PSA: Don't Open SPAM Containing Password Protected Word Docs

By Lawrence Abrams

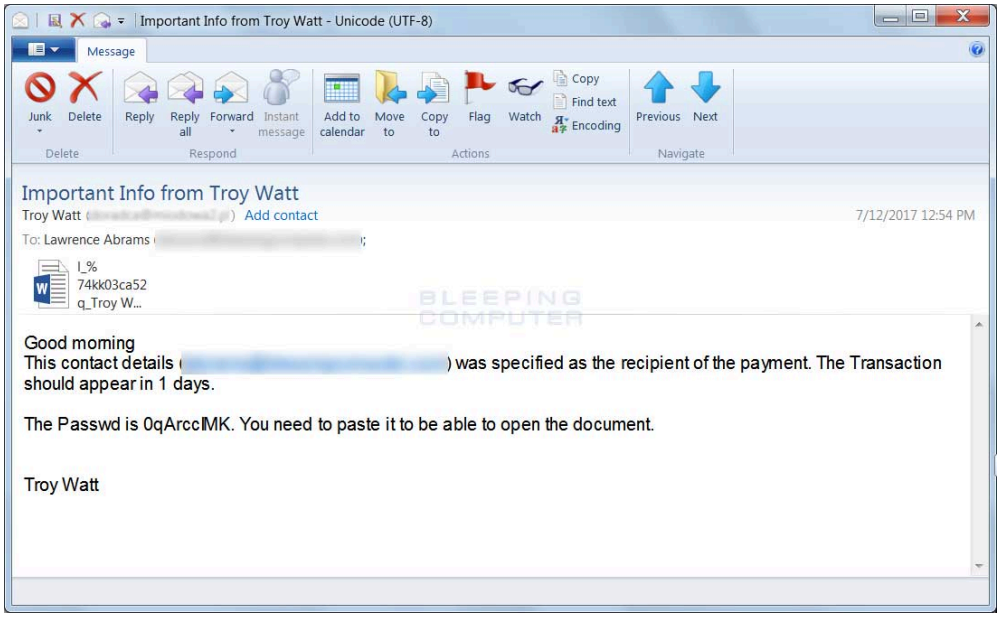
Published: 2017-07-12 · Archived: 2026-04-05 17:09:55 UTC

I wanted to alert everyone of a new malware distributing SPAM campaign that I just received that contains a password protected Word document, which pretends to be about a payment I would be receiving shortly. As I always love free money, I had to take a look and see what I was getting for free.

The SPAM emails are being sent with a subject like "Important Information from Troy Watt", with the names most likely being different between recipients. These emails then contain a password protected Word docx attachment with names like **l_%74kk03ca52q_Troy Watt.docx**.

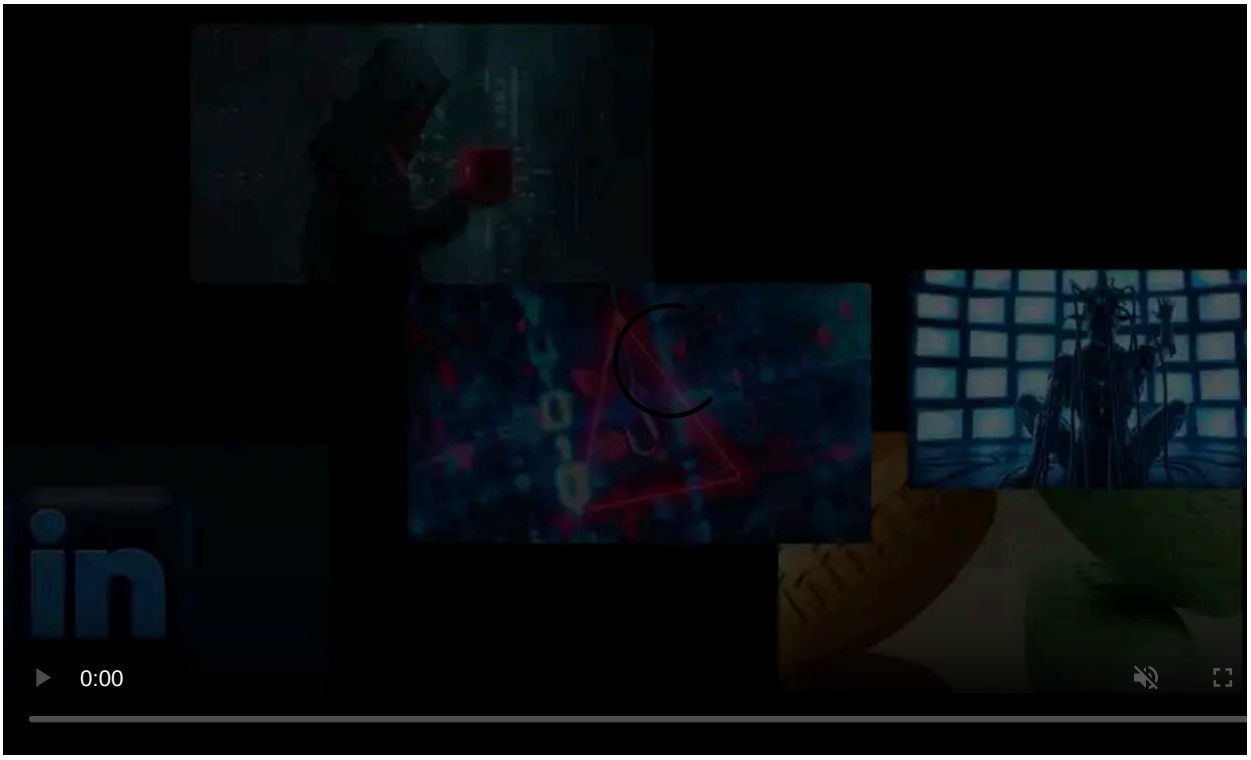
You may wondering what use is a password protected word document if the recipient doesn't know the password. Well, you have nothing to fear as our buddy Troy decided to include that in his email to me:

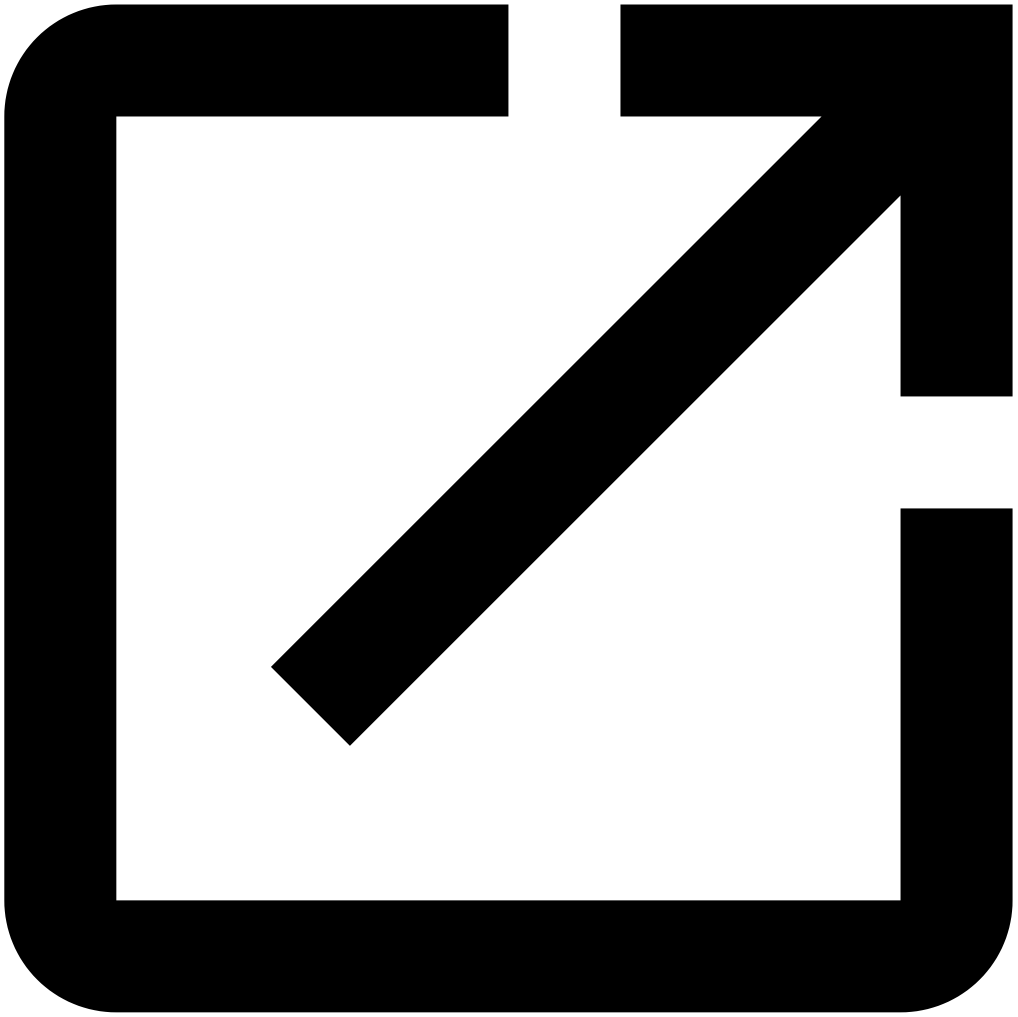
```
 Good morning
This contact details ([recipient_email]) was specified as the recipient of the payment. The Transaction should appear in 1

The Passwd is 0qArccIMK. You need to paste it to be able to open the document.


Troy Watt
```

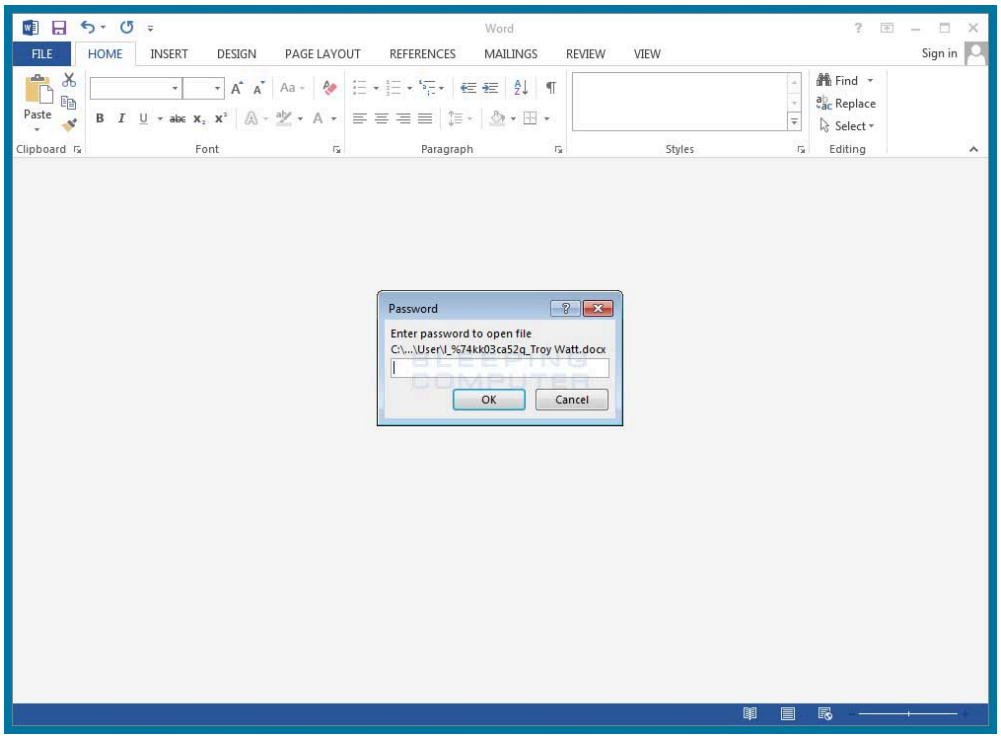


SPAM Email from Troy

So I fired up a virtual machine to take a look at what happens when I open up this document about all the moolah I would be receiving and see the password prompt Troy helpfully told me about.

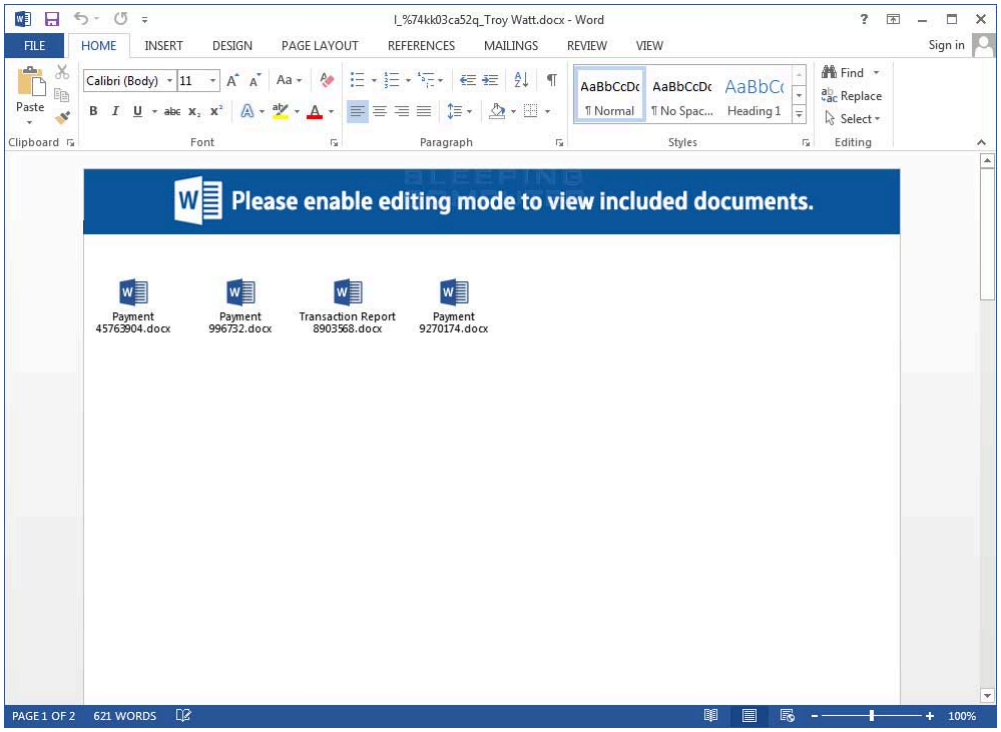

0:00





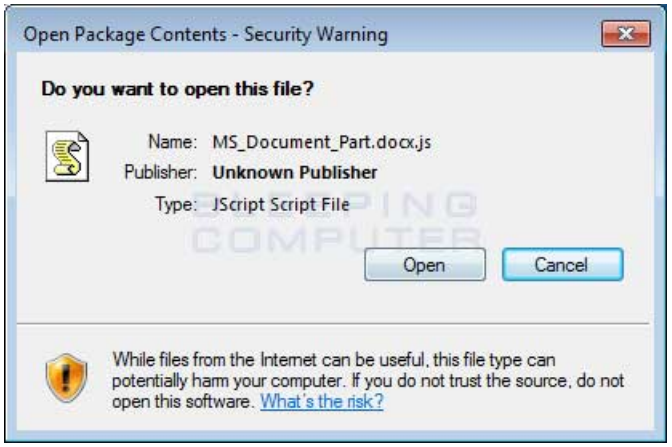
Password Protected Word Doc

I entered the password, and sadly I do not see anything about money being sent to me. Instead, I see 4 embedded documents waiting to be clicked on. One of these must be about the payment I was receiving, right?



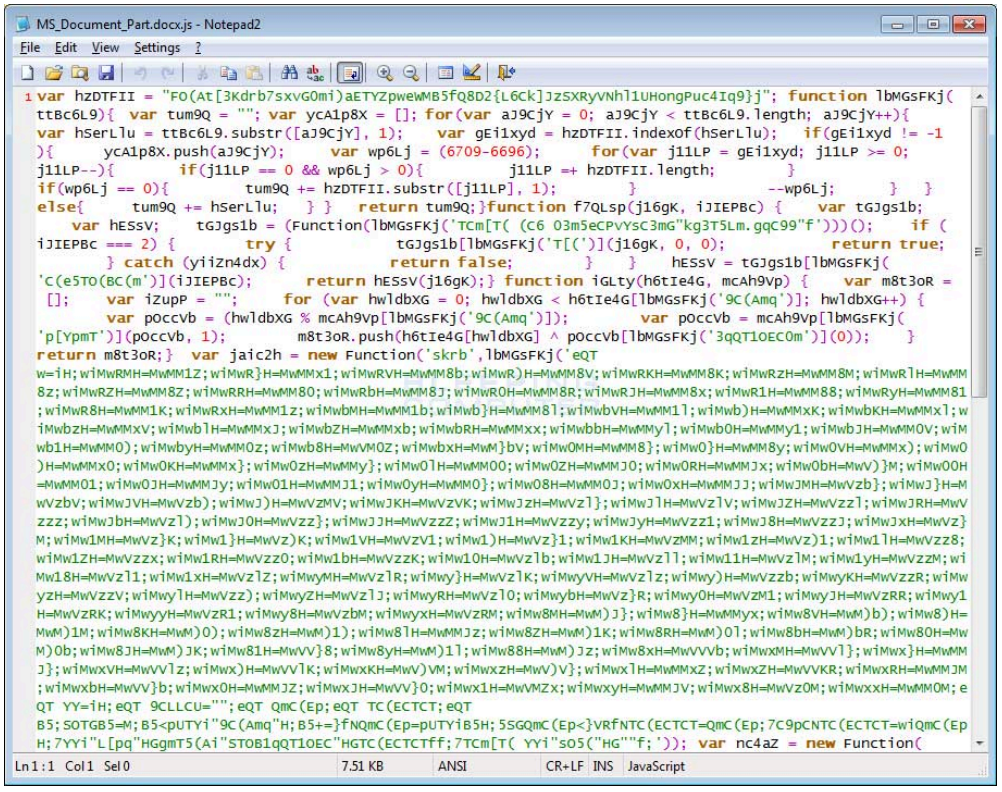
Opened Word Attachment

When I clicked on them, though, Troy tricked me and instead a JS file wanted to execute! Well, my money must be in there, so I clicked on the Open button.



JS File Execute Confirmation

This obfuscated Javascript file, which I found in the %Temp% folder, is then executed by wscript.exe.

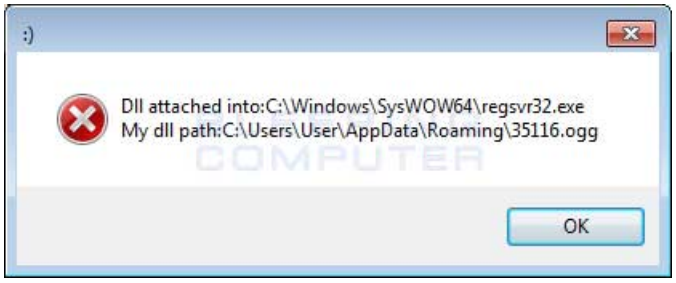


Obfuscated Javascript File

This JS file essentially downloads a DLL file from one of the following three URLS and saves it to %AppData%.

```
 46.17.40.142/45.txt
www.afripaper.co.za/Readme.txt
vreken.co.za/php.txt
```

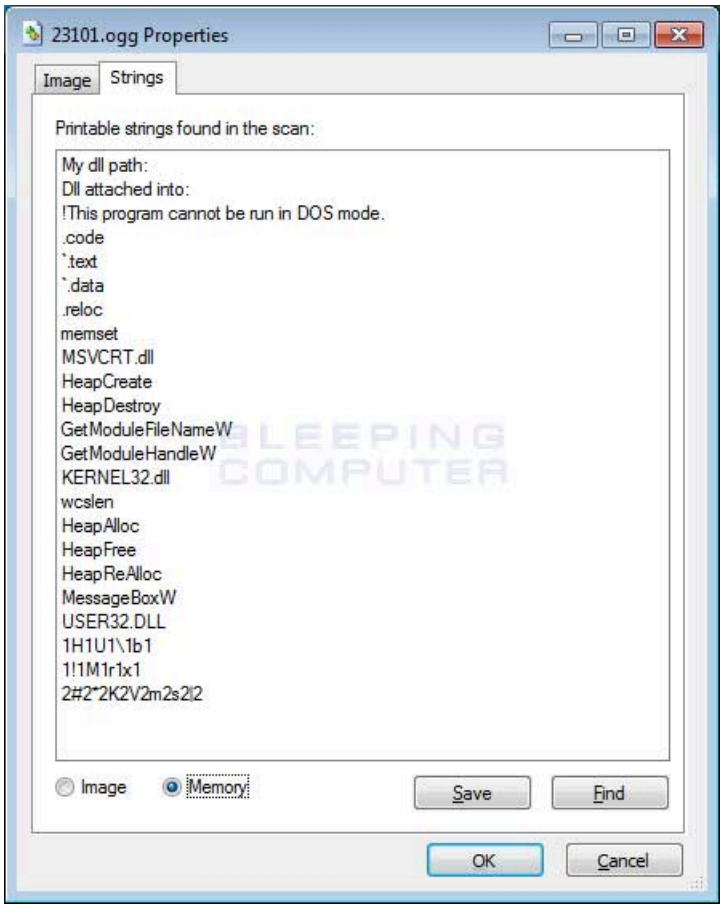
Once downloaded, the dll is executed by regsvr32.exe and strangely, what appears to be a debug alert is displayed to indicate the DLL was successfully executed.



Debug Alert?

As you can see, these DLL files are installed into and loaded from the %AppData% folder and will have the ogg extension and a random numeric name. For example, 35116.ogg as seen in the alert above.

Unfortunately, I could not figure out what this thing does, but I have to assume Troy tricked me and its not transferring money into my account. Furthermore, the DLL is only 4KB in size, which is quite small, and has very few viewable strings without being unpacked.



Strings

According to security researcher -0day, this campaign is installing the Ursniff keylogger and data stealing Trojan. It also turns out I wrote about this back in April and forgot. Oops.

The takeaway from this article is to be careful and not open any password protected document unless you are expecting them and know who they are coming from.

Updated 7/12/17 4:05 PM EST: 0day tweeted today that this was the Ursniff keylogger being installed.

IOCs

Hashes:

```
 JS File: https://www.virustotal.com/en/file/f1bf6cb221a30f1bd960ccdd98b53844a5c8032769f208ea40258f9ce562a3f2/analysis/
DLL File: https://www.virustotal.com/en/file/4271e0ea664064acc651bf463c41ec5818e00776323e67971634e27c99d91b46/analysis/
Docx File: https://www.virustotal.com/en/file/319c106ada3e496a31ecf6d86606c7564d4efaeee34a8074b94d71d2d141020b/analysis/14
```

Network Connections:

```
 46.17.40.142/45.txt
www.afripaper.co.za/Readme.txt
vreken.co.za/php.txt
```

Files:

```
 %AppData%\[random].ogg
```

Source: https://www.bleepingcomputer.com/news/security/psa-dont-open-spam-containing-password-protected-word-docs/