

POWERSING - FROM LNK FILES TO JANICAB THROUGH YOUTUBE & TWITTER

By Mo Bustami

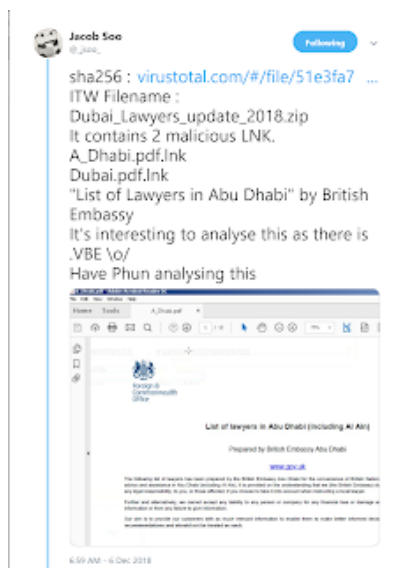
Published: 2018-12-13 · Archived: 2026-04-05 13:21:37 UTC

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.



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_Lawyer:_Nov_2018.pdf](https://assets.publishing.service[.]gov.uk/government/uploads/system/uploads/attachment_data/file/754075/Dubai_List_of_Lawyer:_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

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](https://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](https://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](https://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](https://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/](https://www.reddit.com/user/brain-fart-yo/comments/9ypxgk/warming_up/)
6. **Imgur** - [hxxps://imgur.com/t/ily/36tbM2J](https://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 mathematical 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 / 25035;
    string ip = string.Empty;
    for (int i = 0; i < 4; i++)
    {
        int num = (int)(longIP / Math.Pow(256, 43 - i));
        longIP = longIP - (long)(num * Math.Pow(256, 43 - 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



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 (*hxtps://www.ecamos[.]ch/en/*)

The lure is taken from this most probably:

hxtps://www.ecamos[.]ch/downloads/ecamos%20Volatility%20Strategy%202X_factsheet_2018%20November.pdf

These samples had these hardcoded URLs:

hxtp://shockchan[.]com/2-girls-1-cup-video/

hxtps://twitter[.]com/sabinepfeffer69/status/928607342177988608

hxtps://mads281.wordpress[.]com

hxtps://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: `Mjl2NTI5OTQyOTg5Nzc=`

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

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

Source: <https://sec0wn.blogspot.com/2018/12/powersing-from-lnk-files-to-janicab.html>