

If at first, you don't succeed, try something else

Jim Clausing, PMTS and SANS Instructor
jac@att.com
jclausing@isc.sans.edu

© 2020 AT&T Intellectual Property. AT&T, Globe logo, and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners

A



Agenda

1: Intro

2: The Analysis

3: Questions

**Forensicator,
Malware
analyst,
SANS
instructor,
Cyclist,
Private pilot**



The start of the hunt

- Around Labor Day, nothing going on, needed to practice
- Was made aware of a couple of samples with new (to me) packer
- Several of us decided to look at it independently (nothing like a little competition within the team)

Preliminary exam

c:\users\rem\desktop\ea94ae: indicators (2/14) virstotal (network error) dos-stub (!This program c file-header (Dec.2016) optional-header (GUI) directories (3) sections (1/4) libraries (11) imports (323/21/12/1/46) exports (0) tls-callbacks (n/a) resources (27) strings (72/125/74/16/225C debug (n/a) manifest (n/a) version (ListDemo.EXE) certificate (n/a) overlay (unknown)	property	value	value	value	value
	name	.text	.data	.rsrc	.pe
	md5	16C9A29AB30EF2AD9AE...	10F38FF0E305E57DE96C...	006125F2F74F32DA0E89...	960048F966B32D926FB5...
	file-ratio (95.94 %)	44.59 %	25.67 %	5.41 %	20.27 %
	virtual-size (299764 bytes)	135168 bytes	94208 bytes	12944 bytes	57444 bytes
	virtual-address	0x00001000	0x00022000	0x00039000	0x0003D000
	raw-size (290816 bytes)	135168 bytes	77824 bytes	16384 bytes	61440 bytes
	raw-address	0x00001000	0x00022000	0x00035000	0x00039000
	cave (7436 bytes)	0 bytes	0 bytes	3440 bytes	3996 bytes
	entropy	6.608	6.181	3.344	3.594
	entry-point (0x0000A399)	x	-	-	-
	blacklisted	-	-	-	x
	writable	-	x	-	x
	executable	x	-	-	-
	shareable	-	-	-	-
	discardable	-	-	-	-
	cachable	x	x	x	x
	pageable	x	x	x	x
	initialized-data	-	x	x	-
	uninitialized-data	-	-	-	-
	readable	x	x	x	x

Preliminary exam, cont'd

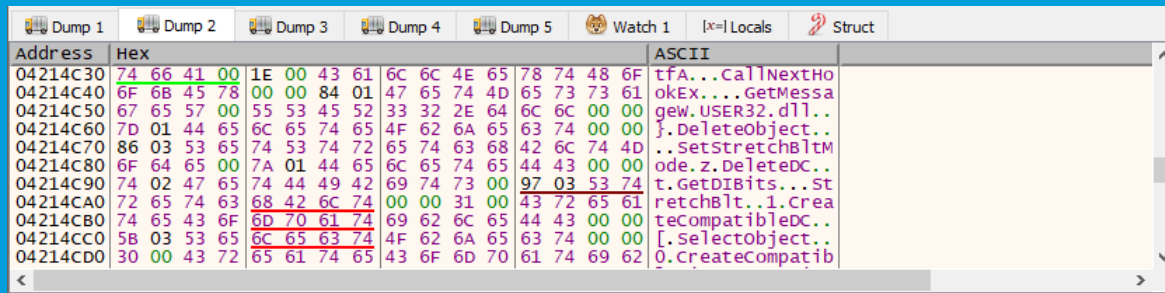
	type	size	blacklist (72)	hint (125)	whitelist (74)	group (16)	value (2324)
indicators (2/14)	ascii	7	-	-	-	-	DDDDDDDD
virustotal (network error)	ascii	5	-	-	-	-	DDDD@
dos-stub (!This program c	ascii	6	-	-	-	-	DDDDD@
file-header (Dec.2016)	ascii	6	-	-	-	-	wwwwwww
optional-header (GUI)	ascii	6	-	-	-	-	wwwwwww
directories (3)	ascii	6	-	-	-	-	wwwwwww
sections (1/4)	ascii	6	-	-	-	-	wwwwwww
libraries (11)	ascii	6	-	-	-	-	wwwwwww
imports (323/21/12/1/46)	ascii	6	-	-	-	-	wwwwwww
exports (0)	ascii	6	-	-	-	-	wwwwwww
tls-callbacks (n/a)	ascii	6	-	-	-	-	wwwwwww
resources (27)	ascii	6	-	-	-	-	wwwwwww
strings (72/125/74/16/2250)	ascii	4	-	-	-	-	wwwwww
debug (n/a)	ascii	4	-	-	-	-	wwwwww
manifest (n/a)	ascii	260	-	-	-	-	yglAAGEyck5SS3ZCSzAwcDhsAAAAAA
version (ListDemo.EXE)	ascii	260	-	-	-	-	3YUQVtkZYC+eu3p8ne/o/uy8AFaf/7/3n
certificate (n/a)	ascii	260	-	-	-	-	vYHNwLmN9P//v/eu/b2BnYS5jYT//7/3r
overlay (unknown)	ascii	260	-	-	-	-	vYGdxLmNRNGNzIXN/b2BfYW5jYSf/7/3
	ascii	260	-	-	-	-	vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3n
	ascii	260	-	-	-	-	vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3n
	ascii	260	-	-	-	-	RQjYeDDYdHo2y+sIN5ZKGFa2w06/dG4A
	ascii	260	-	-	-	-	hQpc2zJo2Tx0wh8nxTZAwg9c0EczM3M
	ascii	260	-	-	-	-	00EXgkqCYj8NsK5qD7LYf3a21UzDz8lvKv
	ascii	260	-	-	-	-	dwJ0hc6b5F/RdqheMp+Ynsz24W5fHAI
	ascii	260	-	-	-	-	C4WWiw9/rw+Kr3N8ibjApkvMZ9uhzH+

Static Code Analysis

- ListDemo.exe – code example
 - Extraneous functions
- Garbage code in actual unpacking routines
- Obviously obfuscated to make analysis difficult
- Moving on...

Unpack with the debugger

- Single-step
- Breakpoints on LoadLibraryA and GetProcAddress
- Try to find the jump to OEP



The screenshot shows a debugger window with a memory dump and disassembly view. The memory dump shows a sequence of bytes, and the disassembly view shows the corresponding instructions. The instructions are: `tfa...CallNextHo`, `okEX...GetMessa`, `gew.USER32.dll..`, `.DeleteObject..`, `..SetStretchBltM`, `ode.z.DeleteDC..`, `t.GetDIBits...St`, `retchBlt...1.Crea`, `teCompatibleDC..`, `[.SelectObject..`, and `0.CreateCompatib`.

Address	Hex	ASCII
04214C30	74 66 41 00 1E 00 43 61 6C 6C 4E 65 78 74 48 6F	tfa...CallNextHo
04214C40	6F 6B 45 78 00 00 84 01 47 65 74 4D 65 73 73 61	okEX...GetMessa
04214C50	67 65 57 00 55 53 45 52 33 32 2E 64 6C 6C 00 00	gew.USER32.dll..
04214C60	7D 01 44 65 6C 65 74 65 4F 62 6A 65 63 74 00 00	.DeleteObject..
04214C70	86 03 53 65 74 53 74 72 65 74 63 68 42 6C 74 4D	..SetStretchBltM
04214C80	6F 64 65 00 7A 01 44 65 6C 65 74 65 44 43 00 00	ode.z.DeleteDC..
04214C90	74 02 47 65 74 44 49 42 69 74 73 00 97 03 53 74	t.GetDIBits...St
04214CA0	72 65 74 63 68 42 6C 74 00 00 31 00 43 72 65 61	retchBlt...1.Crea
04214CB0	74 65 43 6F 6D 70 61 74 69 62 6C 65 44 43 00 00	teCompatibleDC..
04214CC0	5B 03 53 65 6C 65 63 74 4F 62 6A 65 63 74 00 00	[.SelectObject..
04214CD0	30 00 43 72 65 61 74 65 43 6F 6D 70 61 74 69 62	0.CreateCompatib

Try to dump it

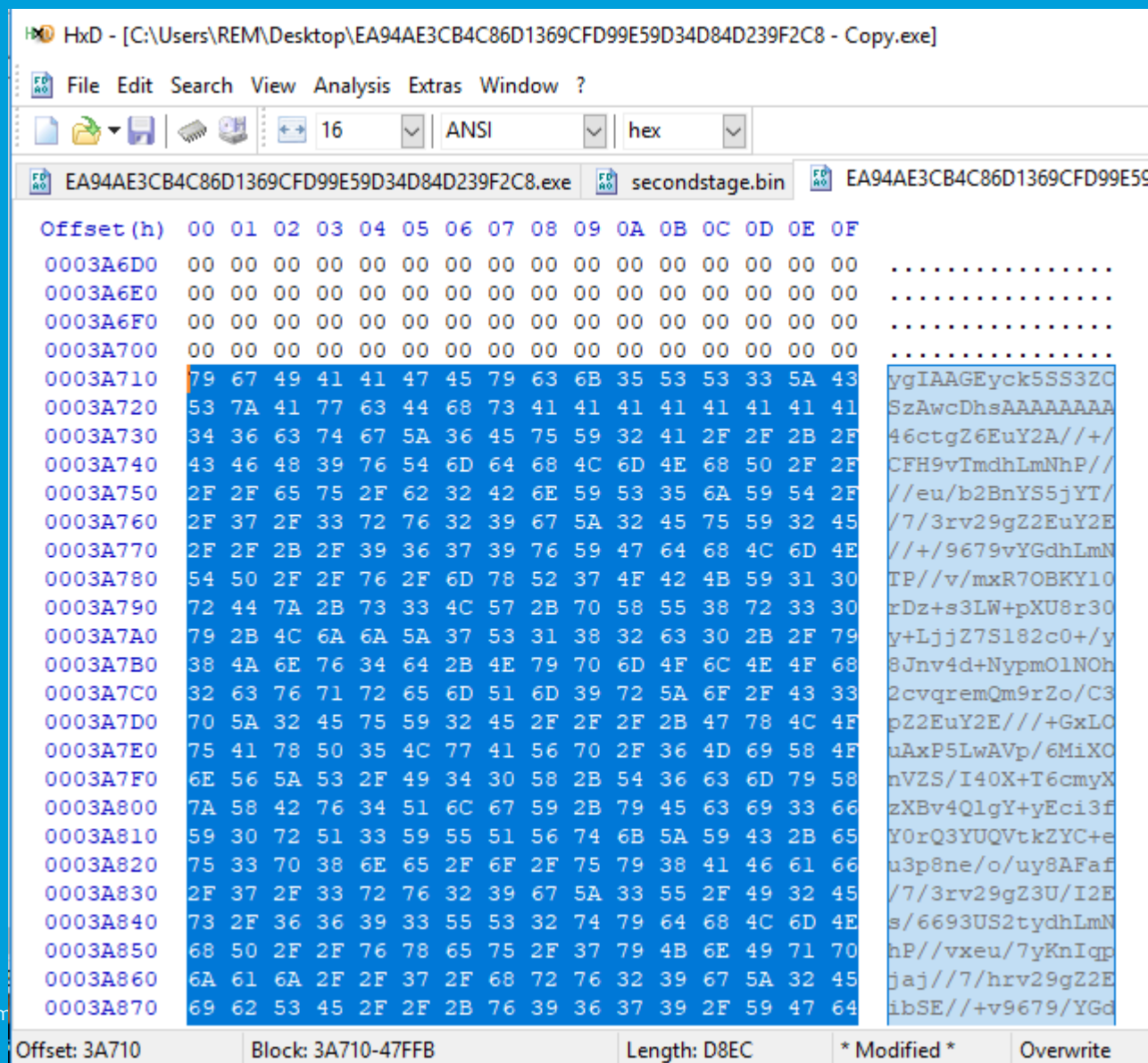
Fail!!!

Regroup

c:\users\rem\desktop\ea94ae:	property	value	value	value	value
indicators (2/14)	name	.text	.data	.rsrc	.pe
virustotal (network error)	md5	16C9A29AB30EF2AD9AE...	10F38FF0E305E57DE96C...	006125F2F74F32DA0E89...	960048F966B32D926FB5...
dos-stub (!This program c	file-ratio (95.94 %)	44.59 %	25.67 %	5.41 %	20.27 %
file-header (Dec.2016)	virtual-size (299764 bytes)	135168 bytes	94208 bytes	12944 bytes	57444 bytes
optional-header (GUI)	virtual-address	0x00001000	0x00022000	0x00039000	0x0003D000
directories (3)	raw-size (290816 bytes)	135168 bytes	77824 bytes	16384 bytes	61440 bytes
sections (1/4)	raw-address	0x00001000	0x00022000	0x00035000	0x00039000
libraries (11)	cave (7436 bytes)	0 bytes	0 bytes	3440 bytes	3996 bytes
imports (323/21/12/1/46)	entropy	6.608	6.181	3.344	3.594
exports (0)	entry-point (0x0000A399)	x	-	-	-
tls-callbacks (n/a)	blacklisted	-	-	-	x
resources (27)	writable	-	x	-	x
strings (72/125/74/16/225C	executable	x	-	-	-
debug (n/a)	shareable	-	-	-	-
manifest (n/a)	discardable	-	-	-	-
version (ListDemo.EXE)	cacheable	x	x	x	x
certificate (n/a)	pageable	x	x	x	x
overlay (unknown)	initialized-data	-	x	x	-
	uninitialized-data	-	-	-	-
	readable	x	x	x	x

HxD - [C:\Users\REM\Desktop\EA94AE3CB4C86D1369CFD99E59D34D84D239F2C8 - Copy.exe]															
File Edit Search View Analysis Extras Window ?															
16 ANSI hex															
EA94AE3CB4C86D1369CFD99E59D34D84D239F2C8.exe secondstage.bin EA94AE3CB4C86D1369CFD99E59D34D84D239F2C8.exe															
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E 0F
00038FF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000390A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000390B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000390C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000390D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000390E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000390F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00039190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
Offset: 3A710 Block: 3A710-47FFB Length: D8EC * Modified * Overwrite															

Hmm...



HxD - [C:\Users\REM\Desktop\EA94AE3CB4C86D1369CFD99E59D34D84D239F2C8 - Copy.exe]

File Edit Search View Analysis Extras Window ?

16 ANSI hex

EA94AE3CB4C86D1369CFD99E59D34D84D239F2C8.exe secondstage.bin EA94AE3CB4C86D1369CFD99E59D34D84D239F2C8 - Copy.exe

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
0003A6D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0003A6E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0003A6F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0003A700	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0003A710	79	67	49	41	41	47	45	79	63	6B	35	53	53	33	5A	43	ygIAAGEyck5SS3ZC
0003A720	53	7A	41	77	63	44	68	73	41	41	41	41	41	41	41	41	SzAwcDhsAAAAA
0003A730	34	36	63	74	67	5A	36	45	75	59	32	41	2F	2F	2B	2F	46ctgZ6EuY2A//+/
0003A740	43	46	48	39	76	54	6D	64	68	4C	6D	4E	68	50	2F	2F	CFH9vTmdhLmNhP//
0003A750	2F	2F	65	75	2F	62	32	42	6E	59	53	35	6A	59	54	2F	//eu/b2BnYS5jYT/
0003A760	2F	37	2F	33	72	76	32	39	67	5A	32	45	75	59	32	45	/7/3rv29gZ2EuY2E
0003A770	2F	2F	2B	2F	39	36	37	39	76	59	47	64	68	4C	6D	4E	//+/9679vYgDhLmN
0003A780	54	50	2F	2F	76	2F	6D	78	52	37	4F	42	4B	59	31	30	TP//v/mxR7OBKY10
0003A790	72	44	7A	2B	73	33	4C	57	2B	70	58	55	38	72	33	30	rDz+s3LW+pXU8r30
0003A7A0	79	2B	4C	6A	6A	5A	37	53	31	38	32	63	30	2B	2F	79	y+LjjZ7S182c0+/y
0003A7B0	38	4A	6E	76	34	64	2B	4E	79	70	6D	4F	6C	4E	4F	68	8Jnv4d+Nypm0lNOh
0003A7C0	32	63	76	71	72	65	6D	51	6D	39	72	5A	6F	2F	43	33	2cvqremQm9rZo/C3
0003A7D0	70	5A	32	45	75	59	32	45	2F	2F	2F	2B	47	78	4C	4F	pZ2EuY2E///+GxLO
0003A7E0	75	41	78	50	35	4C	77	41	56	70	2F	36	4D	69	58	4F	uAxP5LwAVp/6MiXO
0003A7F0	6E	56	5A	53	2F	49	34	30	58	2B	54	36	63	6D	79	58	nVZS/I40X+T6cmYX
0003A800	7A	58	42	76	34	51	6C	67	59	2B	79	45	63	69	33	66	zXBv4QlgY+yEci3f
0003A810	59	30	72	51	33	59	55	51	56	74	6B	5A	59	43	2B	65	Y0rQ3YUQVtkZYC+e
0003A820	75	33	70	38	6E	65	2F	6F	2F	75	79	38	41	46	61	66	u3p8ne/o/uy8AFaf
0003A830	2F	37	2F	33	72	76	32	39	67	5A	33	55	2F	49	32	45	/7/3rv29gZ3U/I2E
0003A840	73	2F	36	36	39	33	55	53	32	74	79	64	68	4C	6D	4E	s/6693US2tydhLmN
0003A850	68	50	2F	2F	76	78	65	75	2F	37	79	4B	6E	49	71	70	hP//vxu/7yKnIqp
0003A860	6A	61	6A	2F	2F	37	2F	68	72	76	32	39	67	5A	32	45	jaJ//7/hrv29gZ2E
0003A870	69	62	53	45	2F	2F	2B	76	39	36	37	39	2F	59	47	64	ibSE//+v9679/YGd

Offset: 3A710 Block: 3A710-47FFB Length: D8EC * Modified * Overwrite

Those base64 strings look interesting

```
remnux@remnux: ~  
File Edit Tabs Help  
remnux@remnux:~$ base64dump.py -n 40 EA94AE3CB4C86D1369CFD99E59D34D84D239F2C8\  
\ Copy.exe  
ID      Size      Encoded      Decoded      MD5 decoded  
--      -  
1:      55532  ygIAAGEyck5SS3ZC 0...a2rNRKvBK00p d733765c63b1c72513c3bbd70e65fe9a  
2:      7396   Fnh11AKWRHGAl0+E .xe0.0Dq00I|0( 94e982c43eaefdcf47e57a80f12e7861  
remnux@remnux:~$
```

C:\Users\REM\Desktop\b64-blob1 - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

res-x64.txt new 1 b64blob1

```
1 ygIAAGEYck5SS3ZCSzAwcDhsAAAAAAA46ctgZ6EuY2A//+/CFH9vTmdhLmNhP////eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNTP//v/mxR7OBKY
10rDz+s3LW+pXU8r30y+Ljj27S182c0+/y8Jnv4d+Nypm01N0h2cvqremQm9rZo/C3pZ2EuY2E//+/GxLOuAxP5LwAVp/6MiXonVZS/I40X+T6cmYXzXBv4QlgY+yE
ci3fY0rQ3YUQVtkZYC+eu3p8ne/o/uy8AFaf/7/3rv29gZ3U/I2Es/6693US2tydhLmNhP//vxeu/7yKnIqpjaJ//7/hrv29gZ2EibSE//+v9679/YGdhLmNhP/vv/
eu/72Bm4S5jYT//7/xrv29gZ2EuY0E//+/8679vYGdhLqNxBHr/v+eu/a2BnYS5nYT/7/3rv29gY2EuY2E//+/9679vZnbhLkthP//v5eu/V2AnYS5jYT//7/3rv29
gZ2EuY2E/4+/98L+vYHNwLmN9P//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhJ
f54YeLv/eufZaBnYS5jYT/07/3rv29gZ2EuY2E//+/9679vYaGdhLmNj9puey5au/VWmNYS5zYT//7H3rv2NgZ2EuY2E//+/9679vYHdhLmNqpu5au/b0pnIS5jdt/
7/1rv29v52EuY2E//+/9679vYGdxLmNRNGNzIXN/b2BfYW5jYSf/7/3rP29gd2EuY2E//+/9679vYGdhLmNhL/RzZLCKt6Bnei6jYT/j7/3rv29gZ3GuY2E//+/96
79vYGdhLmNhP+9v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2B
nYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY
2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//
v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv
29gZ2EuY2E/6o0GyORpdYWRDYaKx2+h81BesLmsO2O3R8AZ+BW8HC8my41PiORv6/96508HV2jYpEDbILg9zb+bI/qsM6c7SK5zXwkoXJhaHczIOLQYi+TL79vYEE
Q7tmi8wkPame8ihCEJjkhYT//4w3KzSyFF2BRnJ7gGZIDCeORQjYeDDYdHo2y+s1N5ZKGfA2w06/dG4AdH7AcZ0N7HWLsbpDfusBjkiuVjTLVHwHtoCqdklqhQn/Mg
cH5sjYLR0KapYJ/xIHB+bIny0T6rpu+dgIVoerPIpa/cmrps1F8ZOK+oSCVoKtjjJPA4yE//+UOaFLisZ2NrY7s3w1QE6u/b0B2m8dtskDgKiCq8bIeeKUTiJPRf6/
967+c44rs/5mDEYAQAjRfnd+kjKOym2IAEAIJbhR38YBefmXe13L/eF0hQpc2zJo2Tx0wh8nxtZAwg9c0ECzM3M7YjFxFVfIdUFIMzPqfEKs7tcWdX7IeP7/v/f5zk
KyVA9jgtM2ekn4Kly9gZ0Ov7Gki/uD/tv++2puuJL5j8PSyvxpuEF+YntGB8L+uU34vuD9xd2Ehb3403VvZyQ/PXuk+5uCOj25PB+eD7LYVgd2jOLwX99qHdtcpJi
eX+LpzeDx9MqT46NkYHJxP/DkYKdd/uA24uRb7jPg5fLl4KZjiNE/w5sz3xw9cjy00EXgkqCYj8NsK5qD7LYf3a21UzDz8IvKwLlIkRhFzY8NzPDON/Gj5gp42XoHgs
Oay/+SuLIEO4S5jQ6p/v13VNayBBmEuY0Oqf75SK/9vYEQxmxjfb4R/eu/bKe2YS5DX7GgKuxoUN/DJENNMRSdeky++Z9R7HgYzxy/ZxFvveu/T541fiIBkU+F7x6
uji8gZ2ES4LdNQ2wrmQPsthXdrbUTg3w5j1c8uRLb4vgr3bwpmV0RvzIWqZVxvCvNb4vBaGkdWJ0hcx6b5F/RdqheMp+Ynsz24W5fHAIR41CfmI+uI2E/3xG/9LGNk
BcbLoAkDr+v/eum9uOggC5jYT//0349z2PjsRPS4LdNA2wrmUPsthWdrbUTw3w5jxc8uRKHmy4+F/ELsDnhTf8joleuX+Lpjq8Hq+ISgRG8LsEt5nw0bJSDrJnXXa2
1EWgoeR8S6B+BEbwuwS3oKGW32+mNmTAR3VBSMDmzcztmXFNUUjsBmisqeh80/U2W559gkLw59RmfB/yC4WWiW9/rw+Kr3N8ibjApkvMZ9uhzH+s8z7iC1va4tBHMz
NzO2IxcU1R0TJh1610yv81J0oKZr9j+65y+43Mdo6eDNN7ukYJrwa6AdrWN4MQzUYFxf5y7QgtE7z0bdvnBkekonxyWImtqk4OvbcJgP43sFF+U4DodubTDzyk4jRi
MXFNUUhlQUgzqjQbLRGB0svTm1cPBnbiHyeARX6IkPjNhHKYd6b+Agph3cS554QA61+37v3tCNhwRjpAv7+/CNspNfi8WkE8QMAygnR6JXB3YTP2w26D0Di5r39gf
eERpg8v7+/cm7yOVIDhLnnha8Aghvuvb0KbQFPggA8/7/3JabBjolaUy3SAOpjt+79OEGSACqNhp9y+i/+q0KUdcT5jXukC0Di6r39gRbJXQ281LJjpiWwXarQXOhy
8QsAgt/uvb3Ryg38YXvqt/+3rpe91st7rLnFv/86N9rYNSr5D+xRrz108i/G3b1Nne6554SorZSyTtZ80c/V6nKR07//91GIUX6ItPnNhKgAqs/uvb3rcdJGmES/v7
/6rv29g83uVdt76jv/t66XvtdikVXNxp90T3JY8jjKYntGBtkXdmIPJYhBCthUgnUPsiuwFbGZAJgfLbCXQCHyvOVJmnlFvFN3tOpAKrf7r291xZ8RpjAv7+/ff6q
636IzPnNhJX76Qi7yf3BneyZjUj/AMojUYht653uuXLxA6xAglaXveud0kaYxL+/vwjBbDUKURcT5jXuka0Dilr39gRT5SQb5B3bKCYU6esRxbhmNhpBQfHqqvR79zM
S5LNIuv79ybomtUKDo6M2EiveG6t6s/YHp+DKWGL+/v6fE/UJWFrEhzcT/r0AhUcjx0N2E0417KK9AIVHI6dDdhNONeyivQCFRyMHQ3YTTjXsodIpX7r290WJsrj4
rr+/VPKs/YH3hE2a1AaPQMLSrP2BPsjozYSV/OAg/gJrCuB8Mvh4XKvut65c4dDdhH7IaP//v/fE/dXpzMS53deV/zbc3qz9gRbZSd7SdsLTpu79QpShxPmN1wDqj7
fu/UL0ae65cpHXvv/3+AKoud3EuQ75E/+wc/X8vYE8+OjNhMw2NMryrP2BGETNPiVgv793kvJC9IUEXyKFUYqud9Lyv0jojn/Ji/5QHov/vb0CXIECRfYkdLKj/729
Cky/bvulcsuHzHiOp8vTh2kIRIvMNfKjroIj14U0+3t8F76CXhahBF3wpAZz1a7Z+LG5vYEXiK8Alv539QgtFbz0byXF3MT/cvcIabhRgJ2Eub5yejawcx39vYEWkf
XcxP90ddxhdPBpF4iOAJjIdMIflPGiCqDY6M2Eitclu5n8h82vhcyTDrPIvc3iz7/0iUK6cg+iE9kw6sq8L1Q1xdzE/xS6xHV04G0eQroAzADEToUbeGb0yg+02dW/
/4Qm2NcwtZW/b/6ntbG8Jys9yeWSm/mNDvFy7Qgmt7wM63s6ZYWKD+Cp9XZY3F4BefnB1DU2ukZ3sZAQlrgFzgB08h8tFbz0crd50tqkdfqgbUW8gZ2E5tPfdBriNF
HIwdDdhDKY2K6/v3yjszBnWw6dnsAfHvz8aOOQcYPXNBHMzNzO2IxcdQWadhhIP7/v3ornUN+YtLp5Yb9/78Iu5n8wZ0Befjhr5W+nawCqO3cxLkGdHwBQIP91fXR
3YRGmOS+v798/vGyPtWO6ADJC3StH48GQn4eQL0lhv//v5EuuE2OKoH23MT/r0Di2rz9gfsN/H8Jug/V5/6rQpTtxfmNAT+HuHxoozZkwEeKtdp0GuI0YjFxtcgPVQ
```

Normal text file length: 55,532 lines: 1 Ln: 1 Col: 1 Sel: 0|0 Windows (CR LF) UTF-8 INS

Lots of repetition, could there be a key in there

```
bd 81 9d 84 89 b4 84 ff ff af f7 ae fd fd 81 9d 84 b9 cd 84 ff ef bf f7 ae ff
bd 81 9b 84 b9 8d 84 ff ff bf f1 ae fd bd 81 9d 84 b9 8d 04 ff ff bf f3 ae fd
bd 81 9d 84 ba 8d c4 7a ff bf e7 ae fd ad 81 9d 84 b9 9d 84 ff ef bf f7 ae fd
bd 81 8d 84 b9 8d 84 ff ff bf f7 ae fd bd 99 db 84 b9 2d 84 ff ff bf 97 ae fd
5d 80 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff 8f bf f7 c2 fe
bd 81 cd c0 b9 8d f4 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd
bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae bd
bd 81 1d 85 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd
bd 81 9d 84 97 f9 e1 87 8b bf f7 ae 7d 96 81 9d 84 a9 8d 84 ff d3 bf f7 ae f9
```


Recipe

From Base64

A-Za-z0-9+/=

☒ Remove non-alphabet chars

XOR

```
bd819d84b98d84ffffbfff7aefd|
```

Standard

Input

length: 55532

```
lines: 1
```

ygIAAGeYck5SS3ZCSzAwcDhsAAAAAAA46ctgZ6Uy2A//+/CFH9vTmdhLmNhP///eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNTP//v/mxR70BKY10rDz+s3Lw+pXU8r30y+LjjZ7S182c0+/y8Jnv4d+Nypm01N0h2cvqremQm9rZo/C3pZ2EuY2E//+GxLOuAxP5LwAVp/6MiX0nVZS/I40X+T6cmYxZxBv4Q1gY+yEci3fY0rQ3YUQvtkZYC+eu3p8ne/o/uy8AFaf/7/3rv29gZ3U/I2Es/6693US2tydhLmNhP//vxeu/7yK nIqpjaj//7/hrv29gZ2EibSE//+v9679/YGdhLnNhP/vv/eu/72Bm455jYT//7/xrv29gZ2EuY0E//+/867 9vYGdhLqLnHr/v+eu/a2BnYS5nYT/7/3rv29gY2EuY2E//+/9679vZnbhLkthP//v5eu/V2AnYS5jYT//7 /3rv29gZ2EuY2E/4+/98L+vYHnWLnM9P//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNh P//v/euvb2BHYW5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhJf54YeLv/eufZaBnYS5jYT/07/3rvm9gZ2E uY2E//+/9679vAGdhNmj9puey5au/VmMnYS5zYT//7H3rv2NgZ2EuY2E//+/9679vYHdhLnNqpuey5au/b0 pnIS5jdT//7/1rv29v52EuY2E//+/9679vYGdxLmNRNGnzIXN/b2BfYW5jYSf/7/3rP29gd2EuY2E//+/96 79vYGdhPmNhL/RzLCLct6Bnei6jYT/j7/3rvm9gZ3GuY2E//+/9679vYGdhLnNhP+9v/eu/b2BnYS5jYT// 7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmN hP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2 EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b 2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9 679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT// 7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E/608Gy8RpdYWRTD :YakX2+h8lBesLmsQ203R8AZ+Bw8HC8my4lP1ORv6/96508HV2jYpEdbILg9zb+bI/qsM6c7SK5zXwkoXJha

Output

```
time: 6ms
length: 41647
lines: 43
```

```
w...0ç±.ô.iq.
±i%Ö..ÿÿç÷MZ.....ÿÿ.....@.....È.....º..´
Í!..LÍ!This program cannot be run in DOS mode.

$......Ai%3..Ò`..Ò`..Ò`~éÓa
.Ò`..Ò`c.Ò`.äÚa..Ò`.ä-
`.Ò`.äÐa..Ò`Rich..Ò`.....PE..L...Ûig].....à.....,.....09.....@....
@.....@.....F.....
~.à.....p..l...PD..p.....@...
.....text.....+......`..rdata..è
..@.....0.....@..@.data...~.....P.....>.....@..Ä.rsrc..à.....
~.....@.....@..@.reloc..l...p.....B.....@..B.....
.....
.....
.....
.....U..ì..ì.W.Á.UìS.Eè.0V..G.¶ð.p vö<.sñ<-u
±.....Môë      3É.Mô<+u..%7G.b0u...<xt.
```

STEP

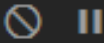
BAKE!

☒ Auto Bake

Recipe



From Base64



Alphabet
A-Za-z0-9+/=

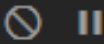
☒ Remove non-alphabet chars

To Hex



Delimiter: Space
Bytes per line: 0

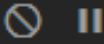
XOR



Key: bd819d84b98d84ffffbfff7aefd
HEX

Scheme: Standard
☐ Null preserving

To Hex



Delimiter: Space
Bytes per line: 0

Input

length: 55532
lines: 1



ygIAAGEyck5SS3ZCSzAwcDhsAAAAAAA46ctgZ6EuY2A//+/CFH9vTmdhLmNhP////eu/b2BnYS5jYT//7/
3rv29gZ2EuY2E//+/9679vYGdhLmNTP//v/mxR7OBKY10rDz+s3LW+pXU8r30y+LjjZ7S182c0+/y8Jnv4d
+NypmOlN0h2cvqremQm9rZo/C3pZ2EuY2E//+/GxLOuAxP5LwAVp/6MiX0nVZS/I40X+T6cmYXzXBv4QlgY
+yEci3fY0rQ3YUQVtkZYC+eu3p8ne/o/uy8AFaf/7/3rv29gZ3U/I2Es/6693US2tydhLmNhP//vxeu/7yK
nIqpjaj//7/hrv29gZ2EibSE//+v9679/YGdhLnNhP/vv/eu/72Bm4S5jYT//7/xrv29gZ2EuY0E//+/867
9vYGdhLqNxHr/v+eu/a2BnYS5nYT/77/3rv29gY2EuY2E//+/9679vZnbhLkthP//v5eu/V2AnYS5jYT//7/
/3rv29gZ2EuY2E/4+/98L+vYHNwLmN9P//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNh
P//v/eu/b2BHYW5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhJf54YeLv/eufZaBnYSpjYT/07/3rvm9gZ2E
uY2E//+/9679vaGdhNmj9puey5au/VWmNYS5zYT//7H3rv2NgZ2EuY2E//+/9679vYHdhLnNqpuey5au/b0
pnIS5jdT//7/1rv29v52EuY2E//+/9679vYGdxLmNRNGNzIXN/b2BfYW5jYSf/7/3rP29gd2EuY2E//+/96
79vYGdhPmNhL/RzZLCkt6Bnei6jYT/j7/3rvm9gZ3GuY2E//+/9679vYGdhLnNhP+9v/eu/b2BnYS5jYT//
7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmN
hP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2
EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b
2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9
679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT/
/7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E/6o0Gy0RpdYWRtD
YaKx2+h8lBesLms0203R8AZ+BW8HC8my4lPi0Rv6/96508HV2jYpEDbILg9zb+bI/qsM6c7SK5zXwkoXJha
.....

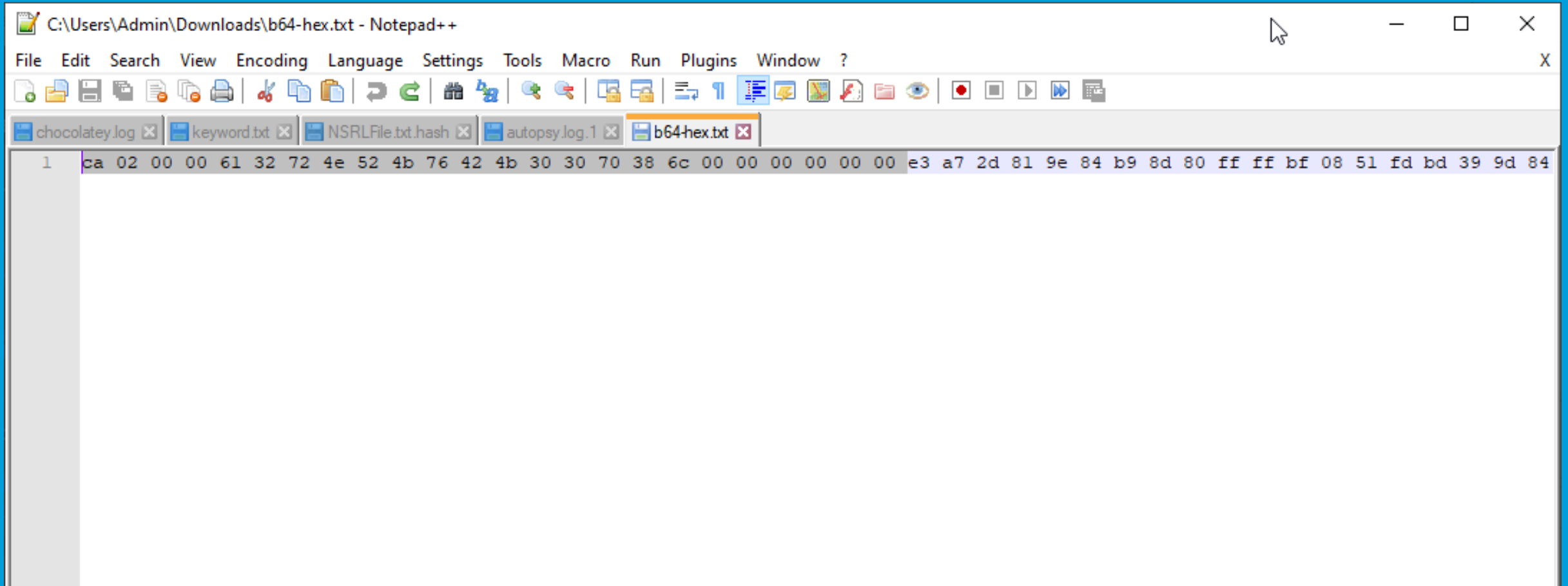
Output

time: 44ms
length: 124940
lines: 1



77	83	9d	84	d8	bf	f6	b1	ad	f4	81	ec	b6	8d	b1	ed	bc	d5	8d	84	ff	ff	bf	f7	4d	5a	90	00
03	00	00	00	04	00	00	00	ff	ff	00	00	b8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
c8	00	00	00	0e	1f	ba	0e	00	b4	09	cd	21	b8	01	4c	cd	21	54	68	69	73	20	70	72	6f	67	72
61	6d	20	63	61	6e	6e	6f	74	20	62	65	20	72	75	6e	20	69	6e	20	44	4f	53	20	6d	6f	64	65
20	0d	0d	0a	24	00	00	00	00	00	00	00	41	ec	bc	33	05	8d	d2	60	05	8d	d2	60	05	8d	d2	60
60	eb	d3	61	0a	8d	d2	60	05	8d	d3	60	63	8d	d2	60	94	e4	da	61	00	8d	d2	60	94	e4	2d	60

Do a little editing of the un-XOR-ed hex



C:\Users\Admin\Downloads\b64-hex.txt - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

chocolatey.log keyword.txt NSRFile.txt.hash autopsy.log.1 b64-hex.txt

```
1 ca 02 00 00 61 32 72 4e 52 4b 76 42 4b 30 30 70 38 6c 00 00 00 00 00 00 00 00 e3 a7 2d 81 9e 84 b9 8d 80 ff ff bf 08 51 fd bd 39 9d 84
```

Recipe



From Base64



Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

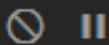
To Hex



Delimiter
Space

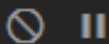
Bytes per line
0

From Hex



Delimiter
Auto

XOR



Key
aefdbd819d84b98d84ffffbfff7

HEX

Scheme
Standard

If at first, you don't succeed, try something else / July 17, 2020 / © 2020 AT&T Intellectual Property

Input

length: 124868
lines: 1



```
e3 a7 2d 81 9e 84 b9 8d 80 ff ff bf 08 51 fd bd 39 9d 84 b9 8d 84 ff ff ff f7 ae fd
bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81
9d 84 b9 8d 4c ff ff bf f9 b1 47 b3 81 29 8d 74 ac 3c fe b3 72 d6 fa 95 d4 f2 bd f4
cb e2 e3 8d 9e d2 d7 cd 9c d3 ef f2 f0 99 ef e1 df 8d ca 99 8e 94 d3 a1 d9 cb ea ad
e9 90 9b da d9 a3 f0 b7 a5 9d 84 b9 8d 84 ff ff fe 1b 12 ce b8 0c 4f e4 bc 00 56 9f
fa 32 25 ce 9d 56 52 fc 8e 34 5f e4 fa 72 6c 97 cd 70 6f e1 09 60 63 ec 84 72 2d df
63 4a d0 dd 85 10 56 d9 19 60 2f 9e bb 7a 7c 9d ef e8 fe ec bc 00 56 9f ff bf f7 ae
fd bd 81 9d d4 fc 8d 84 b3 fe ba f7 75 12 da dc 9d 84 b9 8d 84 ff ff bf 17 ae ff bc
8a 9c 8a a9 8d a8 ff ff bf e1 ae fd bd 81 9d 84 89 b4 84 ff ff af f7 ae fd fd 81 9d
84 b9 cd 84 ff ef bf f7 ae ff bd 81 9b 84 b9 8d 84 ff ff bf f1 ae fd bd 81 9d 84 b9
8d 04 ff ff bf f3 ae fd bd 81 9d 84 ba 8d c4 7a ff bf e7 ae fd ad 81 9d 84 b9 9d 84
ff ef bf f7 ae fd bd 81 8d 84 b9 8d 84 ff ff bf f7 ae fd bd 99 db 84 b9 2d 84 ff ff
bf 97 ae fd 5d 80 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff 8f bf f7
c2 fe bd 81 cd c0 b9 8d f4 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd
bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae bd bd 81
1d 85 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84
97 f9 e1 87 8b bf f7 ae 7d 96 81 9d 84 a9 8d 84 ff d3 bf f7 ae f9 bd 81 9d 84 b9 8d
84 ff ff bf f7 ae fd bd a1 9d 84 d9 a3 f6 9b 9e cb 96 ae fd 55 8c 9d 84 b9 cd 84 ff
```

Output

time: 17ms
length: 41623
lines: 43



```
MZ.....ÿÿ.....@.....È.....e... í!..Lí!This
program cannot be run in DOS mode.

$......Aì%3...ò`..ò`..ò`..éóá
ò`..ó`..ò`..äúá..ò`..ä-
`..ò`..äðá..ò`Rich..ò`.....PE..L...ûig].....à.....09.....@.....
```

Interesting Strings/IOCs

POST

explorer.exe

Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0

51.81.9.201

Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

Admin

/test2/gateway.php

filename.exe

C:\Users\Dhillon\Desktop\Waifu's Work\Release\Waifu's Work.pdb

5|@@@

h D@

F.QP

5X@@@

0123456789abcdef

TaskbarGlomLevel

Shell TrayWnd

\rundll32.exe shell32.dll,#61

Button

Looks like a key logger

pestudio-pro 9.01 - Malware Initial Assessment - www.winitor.com [c:\users\admin\downloads\secondstage.bin]

file help

c:\users\admin\downloads\secondstage.bin

name (88)	group (13)	mitre-technique (5)	mitre-tactic (4)	type (1)	anonymous (7)	blacklist (30)	ar ^
InternetConnectA	network	-	-	implicit	-	x	
HttpSendRequestA	network	-	-	implicit	-	x	
InternetCloseHandle	network	-	-	implicit	-	x	
InternetOpenA	network	-	-	implicit	-	x	
InternetOpenUrlA	network	-	-	implicit	-	x	
HeapCreate	memory	-	-	implicit	-	-	
HeapReAlloc	memory	-	-	implicit	-	-	
HeapFree	memory	-	-	implicit	-	-	
GetProcessHeap	memory	-	-	implicit	-	-	
HeapAlloc	memory	-	-	implicit	-	-	
MapVirtualKeyA	keyboard-and-mouse	-	-	implicit	-	x	
SetWindowsHookExW	hooking	Hooking	Persistence	implicit	-	x	
UnhookWindowsHookEx	hooking	Hooking	Persistence	implicit	-	x	
CallNextHookEx	hooking	Hooking	Persistence	implicit	-	-	
WriteFile	file	-	-	implicit	-	-	
CreateFileA	file	-	-	implicit	-	-	
SHGetFolderPathA	file	-	-	implicit	-	-	
CreateThread	execution	-	-	implicit	-	-	
TerminateThread	execution	-	-	implicit	-	x	
CreateProcessA	execution	Execution through A...	Execution	implicit	-	x	
Sleep	execution	Virtualization/Sandb...	Defense Evasion	implicit	-	-	
PostMessageA	execution	-	-	implicit	-	-	
LoadLibraryW	dynamic-link-library	Execution through A...	Execution	implicit	-	-	
GetProcAddress	dynamic-link-library	-	-	implicit	-	-	
GetModuleHandleW	dynamic-link-library	-	-	implicit	-	-	
GetLastError	diagnostic	-	-	implicit	-	-	
OpenDesktopA	desktop	-	-	implicit	-	x	
SetThreadDesktop	desktop	-	-	implicit	-	x	
CreateDesktopA	desktop	-	-	implicit	-	x	
IstrcpA	-	-	-	implicit	-	-	
CloseHandle	-	-	-	implicit	-	-	
IstrcatA	-	-	-	implicit	-	-	

sha256: B99AAB5CDD5274BC19690981A48FF4B83D8FA4EA80129FCDEA9CD11F5DD3A30 cpu: 32-bit file-type: executable subsystem: console entry-point: 0x00003930 signature: n/a

InternetConnectA
HttpSendRequestA
InternetCloseHandle
InternetOpenA
InternetOpenUrlA

HeapCreate
HeapReAlloc
HeapFree
GetProcessHeap
HeapAlloc

MapVirtualKeyA
SetWindowsHookExW
UnhookWindowsHookEx
CallNextHookEx

WriteFile
CreateFileA
SHGetFolderPathA
CreateThread
TerminateThread
CreateProcessA

Automate it

```
File Edit Selection View Go Run Terminal Help
unpack_listdemo.py - Visual Studio Code

unpack_listdemo.py X
#!/usr/bin/env python
import binascii
import struct
import base64
import argparse
import os

#PE Header
#0x250 0x0 Name: .pe
#0x258 0x8 Misc: 0xE064
#0x258 0x8 Misc_PhysicalAddress: 0xE064
#0x258 0x8 Misc_VirtualSize: 0xE064
#0x25C 0xC VirtualAddress: 0x3D000
#0x260 0x10 SizeOfRawData: 0xF000
#0x264 0x14 PointerToRawData: 0x39000
#0x268 0x18 PointerToRelocations: 0x0
#0x26C 0x1C PointerToLinenumbers: 0x0
#0x270 0x20 NumberOfRelocations: 0x0
#0x272 0x22 NumberOfLinenumbers: 0x0
#0x274 0x24 Characteristics: 0xC0000000
#

def xorit(d,key):
    k1=len(key)
    return ''.join([chr(ord(c)^ord(key[i%k1])) for i,c in enumerate(d)])

def unpackit(fn,args):
    bfn=os.path.basename(fn)
    pe = pefile.PE(fn)
    flag_pesection=False
    pe_section=None
    for section in pe.sections:
        if(section.Name == binascii.unhexlify('2e70650000000000')):#".pe"):
            flag_pesection=True
            pe_section=section
            break
    if(flag_pesection):
        pe_section.Data = xorit(pe_section.Data,pe_section.Name)
        pe_section.Name = bfn
        pe.save(bfn)
        print(bfn)
    else:
        print("Not a PE file")

if __name__ == '__main__':
    parser = argparse.ArgumentParser()
    parser.add_argument('fn', help='File to unpack')
    parser.add_argument('-o', help='Output file name')
    args = parser.parse_args()
    unpackit(args.fn,args.o)
```

Conclusions



Questions?

References:

- https://github.com/att/docker-forensics/blob/master/unpack_listdemo.py

Contact me:

jac@att.com

jclausing@isc.sans.edu

@jclausing on twitter

Thanks for attending

