Black Energy – Analysis

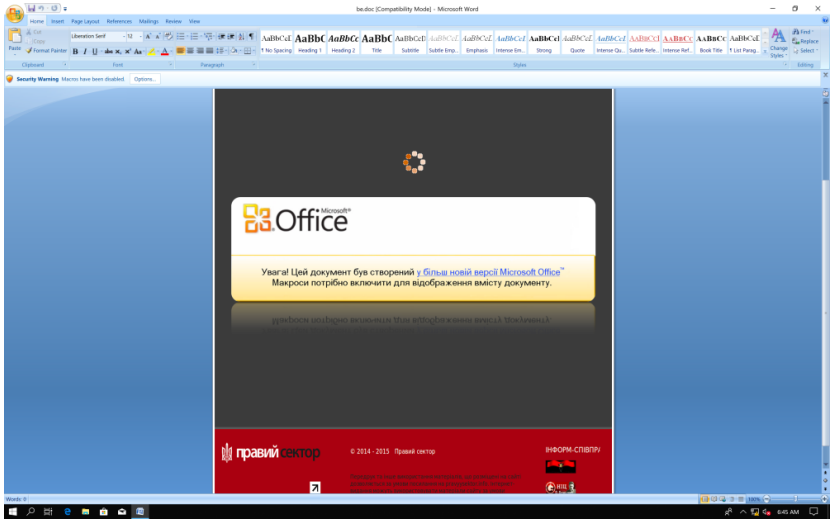
marcusedmondson.com/2019/01/18/black-energy-analysis

View all posts by Marcus Edmondson

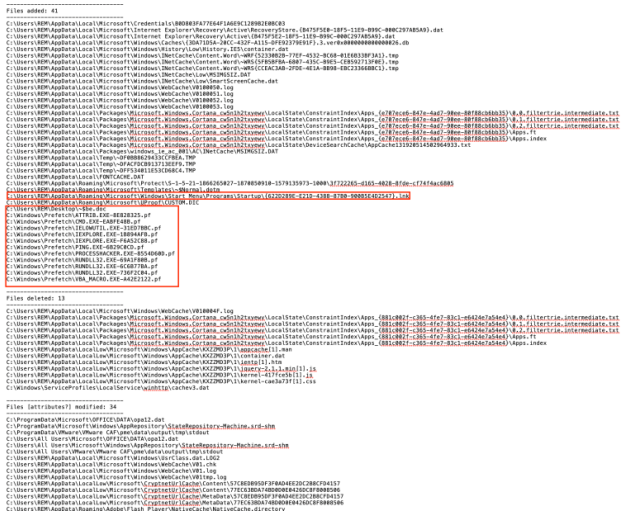
January 18, 2019

So today I wanted to do a blog post on Black Energy. The sample I will be working with was sourced from hybrid analysis here: https://www.hybrid-analysis.com/sample/39d04828ab0bba42a0e4cdd53fe1c04e4eef6d7b26d0008bd0d88b06cc316a81?environmentId=4. This particular piece of malware was used to target the networks used to control power grids and has been associated to the Sandworm Team, who used it to also target organizations in the Ukraine. According to Mitre the Sandworm Team is a Russian cyber espionage group that has operated since approximately 2009. The group likely consists of Russian pro-hacktivists. Sandworm Team targets mainly Ukrainian entities associated with energy, industrial control systems, SCADA, government, and media. Sandworm Team has been linked to the Ukrainian energy sector attack in late 2015. So now that we have a little background lets start our analysis.

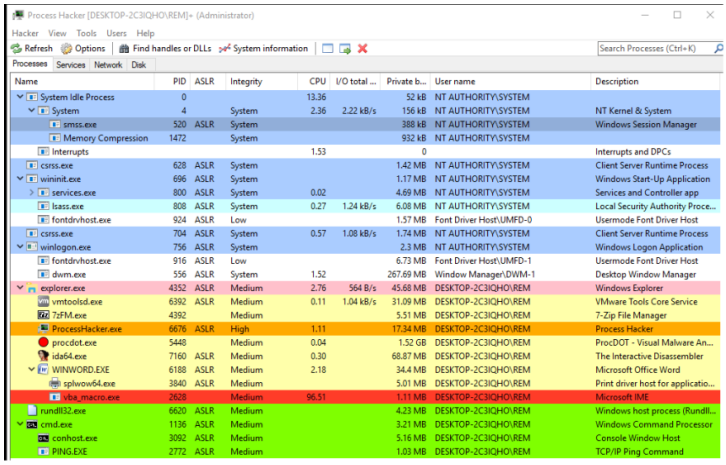
When you initially open up the document you are greeted with this.



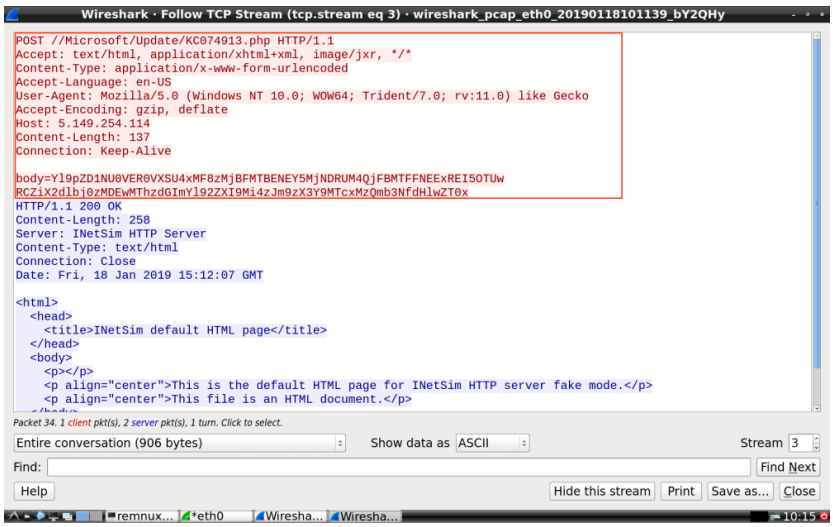
I don't speak Russian but, I'm pretty sure this is telling the user to view this document you need to enable the content. So lets do it and see what we can get. I'm going to use my usual setup of RegShot/Procmon and Process Hacker with my Windows VM pointing to my Remnux VM where I will have fakedns, inestsim and Wireshark running. So here is what RegShot is showing me.



After taking a quick look it looks like we have a .lnk file being dropped into the Startup folder which is a pretty common persistence technique used by malware. Inside the .lnk file the target is: %windir%\System32\rundll32.exe "C:\Users\IEUser\AppData\Local\FONTCACHE.DAT",#1. We also have multiple other processes being kicked off by the word document, one of which is vba_macro.exe that runs and deletes itself. Here is the process listing from Process Hacker.



After looking at Wireshark we also have a network connection going to 5[.]149[.]254[.]114//Microsoft/Update/KC074913[.]php and sending back some base64 to the server.

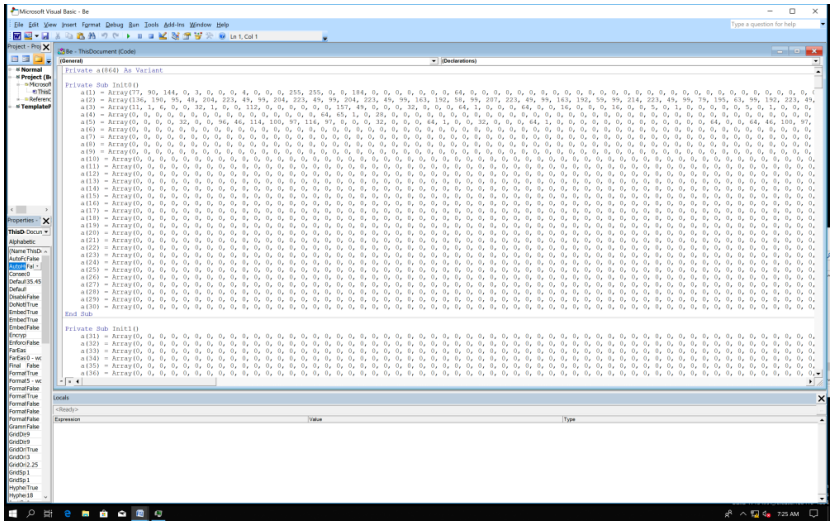


The base64 wil decode to this:

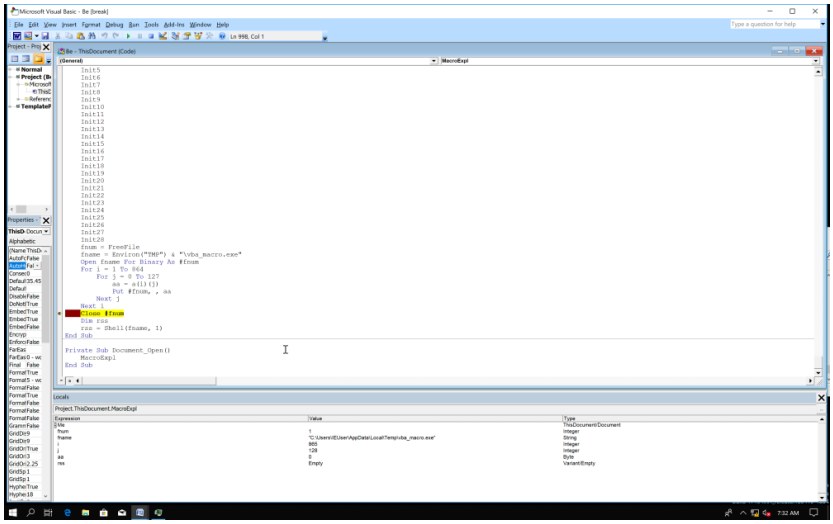
b_id=MSEDGEWIN10_320E10D4F923CEC8B1A11E4A1DB9950D&b_gen=301018stb&b_ver=2.3&os_v=17134&os_type=1

Which is the malware fingerprinting the host OS versions.

I also want to cover a quick way for you to dump vba_macro.exe before it runs and deletes itself. So on the Word document click alt+F11 or on Mac option+F11, this will bring up the Visual Basic window showing the macros. At the very beginning you see array after array of numbers, which appears to possibly be machine code.



If you scroll down to the bottom you will see the meat of what's happening. It is looping over the arrays and writing it to a file called vba_macro. So we will put a breakpoint right after the loop ends and then run the macros to dump the file, which we will then move to the desktop.

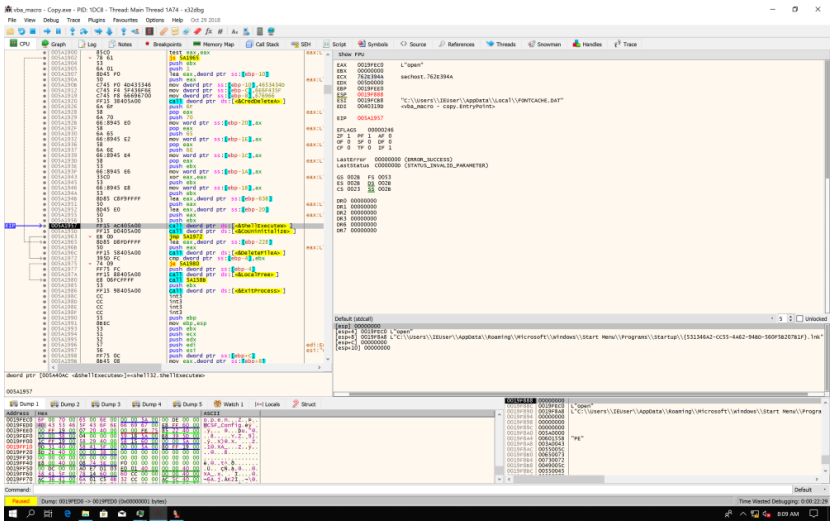


So as I started analyzing vba_macro I loaded it into IDA to get a look at the imports and strings, I noticed most of the imports had no xrefs which puzzled me for a while, I think a lot of the imports are in there to send the analyst down rabbit holes. So I loaded vba_macro up in x32dbg and set breakpoints on some Native API functions like NtWriteFile, NtOpenProcess, etc... I did this because I remember reading that malware will sometimes use these lower level API's to avoid detection. I then started running it to see what I could find.

So here is a call to NtWriteFile where it looks like it is creating the .lnk file.

```
EAX   0019F8A8   L"C:\\Users\\IEUser\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\{531346A2-CC55-4A62-94BD-560F5B207B1F}.l
EBX   00000000
ECX   75EC98B0   kernelbase.75EC98B0
EDX   005D0000
EBP   0019FEE0
ESP   0019F89C   &L"C:\\Users\\IEUser\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\{531346A2-CC55-4A62-94BD-560F5B207B1F}.
ESI   0019FCB8   "C:\\Users\\IEUser\\AppData\\Local\\FONTCACHE.DAT"
EDI   0040319D   <vba_macro - copy.EntryPoint>
```

And here is a call to ShellExecuteW opening the .lnk file.



So to sum things up a quick down and dirty of my interpretation of what this malware is doing:

1. Word document macros run which drop vba_macro to disk.
2. vba_macro creates the .lnk and fontcache.dat and runs .lnk file which in turn runs fontcache.dat with rundll32 which provides the network connectivity to the above address we talked about.
3. vba_macro also kicks off a cmd.exe which is continually running PING.exe and attrib.exe.

So thank you for reading and hope this has helped someone to learn something new and until next time…

Happy hunting,

Marcus

References:

https://attack.mitre.org/groups/G0034/

https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/

https://threatconnect.com/blog/casting-a-light-on-blackenergy/