



FIRST June 2022

# **Reversing Golang Binaries with Ghidra**

**Dorka Palotay** Senior Threat Researcher, CUJO AI

# Who am I

Background

Dorka Palotay (@pad0rka):

- Senior Threat Researcher at CUJO AI
- BSc in Applied Mathematics
- MSc in Security and Privacy Advanced Cryptography
- Worked at financial and security companies as well
- Malware researcher and reverse engineer
- Member of last4ofus CTF team (with Filip Savin, Zoltan Balazs, Albert Zsigovits)
  - o 2020 First CTF winner
  - $\circ~$  2021 First CTF second place





## Research topic

The quest

Background:

• IoT malware research -> more and more (IoT) malware families are written in Go

#### Issue:

- Reverse engineering Go binaries is challenging
  - $\circ$  Huge file size
  - o Unusual string handling
  - o No symbol names due to stripping
- Ghidra open-source development is in early stage compared to other tools
  - $\circ~$  Only a few open-source scripts are available, solving only parts of the problem

#### Goal:

• Making reverse engineering Go binaries with Ghidra easier

#### Steps:

- Understand Go and the differences from usual languages
- Get familiar with Ghidra's features (In this research we used Ghidra 10.0)
- Create our own scripts: <u>https://github.com/getCUJO/ThreatIntel</u>



### Golang Introduction

- Go (also called Golang) is an open source programming language
- Designed by Google in 2007
- Made available to the public in 2012
- Current version is Go 1.18
- https://golang.org/
- Go comes out top of the languages most developers want to learn<sup>1</sup>
- Advantages:
  - o Simple and clear documentation
  - o Easy to learn, ease of coding
  - o Compiled language (faster than Python)
  - o Cross compiling (Windows, Linux, macOS)
  - o Scalability and concurrency
  - o Garbage collection automatic memory management





#### https://unit42.paloaltonetworks.com/the-gopher-in-the-room-analysis-of-golang-malware-in-the-wild/



Malware families

# A surge in Go malware cryptostealer





GoLang Malware Count Over Time

First Seen Time

🔆 CUJOAI

# Static linking

### Big Bad Binaries

- Go binaries are statically linked by default
- All the necessary libraries are included in the executable image
- No dependency issues
- Large size
  - o Difficult malware distribution
  - $\circ~\mbox{Anti}$  virus products have difficulty to detect
  - Reverse engineering can be more time consuming

# Hello World - Unstripped



• C

٠

<pre>#include <stdio.h> int main() {     printf("Hello, World!\n");     return 0; }</stdio.h></pre>	gcc -o world_c world.c	ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, not stripped size: 16,3 kB
Go package main import "fmt"	go build -o world go world.go	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked,
<pre>func main(){     fmt.Printf("Hello, World!\n") }</pre>		not stripped size: 2,0 MB

### Hello World in Ghidra

#### C vs Go

🗐 Functions - 19 items		🌒 🖹 🖹 🗶
Name	Location 🖹 Function Signature Fi	unction Size
_init	00101000 int _init(EVP	27
FUN_00101020	00101020 undefined FUN	13
cxa_finalize	00101040 thunk undefine	11
puts	00101050 thunk int puts	11
_start	00101060 undefined _sta	47
deregister_tm_clones	00101090 undefined dere	34
register_tm_clones	001010c0 undefined regi	51
do_global_dtors_aux	00101100 undefineddo	54
frame_dummy	00101140 thunk undefine	9
main	00101149 undefined main()	27
libc_csu_init	00101170 undefinedli	101
libc_csu_fini	001011e0 undefinedli	5
_fini	001011e8 undefined _fini()	13
_ITM_deregisterTMCloneTable	00105000 thunk undefine	1
puts	00105008 thunk int puts	1
libc_start_main	00105010 thunk undefine	1
gmon_start	00105018 thunk undefine	1
_ITM_registerTMCloneTable	00105020 thunk undefine	1
cxa_finalize	00105028 thunk undefine	1

🔊 Functions - 1790 items			a   🔁 🔳 🗙
Name	Location	🖹 Function Signat	Function Size
internal/cpu.Initialize	00401000	undefined int	78 🔺
internal/cpu.processOptions	00401060	undefined int	1877
internal/cpu.indexByte	004017c0	undefined int	53
internal/cpu.doinit	00401800	undefined int	1029
internal/cpu.cpuid	00401c20	undefined int	27
internal/cpu.xgetbv	00401c40	undefined int	17
typeeq.internal/cpu.CacheLinePad	00401c60	undefined typ	6
typeeq.internal/cpu.option	00401c80	undefined typ	165
typeeq.[15]internal/cpu.option	00401d40	undefined typ	139
runtime/internal/sys.OnesCount64	00401de0	undefined run	119
runtime/internal/atomic.Cas64	00401e60	undefined run	26
runtime/internal/atomic.Casuintptr	00401e80	thunk undefin	5
runtime/internal/atomic.Storeuintptr	00401ea0	thunk undefin	5
runtime/internal/atomic.Store	00401ec0	undefined run	12
runtime/internal/atomic.Store64	00401ee0	undefined run	14
internal/bytealg.init.0	00401f00	undefined int	34
cmpbody	00401f40	undefined cmp	569
runtime.cmpstring	00402180	undefined run	30
memeqbody	004021a0	undefined mem	318
runtime.memequal	004022e0	undefined run	36
runtime.memequal_varlen	00402320	undefined run	35
indexbytebody	00402360	undefined ind	279
internal/bytealg.IndexByteString	00402480	undefined int	24
runtime.memhash128	004024a0	undefined run	89
runtime.strhashFallback	00402500	undefined run	98
runtime.f32hash	00402580	undefined run	282
runtime.f64hash	004026a0	undefined run	284
runtime.c64hash	004027c0	undefined run	110
runtime.cl28hash	00402840	undefined run	110

### 19 functions vs 1790 functions

## **Stripped Binaries**



- Discard debugging symbols
- Reduced size
- No names for routines and variables
- More difficult debugging and reverse engineering
- Malware files are usually stripped

# Hello World - Stripped



• C



gcc -o world\_c\_strip -s world.c

#### ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, **stripped**

size: 14,1 kB

• Go

### package main

import "fmt"

func main(){
 fmt.Printf("Hello, World!\n")

go build -o world\_go\_strip – **Idflags "-s"** world.go ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, **stripped** 

size: 1,3 MB



# Hello World Stripped in Ghidra



🛿 Functions - 19 items	📲   🔁 🗏	×
Name	Location 🕒 Function Signature Function Size	-
_DT_INIT	00101000 undefined _DT	27
FUN_00101020	00101020 undefined FUN	13
cxa_finalize	00101040 thunk undefine	11
puts	00101050 thunk int puts	11
entry	00101060 undefined entry()	47
FUN_00101090	00101090 undefined FUN	34
FUN_001010c0	001010c0 undefined FUN	51
_FINI_0	00101100 undefined _FIN	54
_INIT_0	00101140 thunk undefine	9
FUN_00101149	00101149 undefined FUN	27
FUN_00101170	00101170 undefined FUN	101
FUN_001011e0	001011e0 undefined FUN	5
_DT_FINI	001011e8 undefined _DT	13
_ITM_deregisterTMCloneTable	00105000 thunk undefine	1
puts	00105008 thunk int puts	1
libc_start_main	00105010 thunk undefine	1
gmon_start	00105018 thunk undefine	1
_ITM_registerTMCloneTable	00105020 thunk undefine	1
cxa finalize	00105028 thunk undefine	1

🛿 Functions - 1138 items			🍓   🎦 🔳 🗙
Name	Location	🖹 Function Signat	Function Size
F3N_00401000	00401000	undefined FUN	78 🔺
FUN_00401060	00401060	undefined FUN	1877
FUN_004017c0	004017c0	undefined FUN	53
FUN_00401800	00401800	undefined FUN	1029
FUN_00401c20	00401c20	undefined FUN	27
FUN_00401c40	00401c40	undefined FUN	17
FUN_00401c80	00401c80	undefined FUN	165
FUN_00401de0	00401de0	undefined FUN	119
FUN_00401e60	00401e60	undefined FUN	26
thunk_FUN_00401e60	00401e80	thunk undefin	5
thunk_FUN_00401ee0	00401ea0	thunk undefin	5
FUN_00401ec0	00401ec0	undefined FUN	12
FUN_00401ee0	00401ee0	undefined FUN	14
FUN_00402180	00402180	undefined FUN	599
FUN_004022e0	004022e0	undefined FUN	354
FUN_00402480	00402480	undefined FUN	303
FUN_00402580	00402580	undefined FUN	282
FUN_004026a0	004026a0	undefined FUN	284
FUN_004027c0	004027c0	undefined FUN	110
FUN_00402840	00402840	undefined FUN	110
FUN_004028c0	004028c0	undefined FUN	376
FUN_00402a40	00402a40	undefined FUN	368
FUN_00402bc0	00402bc0	undefined FUN	1640
FUN_004035a0	004035a0	undefined FUN	272
FUN_004036c0	004036c0	undefined FUN	280
FUN_004037e0	004037e0	undefined FUN	198
FUN_004038c0	004038c0	undefined FUN	119
FUN_00403940	00403940	undefined FUN	72
FUN_004039a0	004039a0	undefined FUN	338 🗸

### 19 functions vs 1138 functions

### strings

<pre>&gt; strings world_c   grep -o ".`</pre>	\{0,10\}main.\{0,10\}"
<pre>ibc_start_main</pre>	
ibc start main@@GLIBC 2.	
main	> strings world_c_strip   grep -o ".\{0,10\}main.\{0,10\}"
	ibc_start_main
> strings world_go   grep -o ".\{0	,10\}main.\{0,10\}"
hasmain	
edruntime.main not on m0	
p stateremaining pointe	
out of domainpanic whil	$\sim$ strings world so strip   srop $\sim$ " \ [0, 10\] main \ [0, 10\]
e space remainingreflect	> strings world_go_strip   grep -0 .\{0,10\}main.\{0,10\}
routines (main called ru	hasmain
runtime.main	edruntime.main not on m0
runtime.main.func1	n stateremaining pointe
runtime.main.func2	put of demainments whil
main.main	
maininittask	e space remainingreflect
runtime.main_init_done	routines (main called ru
runtime.mainStarted	runtime.main
runtime.mainPC	nuntimo main funci
runtime.main	
runtime.main.func1	runtime.main.func2
runtime.main.func2	main.main
main.main	





pcIntab

🖼 Listing: wor	ld_go_strip					d 🛍   💽   🛱 🕅	🗟 📄 - 🗙	🛄 Memory Map - I	mage Base: C	0400000					🕈 🚸 🖪 .	Ŧ ± ♦	🗙 🏡 🗙
world c strip	world c	world ao	world ao str	ip 🗙							Memor	y Blocks					
	00534896.0	(4)	22 (	iab				Name	Start 🗎	End	Length	R W	X Volati	e Overlay	/ Type	Initialized	d
	0053de97 0	0	22 (	0h			A	segment 2.1	00400000	00400f9b	0xf9c				Default		
	0053de98 0	0	?? (	00h				.note.go.buildid	00400f9c	00400fff	0x64		ĀĀ		Default		
	0053de99 0	0	?? (	Oh				.text	00401000	0049accf	0x99cd0				Default	V	
	0053de9a 0	0	?? (	Oh				rodata	00496000	004def44	0x43f45				Default	V	
	0053de9b 0	0	?? (	00h				segment 3.2	004def45	004df01f	0xdb				Default	1	
	0053de9c 0	0	?? 0	)0h				typelink	004df020	004df74f	0x730				Default		
	0053de9d 0	0	?? (	Oh			-	itablink	004df750	004df70f	0,750				Default		
	0053de9e 0	0	?? (	00h					00401730	0040791	0x30				Default		
	0053de9f 0	0	?? (	00h				gopcintab	004df/a0	0054028c	Ux6Uaed				Derault		
	0053dea0 e	0	?? E	Oh	? ->	004c86e0		.go.buildinfo	00541000	0054101	0x20				Default		
	0053deal 8	6	?? 8	86h				.noptrdata	00541020	0054f4bf	0xe4a0				Default	<b>v</b>	
	0053dea2 4	c	?? 4	ICh L				.data	0054f4c0	0055692f	0x7470				Default	$\checkmark$	
	0053dea3 0	0	?? (	oh				.bss	00556940	0058624f	0x2f910	<b>v</b>			Default		
	0053dea4 0	0	?? (	OOh				.shstrtab	OTHER:00	OTHER:00	0xa5			$\checkmark$	Default	$\checkmark$	
	0053dea5 0	0	?? (	ooh													
	0053dea6 0	0	?? (	oon													
	0053dea7 0		// (	ion													
•	0053dea8	0 01 09	as	main.main													
	0																
	0052dab2	6 6d 74	de '	fmt Printf"													
	000002 0	6 50 72	us	The Contraction of the Contracti													
	6	9 6e 74															
	0053debd 0	2	?? (	)2h													
	0053debe 1	3	?? 1	3h													
	0053debf b	0	?? E	BOh													
	0053dec0 0	1	?? (	lh													
	0053dec1 5	5	?? 5	5h U													
	0053dec2 a	f	?? /	Fh													
	0053dec3 0	1	?? (	lh													
	0053dec4 0	8	?? (	)8h													
	0053dec5 0	0	?? (	OOh													
	0053dec6 d	4	?? [	)4h													
	0053dec7 0	2	?? (	)2h													
	0053dec8 2	4	?? 2	24h \$			<b>T</b>			Lou :	<b>X</b>			F			
	•						7 Þ	🕞 Decompiler	× Loar Define	ea Strings ×	Function	is ×	Memory I	лар ×			



pcIntab

• Detailed documentation of pcIntab<sup>1</sup> is available



pcIntab

• Function metadata

struct {	Func		- Function name offset
-	uintptr	entry;	// start pc
	int32 name;	//	name (offset to C string)
	int32 args;	//	size of arguments passed to function
	int32 frame;	11	size of function frame, including saved caller PC
	int32	pcsp;	<pre>// pcsp table (offset to pcvalue table)</pre>
	int32	<pre>pcfile;</pre>	<pre>// pcfile table (offset to pcvalue table)</pre>
	int32	pcln;	<pre>// pcln table (offset to pcvalue table)</pre>
	int32	nfuncdata	// number of entries in funcdata list
	int32	npcdata;	// number of entries in pcdata list
};			



pcIntab (from go 1.16 and go 1.18)

// pcHeader holds data used by the pclntab lookups.

}

#### type pcHeader struct {

}

magic	uint32	// 0xFF	FFFFA			
pad1, pad2	uint8	// 0,0				
minLC	uint8	// min	instruction s	ize		
ptrSize	uint8	// size	of a ptr in H	oytes		
nfunc	int	// pcHe	ader holds data	used by	the	e pclntab lookups.
nfiles	uint	type pc	Header struct {			
funcnameOffset	uintptr	ר	magic	uint32	//	0xFFFFFF0
auOffeet			pad1, pad2	uint8	//	0,0
cuuttset	uintptr	4	minLC	uint8	//	min instruction size
filetab0ffset	uintptr		ptrSize	uint8	//	size of a ptr in bytes
pctab0ffset	uintptr		nfunc	int	//	number of functions in the module
ncln0ffset	uintptr	ר	nfiles	uint	//	number of entries in the file tab
pechorisee	uincpei	J	textStart	uintptr	//	base for function entry PC offsets in this module, equal t
		[	funcname0ffset	uintptr	//	offset to the funcnametab variable from pcHeader
			cuOffset	uintptr	11	offset to the cutab variable from pcHeader
			filetab0ffset	uintptr	//	offset to the filetab variable from pcHeader
		_	pctab0ffset	uintptr	//	offset to the pctab variable from pcHeader
		ſ	pcln0ffset	uintptr	11	offset to the pclntab variable from pcHeader



pcIntab in Windows

#### • Not a separate section -> Look for the structure

🖼 Listing: wo	rld_go_strip.exe					🗅 🜔   💽   🗮 📝   💩	- ×	🛄 Memory Map - Ir	nage Base: 004	00000					🗕 🕈 🔶	⊟∓±	- 🔶 🗙 🏡 🗙
world c stri	p world c	world ao	*world go strip	*world go strip.exe 🗙				1			Memo	ry Blocks					1
			1					Name	Start 🗎	End End	Length	R W X	Volatile	Overlay	Туре	Initialized	J B
		DAT	004610-0		VDEE [1]	0055h2-0(*)	A	Headers	00400000	004005ff	0x600				Default	<b>v</b>	F
	004510-0	DAT	_004119e0		XREF[1]:	00550200(*)		tout	00401000	004o72ff	0x26400			Ē	Default		F
	004119e0 1	if i	22 EEb					.rdata	004a8000	005557ff	0xad800				Default	<b>v</b>	E
	004f19e2 f	f	22 FEh					.data	00556000	0056b3ff	0x15400				Default	V	F
	004f19e3 f	f	?? FFh					data	0056b400	005a07c7	0x353c8				Default		
	004f19e4 C	00	?? 00h					idata	005a1000	005a15ff	0x600				Default	<b>J</b>	F
	004f19e5 0	00	?? 00h					reloc	005a2000	005a9bff	0x7c00				Default		5
	004f19e6 C	01	?? 01h					sumtab	005a2000	005a301	0x200				Default		E
	004f19e7 C	8	?? 08h					.synicab	00544000	UUSaain	0x200				Delault	•	F
	004f19e8 f	d	?? FDh														
	004f19e9 C	6	?? 06h														
	004f19ea C	00	?? 00h														
	004f19eb G	00	?? 00h														
	004f19ec C	00	?? 00h				8										
	004f19ed C	00	?? 00h														
	004f19ee C	00	?? 00h														
0	004f19ef C	00	?? 00h														
U	004f19f0 C	00	?? 00h			? -> 00401000											
	004f19f1 1	.0	?? 10h														
	004f19f2 4	0	?? 40h	0													
	004f19f3 0	00	?? 00h														
	004f19f4 C	00	?? 00h														
	004f19f5 C	00	?? 00h														
	004f19f6 C	00	?? 00h														
	004f19f7 C	00	?? 00h														
	004f19f8 f	0	?? F0h														
	004f19f9 6	of	?? 6Fh	0													
	004f19fa 🕻	00	?? 00h				5										
	004f19fb 0	00	?? 00h														
	004f19fc C	00	?? 00h														
	004f19fd C	00	?? 00h														
	004f19fe C	00	?? 00h														
	004f19ff C	00	?? 00h				-										
	004fla00 8	30	?? 80h			? -> 00401080											
	004f1a01 1	0	22 1.0h			1			0101 Defined	Strings x	Eunctions ×	Memony M	lan x				
							/	- Decomplier ,	L DAI Denneu	strings	, anctions a	- Hennery I	- ap				

Binary: world\_go\_strip.exe



Binary: world\_go\_strip



### Executing our script

🛿 Functions - 1138 items			🌒   🎦 🗏 🗙
Name	Location	🖹 Function Signat	Function Size
FUN_00401000	00401000	undefined FUN	78 🔺
FUN_00401060	00401060	undefined FUN	1877 🗋
FUN_004017c0	004017c0	undefined FUN	53
FUN_00401800	00401800	undefined FUN	1029
FUN_00401c20	00401c20	undefined FUN	27
FUN_00401c40	00401c40	undefined FUN	17
FUN_00401c80	00401c80	undefined FUN	165
FUN_00401de0	00401de0	undefined FUN	119
FUN_00401e60	00401e60	undefined FUN	26
thunk_FUN_00401e60	00401e80	thunk undefin	5
thunk_FUN_00401ee0	00401ea0	thunk undefin	5
FUN_00401ec0	00401ec0	undefined FUN	12
FUN_00401ee0	00401ee0	undefined FUN	14
FUN_00402180	00402180	undefined FUN	599
FUN_004022e0	004022e0	undefined FUN	354
FUN_00402480	00402480	undefined FUN	303
FUN_00402580	00402580	undefined FUN	282
FUN_004026a0	004026a0	undefined FUN	284
FUN_004027c0	004027c0	undefined FUN	110
FUN_00402840	00402840	undefined FUN	110
FUN_004028c0	004028c0	undefined FUN	376
FUN_00402a40	00402a40	undefined FUN	368
FUN_00402bc0	00402bc0	undefined FUN	1640
FUN_004035a0	004035a0	undefined FUN	272
FUN_004036c0	004036c0	undefined FUN	280
FUN_004037e0	004037e0	undefined FUN	198
FUN_004038c0	004038c0	undefined FUN	119
FUN_00403940	00403940	undefined FUN	72
FUN_004039a0	004039a0	undefined FUN	338 🗸
FUEL AD LOOL AD	00100100	1.61.1.00000	105

🗿 Functions - 1790 items			🔁   🎦 🔳 🗙
Name	Location	🖹 Function Signat	Function Size
fmt.(*pp).Flag	00492de0	undefined fmt	143
fmt.(*pp).Write	00492e80	undefined fmt	271
fmt.Fprintf	00492fa0	undefined fmt	268
fmt.getField	004930c0	undefined fmt	183
fmt.parsenum	00493180	undefined fmt	219
fmt.(*pp).unknownType	00493260	undefined fmt	784
fmt.(*pp).badVerb	00493580	undefined fmt	1649
fmt.(*pp).fmtBool	00493c00	undefined fmt	111
fmt.(*pp).fmt0x64	00493c80	undefined fmt	149
fmt.(*pp).fmtInteger	00493d20	undefined fmt	820
fmt.(*pp).fmtFloat	00494060	undefined fmt	408
fmt.(*pp).fmtComplex	00494200	undefined fmt	583
fmt.(*pp).fmtString	00494460	undefined fmt	457
fmt.(*pp).fmtBytes	00494640	undefined fmt	2303
fmt.(*pp).fmtPointer	00494f40	undefined fmt	1358
fmt.(*pp).catchPanic	004954a0	undefined fmt	1534
fmt.(*pp).handleMethods	00495aa0	undefined fmt	1748
fmt.(*pp).printArg	00496180	undefined fmt	2348
fmt.(*pp).printValue	00496ae0	undefined fmt	9767
fmt.intFromArg	00499140	undefined fmt	529
fmt.parseArgNumber	00499360	undefined fmt	293
fmt.(*pp).argNumber	004994a0	undefined fmt	278
fmt.(*pp).badArgNum	004995c0	undefined fmt	367
fmt.(*pp).missingArg	00499740	undefined fmt	367
fmt.(*pp).doPrintf	004998c0	undefined fmt	4490
fmt.globfunc1	0049aa60	undefined fmt	84
fmt.init	0049aac0	undefined fmt	197 -
typeea.fmt.fmt	0049aba0	undefined typ	172
main.main	0049ac60	undefined mai	112



Real world example – eChOraix

🕑 Functions - 2827 iter	ms		🗏 🚵 🖹	🛿 Functions - 5104 ite	ms		🔳 💽 🔁 🗙
Label	Location	🖹 Function Signature	Function Size	Label	Location	🖹 Function Signature	Function Size
FUN_08049000	08049000	undefined FUN_08	135 🔺	os/exec.ExitError.Str	08208510	undefined os/exe	1
FUN_08049090	08049090	undefined FUN_08	268	os/exec.ExitError.Svs	08208560	undefined os/exe	1
thunk_FUN_08049d30	080491a0	thunk undefined	5	main.getInfo	082085b0	undefined main.g	1527
thunk_FUN_08049d30	080491b0	thunk undefined	5	main.checkReadme	08208bb0	undefined main.c	144
thunk_FUN_08049dc0	080491c0	thunk undefined	5	main.init.0	08208c40	undefined main.i	715
thunk_FUN_08049e10	080491d0	thunk undefined	5	main.main	08208f10	undefined main.m	1032
thunk_FUN_08049e10	080491e0	thunk undefined	5	main.randSeq	08209320	undefined main.r	254
thunk_FUN_08049e30	080491f0	thunk undefined	5	main.in	08209420	undefined main.i	134
thunk_FUN_08049d10	08049200	thunk undefined	5	main.writemessage	082094b0	undefined main.w	346
thunk_FUN_08049d10	08049210	thunk undefined	5	main.chDir	08209610	undefined main.c	752
thunk_FUN_08049ee0	08049220	thunk undefined	5	main.encrypt	08209900	undefined main.e	1999
thunk_FUN_08049d10	08049230	thunk undefined	5	main.makesecret	0820a0d0	undefined main.m	399
thunk_FUN_08049d20	08049240	thunk undefined	5	main.main.func1	0820a260	undefined main.m	502
thunk_FUN_08049ed0	08049250	thunk undefined	5	main.init	0820a460	undefined main.i	179
thunk_FUN_08049ed0	08049260	thunk undefined	5	golang.org/x/net/pro	0820a520	undefined golang	110
thunk_FUN_08049ed0	08049270	thunk undefined	5	typehash.main.Info	0820a590	undefined type	83
FUN_08049280	08049280	undefined FUN_08	57	typeeq.main.Info	0820a5f0	undefined type	143
FUN_080492c0	080492c0	undefined FUN_08	462	typehash.[604]string	0820a680	undefined type	83
FUN_08049490	08049490	undefined FUN_08	80 🗸	typeeq.[604]string	0820a6e0	undefined type	138
Filter:			图 幸 -	Filter:			🙆 🛱 •



Challenges

#### • Undefined function name strings

			*****	*****	****	******	*******	****		
			ŧ.		FU	VCTION		*		
			******	********	****	*****	*******	*****		
		1	undefined FUN	08184fa0(un	defi	ned4 param 1, undef	fined4 pa			func
undefin	ed		AL:1	<return></return>		10 <b>T</b> (1)				·
undefin	ed4		Stack[0x4]:4	param l				XREF[1]:	08184fc7(R)	
undefin	ed4		Stack[0x8]:4	param 2				XREF[2]:	08184fd8(R),	#Try
									0818501d(R)	if fi
undefin	ied4		Stack[Oxc]:4	param_3				XREF[2]:	08184ff0(R),	
									0818500b (R)	1
undefin	ed4		Stack[0x10]:	4 param_4				XREF[1]:	08184fdf(R)	
undefin	ied4		Stack[0x14]:	4 param_5				XREF[1]:	08184ff7(R)	
undefin	ed4		Stack[0x18]:	4 param_6				XREF[1]:	08184ffe(W)	
undefin	ed4		Stack[-0x4]:	4 local_4				XREF[1]:	08184fc3(R)	
undefin	ed4		Stack[-0x8]:	4 local_8				XREF[1]:	08184fbb(*)	
		1	-UN_08184fa0				XREF[2]:	081850	2f(c),	
								log.in	it:08186012(c)	
08184fa0 <mark>65</mark>	8b 00	d i	MOV	ECX, dword	ptr	GS: [0x0]				
00	00 00	00 0								
08184fa7 <mark>8b</mark>	89 f	8	MOV	ECX, dword	ptr	[ECX + Oxfffffffc]				
ff	ff f	f								
							col			
			08	Jaaue4 bc		11	6Ch	L		
			08	3aa0e5 6T		77	6Hh	0		
			08	3aa0e6 67		??	67h	g		
			08	3aa0e7 2e		??	2Eh	•		
			08	3aa0e8 <mark>4e</mark>		??	4Eh	N		
			08	3aa0e9 <mark>65</mark>		??	65h	e		
			08	3aa0ea 77		??	77h	W		
			08	3aa0eb 00		??	00h			

<pre>func_name = getDataAt(name_address)</pre>
<pre>#Try to define function name string. if func_name is None:     try:</pre>
<pre>func_name = createAsciiString(name_address) except:     print "ERROR: No name"     continue</pre>

Binary: eChOraix - x86

# Hello World Strings in Ghidra

🚻 Defined Strings -	· 70 items		🍫 📄 🔁
Location	String Value	String Representat	Data Type
.strtab::000000db	GNU EH FRAME HDR	" GNU EH FRAME	ds
.strtab::000000ee	_GLOBAL_OFFSET_TABLE_	"_GLOBAL_OFFSET	ds
.strtab::00000104	libc_csu_fini	"_libc_csu_fini"	ds
.strtab::00000114		"_ITM_deregisterTM	ds
.strtab::00000130	puts@@GLIBC_2.2.5	"puts@@GLIBC_2.2	ds
.strtab::00000142	_edata	"_edata"	ds
.strtab::00000149	_libc_start_main@@GLIBC_2.2.5	"libc_start_main	ds
.strtab::00000168	data_start	"data_start"	ds
.strtab::00000175	_gmon_start_	"_gmon_start_"	ds
.strtab::00000184	_dso_handle	"dso_handle"	ds
.strtab::00000191	_IO_stdin_used	"_IO_stdin_used"	ds
.strtab::000001a0	libc_csu_init	"_libc_csu_init"	ds
.strtab::000001b0	bss_start	"bss_start"	ds
.strtab::000001bc	main	"main"	ds
.strtab::000001c1	TMC_END	"TMC_END"	ds
.strtab::000001cd	_ITM_registerTMCloneTable	"_ITM_registerTMCl	ds
.strtab::000001e7	cxa_finalize@@GLIBC_2.2.5	"cxa_finalize@@G	ds
00100001	ELF	"ELF"	ds
00100318	/lib64/ld-linux-x86-64.so.2	"/lib64/ld-linux-x86	ds
00100471	libc.so.6	"libc.so.6"	ds
0010047b	puts	"puts"	ds
00100480	cxa_finalize	"cxa_finalize"	ds
0010048f	libc_start_main	"libc_start_main"	ds
001004al	GLIBC_2.2.5	"GLIBC_2.2.5"	ds
001004ad	_ITM_deregisterTMCloneTable	"_ITM_deregisterTM	ds
001004c9	_gmon_start	"_gmon_start_"	ds
001004d8	_ITM_registerTMCloneTable	"_ITM_registerTMCl	ds
00102004	Hello, World!	"Hello, World!"	ds
00102061	zR	"zR"	ds 🔻

🕅 Defined Strings - 6544 it	ems			🎸 📄 🔁 🗙
Location	E String Value	String Representation	Data Type	
.shstrtab::00000001	.text	".text"	ds	
.shstrtab::00000007	.noptrdata	".noptrdata"	ds	
.shstrtab::00000012	data	".data"	ds	
.shstrtab::00000018	.bss	".bss"	ds	
.shstrtab::0000001d	.noptrbss	".noptrbss"	ds	
.shstrtab::00000027	_libfuzzer_extra_counters	"_libfuzzer_extra_coun	ds	
.shstrtab::00000042	.go.buildinfo	".go.buildinfo"	ds	
.shstrtab::00000050	.note.go.buildid	".note.go.buildid"	ds	
.shstrtab::00000061	.elfdata	".elfdata"	ds	
.shstrtab::0000006a	.rodata	".rodata"	ds	
.shstrtab::00000072	.typelink	".typelink"	ds	
.shstrtab::0000007c	.itablink	".itablink"	ds	
.shstrtab::00000086	.gosymtab	".gosymtab"	ds	
.shstrtab::00000090	.gopcIntab	".gopcIntab"	ds	
.shstrtab::0000009b	.symtab	".symtab"	ds	
.shstrtab::000000a3	.strtab	".strtab"	ds	
.shstrtab::000000ab	.debug_abbrev	".debug_abbrev"	ds	
.shstrtab::000000b9	.zdebug_abbrev	".zdebug_abbrev"	ds	
.shstrtab::000000c8	.debug_frame	".debug_frame"	ds	
.shstrtab::000000d5	.zdebug_frame	".zdebug_frame"	ds	
.shstrtab::000000e3	.debug_info	".debug_info"	ds	
.shstrtab::000000ef	.zdebug_info	".zdebug_info"	ds	
.shstrtab::000000fc	.debug_loc	".debug_loc"	ds	
.shstrtab::00000107	.zdebug_loc	".zdebug_loc"	ds	
.shstrtab::00000113	.debug_line	".debug_line"	ds	
.shstrtab::0000011f	.zdebug_line	".zdebug_line"	ds	
.shstrtab::0000012c	.debug_pubnames	".debug_pubnames"	ds	
.shstrtab::0000013c	.zdebug_pubnames	".zdebug_pubnames"	ds	
.shstrtab::0000014d	.debug_pubtypes	".debug_pubtypes"	ds	

### 70 defined strings vs 6544 defined strings

Binaries: world\_c, world\_go

### Hello World Strings in Ghidra C vs Go

Defined Strings	s - 0 items (of 6544)	See 1997 - S
Location	E String Value	String Representati Data Type

🚻 Defined Strings -	70 items					🌮 🔳	2	×
Location	🖻 St	ring Value		String Representat	Data Type			
.strtab::000000db	_	GNU EH FRAME HDR		" GNU EH FRAME	ds			
.strtab::000000ee	G	LOBAL OFFSET TABLE		" GLOBAL OFFSET	ds			
.strtab::00000104	_	libc_csu_fini		"_libc_csu_fini"	ds			
.strtab::00000114		M_deregisterTMCloneTable		"_ITM_deregisterTM	ds			
.strtab::00000130	pu	its@@GLIBC_2.2.5		"puts@@GLIBC_2.2	ds			L
.strtab::00000142	_e	data		"_edata"	ds			
.strtab::00000149	_	libc_start_main@@GLIBC_2.2.	5	"libc_start_main	ds			
.strtab::00000168		data_start		"data_start"	ds			L
.strtab::00000175	_	gmon_start		"_gmon_start_"	ds			
.strtab::00000184	_	dso_handle		"dso_handle"	ds			
.strtab::00000191	_10	D_stdin_used		"_I0_stdin_used"	ds			
.strtab::000001a0	_	libc_csu_init		"libc_csu_init"	ds			
.strtab::000001b0	_	bss_start		"bss_start"	ds			
.strtab::000001bc	m	ain		"main"	ds			L
.strtab::000001c1	_	TMC_END		"TMC_END"	ds			
.strtab::000001cd	_n	TM_registerTMCloneTable		"_ITM_registerTMCl	ds			L
.strtab::000001e7	_	cxa_finalize@@GLIBC_2.2.5		"cxa_finalize@@G	ds			
00100001	EL	F		"ELF"	ds			
00100318	/lil	o64/ld-linux-x86-64.so.2		"/lib64/ld-linux-x86	ds			
00100471	lib	c.so.6		"libc.so.6"	ds			
0010047b	pu	uts		"puts"	ds			
00100480		cxa_finalize		"cxa_finalize"	ds			
0010048f	_	libc_start_main		"_libc_start_main"	ds			
001004al	GL	IBC_2.2.5		"GLIBC_2.2.5"	ds			
001004ad	_0	TM_deregisterTMCloneTable		"_ITM_deregisterTM	ds			
001004c9		gmon_start		"_gmon_start_"	ds			
00100408		M_register Mcione rable		_rrm_registerrmci	as			
00102004	He	ello, World!		"Hello, World!"	ds			
00102001				<u></u>				۷



# Hello World Strings



C vs Go

### C: "Hello, World!" is easy to find

> strings world\_c | grep Hello
Hello, World!

### Go: "Hello, World!" is part of a huge string

#### > strings world\_go | grep Hello

entersyscallgcBitsArenasgcpacertracehost is downillegal seekinvalid slotlfstack.pushmadvdontneedmheapSpecialmspanSpecialnot pollableraceF iniLockreleasep: m=runtime: gp=runtime: sp=short bufferspanSetSpinesweepWaiterstraceStringsuname failedwirep: p->m= != sweepgen MB) work ers= called from failed with flushedWork heap\_marked= idlethreads= is nil, not nStackRoots= s.spanclass= span.base()= syscalltick= wo rk.nproc= work.nwait= , gp->status=, not pointer-byte block (3814697265625GC sweep waitGunjala\_GondiHello, World!Masaram\_GondiMende\_Kika kuiOld\_HungarianSIGKILL: killSIGQUIT: quitbad flushGen bad map statedebugCall2048exchange fullfatal error: level 3 resetload64 failedmin too largenil stackbaseout of memorysrmount errortimer expiredtraceStackTabtriggerRatio=value method xadd64 failedxchg64 failed}

### String Representation C vs Go

### С

• sequence of characters terminated with a null character

#### Go

- sequence of bytes with a fixed length
- not null terminated
- str sequence of bytes
- len number of bytes
- <u>https://golang.org/src/runtime/string.go</u>
- Large string blobs from concatenated strings until null character
- Ghidra has a hard time defining strings in Go binaries

#### Idea: help Ghidra to find string structures

- Static vs dynamic allocation
- Per architecture (different instruction set)
- Multiple solution within one architecture
- Possible changes per Go version

type stringStruct struct {
 str unsafe.Pointer
 len int
}





main:00101151(\*)

XREF[1]:

s Hello, World! 00102004

"Hello, World!"

ds



- Several different scenarios
- Let's look at the Hello World examples again



00102004 48 65 6c

6c 6f 2c

20 57 6f ...

Binary: world\_c



x86

	main.main	XREF[4]:	Entry Point(*), runtime.main:00434ac7(c), 0049acce(c), 004c5cb8(*)
0049ac60 64 48 8b 0c 25 f8 ff ff ff	MOV	<pre>RCX,qword ptr FS:[0xfffffff8]</pre>	
0049ac69 48 3b 61 1	0 CMP	RSP gword ptr [RCX + $0x10$ ]	
0049ac6d 76 5a	1BE	LAB 0049acc9	
0049ac6f 48 83 ec 5	8 SUB	BSP. 0x58	
0049ac73 48 89 6c 24 50	MOV	qword ptr [RSP + local_8], RBP	
0049ac78 48 8d 6c 24 50	LEA	RBP=>local_8, [RSP + 0x50]	
0049ac7d 48 8b 05 0c bd 0b 0	MOV 0	RAX,qword ptr [os.Stdout]	= ??
0049ac84 48 8d 0d 95 26 04 0	LEA	RCX,[go.itab.*os.File,io.Writer]	=
0049ac8b 48 89 0c 2	4 MOV	gword ptr [RSP]=>local 58.RCX=>go.itab.*os.F	ile.i =
0049ac8f 48 89 44	MOV	qword ptr [RSP + local_50],RAX	
0049ac94 48 8d 05 89 45 02 0	LEA 0	RAX, [DAT_004bf224]	= 48h H
0049ac9b 48 89 44 24 10	MOV	<pre>qword ptr [RSP + local_48], RAX=&gt;DAT_004bf224</pre>	= 48h H
0049aca0 48 c7 44 24 18 0e 00 00 00	MOV	<pre>qword ptr [RSP + local_40],0xe</pre>	
0049aca9 48 c7 44 24 20 00 00 00 00	MOV	<pre>qword ptr [RSP + local_38],0x0</pre>	
0049acb2 0f 57 c0	XORPS	XMMO, XMMO	
0049acb5 0f 11 44 24 28	MOVUPS	<pre>xmmword ptr [RSP + local_30[0]],XMM0</pre>	
0049acba e8 el 82 ff ff	CALL	fmt.Fprintf	undefined fmt.Fprintf(



ma:	in.main	XREF[4]:	Entry Point(*), runtime.main:00434ac7(c), 0049acce(c), 004c5cb8(*)				
0049ac60 64 48 8b 0c 25 f8 ff ff ff	MOV	<pre>RCX,qword ptr FS:[0xfffffff8]</pre>			DAT_004bf224		
0049ac69 48 3b 61 10	CMP	BSP award ptr [RCX $\pm$ 0x10]		004bf224 49	22	19h	E.
0049ac6d 76 5a	1RE			00457225 48	22	40H	
0049ac6f 48 83 ec 58	SUB	BSP 0v58		00455225 65	11	CCh	1
0049ac73 48 89 6c	MOV	aword ntr [RSP + local 8] RBP		00401226 60	rr 20	6Ch	
24 50	1101	divid per (ror r cocac_of)(b)		00467227 60		6Ch	l
0049ac78 48 8d 6c	LEA	BBP=>local 8 [BSP + 0x50]		004b1228 61	25	6Fh	0
24 50	LLA			004bf229 2c	??	2Ch	,
0049ac7d 48 8b 05	MOV	RAX gword ntr [os.Stdout]	= ??	004bf22a 20	??	20h	
0c bd 0b 00		low, quot a per (obrocadae)		004bf22b 57	??	57h	W
0049ac84 48 8d 0d	I FA	<pre>BCX.[go.itab.*os.File.io.Writer]</pre>	-	004bf22c 6f	??	6Fh	0
95 26 04 00		nen, (gerittabi een ite) iennitter,		004bf22d 72	??	72h	r
0049ac8b 48 89 0c 24	MOV	gword ptr [RSP]=>local 58.RCX=>go 2.ab.*os	File.i=	004bf22e 6c	??	6Ch	1
0049ac8f 48 89 44	MOV	gword ptr [RSP + local 50].RAV		004bf22f 64	22	64h	d
24 08		dieta per tres i const_oothing		004bf220 21	22	21h	ĩ
0049ac94 48 8d 05	LEA	RAX. [DAT 004bf224]	= 48h H	004bf230 21	22	046	
89 45 02 00				00401231 08	11	UAIT	
0049ac9b 48 89 44	MOV	gword ptr [RSP + local 48].RAX=>DAT 004bf2	<b>24</b> = 48h H				
24 10							
0049aca0 48 c7 44	MOV	gword ptr [RSP + local 40].0xe					
24 18 Oe		deren han deren in eren Grettenen.	_				
00 00 00							
0049aca9 48 c7 44	MOV	oword ptr [RSP + local 38].0x0					
24 20 00		1					
00 00 00				Length			
0049acb2 0f 57 c0	XORPS	XMMO, XMMO		Lengui			
0049acb5 Of 11 44	MOVUPS	xmmword ptr [RSP + local 30[0]].XMMO					
24 28							
0049acba e8 e1 82	CALL	fmt.Fprintf	undefined fmt.Fprintf	(			
ff ff	Contract of Contract						

Binary: world\_go



#### • Search for these instructions and define strings

#x86		
#LEA	REG,	[STRING_ADDRESS]
#MOV	[ESP	+], REG
#M0V	[ESP	+], STRING_SIZE

08208bdc	8d	05	0e		LEA
	de	27	08		
08208be2	89	44	24	0c	MOV
08208be6	c7	44	24		MOV
	10	17	00		

#### EAX, [DAT\_0827de0e]

dword ptr [ESP + local\_10],EAX=>DAT\_0827de0e
dword ptr [ESP + local\_c],0x17

#x86_	_64	
#LEA	REG,	[STRING_ADDRESS]
#MOV	[RSP	+], REG
#MOV	[RSP	+], STRING_SIZE

0049ac94	48	8d	05		LEA
	89	45	02	00	
0049ac9b	48	89	44		MOV
	24	10			
0049aca0	48	c7	44		MOV
	24	18	0e		
	00	00	00		

RAX, [DAT_0	)04bf224	4]		
qword ptr	[RSP +	local	48], RAX=>DAT	004bf224

qword ptr [RSP + local\_40],Oxe



🗶 🛃 🏛 🔹

• Results after executing the script

		-				
	main.main	XREF[4]:	Entry Point(*), runtime.main:0043 0049acce(c), 004c	4ac7(c), 5cb8(*)		
0049ac60 64 48 8b 0c 25 f8 ff ff ff	MOV	RCX, qword ptr FS: [0xffffffff8]				
0049ac69 48 3b 61	10 CMP	RSP. gword ptr [RCX + $0x10$ ]				
0049ac6d 76 5a	1BE	LAB 0049acc9				
0049ac6f 48 83 ec	58 SUB	BSP. 0x58				
0049ac73 48 89 60	MOV	gword ptr [BSP + local 8], BBP				
24 50		duora per (nor r cocac_offici				
0049ac78 48 8d 6c	I EA	BBP=>local 8 [BSP + 0x50]				
24 50						
0049ac7d 48 8b 05	MOV	BAX aword ntr [os Stdout]	= 22			
Oc bd Ob	00					
0049ac84 48 8d 0d	I FA	RCX [do itab *os File io Writer]				
95 26 04	00	(co.) [goritub: obirite; io:miter]				
0049ac8h 48 89 0c	24 MOV	gword ntr [RSP]=>local 58 RCX=>go itab *os	File i=			
0049ac8f 48 89 44	MOV	gword ptr [RSP + local 50] RAX	1 2 (0) 2 111 -			
24 08	1101	duora per (ros r cocac_oof)rost				
0049ac94 48 8d 05	LEA	BAX [s Hello World: 004bf224]	- "Hello W	orldi\n"		
89 45 02	00	1000, [5_10 (CO)_NOT (000401224)				
0049ac9h 48 89 44	MOV	aword ntr [RSP + local 48] RAX=>s Hello Wo	rldi e - "Hello W	orldi\n"		
24 10		diena per (ner i cocat_io)), en o_necco)_ne		or car (ii		
0049aca0 48 c7 44	MOV	gword ptr [RSP + local 40].0xe				
24 18 0e		diena per (ner i coost_ ref) ere				
00 00 00						
0049aca9 48 c7 44	MOV	gword ptr [RSP + local 38].0x0				
24 20 00		diene bei (im i teeni_ee); eue				
00 00 00						
0049ach2 0f 57 c0	XORPS	XMMO, XMMO				
0049ach5 0f 11 44	MOVUES	xmmword ptr [RSP + local 30[0]], XMM0				
24 28						
	s Hello Worl	ld1_004bf224	XREE[2]	main main 0049ac94(*)		
	o_notco,_nor	G1_00101221	ALC: [2] .	main main 0040ac04(*)	Filter: Hello	
				main.main:0049ac9b(*)		
004DT224 48 65 6C	ds	"Hello, World!\n"				

🔛 Defined Strings	- 1 items (of 7502)	🌮 🗏 🔁 🗴
Location	E String Value	String Representati Data Type
004bf224	Hello, World!	"Hello, World!\n" ds

6c 6f 2c 20 57 6f ...

#### Binary: world\_go



• After executing our script the number of defined strings grew from 9719 to 11213

main.checkReadmeExists >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>			XREF[2]:	08208c3b(c), main.init.0:08208cda(c)				
08208bb0 65 8b 0d	MOV	ECX, dword ptr GS: [0x0]						
08208bb7 8b 89 fc	MOV	<pre>ECX, dword ptr [ECX + 0xfffffffc]</pre>						
08208bbd 3b 61 08	CMP	ESP, dword ptr [ECX + 0x8]		ma	in.checkReadm	neExists	XREF[2]:	08208c3b(c), main.init.0:08208cda(c)
08208bc0 76 74 08208bc2 83 ec lc	JBE SUB	LAB_08208c36 ESP,0x1c		08208bb0 65 8b 0d	MOV	ECX,dword ptr GS:[0x0]		
08208bc5 c7 04 24	MOV	<pre>dword ptr [ESP]=&gt;local_lc,0x0</pre>		08208bb7 8b 89 fc	MOV	ECX, dword ptr [ECX + Oxfffffffc]	I	
08208bcc 8b 44 24 20	MOV	EAX, dword ptr [ESP + param_1]		08208bbd 3b 61 08	CMP	ESP, dword ptr [ECX + 0x8]		
08208bd4 8b 44 24 24	MOV	EAX, dword ptr [ESP + totat_18], EAX		08208bc0 76 74 08208bc2 83 ec lc	JBE SUB	LAB_08208c36 ESP.0x1c		
08208bd8 89 44 24 08 08208bdc 8d 05 0e	MOV LEA	dword ptr [ESP + local_14],EAX EAX,[DAT 0827de0e]		08208bc5 c7 04 24	MOV	dword ptr [ESP]=>local_lc,0x0		
de 27 08	MOV	dword ntr [ESP + local 10] EAX=>	DAT 0827de0e	08208bcc 8b 44 24 20	MOV	EAX.dword ptr [ESP + param_1]		
08208be6 c7 44 24	MOV	dword ptr [ESP + local_c],0x17	002/4000	08208bd0 89 44 24 04 08208bd4 8b 44 24 24	MOV MOV	dword ptr [ESP + local_18],EAX EAX,dword ptr [ESP + param_2]		
00 00				08208bd8 89 44 24 08	MOV	dword ptr [ESP + local_14], EAX	1827de0e1	
08208bee e8 dd cl e7 ff	CALL	runtime.concatstring2		de 27 08			.02/4000]	
				08208be2 89 44 24 0c 08208be6 c7 44 24	MOV	<pre>dword ptr [ESP + local_10],EAX=&gt; dword ptr [ESP + local_c],0x17</pre>	*S_/README_FO	R_DECRYPI.txt_082/de0e
				10 17 00 00 00				
				08208bee e8 dd cl e7 ff	CALL	runtime.concatstring2		



ARM – before executing the script





ARM – after executing the script





- Different instruction sets
- Can be implemented in different ways within the same architecture
- Easy to break intentionally
  From Go 1.17 new way of passing function arguments and results using registers instead of the stack

0028bbff	6c	??	6Ch	l
0028bc00	69	??	69h	i
0028bc01	6e	??	6Eh	n
0028bc02	75	??	75h	u
0028bc03	78	??	78h	х
0028bc04	5f	??	5Fh	
0028bc05	61	??	61h	а
0028bc06	72	??	72h	r
0028bc07	6d	??	6Dh	m

DAT 0028bbff

ddos.sshgo:00lfd7a4(\*), ddos.sshgo:00lfd7c0(\*), ddos.sshgo:00lfd7dc(\*)

001fd734	21	01	80	d2	
001fd738	el	4b	00	f9	
001fd73c	62	04	00	dO	
001fd740	42	fc	2f	91	
001fd744	e2	4f	00	f9	
001fd748	el	53	00	f9	

mov	param_2,#0x9
str	param_2,[sp, #local_c0]
adrp	param_3,0x28b000
add	param_3=>DAT_0028bbff,param_3,#0xbff
str	param_3=>DAT_0028bbff,[sp, #local_b8]
str	param_2,[sp, #local_b0]



Idea

- Look for pointer to string followed by possible length value
- To eliminate FPs limit string length and search for printable characters only
- Check only in data sections
- Not architecture specific





Example - before executing the script





Example - before executing the script



#### Strings are not defined

DAT 082785el ?? 2Eh ?? 64h d ?? 61h а ?? 74h t ?? 2Eh ?? 64h d ?? 62h b 22 30h 0 ?? 2Eh ?? 64h d 22 b 62h ?? 61h a ?? 2Eh 22 64h d ?? 62h b ?? f 66h ?? 2Eh ?? 64h d ?? b 62h 22 6Dh m

XREF[1]: 08436680(\*)



Example - after executing the script



Falsely defined data types by Ghidra

- undefined4 or undefined8 (depends on pointer size)
- Already defined data types cannot be redefined (undifined4 and undifined8 are defined data types)
- First the data type has to be removed
- Then the new data type can be defined

08431984	39	00	00	D. 00	AT 0843198 undefir	4 ied4	0000039h		
08431988	bb	c7	27	P 08	TR_DAT_084 addr	31988 D	AT_0827c7b	þ	
0843198c	13	00	00	D. 00	AT 0843198 undefir	c ied4	0000013h		
08431990	сс	aO	27	P' 08	TR_DAT_084 addr	31990 C	0AT_0827a0c	c	
08431994	0a	00	00	D. 00	AT_0843199 undefir	4 ied4 C	000000Ah		
							DAT_08	286f15	
					08286f15 6	8	2	2	68h
				(	08286f16 7	4	2	2	74h
3				(	08286f17 7	4	2	2	74h
				(	08286f18 7	0	?	2	70h
				(	08286f19 3	a	?	2	ЗAh
				(	08286fla 2	f	?	2	2Fh
				(	08286f1b 2	f	?	2	2Fh
				(	08286flc 7	3	?	2	73h
				(	08286fld 6	7	?	2	67h
				(	08286fle 3	3	?	2	33h
				(	08286flf 6	4	?	2	64h
				(	08286f20 7	7	?	2	77h

PTR DAT 08431980

DAT 08286f15

addr

08431980 15 6f 28 08

XREF[1]:	main.init.0:08208cf2(R)
XREF[1]:	main.getInfo:08208629(R)
XREF[1]:	main.getInfo:08208623(R)
XREF[1]:	net.readHosts:081448a0(R)
XREF[1]:	net.readHosts:08144896(R)

XREF[1]:

h

W

f getDataAt(length\_address) is not None: data\_type = getDataAt(length\_address).getDataType() #Remove undefined data to be able to create int. #Keep an eye on other predefined data types. if data\_type.getName() in ["undefined4", "undefined8"]: removeData(getDataAt(length\_address))

Binary: eCh0raix – x86



main.init.0:08208cec(R)

Falsely defined data types by Ghidra

- undefined4 or undefined8 (depends on pointer size)
- PTR s http://sq3dwqfpnr4sl5hh.onion/ap 08431980 XREF[1]: main.init.0:08208cec(R) Already defined data types cannot be • s http://sq3dwqfpnr4sl5hh.onion/ap 08286f15 08431980 15 6f 28 addr redefined INT 08431984 XREF[1]: main.init.0:08208cf2(R) 08431984 39 00 00 int (undifined4 and undifined8 are defined data PTR s 192.99.206.61:65000 08431988 XREF[1]: main.getInfo:08208629(R) types) s 192.99.206.61:65000 0827c7bb 084319 8 bb c7 27 08 addr First the data type has to be removed • main.getInfo:08208623(R) INT 0843198c XREF[1]: 843198c 13 00 00 00 int 13h Then the new data type can be defined PTR s /etc/hosts 08431990 XREF[1]: net.readHosts:081448a0(R) 08431990 cc a0 27 08 addr s /etc/hosts 0827a0cc XREF[1]: net.readHosts:08144896(R) TNT 08431994 08431994 0a 00 00 00 int s http://sg3dwqfpnr4sl5hh.onion/ap 08286f15 XREF[2]: main.init.0:08208cf8(\*), 08431980(\*)"http://sg3dwqfpnr4sl5hh.onion/api/GetAvailKeysByCampId/13" 08286f15 68 74 74 ds 70 3a 2f 2f 73 67 ...



Falsely defined data types by Ghidra

• A large string blob (containing multiple strings) defined as one string



#### Offcut references

s tls: received new session ticket 00297a6f

s\_tls:\_server\_chose\_an\_unconfigure\_00297a9d s\_tls:\_server\_did\_not\_echo\_the\_leg\_00297acb XREF[0, 274]...runtime.panicwrap:00017c14(\*), runtime.panicwrap:00017c98(\*), runtime.(\*mheap).sysAlloc:0001ab... runtime.(\*mcache).nextFree:0001a... runtime.mallocgc:0001b7c4(\*), runtime.sysMap:00025c04(\*), runtime.gcMark:00029fb8(\*), runtime.bgscavenge:0002e9dc(\*), runtime.(\*pageAlloc).sysGrow:000... runtime.newosproc:0003ca88(\*), runtime.startpanic m:0003fd64(\*), runtime.casgstatus:00043ef4(\*), runtime.doInit:0004eefc(\*), runtime.sigpanic:00055da4(\*), runtime.sigpanic:00055de4(\*), runtime.sigpanic:00055f24(\*), runtime.sigpanic:00055f64(\*), runtime.getStackMap:0005a7d4(\*), runtime.morestackc:0005a834(\*), runtime.resolveNameOff:00065blc(...



Falsely defined data types by Ghidra

• A large string blob (containing multiple strings) defined as one string

s_runtime:_panic_before_malloc_hea_002978ff runtim	🕅 Defined Strings - 1081	l items			🌮 🖹 🔁
s_runtime:_text_offset_base_pointe_0029792d runtim	Location	String Value	Data Type	Byte Count	Offcut Reference Count 🕒
s_runtime:_type_ottset_base_pointe_0029/95b runtim s_slice_bounds_out_of_range_[:%x] w_00297989 runtim	0022073d	certificateAuthorities	ds	23	1 🔺
s ssh: unmarshal error for field % 002979b7 runtim	00220ecl	ReplaceAllLiteralString	ds	24	1
s_sysGrow_bounds_not_aligned_to_pa_00297a13 runtim	00220ef5	responseMessageReceived	ds	24	1
s_tls:_failed_to_parse_certificate_00297a41 runtim	00220f29	verifyServerCertificate	ds	24	1
s_led_to_parse_certificate_from_se_00297a49 runtim	00221561	hashForClientCertificate	ds	25	1
s_tls:_received_new_session_ticket_00297a6f runtim	00221ele	asn1:"explicit,tag:1"	ds	22	1
s_tls:_server_chose_an_unconfigure_0029/a9d	00221e53	handlePostHandshakeMessage	ds	27	1
s_tis:_server_did_not_ecno_the_teg_00297acb	00222552	secureRenegotiationSupported	ds	30	1
s x509: failed to unmarshal ellipt 00297b27	00222ebd	asn1:"optional,tag:2"	ds	23	1
s x509: invalid elliptic curve pri 00297b55	00290069	ckunpa	ds	6	1
s_P_has_cached_GC_work_at_end_of_m_00297b83	002903f7	queuefinalizer during GC	ds	24	1
s_attempting_to_link_in_too_many_s_00297bb2	00330cff	runtime.dropg	ds	14	1
s_bufio:_reader_returned_negative_c_00297bel	00460248	END	ds	12	1
s_chacha20poly1305:_message_authen_00297c10	00460258	BEGIN	ds	16	1
s_curve25519:_global_Basepoint_val_0029/c3f	0029bb9c	0001020304050607080910111	ds	969	2
de "**	002e9100	expand 32-byte k	ds	20	3
us	002e91a0	expand 32-byte k	ds	20	3
	00293a08	3552713678800500929355621	ds	170	4
	0028b3b3	= is not mcount= minutes nallo	ds	225	23 )
	002976f3	*-+ *-+ ####@@@@!!!!first pat	ds	4517	95 🔻

002976f3 2a 2d 2b 2a 2d 2b 23 23 23 ...

#### Types

- Description for types is available within the binary
- Basic types: string, bool, numeric types (e.g. int8) etc.
- Composite types: pointer, struct, func, interface etc.
- <u>https://golang.org/src/reflect/type.go</u>

#### type miner.Process struct{

pid int name string path string cmdline string buf []uint8

type exploit.exploiter interface {
 check(\*exploit.Session) int
 init() []uint16
 run(\*exploit.Session) bool

#### func(string, string, \*tls.Config) (net.Conn, error)



const ( Invalid Kind = iota Bool Int Int8 Int<sub>16</sub> Int32 Int64 Uint Uint8 Uint16 Uint32 Uint64 Uintptr Float32 Float64 Complex64 Complex128 Array Chan Func Interface Map Pointer Slice String Struct UnsafePointer





### Example

- shell/miner.NewProcess function
- Call to runtime.newobject memory allocation

	006cab44	48 8b	4c	MOV	param_4,qword	ptr [RSP + loc	al_b0[8]]			
	006cab49	48 89 24 58	4c	MOV	qword ptr [ <mark>RS</mark> F	P + local_60],p	aram_4			
	006cab4e	48 8d 6b ce	15 Of 00	LEA	param_3, <mark>[DAT_0</mark>	007c79c0]			= 50h P	
	006cab55	48 89	14 24	MOV	qword ptr [RSF	p]=>local_b8,pa	ram_3=>DA	T_007c79c0	= 50h P	
	006cab59	e8 c2 d4 ff	54	CALL	runtime.newobj	ject			undefined runtime.ne	wobject(unde
	006cab5e	48 8b	44	MOV	RAX, gword ptr	[RSP + local b	0[0]]			
		24 08				DAT 007c79c	0		XREF[2]:	shell/miner.NewProcess:006cab4e(
	006cab63	48 8b	8c	MOV		_				shell/miner.NewProcess:006cab55(
		24 c0	00		007c79c0 50	??	50h	Р		
		00 00			007c79c1 00	??	00h			
					007c79c2 00	??	00h			
					007c79c3 00	??	00h			
					007c79c4 00	??	00h			
					007c79c5 00	??	00h			
					007c79c6 00	??	00h			? -> 00400000
					007c79c7 00	??	00h			
					007c79c8 40	??	40h	0		
					007c79c9 00	??	00h	-		
					007c79ca 00	??	00h			
					007c79cb 00	??	00h			
Bina	ry: sysrv				007c79cc 00	??	00h			

### rtype

// rtype	e is the com	mmon implementation of most values.			
// It is	embedded	LONG 007c79c0			
11			20110_00707000		
// rtype	must be ke	<pre>ept in sync with/runtime/type.go:/^typetype.</pre>	007c79c0 50 00 00	long	50h
type rty	pe struct	{	00 00 00		
	size	uintptr	00 00	long	10h
	ptrdata	uintptr // number of bytes in the type that can	00/07908 40 00 00	tong	4011
	hash	<pre>uint32 // hash of type; avoids computation in h</pre>	00 00		
	tflag	tflag // extra type information flags	007c79d0 4d 48 2e 23	3 int	232E484Dh
	align	<pre>uint8 // alignment of variable with this type</pre>	007c79d4 07	db	7h
	fieldAlian	<pre>uint8 // alignment of struct field with this t</pre>	007c79d5 08	db	8h eh
ſ	kind	uint8 // enumeration for C	007c79d7 19	db	1.9h
Ľ	// function	n for comparing objects of this type	007c79d8 00 5a f9	addr	DAT 00195a00
	// (ntr to	object A, ptr to object B) $\rightarrow ==?$	00 00 00		
	equal	func(unsafe Pointer unsafe Pointer) bool	00 00		
	acdata	*hyte // garbage collection data	007c79e0 4c 5a 84	addr	DAT_00845a4c
1	str i	<pre>page of the second second</pre>	00 00 00		
l	ntrToThic	$t_{vneOff}$ // type for pointer to this type may be	007c79e8 85 15 01 00	) int	11585h
ι	perionits	cypeoil // cype for poincer to this type, may be	007c79ec e0 29 05 00	) int	529E0h
1					



### rtype

// rtyp	e is the common implementation of most values.			
// It i	s embedded in other struct types.	L	ONG 007c79c0	
11				
// rtyp	e must be kept in sync with/runtime/type.go:/^typety	pe. 007c79c0 50 00 00	long 5	50h
type rt	<pre>ype struct {</pre>	00 00 00		
	size uintptr	00767968 40 00 00	long /	lOb
	ptrdata uintptr // number of bytes in the type that c	an 00 00 00	cong 4	ion i
	<pre>hash uint32 // hash of type; avoids computation i</pre>	n ł 00 00		
	tflag tflag // extra type information flags	007c79d0 4d 48 2e 23	int 2	232E484Dh
	align uint8 // alignment of variable with this ty	pe 007c79d4 07	db 7	7h
	fieldAlign uint8 // alignment of struct field with thi	S t 007c79d5 08	db s	sn sh
	kind uint8 // enumeration for C	007c79d7 19	db 1	.9h
	<pre>// function for comparing objects of this type</pre>	007c79d8 00 5a f9	addr D	AT_00195a00
	// (ptr to object A, ptr to object B) $\rightarrow ==?$	00 00 00		
	equal func(unsafe.Pointer, unsafe.Pointer) bool	00 00	odde - F	AT 0094554c
	<pre>gcdata *byte // garbage collection data</pre>	00 00 00	auui L	AT_00845840
	str nameOff // string form	00 00		
	ptrToThis typeOff // type for pointer to this type, may	be 007c79e8 85 15 01 00	int 1	.1585h
}	0073f585_01 ??	007c79ec e0 29 05 00 01h	int 5	529E0h
	0073f586 00 ??	00h		
	0073f587 0e ??	OEh		
	0073f588 2a 6d 69 ds	"*miner.Process"		
Binary: sysry	6e 65 72			
	2e 50 72			



Finding type descriptions

- Moduledata records information about the layout of the executable image
- type, etype memory location storing type information
- Typelinks stores offsets of type descriptions (from type)
- PE and ELF binary differences
  - ELF .typelink section, type = .rodata section
  - $\circ~$  PE parse moduled ata to find the necessary addresses
- Version differences
  - o Pclnatb header updates (from 1.2, changes in 1.16, 1.18)
  - o Moduldata structure update
    - (from 1.5, changes in 1.7, 1.8, 1.10, 1.16)
  - Type name struct update (1.18)

<pre>moduledata struct {    pcHeader *pcHeader    funcnametab []byte    cutab []uint32    filetab []byte    pctab []byte    pclntable []byte    ftab []functab    findfunctab uintptr    minpc, maxpc uintptr</pre>	
text, etext	uintptr
noptrdata, enoptrdata	uintptr
data, edata	uintptr
bss, ebss	uintptr
noptrbss, enoptrbss	uintptr
end, gcdata, gcbss	uintptr
types, etypes	uintptr
rodata	uintptr
gofunc	uintptr // go.func.*

type

textsectmap []textsect
typelinks []int32 // offsets from types
itablinks []\*itab



Туре е	extract	ion		C	type miner	.Process struct{	
Example – (	executing c	our scr	ipt		pa pa cm bu }	me string th string dline string f []uint8	
	DAT_007c79c0				miner.Proc	ess	
007c79c0         50           007c79c1         00           007c79c2         00           007c79c3         00           007c79c4         00           007c79c5         00           007c79c6         00           007c79c79c7         00           007c79c8         40           007c79c9         00           007c79c9         00	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??	50h 00h 00h 00h 00h 00h 00h 40h 00h	P	007c79c0 50 007c79c1 00 007c79c2 00 007c79c3 00 007c79c4 00 007c79c5 00 007c79c6 00 007c79c7 00 007c79c8 40 007c79c9 00 007c79c9 00	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??	50h P 00h 00h 00h 00h 00h 00h 00h 40h @ 00h 00h	
	006cab44 48 8b 24 10 006cab49 48 89 24 58 006cab54 48 80 6b ce 006cab55 48 89 006cab55 48 89 006cab56 48 8b 24 08 006cab56 48 8b 24 00 006cab63 48 8b	4c 4c 15 0f 00 14 24 254 44 8c 00	MOV MOV LEA MOV CALL MOV MOV	<pre>param_4,qword ptr [RSP + local_b0[8]] qword ptr [RSP + local_60],param_4 param_3,[miner.Process] qword ptr [RSP]=&gt;local_b8,param_3=&gt;miner. runtime.newobject RAX,qword ptr [RSP + local_b0[0]] param_4,qword ptr [RSP + param_7]</pre>	= 5 Process = 5 und	iOh P iOh P lefined runtime.new	object(unde

### Example II. – before script execution

l l	main.getInfo	XREF	2]: 08208ba2(c), main init 0:08208cff(c)						
082085b0 65 8b 0d	MOV	ECX.dword ptr GS:[0x0]							
00 00 00	00								
082085b7 8b 89 fc	MOV	ECX, dword ptr [ECX + 0xfffffffc]				_			
ff ff ff					DAT_0824bd20			XREF[2]:	main.getInfo:082085fc(*)
082085bd 8d 44 24	f4 LEA	EAX=>local_c,[ESP + -Oxc]							main.getInfo:08208602(*)
082085c1 3b 41 08	CMP	EAX, dword ptr [ECX + 0x8]		0824bd25 10	??	10h			
082085c4 Of 86 d3	JBE	LAB_08208b9d		082+0d21 00	??	OOh			
05 00 00				0824bd22 00	??	00h			
082085ca <mark>81 ec 8</mark> c	SUB	ESP, 0x8c		0824bd23 00	22	00h			
00 00 00				0824bd24 0c	22	OCh			
082085d0 c7 84 24	MOV	dword ptr [ESP + param_3],0x0		0924bd25 00	22	ooh			
98 00 00				0824bd25 00	22	ooh			
00 00 00				08240026 00	11	001			
082085db c7 84 24	MOV	dword ptr [ESP + param_4],0x0		08240027 00	rr og	000			
9c 00 00				0824bd28 15	<i></i>	15n			
00 00 00		the second distance attacks		0824bd29 e7	??	E7h			
082085e6 c7 84 24	MOV	dword ptr [ESP + param_5],0x0		0824bd2a c0	??	COh			
a0 00 00				0824bd2b 27	??	27h			
00 00 00				0824bd2c 07	??	07h			
082085†1 c7 84 24	MOV	dword ptr [ESP + param_6],0x0		0824bd2d 04	??	04h			
a4 00 00				0824bd2e 04	??	04h			
00 00 00			2.01	0824bd2f 19	??	19h			
082085TC 80 05 20	LEA	EAX, [DA1_0824bd20]	= 10h	0824bd30 28	??	28h	(		? -> 0820c828
bd 24 08	101	a dead at a [Sop] a local on Strandit on	a thulan a shi	0824bd31 c8	??	C8h			
08208602 89 04 24	MOV	dword ptr [ESP]=>local_8c,EAX=>DAI_08	24bd20 = 10h	0824bd32 20	??	20h			
08208605 68 66 97	CALL	runtime.newobject	underined runtime.newobject(	0824bd33_08	22	08h			
64 11 0000050a 0b 44 04	OA MOV	FAV drand ata [FCD + local 00]		0824bd34 fc	22	ECh			2 -> 082ba0fc
	40 MOV	dword ptr [ESP + local_oo]		0824bd35 a0	22	AOh			1 00204010
0020000e 89 44 24	40 100	ECX [s top 09279422]	- "ten"	00240035 00		AUII			
00200012 80 00 23 84 27 09	LEA	Ecx, [5_(cp_08278423)	= tep						
08208618 89 0c 24	MOV	dword ntr [ESP]=>local 8c ECX=>s ton	08278423 - "ten"						
0820861b c7 44 24	MOV	dword ptr [ESP + local 88] 0x3	- top						
04 03 00									
00 00									
08208623 8b 0d 8c	MOV	ECX.dword ptr [INT 0843198c]	= 1.3h						
19 43 08									
08208629 8b 15 88	MOV	EDX, dword ptr [PTR s 192,99,206,61:65	000 08431988] = 0827c7bb						
19 43 08			_						
0820862f 89 54 24	08 MOV	dword ptr [ESP + local_84], EDX=>s 192	.99.206.61:6 = "192.99.206.61:65000"						
08208633 89 4c 24	OC MOV	dword ptr [ESP + local 80], ECX							
08208637 c7 44 24	MOV	dword ptr [ESP + local_7c],0x0							
10 00 00									
00 00									

Binary: eCh0raix - x86



### Example II. – after script execution

(	main.getInfo	XRE	[2]: 08208ba2(c), main_init_0:08208cff(c)						
082085b0 65 8b 0d	MOV	ECX, dword ptr GS: [0x0]							
00 00 00	00								
08208507 80 89 TC	MOV	ECX, aword ptr [ECX + 0xtttttttc]			type main.In	fo struct{			
082085bd 8d 44 24	f4 LEA	EAX=>local c.[ESP + -0xc]			RsaP	ublicKey st	tring		
082085c1 3b 41 08	CMP	EAX. dword ptr [ECX + 0x8]		_	Read	me string			
082085c4 Of 86 d3	JBE	LAB 08208b9d			}				
05 00 00		-			main.Info			XREF[2]:	main.getInfo:082085fc(*)
082085ca <mark>81 ec 8</mark> c	SUB	ESP, 0x8c			$\frown$				main.getInfo:08208602(*)
00 00 00				bd20 10	??	10h			
082085d0 c7 84 24	MOV	dword ptr [ESP + param_3],0x0		bd21 00	??	00h			
98 00 00				bd22 00	??	00h			
00 00 00				bd23 00	??	00h			
082085db c7 84 24	MOV	dword ptr [ESP + param_4],0x0		bd24 Oc	??	OCh			
90 00 00				bd25 00	??	00h			
00 00 00	MOV	dword ptr [ESP + param 5] 0x0		bd26 00	??	00h			
20 00 00	HOV	dword per [ESF + param_5],0x0		bd27 00	??	ooh			
00 00 00				bd28 15	??	15h			
082085f1 c7 84 24	MOV	dword ptr [ESP + param 6],0x0		bd29 e7	??	E7h			
a4 00 00				bd2a c0	??	COh			
00 00 00				bd2b 27	??	27h	C		
082085fc 8d 05 20	LEA	EAX [main.Info]	= 10h	bd2c 07	??	07h			
bd 24 08				bd2d 04	??	04h			
08208602 89 04 24	MOV	dword ptr [ESP]=>local_8c,EAX=>main.	Info = 10h	bd2e 04	??	04h			
08208605 e8 66 97	CALL	runtime.newobject	undefined runtime.newob	ject(unde bd2f 19	??	19h			
e4 TT		Sty durad ata (SOD - local col		bd30 28	??	28h	(		? -> 0820c828
08208603 80 44 24	04 MOV	dword ptr [ESP + local_88]		bd31 c8	??	C8h			
0820800e 89 44 24	40 100	ECY [s top 09279422]	- "tcn"	bd32 20	??	20h			
84 27 08	LLA	Ecx, [3_(cp_002/0423)	= tcp	bd33 08	??	08h			
08208618 89 0c 24	MOV	dword ptr [ESP]=>local 8c.ECX=>s tcp	08278423 = "tcn"	bd34 fc	??	FCh			? -> 082ba0fc
0820861b c7 44 24	MOV	dword ptr [ESP + local 88],0x3		bd35 a0	??	AOh			
04 03 00		=							
00 00									
08208623 8b 0d 8c	MOV	ECX, dword ptr [INT_0843198c]	= 13h						
19 43 08									
08208629 8b 15 88	MOV	EDX, dword ptr [PTR_s_192.99.206.61:6	5000_08431988] = 0827c7bb		type	main	Info st	ruct{	
19 43 08	00 101	durad sta (FCD - level oil FCV - 10			cype	noren	into se	ucci l	
08208621 89 54 24	US MOV	dword ptr [ESP + local_84], EDX=>S_19	2.99.200.01:0 = "192.99.206.61:65000"			Rsi	aPublic	Kev strina	
00200033 89 40 24	MOV	dword ptr [ESP + local_80],ECX						· · · · · · · · · · · · · · · · · · ·	
10 00 00	HOV	uworu pri [ESF + tocat_/c],0x0				Rea	adme st	ring	
00 00								and the second	

Binary: eCh0raix - x86





### Challenges Problems to solve

- Continuous version changes
- Go version identification
  - o Currently string based

#### strings sys.x86\_64\_unp | grep "go1\."

stack=[ ABSTIME ACLITEM CSTRING MACADDR NUMERIC POLYGON REGOPER REGPROC REGROLE REG TYPE RELTIME TSQUERY TSRANGE VARCHAR wpnonceallllllllal234567alb2c3d4als2d3f4a@123456aAl2345 6aB123456ab123456abc#1234abc123!@abc@1234abc@123@abcd1234abcd@123abcdefghaddress admin123ad min520adminsunalefsym;angelicaangrtvb;angzarr;asdf1234asdfasdfasdfghjkasympeg;b42207 lbacks im;bad instbeEfFgGvbecause;bemptyv;between;bigcirc;bigodot;bigstar;bnequiv;boxplus;ccupssm; cemptyv;cgocheckcirscir;cisco123coloneg;congdot;continuecudarrl;cudarrr;cularrp;curarrm;dat abasedbkarow;ddagger;ddotseg;default:demptyv;diamond;digamma;disableddotplus;dump.rdbdwangl e;echo -n epsilon;egcolon;eguivDD;fc00::/7filenameflushallftpadminfunctiongesdoto go1,10.7c tquest;gtrless;harrcir;hijackedhost keyhttp/1.1if-matchif-rangeinfinityintprod;invalid io e rrorisindot; it123456larrbfs; larrsim; lbrksld; lbrkslu; ldrdhar; lesdoto; lessdot; lessgtr; lesssim ;locationloopbacklotimes;lozenge;ltguest;luruhar;maltese;minusdu;mysgl123napprox;natural;ne arrow;nexists;nistp256nistp384nistp521no anodeno-cacheno proxynotinva;notinvb;notinvc;notni va;notnivb;notnivc;npolint;npreceq;nsqsube;nsqsupe;nsubset;nsucceq;nsupset;nvinfin;nvltrie; nvrtrie;nwarrow;olcross;omicron;orderof;orslope;os:Linuxp@55w0rdp@ssw0rdp@sswordpa55wordpas s1234passw0rdpassw0rdpasswordpertenk;planckh;pluscir;plussim;plustwo;postgresprecsim;glw2e3 r4qQ123456qq111111qq112233qq123123qq123456quatint;questeq;qwe123!@qwe123..qwer1234qwerasdfq wergwerrarrbfs;rarrsim;rbrksld;rbrkslu;rdldhar;readfromreadlinkrealine;recvfromredis - redi s123responseroot.123root123!root1234root@123rootrootrotimes;ruluhar;runnableruntime.scaveng esearrow;sendfileshutdownsignal: simplus;simrarr;socket:[strconv.subedot;submult:subplus:su brarr;succsim;supdsub;supedot;suphsol;suphsub;suplarr;supmult;supplus;swarrow;testusertext/ xmltimeout:timezonetopfork;triplus;tritime;unixgramunknown(uparrow;upsilon;uwangle;vzigzag; weblogicxx123456xxxx1234zaq1@WSXzigrarr;zxcv1234 (forced) (normal) -> node= blocked= defers c= in use)

ao1.18.1

**qol.**18.1

strings go mal v118 elf | grep "go1\."

/usr/lib/go-1.18/src/vendor/golang.org/x/crypto/internal/poly1305/bits gol.13.go

## Other researcher's work



Links

#### **IDA Pro**

- https://github.com/sibears/IDAGolangHelper
- https://github.com/strazzere/golang\_loader\_assist
- https://github.com/sentinelabs/alphagolang

#### radare2 / Cutter

- https://github.com/f0rki/r2-go-helpers
- https://github.com/JacobPimental/r2-gohelper/blob/master/golang\_helper.py
- https://github.com/CarveSystems/gostringsr2

#### **Binary Ninja**

https://github.com/f0rki/bn-goloader

#### Ghidra

- https://github.com/felberj/gotools
- <u>https://github.com/ghidraninja/ghidra\_scripts/blob/master/golang\_renamer.py</u>

#### Other

https://go-re.tk/

## Files used during the presentation



Hashes

File name	SHA-256
world.c	761301bb14ea3b678650fc1b6da768f009387ee726712e291d57e2d7985613d0
world.go	7cb3316a7b89eb996e8dbb0d0fb277136cd588cc54642f3b09aa84cd177cb3a2
world_c	76a5c4ef9277b97660f2c412e67ff2c3826e699913db86cd333e8f1d4fb5b8a3
world_c_strip	486a93362a6a8bc3b449fd6ba07656011c687ed31a19091c329a434bff4d75bb
world_go	d0d4781de4ffd5fbe18d59328eccd373a782eecdf55a2c5199b7dc6598cfb99e
world_go_strip	9b975bd9406a8b79a414195e184be0c82bb1593979577f0344c797f9bcd4ad0b
world_go.exe	9e36291f5fc67fdb9e5e17b636d34b39f2cc39f328916a9012a8f8d545e9d0c8
world_go_strip.exe	c5b66623942a0cea6df30541e92afe93172be7bb4dbdd42a1fa354e9edd79a1d
world_go_println	fa00f5ad2aa79a6245a28516bc285ae8c36f075d818787aadff6f3e850e2ec5c
eCh0raix - x86	154dea7cace3d58c0ceccb5a3b8d7e0347674a0e76daffa9fa53578c036d9357
eCh0raix - ARM	3d7ebe73319a3435293838296fbb86c2e920fd0ccc9169285cc2c4d7fa3f120d
Kaiji - x86_64	f4a64ab3ffc0b4a94fd07a55565f24915b7a1aaec58454df5e47d8f8a2eec22a
Kaiji - ARM	3e68118ad46b9eb64063b259fca5f6682c5c2cb18fd9a4e7d97969226b2e6fb4
sysrv	c543f137a9e9380203ab12b29662b10810afe7e10c2af24b3b0cf0c3669193a1

### References, additional reading



Other Go malware research

- <u>https://rednaga.io/2016/09/21/reversing\_go\_binaries\_like\_a\_pro/</u>
- https://2016.zeronights.ru/wp-content/uploads/2016/12/GO\_Zaytsev.pdf
- <u>https://carvesystems.com/news/reverse-engineering-go-binaries-using-radare-2-and-python/</u>
- https://www.pnfsoftware.com/blog/analyzing-golang-executables/
- https://github.com/strazzere/golang\_loader\_assist/blob/master/Bsides-GO-Forth-And-Reverse.pdf
- https://github.com/radareorg/r2con2020/blob/master/day2/r2\_Gophers-AnalysisOfGoBinariesWithRadare2.pdf
- <u>https://securelist.com/extracting-type-information-from-go-binaries/104715/</u>





Dorka Palotay Senior Threat Researcher, CUJO AI @pad0rka

https://github.com/getCUJO/ThreatIntel @CujoaiLabs

FIRST June 2022