi of RANA - a cyber division of the Iranian Ministry of Intelligence (MOIS).

However, Clearsky's Threat Intelligence team investigation indicate that MuddyWater's activities were unaffected. This report will reveal the group's latest exploit usage and TTPs.

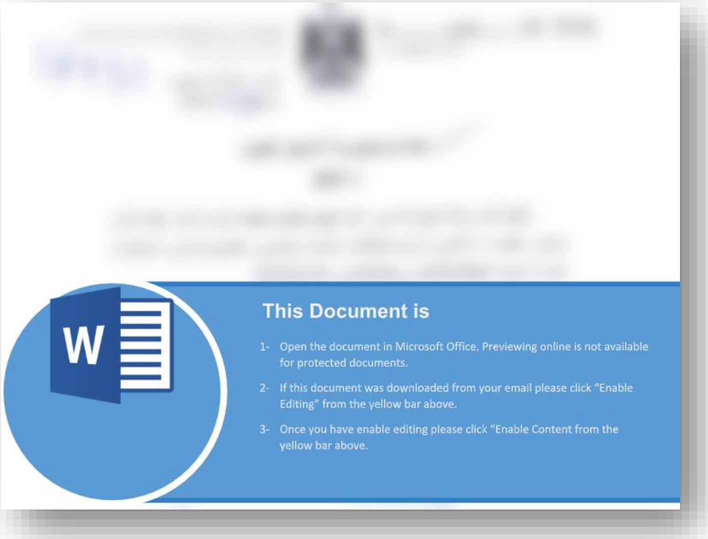
Clearsky has detected new and advanced attack vector used by MuddyWater to target governmental entities and the telecommunication sector. Notably, the TTP includes decoy documents exploiting CVE-2017-0199 as the first stage of the attack. This is followed by the second stage of the attack – communication with the hacked C2 servers and downloading a file infected with the macros.

MuddyWater (aka SeedWorm/Temp.Zagros) is a high-profile Advanced Persistent Threat (APT) actor sponsored by Iran. The group was first observed in 2017, and since has operated multiple global espionage campaigns. With that in mind, their most significant operations mainly focus on Middle Eastern and Middle Asian nations[3].

The group targets a wide gamut of sectors, including governmental, military, telecommunication, and academia. In the past months, Clearsky had monitored and detected malicious files of each one of these TTPs - decoy Microsoft software with embedded Macros[4]; and documents exploiting vulnerability CVE-2017-0199[5]. **This is the first time MuddyWater has used these two vectors in conjunction**.

By analyzing the Rana documents[6], it appears that the MOIS attack teams are divided in to two branches, each with different purposes.

The first is the espionage team that specialize with hacking systems, while the other is the social engineering team that compromises assets via social engineering and spear-phishing methods. Clearsky assessment is that MuddyWater is likely the latter group.



This Document is

1- Open the document in Microsoft Office, Previewing online is not available for protected documents.

2- If this document was downloaded from your email please click "Enable Editing" from the yellow bar above.

3- Once you have enable editing please click "Enable Content from the yellow bar above.

[1] https://www.bleepingcomputer.com/news/security/hacker-group-exposes-iranian-apt-operations-and-members/

[2] https://www.zdnet.com/article/new-leaks-of-iranian-cyber-espionage-operations-hit-telegram-and-the-dark-web/

[3] https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/

[4] https://www.clearskysec.com/muddywater-targets-kurdish-groups-turkish-orgs/

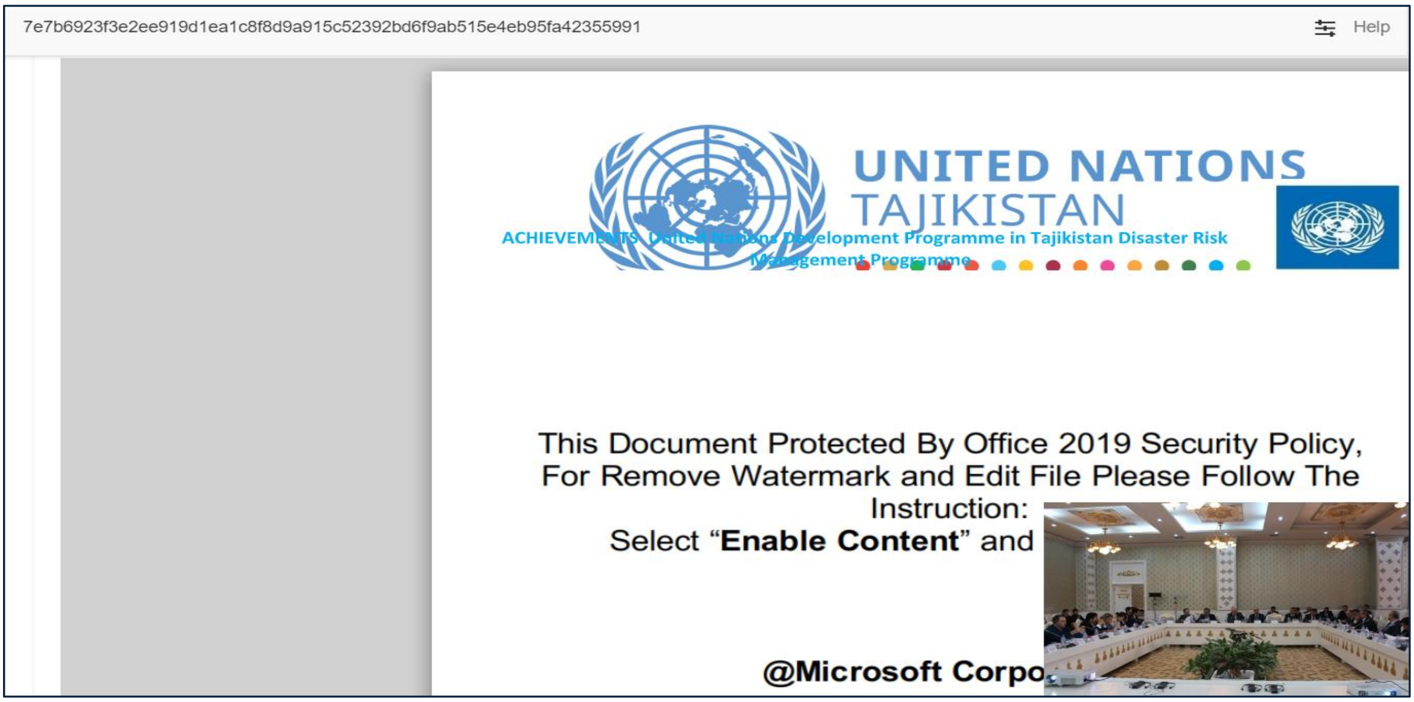
[5] https://twitter.com/ClearskySec/status/1118511605359304705

[6] https://www.clearskysec.com/iranian-apt-black-box/

Attack Vector 1 – malicious macro

It appears that in the recent campaign, the group returned to use (in certain cases) compromised servers. They leveraged the servers to host malicious code segment used in the second stage of the attacks; similar to previous operations. Concurrently we identified several files by MuddyWater that targeted various entities in Tajikistan while using the group's classic attack vector – a malicious VBA macro.

We were notified about one of the files by a colleague of us[7]. This file, named 'UNDP_TJK_Agreement_ORGS.doc', was disguised as an official document of a UN development plan in Tajikistan.



7e7b6923f3e2ee919d1ea1c8f8d9a915c52392bd6f9ab515e4eb95fa42355991

UNITED NATIONS
TAJIKISTAN

ACHIEVEMENTS United Nations Development Programme in Tajikistan Disaster Risk Management Programme

This Document Protected By Office 2019 Security Policy, For Remove Watermark and Edit File Please Follow The Instruction:
Select “**Enable Content**” and

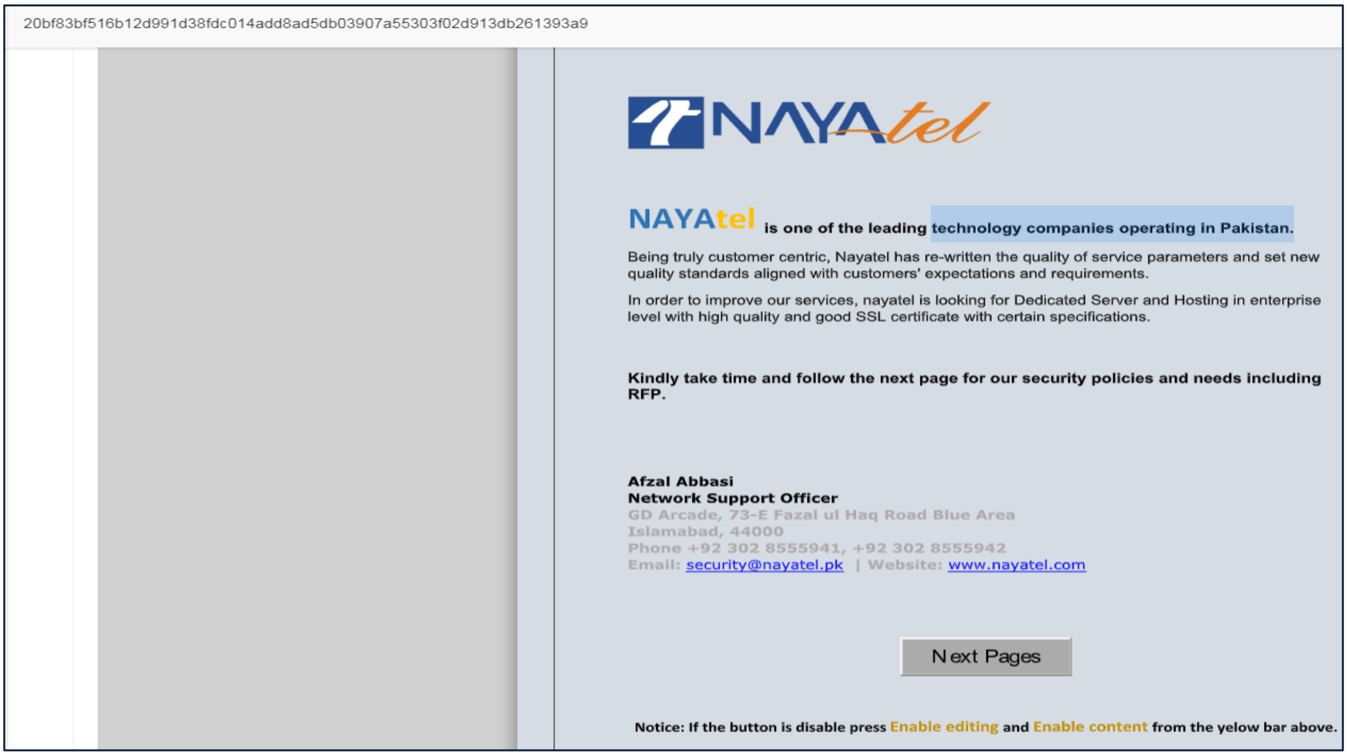
@Microsoft Corpo

After opening the document, a VBS file is created. It is encoded with multiple VBE, JavaScript, and Base64 layers; similar to previous attack vectors by MuddyWater. The malware's second stage is downloaded from IP address 185.244.149[.]218.

Moreover, it appears MuddyWater hacked servers located in countries targeted by them. For example, Omri Segev Moyal, who recently joined Clearsky as a strategic advisor, identified the following compromised website uses by the group – a website from Pakistan: hxxp://corplink[.]com[.]pk/wp-content/themes/buisson/16433.jpg

This address communicates with several malicious files, one of them is a file named 'Nayatel.server.docx' which impersonating a Pakistani 'Fiber-to-the-Home' (FTTH) services provider:

[7] https://twitter.com/Timele9527



20bf83bf516b12d991d38fdc014add8ad5db03907a55303f02d913db261393a9

NAYAtel is one of the leading technology companies operating in Pakistan.

Being truly customer centric, Nayatel has re-written the quality of service parameters and set new quality standards aligned with customers' expectations and requirements.

In order to improve our services, nayatel is looking for Dedicated Server and Hosting in enterprise level with high quality and good SSL certificate with certain specifications.

Kindly take time and follow the next page for our security policies and needs including RFP.

Afzal Abbasi
Network Support Officer
GD Arcade, 73-E Fazal ul Haq Road Blue Area
Islamabad, 44000
Phone +92 302 8555941, +92 302 8555942
Email: security@nayatel.pk | Website: www.nayatel.com

Notice: If the button is disable press Enable editing and Enable content from the yelow bar above.

Furthermore, we identified a compromised server by MuddyWater in China: hxxps://bbs[.]kafan[.]cn/thread-2150909-1-1.html

Attack Vector 2 – CVE-2017-0199

CVE-2017-0199 is a Microsoft Office allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API[8].

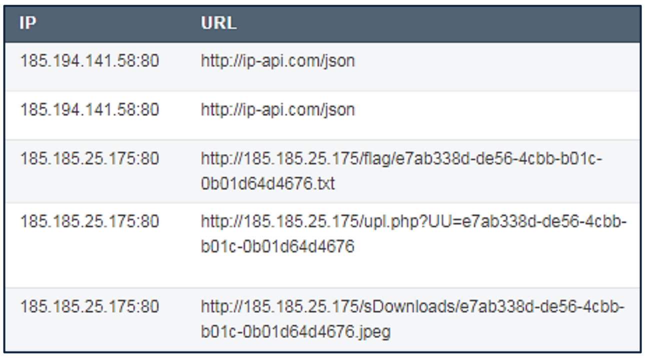
Vulnerable versions

Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1

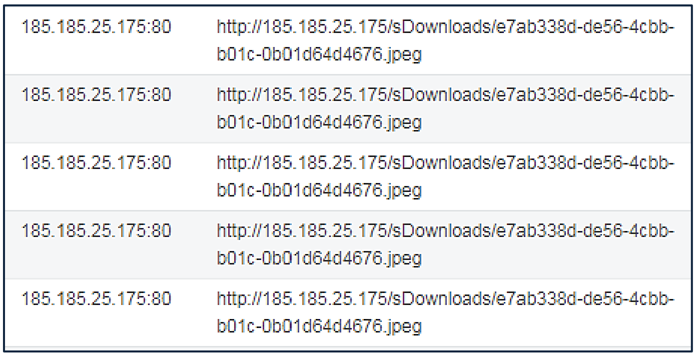
MuddyWater has not used this TTP previously. In contrast, two years ago Palo Alto revealed that this penetration vector was used by another Iranian group named OilRig[9].

For example, recently a file was uploaded to VirusTotal that impersonated a document written in Russian. **The document was identical to previous ones we have seen.** In the known attack vector, the file communicates with IP address 185.185.25[.]175 on port 80. If the file receives positive indication from the server, the following redirections are carried out to the server[10].

[8] https://nvd.nist.gov/vuln/detail/CVE-2017-0199
[9] https://unit42.paloaltonetworks.com/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/
[10] https://any.run/report/36ccae4dffc70249c79cd3156de1cd238af8f7a3e47dc90a1c33476cf97a77b0/3bf82792-2ba1-4823-a7d8-b8c8c792cf61#http

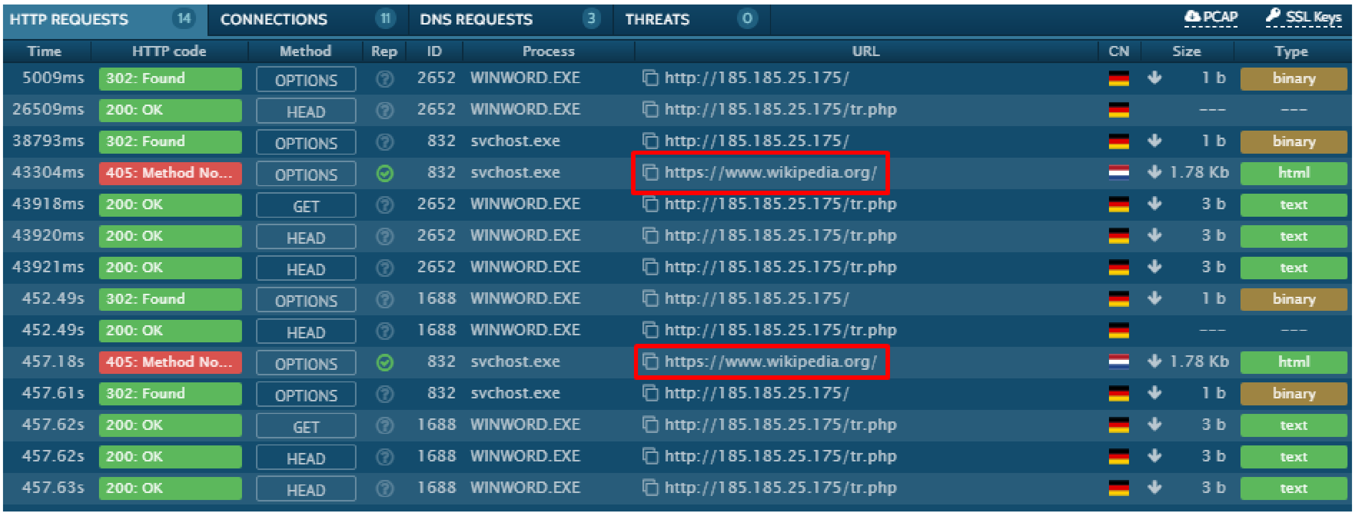


IP	URL
185.194.141.58:80	http://ip-api.com/json
185.194.141.58:80	http://ip-api.com/json
185.185.25.175:80	http://185.185.25.175/flag/e7ab338d-de56-4cbb-b01c-0b01d64d4676.txt
185.185.25.175:80	http://185.185.25.175/upl.php?UU=e7ab338d-de56-4cbb-b01c-0b01d64d4676
185.185.25.175:80	http://185.185.25.175/sDownloads/e7ab338d-de56-4cbb-b01c-0b01d64d4676.jpeg



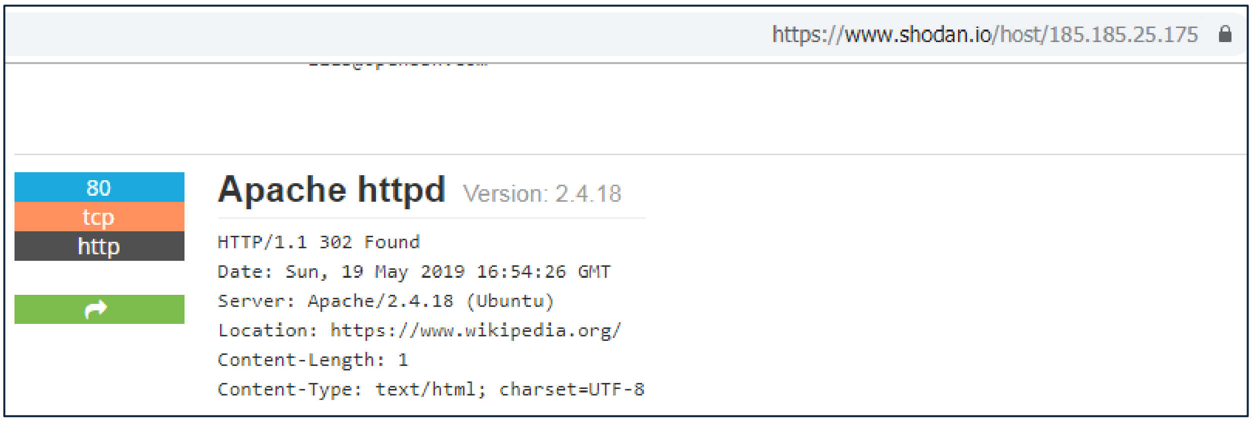
185.185.25.175:80	http://185.185.25.175/sDownloads/e7ab338d-de56-4cbb-b01c-0b01d64d4676.jpeg
185.185.25.175:80	http://185.185.25.175/sDownloads/e7ab338d-de56-4cbb-b01c-0b01d64d4676.jpeg
185.185.25.175:80	http://185.185.25.175/sDownloads/e7ab338d-de56-4cbb-b01c-0b01d64d4676.jpeg
185.185.25.175:80	http://185.185.25.175/sDownloads/e7ab338d-de56-4cbb-b01c-0b01d64d4676.jpeg
185.185.25.175:80	http://185.185.25.175/sDownloads/e7ab338d-de56-4cbb-b01c-0b01d64d4676.jpeg

If the redirection fails, like in previous files we detected, the user is redirected to Wikipedia instead:



Time	HTTP code	Method	Rep	ID	Process	URL	CN		Size	Type
5009ms	302: Found	OPTIONS	?	2652	WINWORD.EXE	http://185.185.25.175/	🇩🇪	↓	1 b	binary
26509ms	200: OK	HEAD	?	2652	WINWORD.EXE	http://185.185.25.175/tr.php	🇩🇪		---	---
38793ms	302: Found	OPTIONS	?	832	svchost.exe	http://185.185.25.175/	🇩🇪	↓	1 b	binary
43304ms	405: Method No...	OPTIONS	✓	832	svchost.exe	https://www.wikipedia.org/	🇳🇱	↓	1.78 Kb	html
43918ms	200: OK	GET	?	2652	WINWORD.EXE	http://185.185.25.175/tr.php	🇩🇪	↓	3 b	text
43920ms	200: OK	HEAD	?	2652	WINWORD.EXE	http://185.185.25.175/tr.php	🇩🇪	↓	3 b	text
43921ms	200: OK	HEAD	?	2652	WINWORD.EXE	http://185.185.25.175/tr.php	🇩🇪	↓	3 b	text
452.49s	302: Found	OPTIONS	?	1688	WINWORD.EXE	http://185.185.25.175/	🇩🇪	↓	1 b	binary
452.49s	200: OK	HEAD	?	1688	WINWORD.EXE	http://185.185.25.175/tr.php	🇩🇪		---	---
457.18s	405: Method No...	OPTIONS	✓	832	svchost.exe	https://www.wikipedia.org/	🇳🇱	↓	1.78 Kb	html
457.61s	302: Found	OPTIONS	?	832	svchost.exe	http://185.185.25.175/	🇩🇪	↓	1 b	binary
457.62s	200: OK	GET	?	1688	WINWORD.EXE	http://185.185.25.175/tr.php	🇩🇪	↓	3 b	text
457.62s	200: OK	HEAD	?	1688	WINWORD.EXE	http://185.185.25.175/tr.php	🇩🇪	↓	3 b	text
457.63s	200: OK	HEAD	?	1688	WINWORD.EXE	http://185.185.25.175/tr.php	🇩🇪	↓	3 b	text

Below is a screenshot from Shodan of the server. As seen, it still redirects to Wikipedia:

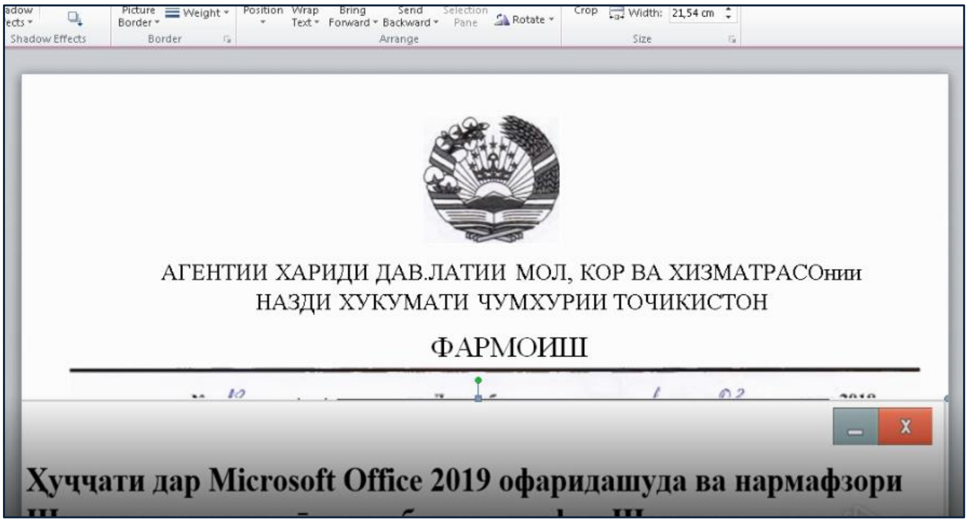


Apache httpd Version: 2.4.18

```
HTTP/1.1 302 Found
Date: Sun, 19 May 2019 16:54:26 GMT
Server: Apache/2.4.18 (Ubuntu)
Location: https://www.wikipedia.org/
Content-Length: 1
Content-Type: text/html; charset=UTF-8
```

The documents were identified by only three antivirus engines. This is in stark comparison to a previous attack we reported on[11], in which the documents were identified 32 times.

Moreover, in May we reported on twitter about another suspicious file that targeted entities in Turkey, via the same attack vector.



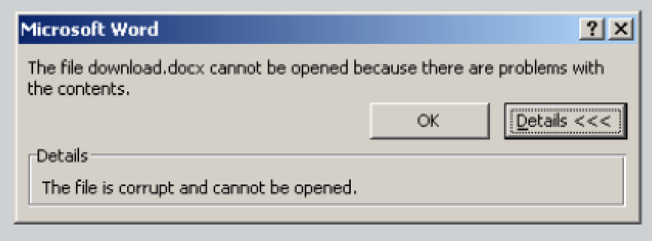
АГЕНТИИ ХАРИДИ ДАВ.ЛАТИИ МОЛ, КОР ВА ХИЗМАТРАСОнии
НАЗДИ ХУКУМАТИ ЧУМХУРИИ ТОЧИКИСТОН

ФАРМОИШ

Ҳуҷҷати дар Microsoft Office 2019 офаридашуда ва нармафзори

First type of file

In the first stage, after the file is opened the following error message appears.



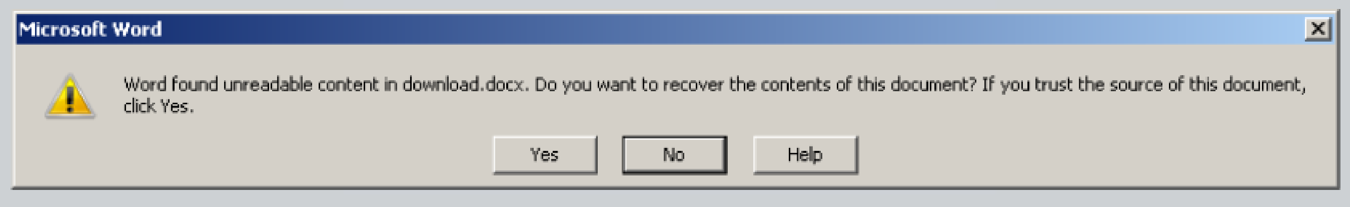
Microsoft Word

The file download.docx cannot be opened because there are problems with the contents.

Details

The file is corrupt and cannot be opened.

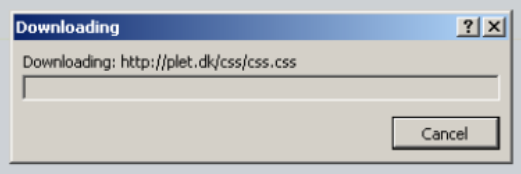
After the victim approves, another error message appears which requests the victim to recover the contents of the document:



Microsoft Word

Word found unreadable content in download.docx. Do you want to recover the contents of this document? If you trust the source of this document, click Yes.

If the victim confirms, the vulnerability will activate, and the Word software will communicate to the C2 server:

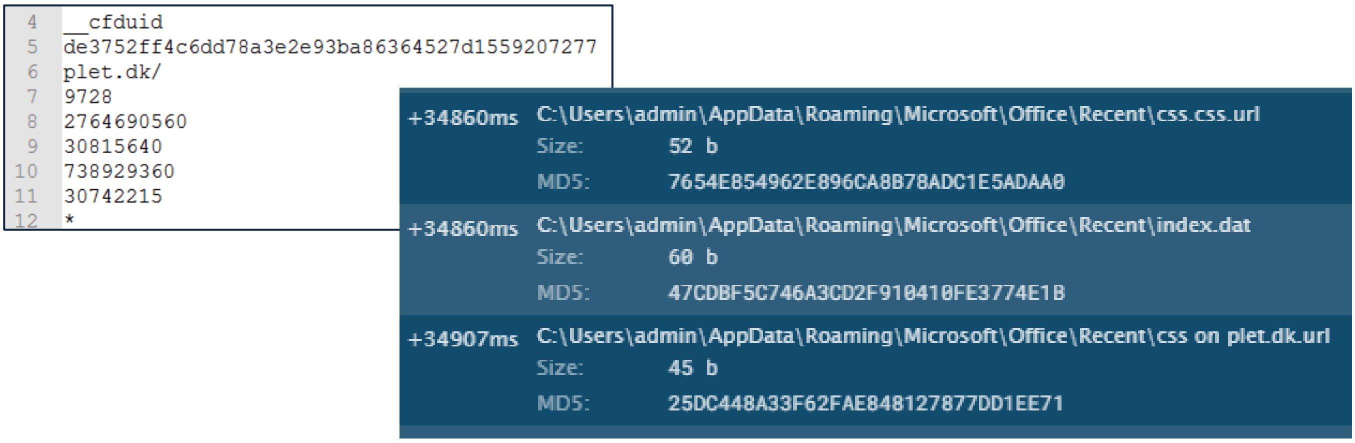


Downloading

Downloading: http://plet.dk/css/css.css

The contents of the text file redirect to the malware's C2 server. Then, several communications are carried out to the C2 server with the address hxxp://plet[.]dk/css/css.css:

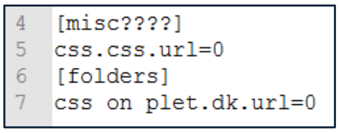
[11] https://www.clearskysec.com/muddywater-targets-kurdish-groups-turkish-orgs
https://www.clearskysec.com/muddywater-operations-in-lebanon-and-oman/



```
__cfduid
de3752ff4c6dd78a3e2e93ba86364527d1559207277
plet.dk/
9728
2764690560
30815640
738929360
30742215
*
```

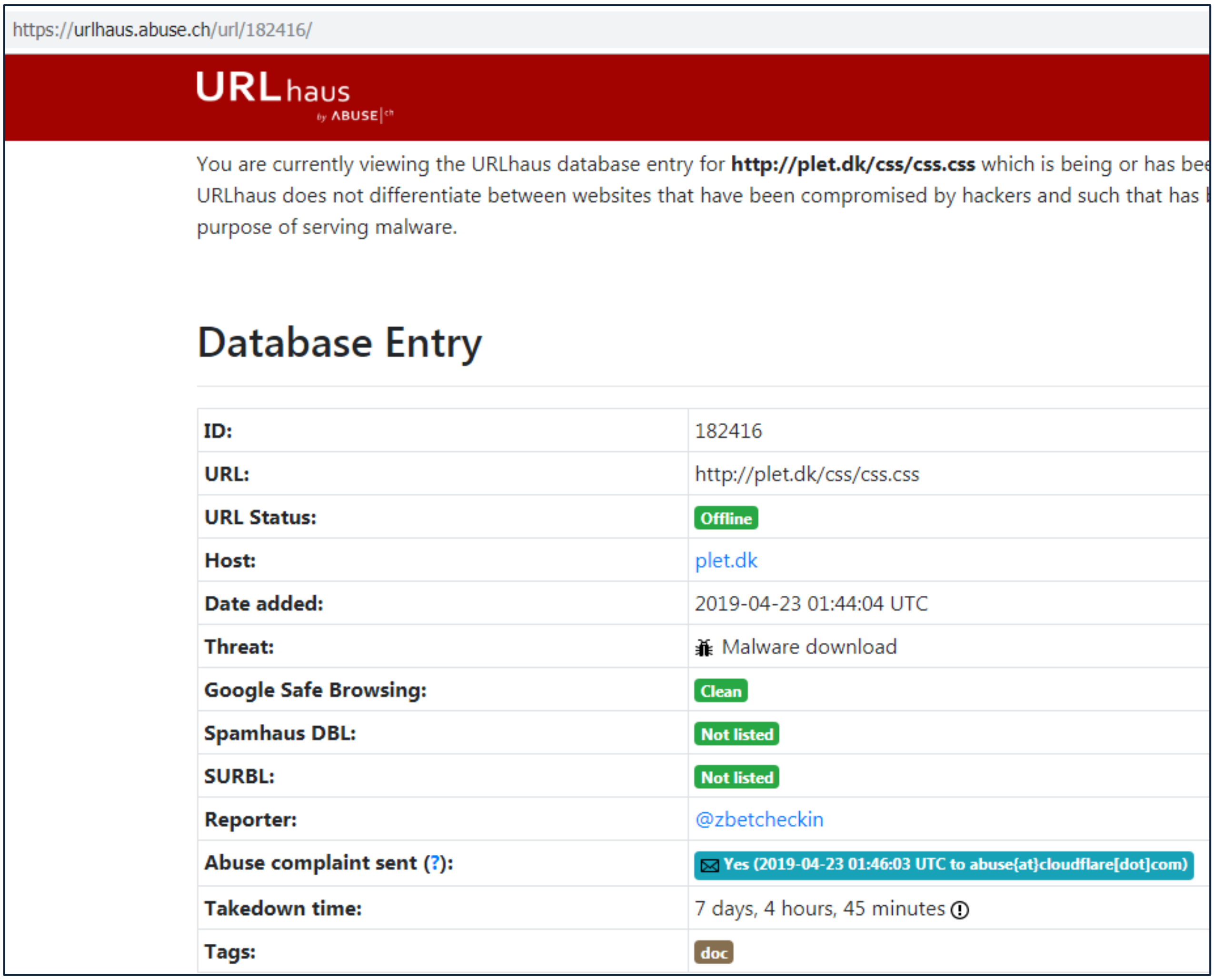
```
+34860ms  C:\Users\admin\AppData\Roaming\Microsoft\Office\Recent\css.css.url
          Size:     52 b
          MD5:      7654E854962E896CA8B78ADC1E5ADAA0
+34860ms  C:\Users\admin\AppData\Roaming\Microsoft\Office\Recent\index.dat
          Size:     60 b
          MD5:      47CDBF5C746A3CD2F910410FE3774E1B
+34907ms  C:\Users\admin\AppData\Roaming\Microsoft\Office\Recent\css on plet.dk.url
          Size:     45 b
          MD5:      25DC448A33F62FAE848127877DD1EE71
```

As of June 1, the files on the server receives the value 0:



```
[misc????]
css.css.url=0
[folders]
css on plet.dk.url=0
```

According to URLhaus[12], the website is likely hacked:



https://urlhaus.abuse.ch/url/182416/

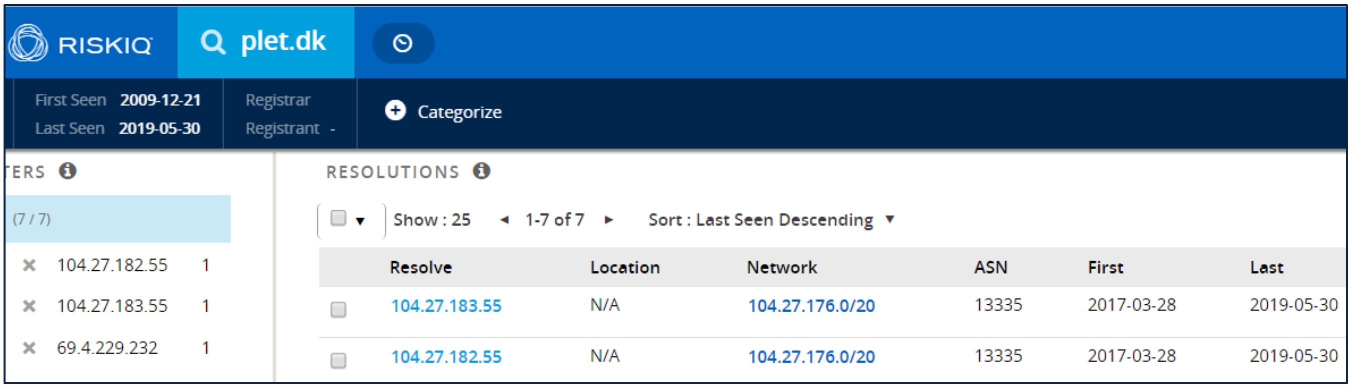
You are currently viewing the URLhaus database entry for **http://plet.dk/css/css.css** which is being or has bee URLhaus does not differentiate between websites that have been compromised by hackers and such that has l purpose of serving malware.

Database Entry

ID:	182416
URL:	http://plet.dk/css/css.css
URL Status:	Offline
Host:	plet.dk
Date added:	2019-04-23 01:44:04 UTC
Threat:	Malware download
Google Safe Browsing:	Clean
Spamhaus DBL:	Not listed
SURBL:	Not listed
Reporter:	@zbetcheckin
Abuse complaint sent (?):	✉ Yes (2019-04-23 01:46:03 UTC to abuse{at}cloudflare[dot]com)
Takedown time:	7 days, 4 hours, 45 minutes ⓘ
Tags:	doc

Currently the domain's IP address is using Cloudflare service:

[12] https://urlhaus.abuse.ch/



First Seen 2009-12-21
Last Seen 2019-05-30

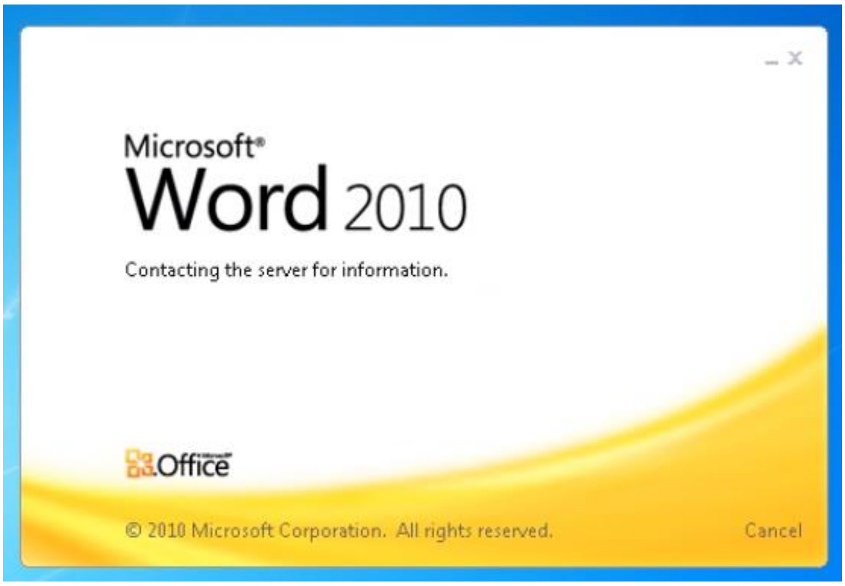
104.27.182.55	1
104.27.183.55	1
69.4.229.232	1

Resolve	Location	Network	ASN	First	Last
104.27.183.55	N/A	104.27.176.0/20	13335	2017-03-28	2019-05-30
104.27.182.55	N/A	104.27.176.0/20	13335	2017-03-28	2019-05-30

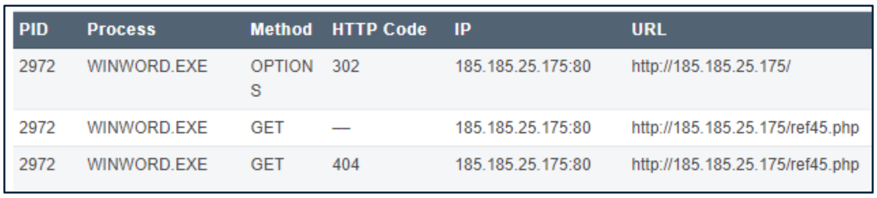
Furthermore, it is inaccessible and only shows a warning by Cloudflare about a malicious page.

Second type of file

The second type of file exploits CVE-2017-0199 vulnerability, but unlike the first file, communication is carried out directly to servers used in previous MuddyWater's attacks (187.185.25[.]175). We believe that in future attack MuddyWater will adopt vulnerability exploitation as a first stage.

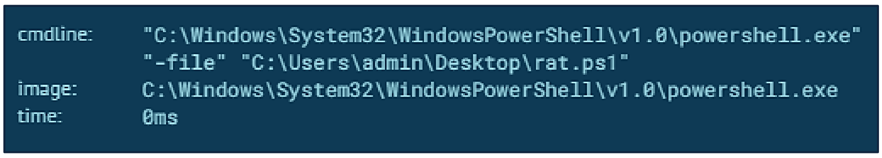


Contacting the server for information.

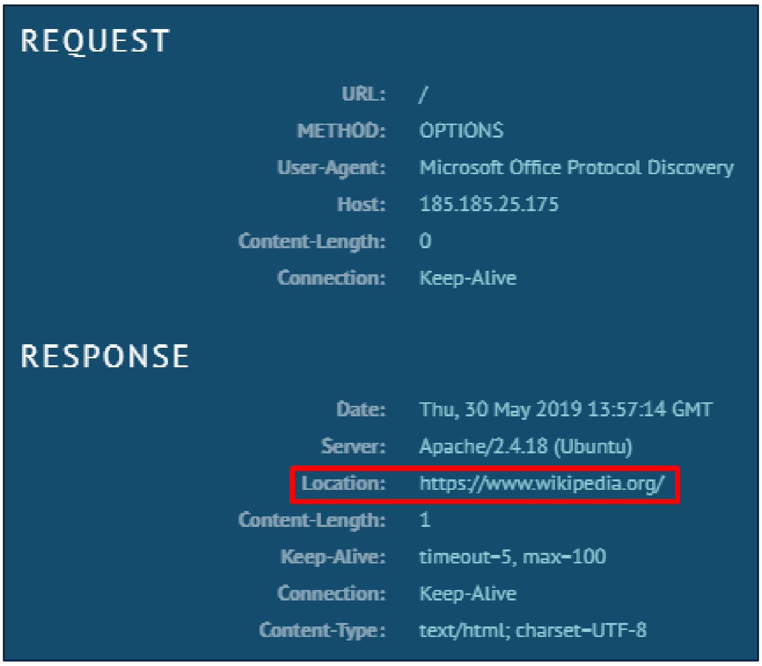


PID	Process	Method	HTTP Code	IP	URL
2972	WINWORD.EXE	OPTIONS	302	185.185.25.175:80	http://185.185.25.175/
2972	WINWORD.EXE	GET	—	185.185.25.175:80	http://185.185.25.175/ref45.php
2972	WINWORD.EXE	GET	404	185.185.25.175:80	http://185.185.25.175/ref45.php

Note that this file also redirects to Wikipedia if it does not receive a reply from the server:



```
cmdline:    "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
            "-file" "C:\Users\admin\Desktop\rat.ps1"
image:      C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
time:       0ms
```



REQUEST

URL: /
METHOD: OPTIONS
User-Agent: Microsoft Office Protocol Discovery
Host: 185.185.25.175
Content-Length: 0
Connection: Keep-Alive

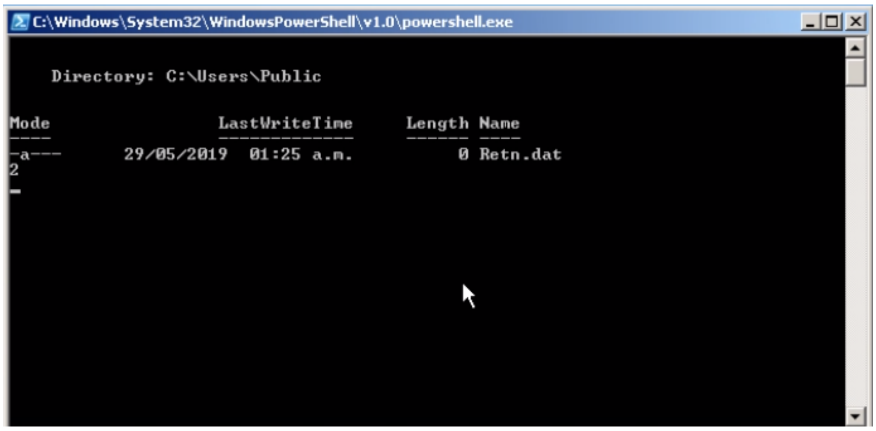
RESPONSE

Date: Thu, 30 May 2019 13:57:14 GMT
Server: Apache/2.4.18 (Ubuntu)
Location: https://www.wikipedia.org/
Content-Length: 1
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Malware analysis – RAT

We discovered a RAT file that communicates to the aforementioned IP address. The RAT was scanned on AnyRun by an unknown user in late May.

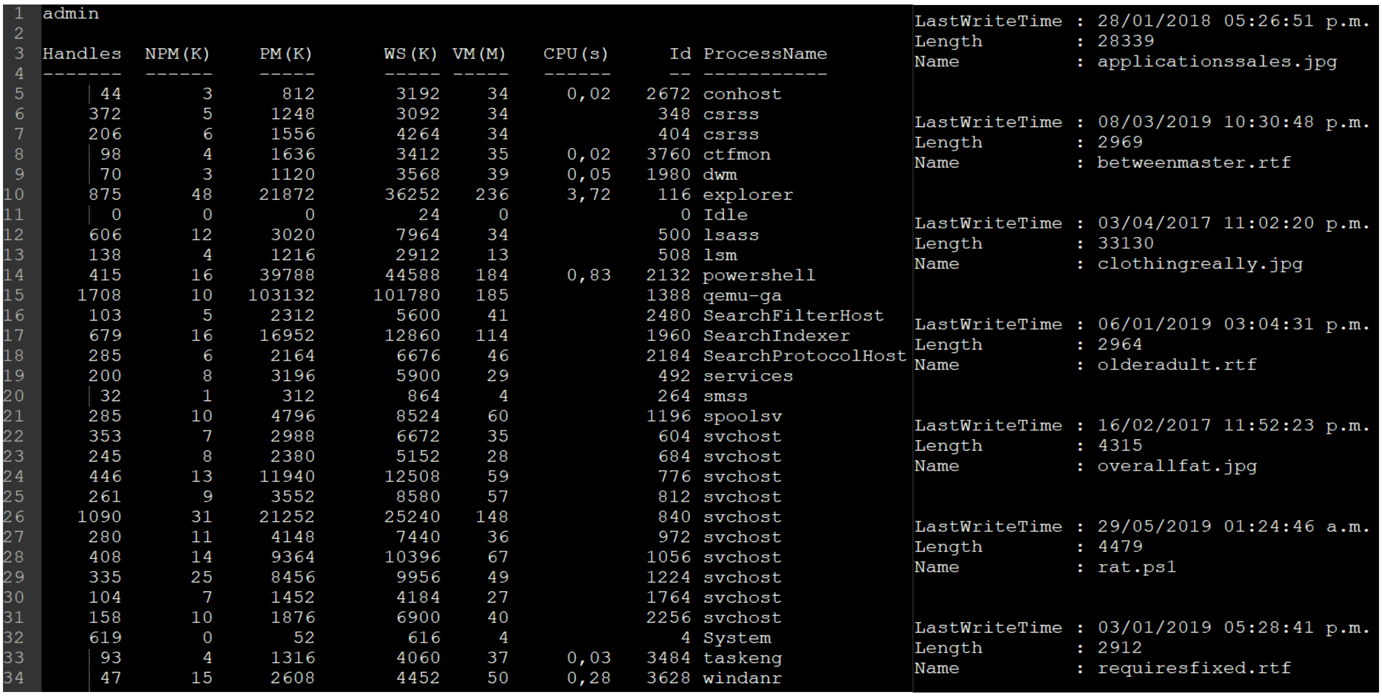
First, the RAT is extracted with the PowerShell. Seen in the following image is its execution. Initially it communicates with the server, which activates a php script named 'game'.



C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
    Directory: C:\Users\Public

Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---        29/05/2019   01:25 a.m.        0 Retn.dat
2
_
```

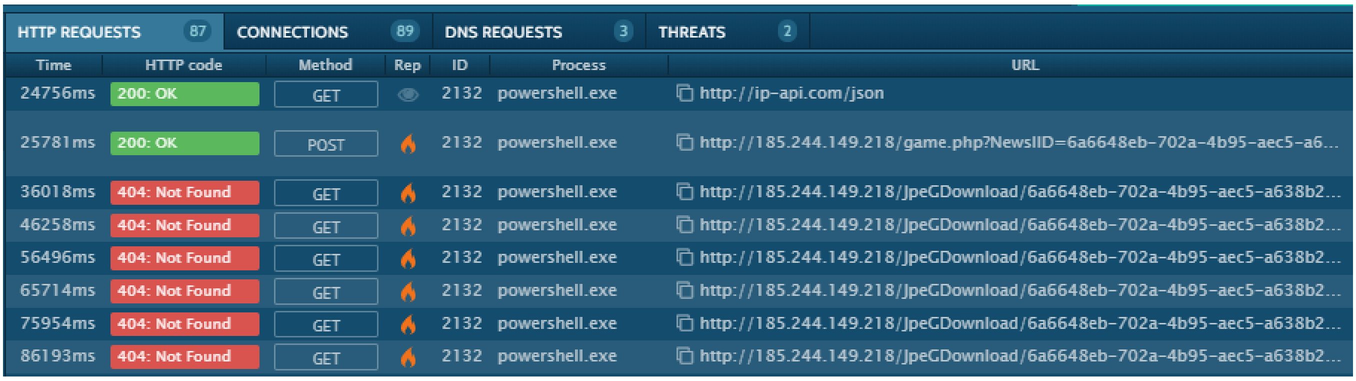
To our understanding, this is an initial script which requests the compromised computer to report back to the attacker about processes running on the system. After receiving indication from the C2 server (hxxp://185.244.149[.]218/game.php), an encoded base64 output is sent to the attacker about these processes:



```
admin

Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
     44       3      812       3192    34     0,02   2672 conhost
    372       5     1248       3092    34             348 csrss
    206       6     1556       4264    34             404 csrss
     98       4     1636       3412    35     0,02   3760 ctfmon
     70       3     1120       3568    39     0,05   1980 dwm
    875      48    21872      36252   236     3,72    116 explorer
      0       0        0         24     0               0 Idle
    606      12     3020       7964    34             500 lsass
    138       4     1216       2912    13             508 lsm
    415      16    39788      44588   184     0,83   2132 powershell
   1708      10   103132     101780   185            1388 qemu-ga
    103       5     2312       5600    41            2480 SearchFilterHost
    679      16    16952      12860   114            1960 SearchIndexer
    285       6     2164       6676    46            2184 SearchProtocolHost
    200       8     3196       5900    29             492 services
     32       1      312        864     4             264 smss
    285      10     4796       8524    60            1196 spoolsv
    353       7     2988       6672    35             604 svchost
    245       8     2380       5152    28             684 svchost
    446      13    11940      12508    59             776 svchost
    261       9     3552       8580    57             812 svchost
   1090      31    21252      25240   148             840 svchost
    280      11     4148       7440    36             972 svchost
    408      14     9364      10396    67            1056 svchost
    335      25     8456       9956    49            1224 svchost
    104       7     1452       4184    27            1764 svchost
    158      10     1876       6900    40            2256 svchost
    619       0       52        616     4               4 System
     93       4     1316       4060    37     0,03   3484 taskeng
     47      15     2608       4452    50     0,28   3628 windanr
```

```
LastWriteTime : 28/01/2018 05:26:51 p.m.
Length        : 28339
Name          : applicationssales.jpg

LastWriteTime : 08/03/2019 10:30:48 p.m.
Length        : 2969
Name          : betweenmaster.rtf

LastWriteTime : 03/04/2017 11:02:20 p.m.
Length        : 33130
Name          : clothingreally.jpg

LastWriteTime : 06/01/2019 03:04:31 p.m.
Length        : 2964
Name          : olderadult.rtf

LastWriteTime : 16/02/2017 11:52:23 p.m.
Length        : 4315
Name          : overallfat.jpg

LastWriteTime : 29/05/2019 01:24:46 a.m.
Length        : 4479
Name          : rat.ps1

LastWriteTime : 03/01/2019 05:28:41 p.m.
Length        : 2912
Name          : requiresfixed.rtf
```

Afterwards, similarly to other files attributed to files in this camgains, it sends dozens of communicates requests to its C2 server in order to receive commands. However, this sample did not receive any response from the server, and therefore no new actions were taken:



Time	HTTP code	Method	Rep	ID	Process	URL
24756ms	200: OK	GET	👁	2132	powershell.exe	http://ip-api.com/json
25781ms	200: OK	POST	🔥	2132	powershell.exe	http://185.244.149.218/game.php?NewsIID=6a6648eb-702a-4b95-aec5-a6...
36018ms	404: Not Found	GET	🔥	2132	powershell.exe	http://185.244.149.218/JpeGDownload/6a6648eb-702a-4b95-aec5-a638b2...
46258ms	404: Not Found	GET	🔥	2132	powershell.exe	http://185.244.149.218/JpeGDownload/6a6648eb-702a-4b95-aec5-a638b2...
56496ms	404: Not Found	GET	🔥	2132	powershell.exe	http://185.244.149.218/JpeGDownload/6a6648eb-702a-4b95-aec5-a638b2...
65714ms	404: Not Found	GET	🔥	2132	powershell.exe	http://185.244.149.218/JpeGDownload/6a6648eb-702a-4b95-aec5-a638b2...
75954ms	404: Not Found	GET	🔥	2132	powershell.exe	http://185.244.149.218/JpeGDownload/6a6648eb-702a-4b95-aec5-a638b2...
86193ms	404: Not Found	GET	🔥	2132	powershell.exe	http://185.244.149.218/JpeGDownload/6a6648eb-702a-4b95-aec5-a638b2...

MuddyWater impersonation entities

Like previous attacks, most of the targets impersonate to entities in countries that surround Iran. They impersonate in this campaign to the following actors:

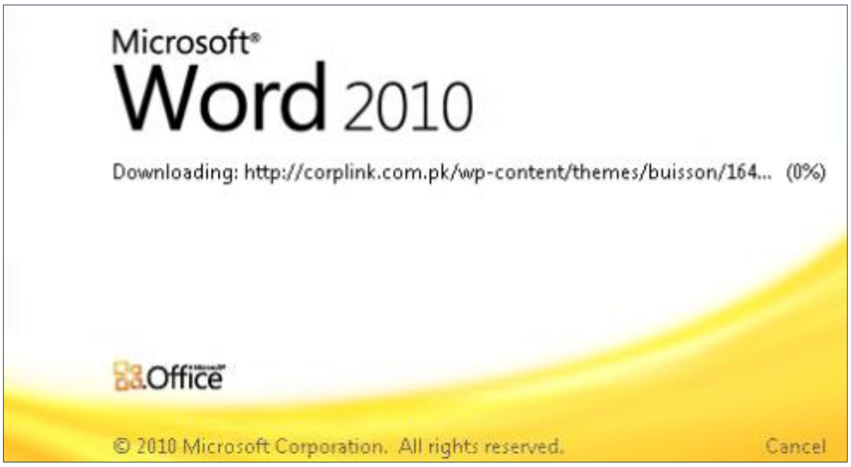
- Kurdish groups (for example Komala – a Kurdish-Iranian party in Iraq).
- Actors connected to the Iraq government.
- Actors connected to the Tajikistan government.
- Actors connected to the Pakistan government.
- Actors connected to communication company in Pakistan.
- Unknown actors that are connected to India.
- Unknown actors in the UAE.
- Unknown actors in Cyprus.

The combained attack vector

We identified several files that leverage both of the TTPs, presented above.

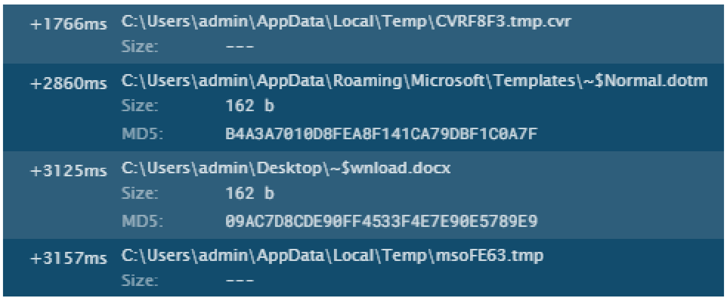
Opening the file leverages CVE-2017-0199 and sends a request to the hacked server.

Concurrently, the aforementioned files are created. The file conducts several communication requests with the compromised server in an attempt to download a JPG file that contains that malicious macro.

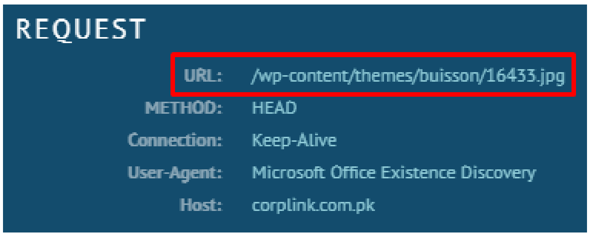


Downloading: http://corplink.com.pk/wp-content/themes/buisson/164... (0%)

© 2010 Microsoft Corporation. All rights reserved.

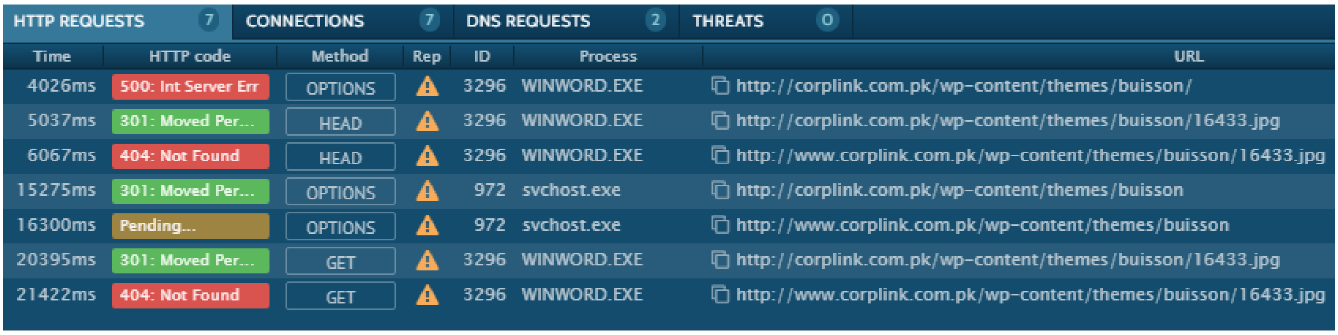


```
+1766ms  C:\Users\admin\AppData\Local\Temp\CVRF8F3.tmp.cvr
         Size:      ---
+2860ms  C:\Users\admin\AppData\Roaming\Microsoft\Templates\~$Normal.dotm
         Size:      162 b
         MD5:       B4A3A7010D8FEA8F141CA79DBF1C0A7F
+3125ms  C:\Users\admin\Desktop\~$wnload.docx
         Size:      162 b
         MD5:       09AC7D8CDE90FF4533F4E7E90E5789E9
+3157ms  C:\Users\admin\AppData\Local\Temp\msoFE63.tmp
         Size:      ---
```



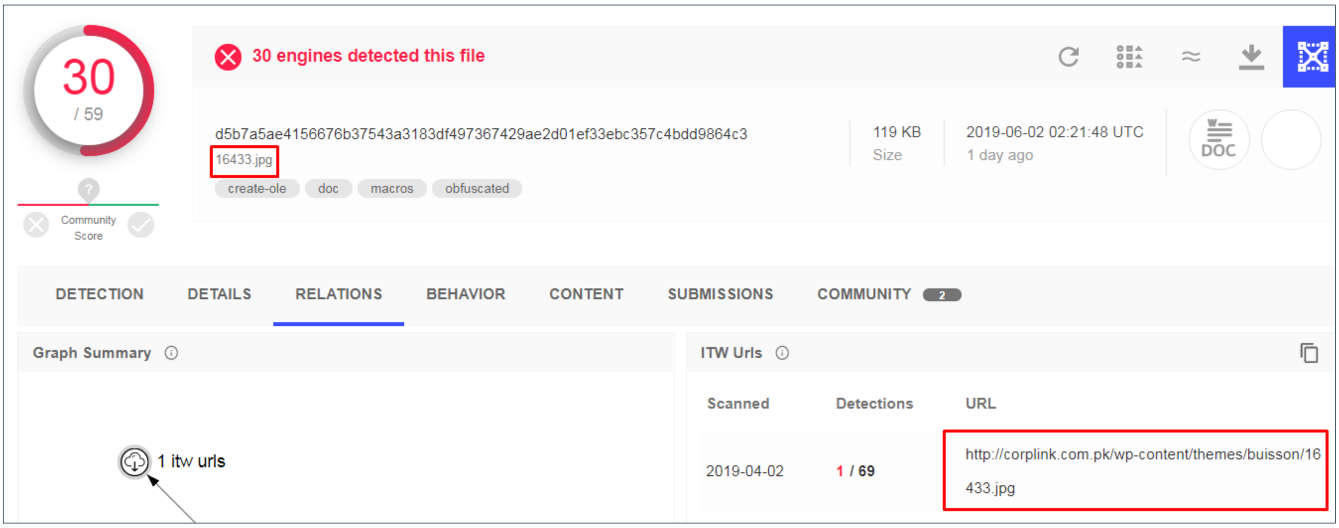
REQUEST

URL:	/wp-content/themes/buisson/16433.jpg
METHOD:	HEAD
Connection:	Keep-Alive
User-Agent:	Microsoft Office Existence Discovery
Host:	corplink.com.pk



Time	HTTP code	Method	Rep	ID	Process	URL
4026ms	500: Int Server Err	OPTIONS	⚠	3296	WINWORD.EXE	http://corplink.com.pk/wp-content/themes/buisson/
5037ms	301: Moved Per...	HEAD	⚠	3296	WINWORD.EXE	http://corplink.com.pk/wp-content/themes/buisson/16433.jpg
6067ms	404: Not Found	HEAD	⚠	3296	WINWORD.EXE	http://www.corplink.com.pk/wp-content/themes/buisson/16433.jpg
15275ms	301: Moved Per...	OPTIONS	⚠	972	svchost.exe	http://corplink.com.pk/wp-content/themes/buisson
16300ms	Pending...	OPTIONS	⚠	972	svchost.exe	http://www.corplink.com.pk/wp-content/themes/buisson
20395ms	301: Moved Per...	GET	⚠	3296	WINWORD.EXE	http://corplink.com.pk/wp-content/themes/buisson/16433.jpg
21422ms	404: Not Found	GET	⚠	3296	WINWORD.EXE	http://www.corplink.com.pk/wp-content/themes/buisson/16433.jpg

In our investigation, the C2 server communication failed; however, we detected a sample of this file on VT.



30 engines detected this file

d5b7a5ae4156676b37543a3183df497367429ae2d01ef33ebc357c4bdd9864c3

16433.jpg

create-ole doc macros obfuscated

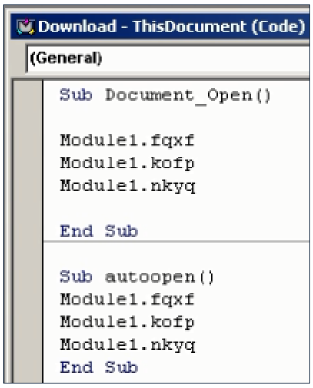
119 KB
Size

2019-06-02 02:21:48 UTC
1 day ago

ITW Urls

Scanned	Detections	URL
2019-04-02	1 / 69	http://corplink.com.pk/wp-content/themes/buisson/16433.jpg

Despite having the file extension 'JPG', it is in fact a Doc file embedded with the following Macro. Similar to the first vector we described, the Macro executed an embedded Excel file via DCOMLaunch:

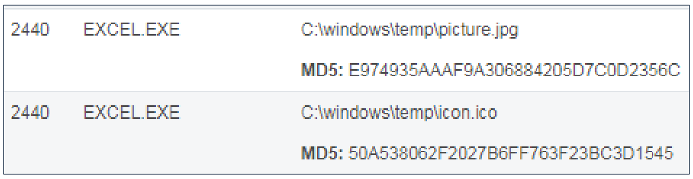


```
Sub Document_Open()

Module1.fqxf
Module1.kofp
Module1.nkyq

End Sub

Sub autoopen()
Module1.fqxf
Module1.kofp
Module1.nkyq
End Sub
```

```
"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
```

In a similar fashion to previous attacks, two files are created within the 'Temp' folder. These files contain segments of the malicious code used to extract the POWERSTATS malware:

1. 'icon.ico' create "Wscript.Shell" Object and run WScript.Arguments.
2. 'Picture.jpg' contains the malicious code of the second stage malware. It is encoded by multiple layers of obfuscated VBScript (VBE), JavaScript and PowerShell code.



2440	EXCEL.EXE	C:\windows\temp\picture.jpg **MD5:** E974935AAAF9A306884205D7C0D2356C
2440	EXCEL.EXE	C:\windows\temp\icon.ico **MD5:** 50A538062F2027B6FF763F23BC3D1545

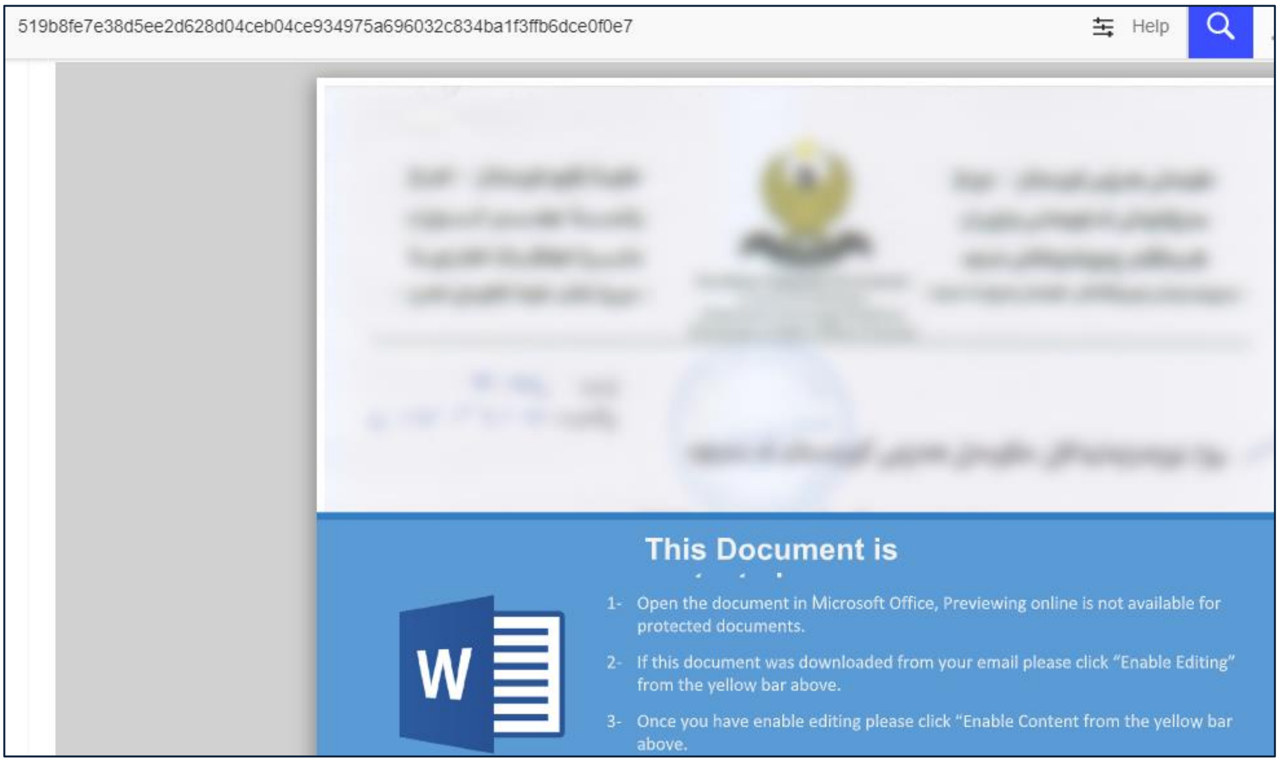
The contents of the documents

The documents can be categorized into two groups.

The first group

Documents that resemble the previous documents used by MuddyWater. Some of these documents are almost exact copies in terms of content (while changing the attack method). Below is a comparison between them:

A document that exploits a macro code in order to communicate with the server (from the report Iranian APT MuddyWater Attack Infrastructure Targeting Kurdish Political Groups and Organizations in Turkey):



519b8fe7e38d5ee2d628d04ceb04ce934975a696032c834ba1f3ffb6dce0f0e7
Help
W

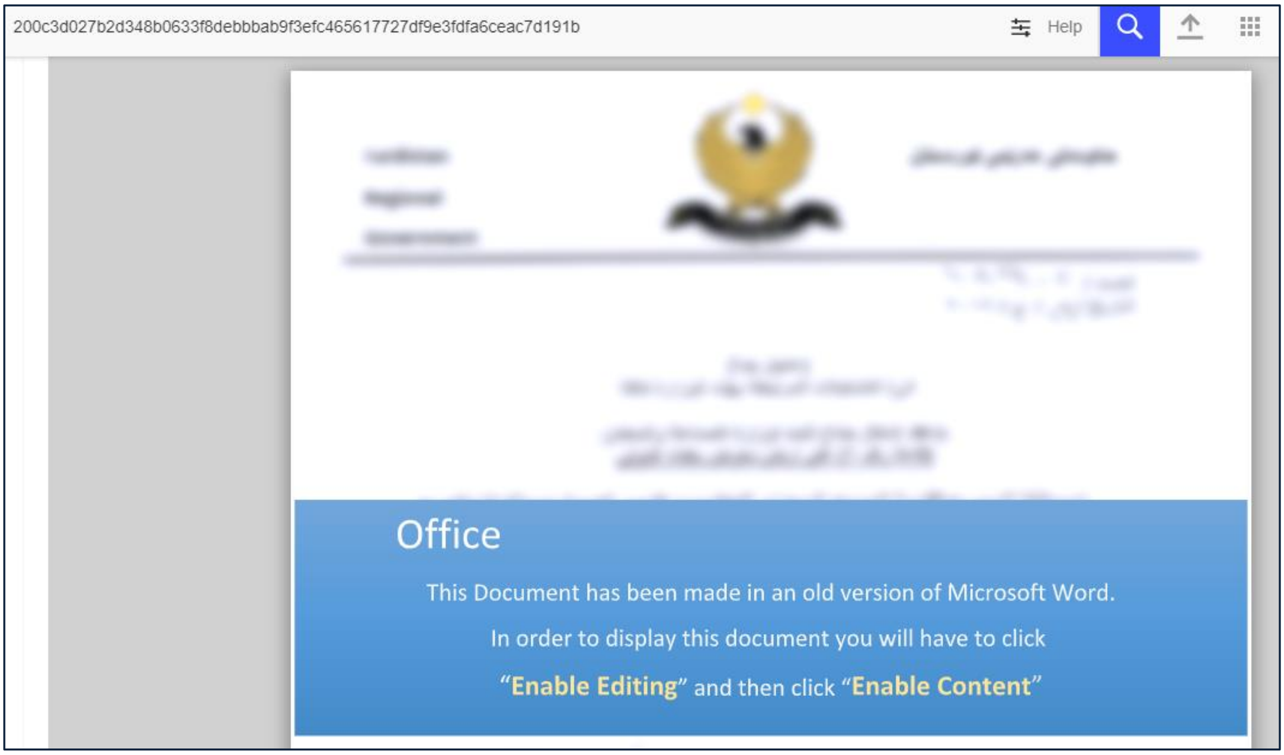
This Document is

1- Open the document in Microsoft Office, Previewing online is not available for protected documents.

2- If this document was downloaded from your email please click "Enable Editing" from the yellow bar above.

3- Once you have enable editing please click "Enable Content from the yellow bar above.

A document from the current campaign that exploits the CVE-2017-0199 vulnerability:



200c3d027b2d348b0633f8debbbab9f3efc465617727df9e3fdfa6ceac7d191b

Office

This Document has been made in an old version of Microsoft Word.

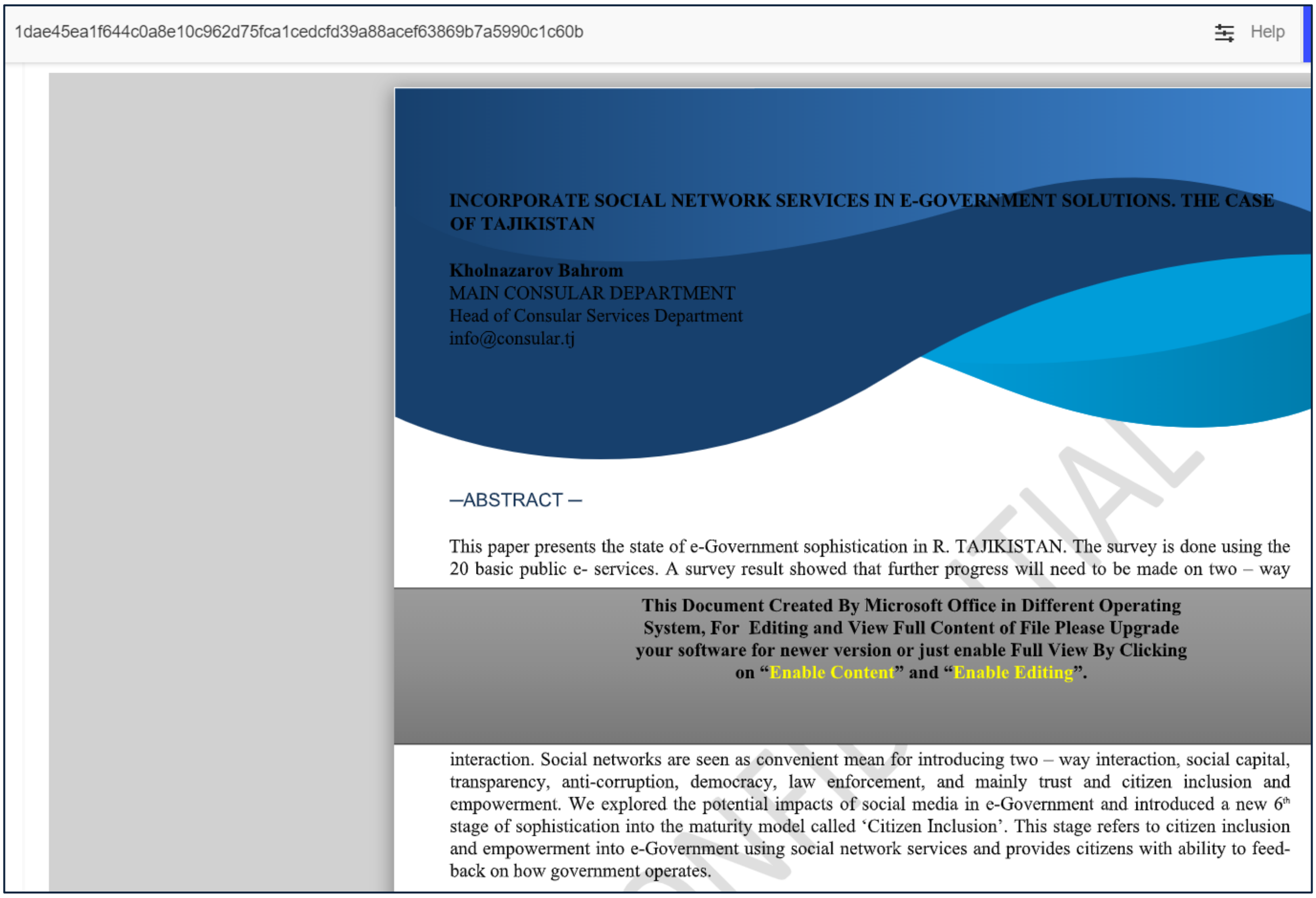
In order to display this document you will have to click

"Enable Editing" and then click "Enable Content"

Both of them are disguised as official documents of the regional government of Kurdistan. Moreover, the new documents' OLE data is generic, while in previous attacks they contained fraudulent names.

The second group

Documents written in English and disguised as unofficial documents from countries surrounding Iran (India and Tajikistan for example). Unlike MuddyWater's known attack vectors, the content is not blurred, and has no request to click on 'Enable Content'.



1dae45ea1f644c0a8e10c962d75fca1cedcfd39a88acef63869b7a5990c1c60b

INCORPORATE SOCIAL NETWORK SERVICES IN E-GOVERNMENT SOLUTIONS. THE CASE OF TAJIKISTAN

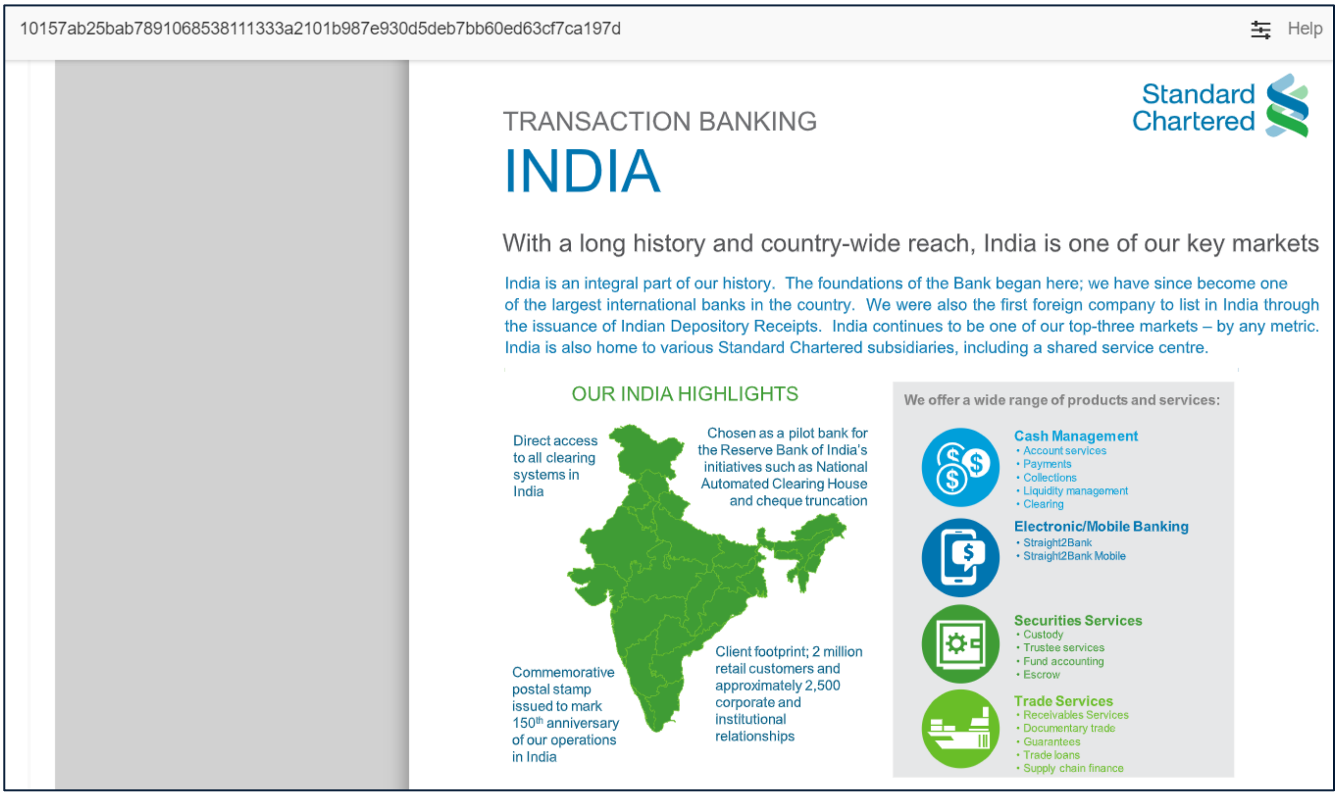
Kholnazarov Bahrom
MAIN CONSULAR DEPARTMENT
Head of Consular Services Department
info@consular.tj

—ABSTRACT—

This paper presents the state of e-Government sophistication in R. TAJIKISTAN. The survey is done using the 20 basic public e- services. A survey result showed that further progress will need to be made on two – way

This Document Created By Microsoft Office in Different Operating System, For Editing and View Full Content of File Please Upgrade your software for newer version or just enable Full View By Clicking on "Enable Content" and "Enable Editing".

interaction. Social networks are seen as convenient mean for introducing two – way interaction, social capital, transparency, anti-corruption, democracy, law enforcement, and mainly trust and citizen inclusion and empowerment. We explored the potential impacts of social media in e-Government and introduced a new 6th stage of sophistication into the maturity model called 'Citizen Inclusion'. This stage refers to citizen inclusion and empowerment into e-Government using social network services and provides citizens with ability to feed-back on how government operates.



10157ab25bab7891068538111333a2101b987e930d5deb7bb60ed63cf7ca197d

TRANSACTION BANKING

INDIA

With a long history and country-wide reach, India is one of our key markets

India is an integral part of our history. The foundations of the Bank began here; we have since become one of the largest international banks in the country. We were also the first foreign company to list in India through the issuance of Indian Depository Receipts. India continues to be one of our top-three markets – by any metric. India is also home to various Standard Chartered subsidiaries, including a shared service centre.

OUR INDIA HIGHLIGHTS

Direct access to all clearing systems in India

Chosen as a pilot bank for the Reserve Bank of India's initiatives such as National Automated Clearing House and cheque truncation

Commemorative postal stamp issued to mark 150th anniversary of our operations in India

Client footprint; 2 million retail customers and approximately 2,500 corporate and institutional relationships

We offer a wide range of products and services:

Cash Management
- Account services
- Payments
- Collections
- Liquidity management
- Clearing

Electronic/Mobile Banking
- Straight2Bank
- Straight2Bank Mobile

Securities Services
- Custody
- Trustee services
- Fund accounting
- Escrow

Trade Services
- Receivables Services
- Documentary trade
- Guarantees
- Trade loans
- Supply chain finance

Indicators of Compromise

f5ef4a45e19da1b94c684a6c6d51b86aec622562c45d67cb5aab554f21eb9061

d5b7a5ae4156676b37543a3183df497367429ae2d01ef33ebc357c4bdd9864c3

d77d16c310cce09b872c91ca223b106f4b56572242ff5c4e756572070fac210f

98f0f2c42f703bfbb96de87367866c3cced76d5a8812c4cbc18a2be3da382c95

200c3d027b2d348b0633f8debbbab9f3efc465617727df9e3fdfa6ceac7d191b

951585840a07a6496b0270f1028281fcb65d5b9e9a6ed613ca8809b258ed729f

1dae45ea1f644c0a8e10c962d75fca1cedcfd39a88acef63869b7a5990c1c60b

10157ab25bab7891068538111333a2101b987e930d5deb7bb60ed63cf7ca197d

0a9d295016417b00457d4a031b5c52eea41bcde3465ac517767d8795a6a213eb

20bf83bf516b12d991d38fdc014add8ad5db03907a55303f02d913db261393a9

e2867e2255cad213fcc5752a7062882e92870c57

8d1464e0cac7ea8f37e83fd142212c95db20fe77

4fe389bc1ea85896b4ebb6fe26aa40a6e3f8e9ca

592f0d9d7185eadab0509fdafdc305ab

65978dd3d6b3a518f465676aa6bd876e

bb6fda2cdc852112544d2598a784d04f

6cb076f1f42573c5c43083a89bcfe442

BEB6A4354549AE4F5579F25865EA8967

66[.]219[.]22[.]235

83[.]171[.]238[.]62

185[.]185[.]25[.]175

185[.]244[.]14[.]218

hXXp://185[.]185[.]25[.]175/sDownloads/

hXXp://185[.]185[.]25[.]175/upl[.]php

hXXp://185[.]185[.]25[.]175/ref45[.]php

MISP event 1583

Email: info@clearskysec.com
Website: clearskysec.com

CLEARSKY
Cyber Security

Ahead of the Threat Curve

ClearSky cyber security solutions assists companies and organizations in preparing, identifying and resolving cyber security threats. Our team of security experts helps prevent security breaches by detecting early attack indicators, and providng in-depth analysis and intelligence that enable you to make informed mitigation decisions in real time.

ClearSky is comprised of intelligence researchers and cyber experts, who monitor, research and expose attack groups and cyberattacks around the globe. Our unique ClearSkySec© methodology is based on years of experience in mitigating cyberattacks targeting numerus sectors, including the financial sector, the pharma sector, as well as public and critical infrastructure sectors.