APT27 ZxShell RootKit module updates

Iab52.io/blog/apt27-rootkit-updates

JagaimoKawaii

Within the toolset of the different APT groups, one of the most interesting elements and the one that generally worries the most, are their capabilities in Ring0, generally RootKit/Bootkit type threats that act with the maximum level of privileges.

An example of this type of threats is the RootKit module of ZxShell RAT used by Emissary Panda (APT27), of which there is a relatively recent sample (Uploaded to Virustotal since 2019-09-21 17:59:39) that is also correctly signed, so it can be loaded in the latest version of Windows 10 and is perfectly functional as far as we have been able to check.

Driver loaded:
RuleName:
UtcTime: 2020-01-09 08:15:15.213
ImageLoaded: C:\Windows\System32\drivers\autochk.sys
Hashes: SHA1=CE52808FBF36A1F08C80C313C689115212459717
Signed: true
Signature: Microsoft Windows
SignatureStatus: Valid
-

Sysmon DriverLoaded event

A complete analysis of this threat can be found made by the analyst Ori Damari (@0xrepnz) in his blog (https://repnz.github.io/posts/autochk-rootkit-analysis/). After analyzing this threat and describing its capabilities, he has rewritten the source code from a sample of this threat uploaded in 2018 to Virustotal, and published it in GitHub, which greatly facilitates the analysis of newer versions. As he describes in his blog, the capabilities of this Rootkit are basically the following:

File Redirection – Redirect malicious files to benign files. If you try to call CreateFile() to open a malicious file you'll get a handle to a benign file.

autochk.sys		XICINO INICIO CO	mpartir vista			
Property	Value	$\land \leftrightarrow \rightarrow \land \uparrow \square $	Este equipo > Disco local (C:) > Wind	ows > System32 > drivers		
File Name	C:\Windows\System32\drivers\autochk.sys		Nombre	Fecha de modificación	Тіро	Tamaño
File Type	Portable Executable 64	📌 Acceso rápido	AppvVerngr.sys	27/12/2019 19:43	Archivo de sistema	171 KE
File Info	No match found.	Escritorio	AppvVfs.sys	27/12/2019 19:43	Archivo de sistema	151 Ki
	-	Descargas	🖈 💿 arcsas.sys	19/03/2019 5:43	Archivo de sistema	130 KE
File Size	427.52 KB (437776 bytes)	😤 Documentos	🖈 💿 asyncmac.sys	19/03/2019 5:45	Archivo de sistema	31 KE
PE Size	419.00 KB (429056 bytes)	Imágenes	atani svs	19/03/2019 5:43	Archivo de sistema	30 KE
Created	Friday 27 December 2019, 19.43.14	Disco local (C:)	ataport.sys	12/03/2010 5:43	Archivo de sistema	218 KB
Modified	Friday 27 December 2019, 19.43.14	drivers	autochk.sys	10/01/2020 9:55	Archivo de sistema	33 KE
Accessed	Thursday 09 January 2020, 09.22.16		🗟 bam.sys	19/03/2019 5:44	Archivo de sistema	69 KE
MD5	3E149E6CF0C5CA47C89FABAEE220922E	📕 👌 Música	battc.sys	19/03/2019 5:43	Archivo de sistema	41 KE
		patala	bcmfn2.sys	19/03/2019 5:43	Archivo de sistema	10 KE
SHA-1	AF367A93451FE9AE35ADF83DD085547E793D54AF	> OneDrive	beep.sys	19/03/2019 5:44	Archivo de sistema	10 KE
`			bindflt.sys	27/12/2019 19:43	Archivo de sistema	115 KE
Property	Value	Este equipo	bowser.sys	19/03/2019 5:43	Archivo de sistema	115 KE
CompanyName	Microsoft Corporation	🔿 Red	bridge.sys	19/03/2019 5:45	Archivo de sistema	125 KE
FileDescription	Microsoft Filesystem Filter Manago	-	BtaMPM.sys	19/03/2019 5:43	Archivo de sistema	36 KE
FileVersion	10.0.18362.267 (WinBuild 100101.0800)		BthA2dp.sys	27/12/2019 19:42	Archivo de sistema	227 KE
nternalName		_	bthenum.sys	27/12/2019 19:42	Archivo de sistema	112 KE
	fltMgr.sys	_	BthHfEnum.sys	19/03/2019 5:43	Archivo de sistema	128 KE
LegalCopyright	© Microsoft Corporation. All rights reserved.		BthMini.SYS	27/12/2019 19:42	Archivo de sistema	36 KE
OriginalFilenam	e fltMgr.sys		bthmodem.sys	19/03/2019 5:43	Archivo de sistema	75 KE
ProductName	Microsoft® Windows® Operating System		bthport.sys	27/12/2019 19:42	Archivo de sistema	1.396 KE
			BTHUSB.SYS	27/12/2019 19:42	Archivo de sistema	96 KE

Network Connection Hiding – Hide network connections from tools like netstat,proceshacker...

We found interesting to analyze the differences between the 2018 version and the most recent 2019 version in order to try to identify new capabilities or changes in its capabilities. After comparing both samples using the GitHub source code, we have been able to see that most of the functions are identical, except for 5 of them (including the Driver's entrypoint):

Line	Address	Name	Address 2	Name 2	Ratio	BBlocks 1	BBlocks 2	Description
00000	000114b4	NetHookTcpDriver	00011560	NetHookTcpDriver	1.000	6	6	Perfect match, same name
00001	000116b4	NetTcpDriverCompletionRoutine	00011760	NetTcpDriverCompletionRoutine	1.000			Perfect match, same name
00002	00011d1c	FsCreateFileHook	00011bc4	FsCreateFileHook	1.000			Perfect match, same name
00003	0001285c	FsGetRedirectionTarget	00012128	FsGetRedirectionTarget	1.000			Perfect match, same name
00004	00012998	FsAddFileRedirection	00012264	FsAddFileRedirection	1.000	20	20	Perfect match, same name
00005	00011b4c	NetHookNsiProxy	000119f4	NethookNsiProxy	1.000			Same cleaned up assembly or pseudo-code
00006	00011600	NetTcoDriverDeviceIoctHook	000116ac	NetTcpDriverDeviceIoctHook	1.000			Same cleaned up assembly or pseudo-code
00007	000128ec	FsAddIgnoredTarget	000121b8	FsAddIgnoredProcess	1.000			Same cleaned up assembly or pseudo-code
00009	00011178	AutocheckDEviceControl	000112e8	AutochkDeviceControl	1.000		20	Same rare KOKA hash
00010	00011158	AutoChkIrpDefaultDispatcher	000112c8	AutochkIrpDefaultDispatcher	1.000			Mnemonics and names

Identical functions in both versions

Line	Address	Name	Address 2	Name 2	Ratio	BBlocks 1	BBlocks 2	Description
00000	00011008	FsFreeFileRedirection	00011168	FsFreeFileRedirection	0.880	16	17	Perfect match, same name
00002	00011948	NetInitializeConnectionHider	00011008	NetInitializeConnectionHider	0.640	8		Perfect match, same name
00001	000112ac	DriverEntry	0001141c	DriverEntry	0.620	8		Perfect match, same name
00003	00011ee4	FsPutRedirectorHook	00011d8c	FsPutRedirectorHook	0.590	23	21	Perfect match, same name
00004	000120f0	FsInitializeFileRedirection	00011ecc	FsInitializeFileRedirection	0.130	71	4	Perfect match, same name

Different functions

After analyzing the differences between this 5 functions, we have been able to observe that all the changes are focused on avoiding detections by slightly "obfuscating" some IOCs hardcoded as strings and code modification without impact in the capabilities on the driver...

In total, there are three notable changes between the two versions:

The first one basically consists in that they have reversed the list of strings that identify the files that the Driver hides by default when it is loaded:

					's'	.text:00000	000003C	C (1	lld.ipawlhs\\23metsyS\\swodniW\\
's'	.text:00000	0000004A	C (1	\\WINDOWS\\System32\\DRIVERS\\fltMgr.sys	5 '5'	.text:00000	0000003C	C (1 C (1	\\WINDOWS\\System32\\DRIVERS\\fltMgr.sys
's'	.text:00000	0000004C	C (1	\\WINDOWS\\System32\\DRIVERS\\autochk.sys	s'				
's'	.text:00000	000003C	C (1	\\Windows\\System32\\shlwapi.dll		.text:00000	0000004C	C (1	sys.khcotua\\SREVIRD\\23metsyS\\SWODNIW\\
's'	.text:00000	0000003E	C (1	\\Windows\\System32\\odbcwg32.cpl	's'	.text:00000	0000003E	C (1	lpc.23gwcbdo\\23metsyS\\swodniW\\
's'	.text:00000	0000003C	C (1	\\Windows\\System32\\c_21268.nls	's'	.text:00000	0000003C	C (1	sln.86212_c\\23metsyS\\swodniW\\
's'	.text:00000	0000003E	C (1	\\Windows\\System32\\cliconfg.cpl	's'	.text:00000	0000003E	C (1	lpc.gfnocilc\\23metsyS\\swodniW\\
's'	.text:00000	0000003C	C (1	\\Windows\\System32\\imekr61.dll	's'	.text:00000	0000003C	C (1	lld. 16rkemi\\23metsyS\\swodniW\\
's'	.text:00000	0000003E	C (1	\\Windows\\System32\\PINTLGNT.dll	's'	.text:00000	0000003E	C (1	lld.TNGLTNIP\\23metsyS\\swodniW\\
's'	.text:00000	000003C	C (1	\\Windows\\System32\\chrsben.ime	's'	.text:00000	0000003C	C (1	emi.nebsrhc\\23metsyS\\swodniW\\
's'	.text:00000	000003C	C (1	\\Windows\\System32\\bitsprx.ime	's'	.text:00000	0000003C	C (1	emi.xrpstib\\23metsyS\\swodniW\\
's'	.text:00000	0000003A	C (1	\\Windows\\System32\\C_1950.NLS	's'	.text:00000	000003A	C (1	SLN.0591_C\\23metsyS\\swodniW\\
's'	.text:00000	000003C	C (1	\\Windows\\System32\\C_26849.NLS	's'	.text:00000	0000003C	C (1	SLN.94862_C\\23metsyS\\swodniW\\
's'	.text:00000	000003C	C (1	\\Windows\\System32\\chrsben.dll	's'	.text:00000	000003C	C (1	lld.nebsrhc\\23metsyS\\swodniW\\
's'	.text:00000	00000040	C (1	\\Windows\\System32\\mfc100usx.dll	's'	.text:00000	00000040	C (1	lld.xsu001cfm\\23metsyS\\swodniW\\
's'	.text:00000	000003C	C (1	\\Windows\\System32\\wlanseo.dll	's'	.text:00000	000003C	C (1	lld.oesnalw\\23metsyS\\swodniW\\
's'	.text:00000	000003E	C (1	\\Windows\\System32\\KBDDWSKY.DLL	's'	.text:00000	000003E	C (1	LLD.YKSWDDBK\\23metsyS\\swodniW\\
's'	.text:00000	000003C	C (1	\\Windows\\System32\\imseo21.ime	's'	.text:00000	000003C	C (1	emi. 12oesmi\\23metsyS\\swodniW\\
's'	.text:00000	000003C	C (1	\\Windows\\System32\\midiapi.dll	's'	.text:00000	000003C	C (1	lld.ipaidim\\23metsyS\\swodniW\\
's'	.text:00000	0000003E	C (1	\\Windows\\System32\\mfc120du.dll	's'	.text:00000	000003E	C (1	lld.ud021cfm\\23metsyS\\swodniW\\
's'	.text:00000	00000048	C (1	\\Windows\\System32\\wbem\\Joadperf.dll	's'	.text:00000	00000048	C (1	lld.frepdaol\\mebw\\23metsyS\\swodniW\\
's'	.text:00000	0000003E	C (1	\\Windows\\System32\\audiosrc.dll	's'	.text:00000	000003E	C (1	lld.crsoidua\\23metsyS\\swodniW\\
's'	.text:00000	0000003C	C (1	\\Windows\\System32\\bootred.dll	's'	.text:00000	0000003C	C (1	lld.dertoob\\23metsyS\\swodniW\\
's'	.text:00000	0000003E	C (1	\\Windows\\System32\\cryptdns.dll	's'	.text:00000	000003E	C (1	lld.sndtpyrc\\23metsyS\\swodniW\\
's'	.text:00000	00000040	C (1	\\Windows\\System32\\cryptbios.dll	's'	.text:00000	00000040	C (1	lld.soibtpyrc\\23metsyS\\swodniW\\
's'	.text:00000	00000040	C (1	\\Windows\\System32\\dhcpcsvcd.dll	's'	.text:00000	00000040	C (1	lld.dcvscpchd\\23metsyS\\swodniW\\
's'	.text:00000	0000003E	C (1	\\Windows\\System32\\iscsiapi.dll	's'	.text:00000	000003E	C (1	lld.ipaiscsi\\23metsyS\\swodniW\\
's'	.text:00000	000003A	C (1	\\Windows\\System32\\keyzip.dll	's'	.text:00000	000003A	C (1	lld.pizyek\\23metsyS\\swodniW\\
's'	.text:00000	0000003E	C (1	\\Windows\\System32\\odbccx32.dll	's'	.text:00000	0000003E	C (1	lld.23xccbdo\\23metsyS\\swodniW\\
's'	.text:00000	0000003E	C (1	\\Windows\\System32\\samlib32.dll	's'	.text:00000	0000003E	C (1	lld.23bilmas\\23metsyS\\swodniW\\
's'	.text:00000	00000040	C (1	\\Windows\\System32\\salnclc11.dll	\mathbf{s}	.text:00000	00000040	C (1	lld.11clcnlqs\\23metsyS\\swodniW\\
's'	.text:00000	0000003C	C (1	\\Windows\\System32\\shlzapi.dll	's'	.text:00000	000003C	C (1	lld.ipazlhs\\23metsyS\\swodniW\\
's'	.text:00000	0000003C	C (1	\\Windows\\System32\\shlyapi.dll	's'	.text:00000	000003C	C (1	lld.ipaylhs\\23metsyS\\swodniW\\
's'	.text:00000	0000003C	C (1	\\Windows\\System32\\prnfsdk.dll	's'	.text:00000	000003C	C (1	lld.kdsfnrp\\23metsyS\\swodniW\\
's'	.text:00000	0000003E	C (1	\\Windows\\System32\\AudioSdk.dll	's'	.text:00000	000003E	C (1	lld.kdSoiduA\\23metsyS\\swodniW\\
's'	.text:00000	0000003E	C (1	\\Windows\\System32\\stdole32.dll	's'	.text:00000	000003E	C (1	lld.23elodts\\23metsyS\\swodniW\\
		COCCOUL	- (1	In the second process of the second second					there are a strand

Old and New list of file names

At code level, the impact this has had is that the function that redirects these files, now uses the "wcrev" function that flips the strings before passing them to the function that hides the files:

FsAddFileRedirection(v7, L"\\WINDOWS\\System32\\DRIVERS\\fltMgr.sys");	9 FsAddFileRedirection(L"\\WINDOWS\\System32\\DRIVERS\\autochk.sys", L"\\WINDOWS\\System32\\DRIVERS\\fltMg	r.sys")
vB = 0164;	10 FsAddFileRedirection(L"\\Windows\\System32\\odbcwg32.cpl", L"\\Windows\\System32\\shlwapi.dll");	
do	11 FsAddFileRedirection(L"\\Windows\\System32\\c_21268.nls", L"\\Windows\\System32\\shlwapi.dll");	
4	12 FsAddFileRedirection(L"\\Windows\\System32\\cliconfg.cpl", L"\\Windows\\System32\\shlwapi.dll");	
v9 = *(_WORD *)(v8 * 2 + 78320);	13 FsAddFileRedirection(L"\\Windows\\System32\\imekr61.dll", L"\\Windows\\System32\\shlwapi.dll");	
Str[v8] = v9;	14 FsAddFileRedirection(L"\\Windows\\System32\\PINTLGNT.dll", L"\\Windows\\System32\\shlwapi.dll");	
++v8,	15 FsAddFileRedirection(L"\\Windows\\System32\\chrsben.ime", L"\\Windows\\System32\\shlwapi.dll");	
3	16 FsAddFileRedirection(L"\\Windows\\System32\\bitsprx.ime", L"\\Windows\\System32\\shlwapi.dll");	
while (v9);	17 FsAddFileRedirection(L"\\Windows\\System32\\C_1950.NLS", L"\\Windows\\System32\\shlwapi.dll");	
v10 = <u>wcsrev</u> ((wchar_t *)Str);	18 FsAddFileRedirection(L"\\Windows\\System32\\C_26849.NLS", L"\\Windows\\System32\\shlwapi.dll");	
FsAddFileRedirection(v10, (unsignedint16 *)&v106);	19 FsAddFileRedirection(L"\\Windows\\System32\\chrsben.dll", L"\\Windows\\System32\\shlwapi.dll");	
V11 = 0164;	20" FsAddFileRedirection(L"\\Windows\\System32\\mfc100usx.dll", L"\\Windows\\System32\\shlwapi.dll");	
de	21 FsAddFileRedirection(L"\\Windows\\System32\\wlanseo.dll", L"\\Windows\\System32\\shlwapi.dll");	
4	22 FsAddFileRedirection(L"\\Windows\\System32\\KBDDWSKY.DLL", L"\\Windows\\System32\\shlwapi.dll");	
$v12 = *(_WORD *)(v11 * 2 + 78384);$	23 FsAddFileRedirection(L"\\Windows\\System32\\imseo21.ime", L"\\Windows\\System32\\shlwapi.dll");	
Str[v11] = v12;	24 FsAddFileRedirection(L"\\Windows\\System32\\midiapi.dll", L"\\Windows\\System32\\shlwapi.dll");	
++v11;	25 FsAddFileRedirection(L"\\Windows\\System32\\mfcl20du.dll", L"\\Windows\\System32\\shlwapi.dll");	
3	26 FsAddFileRedirection(L"\\Windows\\System32\\wbem\\loadperf.dll", L"\\Windows\\System32\\shlwapi.dll");	
while (v12);	27 FsAddFileRedirection(L"\\Windows\\System32\\audiosrc.dll", L"\\Windows\\System32\\shlwapi.dll");	
<pre>v13 = wcsrev((wchar_t *)Str);</pre>	28 FsAddFileRedirection(L"\\Windows\\System32\\bootred.dll", L"\\Windows\\System32\\shlwapi.dll");	
FsAddFileRedirection(v13, (unsignedint16 *) &v106);	29 FsAddFileRedirection(L"\\Windows\\System32\\cryptdns.dll", L"\\Windows\\System32\\shlwapi.dll");	
v14 = 0164;	30 FsAddFileRedirection(L"\\Windows\\System32\\cryptbios.dll", L"\\Windows\\System32\\shlwapi.dll");	
do	31 FsAddFileRedirection(L"\\Windows\\System32\\dhcpcsvcd.dll", L"\\Windows\\System32\\shlwapi.dll");	
4	32 FsAddFileRedirection(L"\\Windows\\System32\\iscsiapi.dll", L"\\Windows\\System32\\shlwapi.dll");	
v15 = +(_WORD +)(v14 + 2 + 78448);	33 FsAddFileRedirection(L"\\Windows\\System32\\keyzip.dll", L"\\Windows\\System32\\shlwapi.dll");	
Str[v14] = v15;	34 FsAddFileRedirection(L"\\Windows\\System32\\odbccx32.dll", L"\\Windows\\System32\\shlwapi.dll");	
++v14;	35 FsAddFileRedirection(L"\\Windows\\System32\\samlib32.dll", L"\\Windows\\System32\\shlwapi.dll");	
3	36 FsAddFileRedirection(L"\\Windows\\System32\\sqlnclc11.dll", L"\\Windows\\System32\\shlwapi.dll");	
while (v15);	37 FsAddFileRedirection(L"\\Windows\\System32\\shlzapi.dll", L"\\Windows\\System32\\shlwapi.dll");	
<pre>v16 = wcsrev((wchar_t *)Str);</pre>	38 FsAddFileRedirection(L"\\Windows\\System32\\shlyapi.dll", L"\\Windows\\System32\\shlwapi.dll");	
FsAddFileRedirection(v16, (unsignedint16 *)&v106);	39 FsAddFileRedirection(L"\\Windows\\System32\\prnfsdk.dll", L"\\Windows\\System32\\shlwapi.dll");	
v17 = 0164;	40 FsAddFileRedirection(L"\\Windows\\System32\\AudioSdk.dll", L"\\Windows\\System32\\shlwapi.dll");	
do	41 FsAddFileRedirection(L"\\Windows\\System32\\stdole32.dll", L"\\Windows\\System32\\shlwapi.dll");	
4	42 RtlInitUnicodeString(&SystemRoutineName, L"ObReferenceObjectByName");	

New code (Red) and old code (Green)

Secondly, they have tried to disguise their use of the undocumented Microsoft API "ObReferenceObjectByName", which is used to get the pointer to the different Driver_Object drivers they intend to hook in each case. Until now, they had the name of this function in their strings, and used it to resolve it by passing its name to the MmGetSystemRoutineAddress API which returns a pointer to it. Now they only keep part of the name, and complete the rest in a slightly more complex way before calling MmGetSystemRoutineAddress by building it from characters they store in the registers and other areas of the binary:

	_	-
v10 = -1164;		if ((signed int)ObReferenceObjectByName(
<pre>v11 = L"ReferenceObjectBy";</pre>	74	
do	75	64164,
	76	0164.
	77	0164,
	78	
	79	
	80	
	81	
	82	
if (!v10)	83	
break	84	
v2 = *(WORD *)v9 == 0;	85	
$v_2 = (int *)((char *)v_3 + 2);$		leculi lesulo,
		}
while (!v2);		else
	8/	erse
v12 = 18164;		
v13 = (wchart *) ((char *)v9 - 2);		
while (v12)		
*v13 = *v11;		
++v11;		
++v13;		
v12;		
3		
v14 = sv26;		
v15 = -1164;		
do		
4		
if (!v15)		
break;		
v2 = + (_WORD +) v14 == 0;		
v14 = (int *)((char *)v14 + 2);		
v15;		
3		
while (!v2);		
*(_QHORD *)((char *)v14 - 2) = 'e\0m\0a\0N';		
*((_WORD *)v14 + 3) = 0;		
RtlInitUnicodeString(&SystemRoutineName, (PCWSTR)&v26);		
v16 = (int64 (fastcall *)(UNICODE_STRING *, signedint64, _QWORD))MmGetSystemRoutineAddress(&SystemRoutineName)	7	
if (!v16)		
return 3221225473164;		
result = v16(&DestinationString, 64164, 0164);		
if ((signed int)result >= 0)		
		n de la recene de la definit de la definit e relación de la de la definit de la definit de la definit de la de

New code (Red) and old code (Green)

Finally, they have moved part of the logic of some functions to another point, maintaining the same functionality. An example is the end of the driver entry function, where untill now, at the end they only called two functions that initialized the logic of hiding connections and redirecting files, and now, they have extracted part of the logic of these functions and moved it right after each one of them, but without any impact on the capabilities and behavior of the Driver:



New code (Red) and old code (Green)

x64	42eab05c611bf24d86bb6c985-
Sample	caa2ad7380ed7d98340c7f08de9361be14dc244
x86	9b7c1e37d5f56c-
Sample	c0b5e5e22ce9805e237a189297e78405b9c392a0953b6e0321