Lecture 11

Example Rootkit

Intel internship

- Intel CTG (Corporate Technology Group)
 - Advanced research & development
 - System integrity services using AMT
 - Detecting rootkits
 - C programming experience
 - Low-level OS knowledge
 - Embedded programming
- Who can I send?

Rustock.B rootkit

• Frank Boldewin, "A Journey to the Center of the Rustock.B Rootkit", Jan. 20, 2007

– <u>http://reconstructer.org</u>

• Combines a number of obfuscation techniques found in other malware

- Drop from Mother Ship - Gives you rustock.exe, a Windows PE
- Step 1
 - In Ollydbg, search for all referenced text strings
 - Not much shown due to obfuscation/packing
 - Use PEID or Protection-ID tools to determine packer/compiler/protector
 - Not much shown, perhaps a proprietary packer used
 - Check for unrecognized data in code
 - Code loaded at virtual address of 0x400000
 - Entry point of Rustock.B at 0x401000

Looks like obfuscated code at 0x401B82
Find references to this address



- At 0x040198D
 - PUSH of 0x401B82 followed by RETN
 - Same as a CALL
 - Set breakpoint and run
 - Obfuscated code should be unobfuscated now

- [Ref	erennes	m malez	ane: test	to illui	H1822)					
R File	View De	bug Plu	in: pat	nt sui	to p	ush	401	.b82	/r•	tn
Paused	B	(4 ×	» []]	\$;] \$;]	¥ li	≁]	→	L E	M T	 W
Acdress	Disassei	∿Ьly			/	Con	v⊛n¢			
00401310 00401980 00401982	HOU EST PUSH na DBL&B	.nalware luare.00	.0040158 401832	² ८		004(]n	b1E82 itial C	ralware PU sel	.02401 ection	882)
			F CFFFF BW20	OD EDX. EA EDX. EA EDX. EG ESI ICR ESI ICR ESI ICR ESI ICR ESI ICR ESI ICR ESI ICR ESI ICR EX. EMP	ECI DUORD F EHTE F Are: 004 ware: 00 DUFIRUS	TR DS: Ind Siste 401882	EDX+E Fun	ניי ניי גער		

- Not quite, have Ollydbg analyze code
 - Step through API importing code to obtain API names for subsequent call instructions

89933183	2	2000																								140
	. 4	S		1.00							••••••		·····		· C ::: -: :: :	¥× ``.	••••••••••		· · · · · · · · ·	*****			• • • • • • • • • • • • • • •		***********	2.3
246-801-865	alt + 2	ŧ	• •	- 2000	· · 🗟 - e ·	· ·	· ·	· ·	· ·	• •	• •	• •	•	· 3	SHOR .	₹ <u>\$</u> ?^					• •	· ·	:			. · I
NOR COR	31 ° 12	⊈. <u>`</u>	• •	1.000		• •	• •	• •	• •	• •	• •	• •	• •			• •	• •		• •	• •	• •	• •	:			. 1
SN4400	81.1.8	3		-110	· · · · · ·											• • •			• • •							<u> </u>
and the state	· · · · · · · · · · · · · · · · · · ·	×	· . · .	100							· . · .	· . · .												•••••	2010/00/00/00	I
	сįĝ	<u>д</u> .		2000	- 44 H									:												. .
-dahan isis	3)· · 🏽	લેં	• •	- 2010	· • [24]• •	· ·	· ·		· ·				•	· .		· ·					• •					. · ·
	:(···g	а : Э	• •	< 1982.		• •	· ·	• •	• •		· ·	• •	• •			• •	• •		• •	• •		• •				<u> </u>
Selecter and	31 . T.X	à		- 16											. C 🕬 🗮	< <u>₹</u> * .			• • •					1		<u> </u>
12220-01220-	;} @	¥		1.000																					- 20-101.23	ĝ. (
	N#	÷.		2184										:												
nice set (see	ગોર રહે	šy	• •			• •	• •	• •	• •	• •	• •	• •	::::::				********		X6 1		• •	• •				
	:, · · ;	š .	• •	< 1 ().	- G.Q 1	• •	• •	• •	• •	• •	• •	• •	: >: : : :	8 ar ia				× · · · · · · · •	stàr - r		• •	• •			• · · · · · · · · · · · · · · · · · · ·	÷ 1
	eli.i.,	í. [.] . [.]		- 116	181										*******		*****	*******	·** · .					12.3	ì . 22. p. 6	. 1
		à		int.									::::::	NO DA	:			::::: :	: # ·							÷.,
	· · · · 2	ð ·		100	· 6.6														· · ·					120		
	:(· · ð	άr···	• •	< 1982.		• •	• •	• •	• •	• •	• •	• •	: > > :	87.XX	¥		*****	*****	- -		• •	• •				
· · · · · · · · · · · · · · · · · · ·	31. 1. 18	4	• • •	- 6		• •	• •	• •	• •	• •	• •	• •	: >: : : :					********	:: ! • · ·	• •	• •	• •				
->>+<+:	3 . S	¥		1.000										Y () () ()	iy £`y₹&:				÷:						·	
		ä		2000									::::::	Q				000000	::::::::::::::::::::::::::::::::::::::				:			I
Nie se	: · · · é	ě	· ·	- de marc	i deb i i						· ·	· ·			napre			p怅	: . .				:	· · · · · · · · · · · · · · · · · · ·		
ana a ina	r(· · ≱	ŝ	• •	- 000	·	• •	• •	• •	• •	• •	• •	• •	: >: >: :		• >> >> >> >> >>		*****	******	::::::::::::::::::::::::::::::::::::::		• •	• •				
	-1	ĕ.'.	• • • •	- 10		• • •	• • •	• • •	• • •	• • •	• • •	• • •			• • • • • • • • • • •			*******	: * . *		• • •	• • •		1		
i Astar na stea	41.1	ж. ^с		1000										×												10
	:} ¥	ġ., ,		2000															: 1				:			
l de la belarb	:[···\$	÷ ÷	· ·	- 2002	· 600 ·				· ·		· ·	· ·	:	20. A. A.	ann na l			*******	- .			· ·				-21
199200.99	cí i w	3 · ·	• •	- 000		• •	• •	• •	• •	• •	• •	• •	: >: >: :	* **	***		2020222	******	::::::::::::::::::::::::::::::::::::::		• •	• •				
	£}. '.' 4	δi.'.	• • • •	-122	. 49. '	• • •	• • •	• • •	• • •	• • •	• • • •	· . · .		₩t¥	80 6			*******			• • •	• • •	• • • • • • • •			1
ang separation of the second secon	2)Q	÷.		0.000									::::::				****	00000	÷\$.							
••••••••••••••••••••••••••••••••••••	:::· : \$	ji		2184	·help									R. 1										1 1	: :::::: : ::	. : .
-3.0ex.0 (SP)	:(· 9	÷ ·	• •	100	: P.C	• •	· ·	• •	• •		· ·	• •	: >: : : :		: >: : : : >: : : >			********	: * • •	· ·		• •				
	.	Ż.		1000	·	• •							: >: >: :	*****			~~~~~~		::::::::::::::::::::::::::::::::::::::		· · ·					
	:). i 2	2	· . · .	100		· . · .	· · ·	• • •	· · ·	• • • •	· . · .	· . · .		90 U.	×						· · ·	· . · .		1.		
	4 · · 4	ĝi .		2002															÷.				:	1 I I I		. 1
réasatais	:ir · 2	∂r · •	• •	-1.16	·	· ·	• •	• •	• •	• •	• •	• •		ಂಘಾಂಡ	x X X X X X	F.,	*****				• •	· ·		: I ·		· [
1008-584 (507-	n, · ·@	× ·	• •	< 1 884	1-111	• •	• •	• •	• •	• •	• •	• •	: >: >: :	****			\times \times \times \times \times	*****	::::::::::::::::::::::::::::::::::::::	• •	• •	• •	• • • :			
	91 . T Q	€'.'		- 19	·										¥ 2		*****	*****	÷:					1.1		. 1
	3. .	×		08:	. \$13.								::::::	25. # ;	.41 92,4				1.					. 1.		. 1
	S 4 8	3 0S i	30 28	tes	531 3	· ***									tu Ètiyati				÷.				:			
2004-013	7(· · · 2		• •	- and -	- Cult-	••••••	• •	• •	• •	• •	• •	• •	: :		(C) ::: EX8	.c.a.: 3	*****	*****	:::@· ·		• •	• •	:	· · · ·		·
	31. 1. 18	4 . '	• • •	1.46		• • •	• • •	• • •	• • •	• • •	• • •	• • •							· · · · · · · · · · · · · · · · · · ·		• •	• • •		1.		
	6¥1.1.X	∯.'.'		:le	1681.									×			*****		· · · ·					1		. 1
1.00000000000000000	<} 🕸	ι		<u>;</u> ,,,,,,,,,										Contain the second	*******	*****			·							
	း န	¢¥ .	· ·		· •						· ·	· ·	-						i minininin		i e minine i e di a	indindindind				an i
	if · · B	ĝi	• •	< 1.85	· ::!!?	• •	• •	• •	• •	• •	• •	• •		ÚГ Э.	<i>8</i> 33						œle -				. Chr/40	∰÷
	÷. ∴ . °Q	÷	• • • •			• • • •	• • •	• • •	• • •	• • • •	· . · .	• • • •	: ******							1						<u>#</u>
	51 S	ð		300										<u>.</u>					:::::: : R:	stalve i	1 121/2	8 mb a	xods			
t is an in this		h		: : : : : :										i i i i i i i i i i i i i i i i i i i	ev 2 H2			······			··· · · · · · · · · · · · · · · · · ·					

- Find call to kernel32._lcreat
 - Creates a file called lzx32.sys (kernel mode driver)
 - Set breakpoint and run again
 - Select EDI in Registers window and follow it

00401C71 00401C77 00401C79	SPEE MOUL OF RICE GRIVER Gets creat	ed ^e hêre ^{catA}
00401C7C 00401C82 00401C83 00401C83	FF95 C308000 CALL DWORD PTR SS:[EBP+8C3] 5B POP EBX 83F8 FF CMP EAX,-1 75 1A UNZ SHORT malware.00401CA2	kernel32lcreat
00401036	None Short natware.00401CH2 • Resisters if PUA • Resisters if PUA • Resisters if PUA • Resisters • Resisters • Resisters	

- EDI points to C:\windows\system32:lzx32.sys
 - Use of : instead of \setminus
 - Alternative Data Stream (ADS)
 - Hides the driver from easy detection
 - Windows Explorer and cmd.exe do not show ADS
 - Change memory to replace ":" (0x3a) to a "\" (0x5c)
 - Attach ADS to directory since ADS viewers do not show this
 - Rerun code and step through driver creation
 - Stop code at lclose at address 0x401cc7
- Driver has been deobfuscated and unpacked now

Address	He;	: du	IMP	į.										A	DS	Ū,	SE CINA	me
0006FEA0	F4	58	6F	F6 F6	F4	5B 82	6F	F6	00	00 00	00	00 80	90	5B F1	6F	F6	¶[o÷¶[o÷	É[O÷
0006FEC0	43	SA	SC.	57	49	4E	44	4F	57	53	5C	73	79	73	74	65	CUINDOWS	Syste
0006FED0	6D	33	32	3A	60	78	78	33	32	2E	73	79	12	00	BF	E1	m32:1zx32.	SYS. 7B

- Driver now detached
 - Analyze it in IDA to find obfuscated code
 - Detached driver code and .idb file in "stage1" directory
 - Attempt to load in Ollydbg
 - Launch using LOADDLL.EXE fails

- Change driver
 - Currently a DLL, a native executable, and contains imports from kernel libraries (NTOSKRNL.EXE and HAL.DLL)
 - Change to no DLL, a Windows GUI application, and no imports
 - Fix PE-files using PE-Tools
 - Unmark DLL bit in PE-Tools



- Change driver
 - In Optional Header of PE-Tools, change Subsystem value from 1 to 2 (Windows GUI)

	ades estitas Internation		×
		* presel Majur SubSystem version	001
hain Linkei Valson	Q1	Minor Subsystem Version	.
s Manor Linkar Version		ineris Varie	0000000
Sectors	(A.U.A.A.A.U (A.U.A.A.A.U (A.U.A.A.A.A.U)	Cive (Yr Hanadare) Cive (Yr Hanadare)	106127000 1060127000
Size of Unitit Data	00000000	Checkson	ACEDICES
	00001000	D] Supeystem	(00 1)
Sase of Cocs	00000000	OC Far	
336 Of Data		Szeci Stati Roxive	00001300
inaçe Base	80016960	Steffe Start Comme	valua to 2
Ne Abronant	0000000	Son (* Nead (Sno)	00010000 DDA10000
Major Universion	, 	iusie Maix	0000000
Marce Veisco	000	Mancer Or Rive and Stars	1 0000010 + 1 + 1
Major Image Version	90 04 9		
i Marix Irnaya Vetazi Manada da	: XXX		
		E	CANCES

- Change driver
 - Set RVA and size to 0
 - Will be reset later

na seta y na na Na sina e na varian	es and	set to	0 🕺
	•× 	326	1
Expose Ottory 🔨 .	1 0000000 00		f ax 3 de li j ece
incort Exec tory			
	000000000	<u>. (1/1000000)</u>	
Exception Droctory	0000000000	2000000	
žerady Cratkicy		000000000	
Existence in table		2200000 ·	
Contang Constant y		00000073	
- Autrietize Yerdo Cala	00000000	00000 00	····
Rinad G	000000000	000000000	
HELYSCIAN	000000000	- (((6666)	
Lood Colling Divextory	. 99033333	00000072	
: Enling Indext Excently	000000000		
Incont Address Falle		000000000	
Delay Impon Dexempora	00000000	0000000	
COMPANY DESCRIPTION	00000000	00000000	
Aexerved	CINDERD OS	SOCOCIE	
		<u>مبع</u>	

• Driver loads now

– Same as Stage 1: obfuscated code at 0x116a4

	1.1.1				11: A		: 40	-			333	: 1 1	:	472.4	e																			
	100		.2	•	32	Σ¥,	~?~	ني ≉	es.	S.X.	24	22	ş	<u>.</u>		××××				******		×	[.]	•			•	•	•	•	•			•
	2007		1		20	Y N	<u> </u>	×29	~***	6W)	1.1	X.	ंञ्च	Ø.	22	×δ	220	XQ.	\$N	MBC)	20	×:	č.		•	. '	. '		• .	۰.	۰.	•	. '	
	1999	÷.	×.		8.A	¥ 🖓	29					₩.	. %	₩Ņ.	R.S.	n, R	80	889	8U)		987) 1997	÷.,	ķ₩	s :		۰.	۰.	-	. '	. '	. '		۰.	-
	1.00				63	- 27	<u>9</u> 1:	99:	106	ĝ.	: P	£¥	н.	:£2	×З	22	200	æ	16.	233														
	1	41.	2.		Ć3						: 18	201	E.																					
distant d	1		-		ŵà	E.12	- Ar	œ۰		•	-30	77 37	ĩ,	:Ci22	.	-	•	•									•							•
	12.5		7.		àà	àå:	×X.	•.	•		÷.	24	÷ ś	Ϋ́́α	ŵ	no 📾		:::æ		C223)		5. J	rae	×.	•	•	•		•	•	•	•	•	
			·	•	27	- <u>-</u>	×	• A3	i shai	. :		24	÷,	æ	۳×2	23.	22	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	74. Y	٩£.,	garon Saco	ŝ.,	2	ā.,	÷.	•	•	•	•	•	•		•	•
	> m.C	911	٠.		Ħ <u>x</u>	· Qé	85	12.	683	8 · ·	: 11	<u> </u>	÷.,÷	÷	≻ŧ ∀	ΨŸΨ	æ	2	10	. t er	₹÷	÷÷،	6.4	~ . €	ŧ.	•	•		•	•	•	•	•	
		÷1.	·.,	•	¥.	. X.	:,	×2.	. 19	ā .:	Ŧ		Η.	3:3	***	₩7		SS II	3-X-	6 80.	•	. '	. '	. '	. '	۰.	۰.	•	. '	. '	. '		۰.	•
	1.63		. x		€Э	· .					- FR	5201	₿.							. '			· .	· .	· .	. `	. '		• .	۰.	۰.		. '	
	1.623	:1.	<u>}</u> .		***	22	-02	*2/	2013	1.₩	: X	22	ŧ.	Ûü	÷	£	22	Χ.	<u>(</u> 28)	x Ľ.	ŧ21	źĊ	71.	. 23	21									
a hand a	1	÷1			άŤι	È.	- 23	- 44	- 14	÷.	- 64	Χĥ.	Ĩ	τų.	~.¥	``€	÷×.		~~~	·.•	÷	· ·	~	· •.	× ~ .									
	12.5	31.	7.		ãñ,	ŽÃ:	×20	~@?	×770.7	• ***		×	· 2	ž×.	×@	ŵñ	i de como de co		.		e: 20	K 200	~~~	<u></u>	÷	•	•		•	•	·	·	•	
			.1	·	23	erez Grad	77	- 22	÷.,			21	-à	ŵ.	1è	18 M	-	22	20	(B)		şæ:	×		đ		ż.,	÷÷		· ·	•		•	•
	× 10101	211	4.		***	8-1-2	24.		÷.*.,	. 9	: <u>1</u> 1	922	<u>.</u> 8	 ,	¶?#	6×10	×.#9	×Χ	98.	× 420 -	9 9 00	¥:€:	1 (C)	355	≪,v,₹	2.X7	6: 1	÷	:*•	•	•	•	•	
	:	÷.	·.,	•	çφ			·			100	*	Β.			•	· 	· 	·	·	•		. '	. '	. '	• .	۰.	•	. '	. '	. '		• .	•
	169				63	8	912	291	100	2	.P	£4	н.	12	×З	24	200	at	łž	¥8		۰.	۰.	۰.	۰.	. `	. '		• .	۰.	۰.		. '	
	1.444	31.	2.		¢3						: 88	271	E.																					
0000	**.£¥	ā	3. J.	2.1	2.9		÷	2.2.			-00	00.7	10	0.0				:						÷	2.2			2.2		÷	3. A.	22		÷.,
	773	ēr.			ña	• •••	••••			· · · ;		8 °	20	ç	-									••••			• ••	··· ·	••••					•••
			•	•	20	•	•	•		• :	·		::	••••	T	``		•	•	•	•	•	•	•		•	•	•	•	•	•		•	•
	1.2.22	÷	•		32	•	•	•	•			:x			*		~		•	•		•	•	•	•	•	•		•	•	•	•	•	
		. I.	۰.		<u>90</u>	. '	. '	. '		· .:			-	£. 1	· .	• .	· .7	×.	<u>.</u>	۰.	•	. '	. '	. '	. '	۰.	۰.	•	. '	. '	. '		۰.	•
	÷				₩¥							Ш.	÷4.	Ξ.					÷.,															
	:09	91.			.\$1					. :	: 11		01							λ.	٤													
	16.2	ς.	•	·	Ş4					- 3	•		-	ξ.			•	•	•	• *	• •	۰.	. •		:		۰.	•		•				•
	20.00		•		£.∶	•	•	•	·			÷.	i. i	·	5.4	•		<u></u>	#¥ .	.		n, xi			. and	È.		Î 🐲	: 🔶 🕷	-	•	·	•	
	124		•	·	ŤŦ.	•	•	•		• :	· 6,	N:	×.		×			₩.	***	. .	44	(R x)	k #			ŧ.	ч.				•		•	•
	200		•			•	•	•	•				-	•	•	•	•	•	•			•		•		•	•		•	•	•	•	•	
		с.	۰.	•	72	. '	. '	. '		٠.			1		· .	• .	۰.	• .	• .	• .	•	. '	. '	. '	. '	۰.	۰.	•	. '	. '	. '		۰.	
	100		. '		£3				, î.,	. 3				÷.		. `	. `	. '	. '	. '				۰.		. `	. '						. '	
					45					. :																								
	1.648	5			43					•	•	<u>.</u>	48				•	•									•							•
histori d	: .l.d.	ć I -			:32						- h	÷	вd	÷									•							•				

• Find references to this address 0x116a4



• Two places with PUSH 0x116a4/RETN – Set breakpoint and run

	2	2	1	2	ž	Ĩ	2	2		e	ŝ		ľ	2		ŝ		ŝ			ł			ß			2		1	•••	•												8						*
	Ř.		1	6		¥	×	Ŵ		Ę	*	Ь,	ģ	÷	2	٤,	¢,	¥\$		2	¥	þ	្	¥š		2	QQ 4	×	¢	4		ij	ŝţ	¥ .					ļ						X				
i)	- 2	Ì.	ø	à					à	ł	4	i.		×	Ì	2	1	•	Ì	I			•		Ç.	₩.	Ì		2		1			•	IÌ			•			Û	Ì	E,	l	Ń		j.		ü
à	6	ż				Ì	à	÷			ÿ	Ì		2																					S	*	X	<u>.</u>					Ĩ					2	<u> </u>
1918 1918	Ø,	ÿ	1	Q.	ž		X	ŝ	ķ	ł	22	2	Ż	41	9	ð,	1	ğ) S		÷	*				÷			÷			÷			P					÷	2	 ÷			÷					
ø	0	\$1.	3	ŝ₽́	ş4		X	١.	÷	÷	•	•		**	\$3:		•		·	•		•					·		:	·	•	:		\$	ž.	n i	¢	L,	άi		 3		<u>*</u>	٤	Ċ	٤ i	έ¥	ð.	
1																																																	

		_	00	
1	0001100/1	-	OADD -ZCECKAO	WORLERY GENEEZE
	000101004		-7 deteks a a a a	NOT THE HEATON
	APATTABAT		The Treat 412 Print	12U311 22832.000114B8
	GOOT LODE		C2	DETN
	DEDITOPL		LO	BE ID
	00011000		0FAFC7	IMUL EAX.EDI
	00011000		9D40 01	I FO FOY DWODD DTD DC. FEOVA11
	00011000		0040 01	LEA ERA, DWORD FIR DOLLERATIO
	000110C6		83EC Ø4	SUB ESP.4
	00 01 1000	~	EQ OFFEFEE	IMD 1
	00011003		E2 SIFFFFF	JHP 12832.00011005
H	000110CE		68 A4160100	PUSH .zx32.000116A4
	00011003	100	C3	RETN
	00011000			
	00011004	2	891024	MOV DUORD PTR SSILESPI,EBM
	00011007		40	DEC ESP
	00011001		18	BESS ESE
	000110081		40	I DEC IESP

• Analyze code now...

<u> </u>				***
	₩			
50 2 bet X 1				• •
Pet Controls	Copy.			• • •
	· · · · · · · · · · · · · · · · · · ·			• •
	£87.**		· ^	
	M. 45. K. 1.			137
	**************************************			• • •
	Accentite			· ·
	······································			t.at.
	1356			
be dia series seri	. <u>,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,</u>		CHAR.	۴ör
2334633	***			
	fredericht 🕴			
P22000				• •
	100000		in Automatica	 * #4
			white the	.* .
	-FX3H C: 41		. "HOR	t sst.
				÷
24 (58))	x5626			• • •
ea a 64 () (₩¥€₩¥),N##KS		2.0
	toom alveo		, Qra∰r	~¥f.
	ça da de la companya			
	Xearth Tar			• • •
				Ŧ X7.
	kalverest.		. čra	-X4.
8428493				• • •
	∴*`\$\$\$\$*		i (MAR)	• < *
	CORV TO EX MORE ADM		:	
				mmeri i
	Acayon 12	ARCINE CIES	v,T‴∻ù,	
	······································	······································		
RTREE	18:00-18-00-00 P		*****	···· 🗄
24 2 2 2 2		icen object fles	((***)	
+1 3 <u>5</u> 4 2 3	×	· · · · · · · · · · · · · · · · · · ·		· · · · .
	Ista Xp.e.	Kennove object scen introduke		
	Fu unsalahi asus fasaanaa			•••••
	Training descend the second	- Remove analysis browself from	A. Sor	
S. C.	OlyFlow Grant	a servere and be well and a substitution of the second second second second second second second second second		· · · · •
		😳 ūring next andysis, treat selection 😁 .		:*:
	Riaks CURD OF MIX 655			
	·····			
	£#####################################		. metamen	· · · ·
				292

	A C IGCOL	- main thread, module loss(a)
ŀ	1000 M#6 - V	ev Debug Flights Johans Window Help
	tsa. k	
		52 ΕΩ 900900000 ΕΜΕΕ 18×32×20071€94 =5 ΕΩ 50000000 ΕΛΕΕ 18×32×20071€94
		2 200 36 205 100 100 100 100 100 100 100 100 100 1
		SECO 20 DEGISORO PSUO EUS, IND 22.0100 ADEC PSUO EUS, IND 22.0100 ADEC PSUO EUS PER DESTECTIONS
		A 75 F4 302 CHCRTCLY/S2200011600 2 DFB765 AL NORZY EBX.WORD FTW D5(LEAX+AL) 3 REACTS SEASON ONE CHCRL FTW D5(LEAX+ESX)/4000
	issaer istrik. Siere isteide Brechtigten	4 75 57 8902 100 FEX. 54X \$005 1984690(LEA \$\$1,00000000000000000000000000000000000
		. 2000 SZGAGGOLLEG EUI. DODALDETE SSECEROSSEZ 2 EZ 49000000 ERGE IXXSZ.CODIIAZE 3005 SSC46901LEG ESI.SKORD FTR EDISTRASED
	18598 161009 8696 116600 19696 11660	- 55 FUCH EGI - 68 00 FUCH EGI - 68 PUCH EGI
	100940 - 16 KOK 166940 - 16640 166945 - 16640	. 64 DE FUSA NE 2 F793 5-04000(ERSE DECRETERESEDERENSED 8806 D4 ADD CAOPO PTR 12311ES1),1
	idae ikindu Kele ineti Netici (Ciga	FFSS FORM DOCAD FIR DSTREST 60 00 FUSH COMPANY STREST FOR STREST FF9S S24000 COMP DOCAD FIRE STREST FOR FOR STR
	1204-11204. 2384 1223.4 14943 1223.4	. Frss Fush Lucre Fir Ds:[181] . 8700
	12,000 12,008 2399 12,721 14,945 12,721	. \$785 5764696(110) 16060 FSR 1668 FIRT, 56% . 8967 - 1160 EC1. EFX . 66 88 - FUSH S
		FRS6 FUSH DUCKD FIR DS: [SS1] 57 FUSH EDI 58 DE FUSH CS
	1996-1873) K	. FF95 5-04600 CHIL DADAD STALSSEDERANSEN

• Dump debugged process

(IFIE FRED TREE		•••				
Fiz Van Dobuç	Flagers Opbans Windo	a te p				
ned 🛛 🚈 😽 😽 🗙	i i Emkradz 🔹 🕨	11 M		· L · E	x T	X B
	2 Scinnard ine 🔸	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2				
∫* 60 ∫* 950 ≥	3 LATA KEPer →		• • • • • •		· · · ·	
. 64001 3 . 8840 84	SGCLPPick +	* F5:139) * C%:(EA%+	· · · ·			· · · · · ·
20 1201	é Mithe Debugges 🔹 🕨	EFERICINE.	· · · · •		· · · ·	
	7 Öly înviside 🔹 🔸	Į OČULIČEZ	····	· . · . · .	• • • •	· · . · . •••••••••••••••••••
· · · · · · · · · · · · · · · · · · ·	somraa ≯ a⊖kenit ≯	F X XP	by Sec	a Hor	(7) ex e i	n:::::::::::::::::::::::::::::::::::::
	anniantiEM4 ►	Fra XP	by Sed	ian ∺x¢	(1:000)	(1*%) ⁻ .t
	Ohribg PE Dumper 🕨	Cotiens				
	Windwingda 🔹 🕨					
111661 - 1025 3	HURIT LALE LOUXLE RISKI					

• Dump debugged process – Unmark "Rebuild Import"



Stage 2

- After dump, restore PE-File settings
 DLL bit
 - Subsystem native
 - RVA and Size of Import directory field

Stage 3: IDA

• Load dumped file into IDA

000110A4	pusha	
000116A5	call	\$+5
000116AA	рор	ebp
000116AB	sub	<pre>ebp, 6 ; standard "what's my current base address" trick</pre>
000116AE	mov	eax, large fs:38h
000116B4	mov	eax, [eax+4]
000116B7	xor	al, al
00011689		
000116B9 loc_116B9:		; CODE XREF: DllEntryPoint+1Fij
00011689		; DllEntryPoint+2Clj
00011689	sub	eax, 100h
000116BE	cmp	word ptr [eax], 5A4Dh ; MZ
000116C3	jnz	short loc_116B9
000116C5	MOVZX	ebx, word ptr [eax+3Ch]
000116C9	cmp	dword ptr [eax+ebx], 4550h ; PE
000116D0	jnz	short loc_116B9 ; Scan for NTOSKRNL base
AAA116D2	mnu	edx, eax
000116D4	lea	esi, [<mark>ebp</mark> +41Ah] ; First Entry is ExAllocatePool
000116DA	lea	edi, [<mark>ebp</mark> +457h] ; Buffer for API Addresses
000116E0	call	sub_11A2E ; Scan for several APIs
000116E5	lea	esi, [<mark>ebp</mark> +46Bh]
000116EB	push	esi
000116EC	push	0
000116EE	push	esi
000116EF	push	OBh ; Oxb = SystemModuleInformation
000116F1	call	dword ptr [<mark>ebp</mark> +45Fh] ; ZwQuerySystemInFormation
000116F7	add	dword ptr [esi], 4
000116FA	push	dword ptr [esi]
000116FC	push	0
000116FE	call	dword ptr [<mark>pbp</mark> +457h] ; ExAllocatePool
00011704	push	dword ptr [esi]
00011706	рор	dword ptr [eax]
00011708	add	eax, 4
0001170B	mov	[ebp+467h]. eax

Stage 3: IDA

- Obfuscated data
 - Can not use the previous approach

88811880	loc_11AAC:			: CODE XMEF: SUD_11AAAAAFT]
88811880		बर्यच	85 j , %	
BBBIIAAF		inc	SC K	
88811889		jm	short loc_11077	
00011482	: ::			
88811 882				
88611 802	144: <u>11482</u> :			; CDDE XNEF: SUD_11044+661]
88811882				; sub_11844+781j
00011002		pop	<i>铁</i> 琪关	· · · ·
00011683		pop	eb x	
DBD11AB4		aaa	eci.	
BBB11AB5		1 au	85Ì	
88811686		1eale		
88811887		retn	A	
BBB11ABA	r			
BBB11ABA				
00011A0A	Xu:_11488 :			; CODX XHXF: SUD_11044+171)
88811888				; sub_11#44+361j
88811888		Xar	eak, pak	
00011080		jmp	short loc_t1882	
BBB11ABE	NUD_11#44	qbas		
88811880				
88811488	\$ \$			
	AExallocatepoul	du *8×83	llac <i>ste</i> Ponií _s 8	unrecognized data
pininie s s decen.	aExfréepool	db *êxê:	⁺eefaal`,♦	1
BBB11ADB	aZvųverysysteni	db ^Zw	ærysysteniofora	Mion', W 🖌 🔰
ébéléb a a tele . a	a_stricmp	db _^_\$\$)	^i<@p'_\$	
000033086		alige 🌣		14
****		dd 8 duj)(8)	
ê ê ê s sê sa		aa 2000i	dddd:, 4066668314,	, 26965A38h, 4026609h, 81FF/100h
9999338384		dd 1930 3	2996, WEATSC24W,	#E4C09E@h, #F0B&1Fh, 21C0B9846
0-0-0-3-3-0-3-4-		dd 🗰 🕷	201086, 696854 0 0	, 788E2073b, 67676F72b, 63876061b
856585 3 3 FT 3 - 3 - 3		đđ 26 18 (YEAIN, 6562877885,	, Sf9SCfafh, 44066908h, 3537ExFr

Stage 3

- Read code at 0x116a4
 - Import APIs from NTOSKRNL
 - Query system modules running
 - Allocate kernel memory
 - Unpack routine (0x11788)
 - Unpacks code to kernel memory
 - Move unpacked code over packed code area
 - Grab imports from NTOSKRNL and HAL.DLL, destroy PE-Header, rebase API calls
 - Free unused kernel memory
 - JMP EAX at address 0x117c8
- Real driver created dynamically
 - Must rip the unpacking code at 0x117d3 and dump whole data as file before PE-Header destroyed and driver code rebased

Stage 3

• Program included

Stage 3: Reversing Rustock.B

http://www.sarc.com/avcenter/venc/data/back door.rustock.b.html#technicaldetails

Doing it faster with a kernel debugger

- SoftICE+ICEEXT
 - Special function in NTOSKRNL.EXE to load driver
 - IopLoadDriver
 - Is not exported by default
 - Need proper .pdb file of NTOSKRNL.EXE from Microsoft server
 - Need to convert it to SoftICE format .nms
 - Problem: SoftICE symbol retriever unreliable
 - Read Frank Boldewin's SoftICE howto
 - <u>http://reconstructer.org</u>
- Alternative
 - Leech Windows Debugging Tools from MSFT
 - Read paper for recipe

Cleanup

• Run RkUnhooker