Static Analysis: Analyzing Embedded Strings

Tyler Hudak
INCIDENT RESPONDER

@secshoggoth

Overview

Extracting and analyzing embedded strings

Finding hidden strings

Embedded strings analysis extracts and examines groups of readable characters from a file.

What Are Strings?

```
7363 7269 7074 2e70 6174 6800 2573 5c25  script.path.%s\%
7300 0000 2573 5c25 7300 0000 2e70 7331  s...%s\%s....ps1
0000 0000 5700 5300 6300 7200 6900 7000  ....W.S.c.r.i.p.
7400 0000 2573 5c25 7325 7300 2573 5c25  t...%s\%s%s.%s\%
6425 7300 2e68 7461 0000 0000 3c21 2d2d  d%s..hta....<!--
202d 2d2d 2d2d 2045 7865 5363 7269 7074   ----- ExeScript
204f 7074 696f 6e73 2042 6567 696e 202d   Options Begin -
2d2d 2d2d 0000 0000 2d2d 2d2d 2d20 4578  ----....----- Ex
6553 6372 6970 7420 4f70 7469 6f6e 7320  eScript Options
456e 6420 2d2d 2d2d 2d20 2d2d 3e00 0000  End ----- -->...
7773 6372 6970 742e 6578 6500 6373 6372  wscript.exe.cscr
6970 742e 6578 6520 2f42 0000 6373 6372  ipt.exe /B..cscr
6970 742e 6578 6500 2e68 7461 0000 0000  ipt.exe..hta....
6d73 6874 612e 6578 6500 0000 2e70 7331  mshta.exe....ps1
106a 4000 706a 4000 506b 4000 a06b 4000  .j@.pj@.Pk@..k@.
c06b 4000 d070 4000 4071 4000 6071 4000  .k@..p@.@q@.`q@.
c071 4000 b072 4000 0073 4000 2073 4000  .q@..r@..s@. s@.
d07b 4000 407c 4000 607c 4000 c07c 4000  .{@.@|@.`|@..|@.
c07d 4000 107e 4000 307e 4000 9077 4000  .}@..~@.0~@..w@.
2078 4000 3078 4000 4078 4000 6078 4000   x@.0x@.@x@.`x@.
```

What Can Strings Show Us?

Locality – strings next to each other

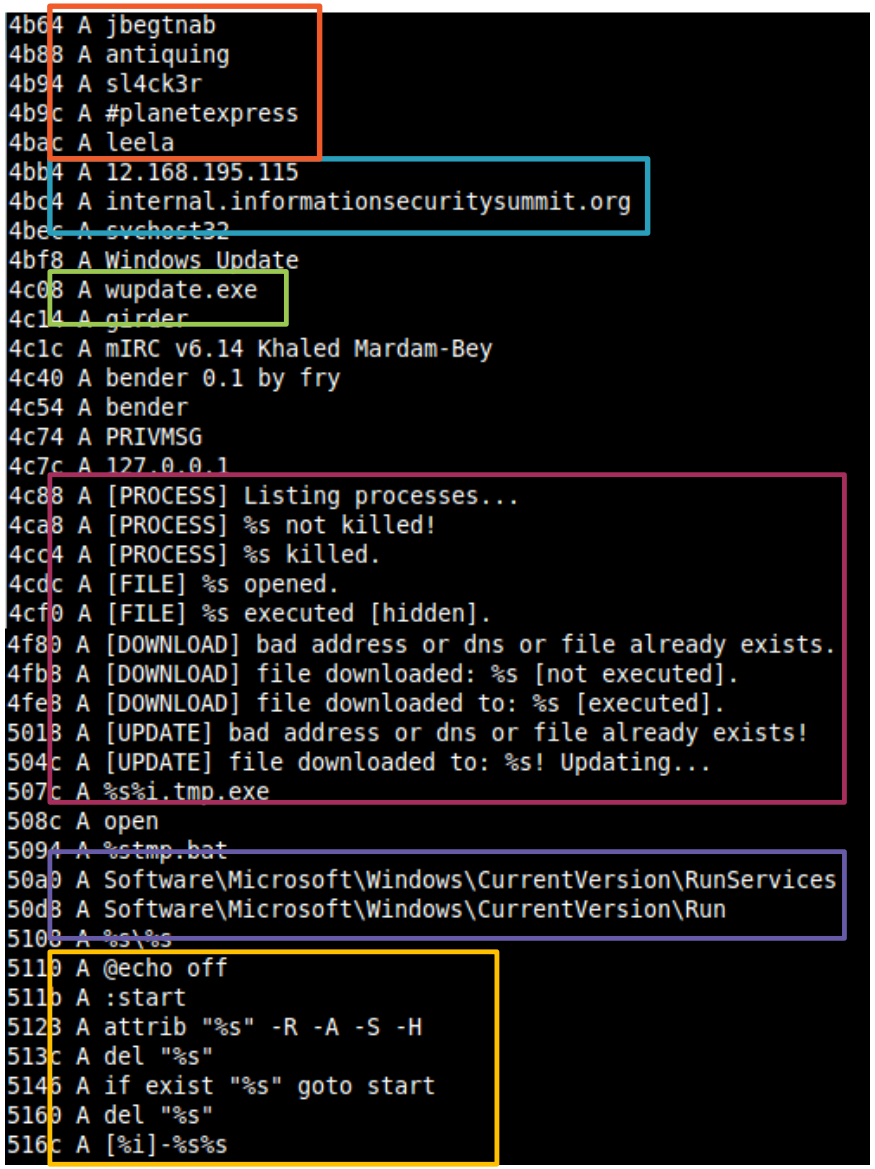
Hostnames, IP addresses, URLs

File names

Strings indicating functionality

Registry Keys

Unique or unusual strings



Types of Strings

String Length

Types of Strings

ASCII

7-bits long

128 characters

45	78	70	6C	6F	72	65	72	00
E	x	p	l	o	r	e	r	.

Unicode

8-, 16-, 32-bit characters

Over 128,000 characters

0045		0078		0070		006C		006F		0072		0065		0072		0000	
.	E	.	x	.	p	.	l	.	o	.	r	.	e	.	r	.	.

String Length

```
v/;F8t
GET
PUT
f9T$
scvhost.exe
SUVWj@Ph
j@hLA
badsite.blogspot.com
PING
FLOOD
D$(_^]
FreeLibrary
GetProcAddress
LoadLibraryA
CreateMutexA
GetSystemTimeAsFileT
ime
uN8E
PSSSSSSVS
```

Minimum Length 4

Minimum Length 6

Know your tool's default minimum string length

Strings

Extracts ASCII and Unicode at the same time

Minimum string length: 3

https://technet.microsoft.com/en-us/sysinternals/strings.aspx

Options

-n # : Set minimum string length

-o : Print decimal offset of string

Bintext

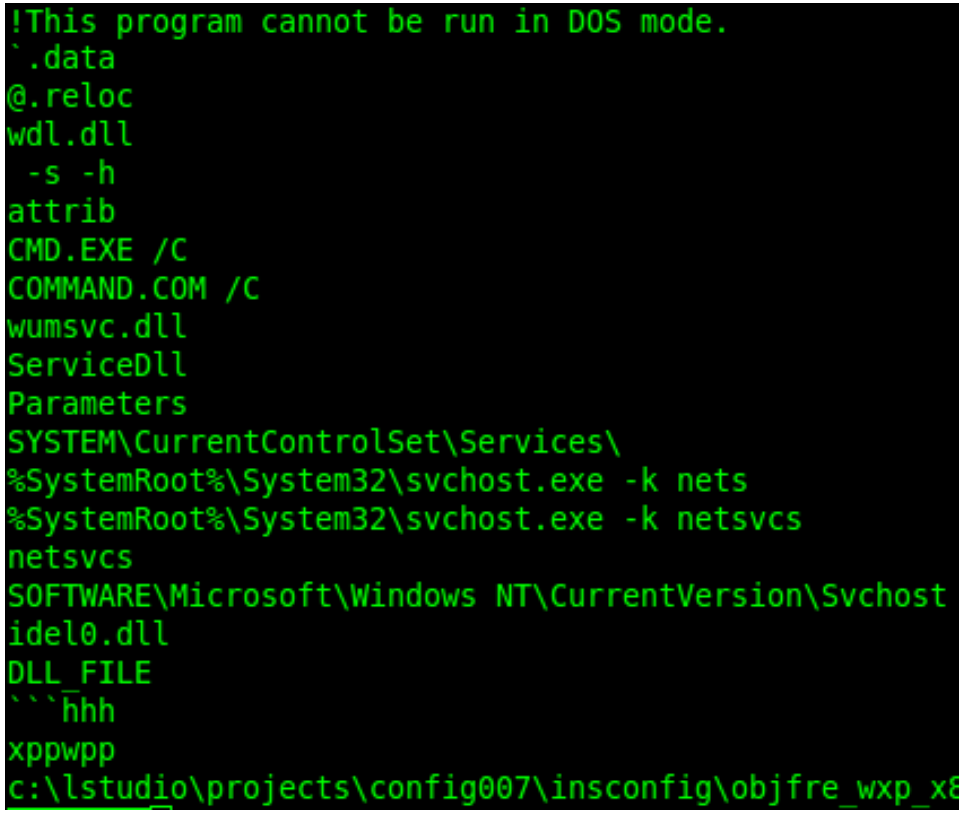
Extracts ASCII and Unicode at the same time

Minimum string length: 5

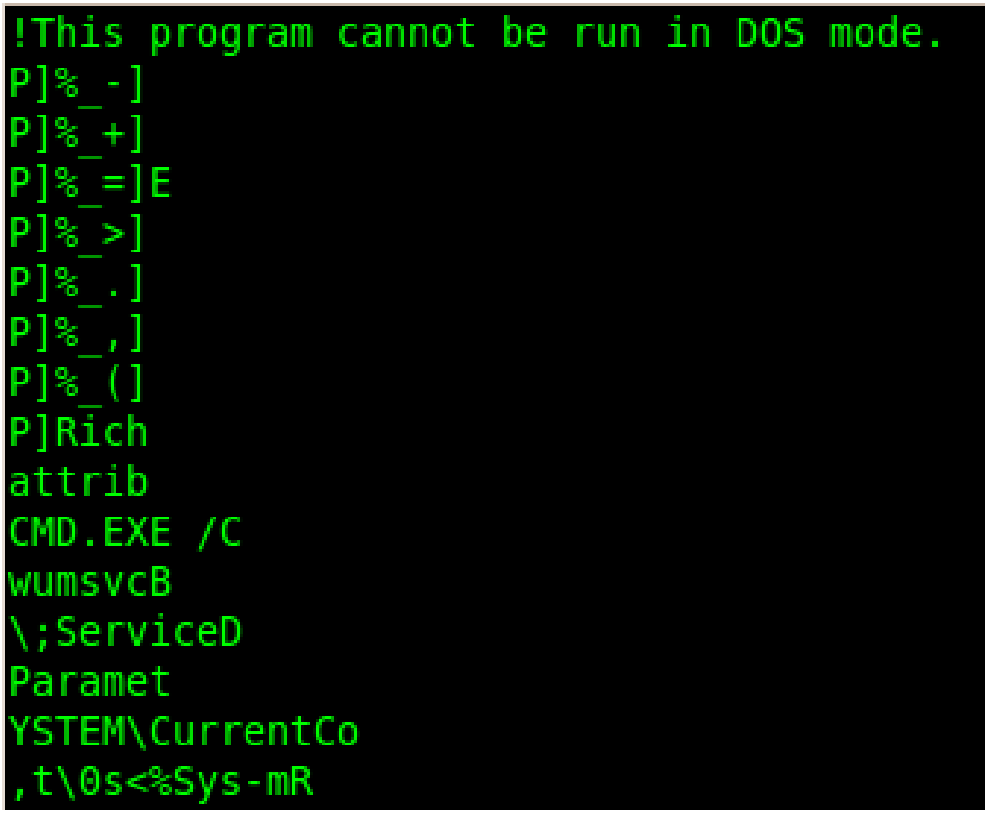
Watch out for the repeating bug!

https://www.mcafee.com/us/downloads/free-tools/bintext.aspx

Packers and Strings

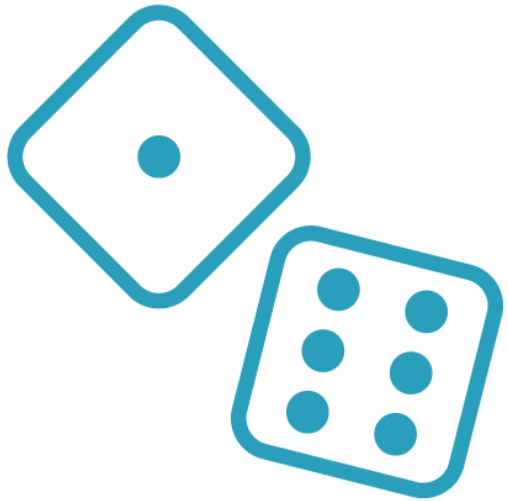


Unpacked



Packed

String Hiding Tricks



Random Strings

Packers may add random or legitimate looking strings to trick you

Encrypted Strings

Strings may be encoded or encrypted

Base64 Encoding

Converts 3 bytes to 4 ASCII characters

A-Za-z0-9+/ are the default characters used

Strings padded to length of 4 with “=“


Hello World!
Base64
SGVsbG8gV29ybGQh
Hello World
Base64
SGVsbG8gV29ybGQ=

Detecting Base64 Strings

Base64 alphabet

```
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
```

Random ASCII strings that end in =

```
Q29tbWFuZHMgZnJvbSB0aGUgd2ViIHNlcnZlciBzaG91bGQgcmVzcG9uZCBpbiB0aGUgZmFzaGlvbj
oKCjxIVFRQIEhFQURFUj4KXHJcblxyXG4KPGNvbW1hbmQ+IDxhcmd1bWVudHM+Cgp3aGVyZSBcclxu
XHJcbiBhcmUgdGhlIGNhcnJpYWdlIHJldHVybiwgbGluZSBmZWVkcwoK==
```

XOR

XOR Truth Table		
Input		Output
0	0	0
0	1	1
1	0	1
1	1	0

$$A \oplus K = C$$

$$C \oplus K = A$$

$$A \oplus 0 = A$$

$$A \oplus A = 0$$

XOR Encoding

E	x	p	l	o	r	e	r	.
45	78	70	6C	6F	72	65	72	00

XOR Encoding

E	x	p	l	o	r	e	r	.
45	78	70	6C	6F	72	65	72	00
⊕ 65								
20								

XOR Encoding

E	x	p	l	o	r	e	r	.
45	78	70	6C	6F	72	65	72	00
	⊕ 65							
20	1D							

XOR Encoding

E	x	p	l	o	r	e	r	.
45	78	70	6C	6F	72	65	72	00
		⊕ 65						
20	1D	15						

XOR Encoding

E	x	p	l	o	r	e	r	.
45	78	70	6C	6F	72	65	72	00
			⊕ 65	⊕ 65	⊕ 65	⊕ 65	⊕ 65	⊕ 65
20	1D	15	09	0A	17	00	17	65

xorsearch

Searches for XOR encoded version of string

https://blog.didierstevens.com/programs/xorsearch/

Strings to Search For
This
http
kernel
Create
~~www~~

Demo

budget-report.exe embedded strings

http://bit.ly/malfund-1

Summary

Embedded strings can reveal much of what the malware will do

If you aren't seeing the strings you expect, they may be hidden.

- Look for them!