

Korištenje alata Volatility za forenzičku analizu radne memorije računala

NCERT-PUBDOC-2018-4-358





Sadržaj

1	UVO	D	3
2	SCEN	IARIJ NAPADA	4
3	ANA	LIZA SLIKE RADNE MEMORIJE	6
	3.1	POPIS PROCESA	6
	3.2	ARGUMENTI NAREDBENE LINIJE	8
	3.3	RUČKE (ENG. HANDLES) PROCESA	9
	3.4	REKONSTRUKCIJA IZVRŠNE (.EXE) DATOTEKE	.1
	3.5	MREŽNE VEZE 1	.3
	3.5.1	Obrnuti DNS (eng. reverse DNS) 1	4
	3.5.2	WHOIS servis	5
	3.5.3	Ostale baze informacija o IP adresama1	6
	3.6	WINDOWS REGISTAR (ENG. REGISTRY)	.7
	3.7	DATOTEČNI SUSTAV	.8
4	ZAKI	LJUČAK 1	9
5	LITE	RATURA2	:0

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

Forenzika radne memorije područje je računalne forenzike koje se bavi prikupljanjem i analizom tragova iz radne memorije računala. Radna memorija računala značajna je za forenziku jer sadržava neke tragove koje nije moguće pronaći drugim forenzičkim metodama, primjerice forenzikom diska ili forenzikom mreže.

Jedna posebno zanimljiva primjena forenzike radne memorije je analiza napada na računalne sustave zlonamjernim softverom (eng. *malware*) jer su u tom slučaju tragovi često namjerno prikrivani. Primjerice, napredni zlonamjerni softver često ne zapisuje nikakve podatke na disk te šifrira sve podatke koje šalje mrežom zbog čega su uobičajene forenzičke metode neefikasne.

Forenzikom radne memorije neke od tih tehnika mogu se lakše zaobići te zbog toga ona predstavlja važan doprinos ostalim mehanizmima koje se koriste u analizi zlonamjernog softvera. Iz tog je razloga forenzika memorije grana računalne forenzike koja se zadnjih godina ubrzano razvija te se kontinuirano stvaraju nove tehnike korištene u analizi radne memorije.

Najpopularniji slobodni (eng. *free and open source*) alat za forenziku radne memorije je Volatility. Upute za instalaciju i osnovno korištenje alata Volatility opisane su u prethodnom dokumentu Nacionalnog CERT-a: <u>"Volatility"</u>. Ovaj dokument proširit će ta znanja te objasniti kako ih primijeniti na stvarnom primjeru forenzičke analize radne memorije računala zahvaćenog zlonamjernim softverom.



2 Scenarij napada

U ovom dokumentu, forenzička analiza radne memorije računala bit će objašnjena kroz primjer. Bit će analizirana slika radne memorije računala zahvaćenog zlonamjernim softverom.

U primjeru je žrtva (korisnik računala) primila poruku elektroničke pošte s datotekom *invoice.doc.exe* u privitku. To je izvršna datoteka koja sadržava zlonamjerni program, a nastavkom *.doc.exe* pokušava zavarati žrtvu i uvjeriti ju da datoteka zapravo sadržava običan dokument. Žrtva je datoteku preuzela na radnu površinu, kao što je prikazano na slici 1.



Slika 1 - Slika radne površine računala prije pokretanja zlonamjernog programa

Zatim, žrtva je, uvjerena da otvara bezopasan dokument, dvostrukim klikom na preuzetu datoteku pokrenula zlonamjerni program. Nakon nekoliko trenutaka, pojavila se poruka koja tvrdi da su datoteke na računalu šifrirane. U poruci se nalazi i zahtjev za otkupninom (eng. *ransom note*), iz čega se može zaključiti kako je računalo zaraženo zlonamjernim programom vrste *ransomware. Ransomware* je vrsta zlonamjernih programa koji šifriraju datoteke ili na neki drugi način onemogućuju rad na računalu te zatim od korisnika traže otkupninu kako bi vratili računalo u upotrebljivo stanje. Slika 2 prikazuje sliku radne površine nakon pokretanja zlonamjernog programa.



6					
Recyce b	E! CryptoLocker-v3			1	
1		Your personal files are	encrypted!		
Crypto.od	Your private key will be destroyed on: 2/22/2018 Show encrypted files Copy a 18xx1 Follow	Your files have been safely encrypted on this PC: phc lick "Show encrypted files" Button to view a complet and you can personally verify this. Encryption was produced using a unique public key R for this computer. To decrypt files you need to obtain the only copy of the private key, which will allow you is located on a secret server in the internet; the serv after a time period specified in this window. Once this Abs been done, mobody will ever be a noder to decrypt the files open your person https://drikholacga/hi/gi,tor2web.org is not open it 18x0/Scm6AcBHmxpKY2D/fpyAFe Click to copy Bitcoin address to a fi https://dricholacga/hi/gi,tor2web.org is not open if https://dricholacga/hi/gi,tor2web.org is none chances are left to recover the files. Any attempt to remove or corrupt this so immediate elimination of the private key Science Academic	Alto, videos, documents, etc. te list of encrypted files, SA-2048 generated the private key. is decrypt your files, et will eliminate the key ble to restore files al page on site oblow the instruction. ar the site: parw344 slipboard ing, please follow the steps: ojects/horbrowser.html.en S4r60q26q2h4jiczj.onion u that the sooner you do, ftware will result ey by the server. Enter Decrypt Key Madaress In the In w344	t files have been encrypted or this computer. rver and nobody can (ey. ons on the locker. the locker program. 4r6hq26q2h4jkzj.onion.cab ver. : zj.onion/	
A Start					* 😼 🖗 🖗 🌜 6:20 AM 💻

Slika 2 - Slika radne površine računala nakon pokretanja zlonamjernog programa

Konkretno u ovom slučaju, zlonamjerni program pokrenut je unutar virtualnog stroja kako bi se ograničila potencijalna šteta. Kada se pojavila poruka sa zahtjevom za otkupninu, forenzičar je zaustavio izvršavanje virtualnog stroja i njegova memorija je snimljena u datoteku pod nazivom *infected_teslacrypt.elf*. Na taj način pribavljena je slika memorije računala te analiza može započeti.



3 Analiza slike radne memorije

Tehnike analize memorije u ovom dokumentu oslanjaju se na osnovna predznanja korištenja alata Volatility opisana u <u>prethodnom dokumentu Nacionalnog CERT-a</u> (instalacija, pozivanje naredbi, razumijevanje argumenata *-f* odnosno *--file* i *--profile*). Također, kako su izlazni podaci alata Volatility u pravilu u tekstualnom obliku, za analizu rezultata očekuju se osnovne vještine baratanja tekstom u naredbenoj liniji, primjerice filtriranje linija teksta po ključnoj riječi. Jedan od poznatijih takvih alata je *grep*, koji se koristi na Unix operacijskim sustavima, a u ovom dokumentu se koristi *findstr*, koji je dostupan na operacijskim sustavima Windows.

Primjeri korištenja alata Volatility u ovom dokumentu napravljeni su na operacijskom sustavu Windows, iz njegovog naredbenog retka (eng. *Command Line*), no u načelu je korištenje alata Volatility jednako i na drugim operacijskim sustavima. Neke naredbe zauzimaju dva reda u ovom dokumentu zbog svoje duljine, no sve naredbe potrebno je napisati u **jednom retku** u naredbenom retku operacijskog sustava.

U narednim primjerima sve naredbe izvršene su iz direktorija *C:\volatility* u kojem se nalazila izvršna datoteka alata Volatility te datoteka sa slikom memorije naziva *infected_teslacrypt.elf.*

3.1 Popis procesa

Jedna od prvih stvari koje forenzičar u ovakvoj situaciji želi saznati o stanju sustava je popis pokrenutih procesa. U prethodnom dokumentu o alatu Volatility opisana je naredba *pslist*. Naredba *pstree* na jednak način pronalazi procese koji su bili pokrenuti na sustavu, no za razliku od naredbe *pslist*, u ispisu i vizualno prikazuje hijerarhiju procesa. Kada jedan proces stvori drugi proces, proces koji je pokrenut naziva se "proces dijete" (eng. *child process*) dok se proces koji ga je pokrenuo naziva "proces roditelj" (eng. *parent process*). U ispisu naredbe *pstree* jasno se može vidjeti koji proces je roditelj, a koji dijete, tj. može se primijetiti koje sve procese je pokrenuo neki proces. Ovakva informacija o vezama između procesa može biti izrazito korisna u analizi.

Kao i u ostalim pokretanjima alata Volatility, potrebno je alatu proslijediti ime datoteke u kojoj se nalazi slika memorije te inačicu operacijskog sustava na kojem je snimljena slika memorije. Parametrom **-f** postavlja se ime datoteke slike memorije (*infected_teslacrypt.elf*), a parametrom **--profile** ime sustava na kojem je slika nastala (*Win7SP1x86*, što označava 32-bitnu verziju Windows 7 Service Pack 1 sustava).

volatility -f infected_teslacrypt.elf --profile=Win7SP1x86 pstree



Command Prompt							_	×
0x83d3ac60:System	4	0	81	554	2018-02-19	23:12:05	UTC+0000	~
. 0x843cc020:smss.exe	216	4	2	29	2018-02-19	23:12:05	UTC+0000	
0x83d9e218:wininit.exe	320	276		77	2018-02-19	23:12:06	UTC+0000	
. 0x84aab180:services.exe	416	320	8	223	2018-02-19	23:12:06	UTC+0000	
0x84dea030:svchost.exe	1708	416	6	92	2018-02-19	14:12:12	UTC+0000	
0x84c1c030:spoolsv.exe	1292	416	17	293	2018-02-19	14:12:10	UTC+0000	
0x84c7c5b0:svchost.exe	1552	416	13	220	2018-02-19	14:12:10	UTC+0000	
0x84108a20:CompatTelRunne	532	416	4	57	2018-02-19	14:15:11	UTC+0000	
0x840f72b0:CompatTelRunne	3856	532	17	542	2018-02-19	14:20:12	UTC+0000	
0x84b2a920:svchost.exe	664	416	8	277	2018-02-19	14:12:09	UTC+0000	
0x84e35950:SearchIndexer.	2308	416	13	678	2018-02-19	14:12:16	UTC+0000	
0x8424a3e0:SearchProtocol	1244	2308	8	284	2018-02-19	14:20:45	UTC+0000	
0x84382030:SearchFilterHo	2612	2308	5	106	2018-02-19	14:20:45	UTC+0000	
0x84b60030:svchost.exe	796	416	17	395	2018-02-19	14:12:09	UTC+0000	
0x84c09030:dwm.exe	1260	796		69	2018-02-19	14:12:10	UTC+0000	
0x84b14b38:svchost.exe	540	416	12	365	2018-02-19	23:12:07	UTC+0000	
0x83de2470:WmiPrvSE.exe	3012	540	7	124	2018-02-19	14:13:14	UTC+0000	
0x84d59030:WmiPrvSE.exe	788	540	11	296	2018-02-19	14:20:16	UTC+0000	
0x84c25b00:svchost.exe	1324	416	18	326	2018-02-19	14:12:10	UTC+0000	
0x84bbd670:svchost.exe	1076	416	16	487	2018-02-19	14:12:09	UTC+0000	
0x84de3410:svchost.exe	3384	416	13	381	2018-02-19	14:14:12	UTC+0000	
0x84b6e7c0:svchost.exe	820	416	17	340	2018-02-19	14:12:09	UTC+0000	
0x83dcc030:cygrunsrv.exe	1752	416	7	102	2018-02-19	14:12:10	UTC+0000	
0x84d8ca98:cygrunsrv.exe	1908	1752	0		2018-02-19	14:12:11	UTC+0000	
0x84d9f030:sshd.exe	1972	1908	4	100	2018-02-19	14:12:11	UTC+0000	
0x84c33030:taskhost.exe	1376	416	10	235	2018-02-19	14:12:10	UTC+0000	
0x83fa29b0:svchost.exe	2436	416	8	96	2018-02-19	14:20:41	UTC+0000	
0x843d9540:svchost.exe	3532	416	5	88	2018-02-19	14:15:56	UTC+0000	
0x84b1e030:VBoxService.ex	600	416	12	116	2018-02-19	23:12:07	UTC+0000	
0x84d85228:wlms.exe	1892	416	5	46	2018-02-19	14:12:11	UTC+0000	
0x84de6030:sppsvc.exe	1116	416	7	150	2018-02-19	14:12:12	UTC+0000	
0x84b77548:svchost.exe	864	416	36	1409	2018-02-19	14:12:09	UTC+0000	
0x84c745d8:svchost.exe	1512	416	13	340	2018-02-19	14:12:10	UTC+0000	
0x84b56778:svchost.exe	752	416	20	446	2018-02-19	14:12:09	UTC+0000	
0x84b8d2a8:svchost.exe	936	416	6	121	2018-02-19	14:12:09	UTC+0000	
0x840b0b48:TrustedInstall	2808	416	7	242	2018-02-19	14:15:00	UTC+0000	
0x840edd28:VSSVC.exe	1564	416	6	124	2018-02-19	14:20:33	UTC+0000	
. 0x84ab04e0:lsass.exe	424	320	7	642	2018-02-19	23:12:06	UTC+0000	
. 0x84ab2320:1sm.exe	432	320	10	149	2018-02-19	23:12:06	UTC+0000	
0x84554030:csrss.exe	284	276	9	506	2018-02-19	23:12:06	UTC+0000	
. 0x84d9c030:conhost.exe	1948	284	2	33	2018-02-19	14:12:11	UTC+0000	
. 0x840e8bc0:conhost.exe	840	284	2	33	2018-02-19	14:15:11	UTC+0000	
0x84062820:ngwksdp.exe	3224	2916	10	401	2018-02-19	14:20:32	UTC+0000	
. 0x83f8ba40:vssadmin.exe	3572	3224	5	66	2018-02-19	14:20:32	UTC+0000	
0x83da8518:csrss.exe	328	312	7	209	2018-02-19	23:12:06	UTC+0000	
. 0x84055d28:conhost.exe	4016	328	2	31	2018-02-19	14:20:32	UTC+0000	
0x8456c030:winlogon.exe	356	312	3	110	2018-02-19	23:12:06	UTC+0000	
0x84c2d500:explorer.exe	1364	1252	32	925	2018-02-19	14:12:10	UTC+0000	
. 0x84ce3c00:VBoxTray.exe	1696	1364	12	141	2018-02-19	14:12:10	UTC+0000	

Slika 3 - Popis procesa dobiven pokretanjem naredbe pstree

Na popisu je moguće primijetiti veći broj procesa, no proces *ngwksdp.exe* izgleda neobično zbog svojeg imena koje izgleda kao da je nasumično generirano. Proces *ngwksdp.exe* ima jedan potproces, tj. proces dijete, imena *vssadmin.exe*. Kratkim istraživanjem moguće je otkriti da je to alat za administraciju Windows mehanizma za stvaranje sigurnosnih kopija (eng. *backup*) datoteka naziva *Volume Snapshot Service* ili *Volume Shadow Copy Service*. Zbog ovakve kombinacije neobičnog imena procesa i korištenja alata za administraciju sigurnosnih kopija, procesi *ngwksdp.exe* i *vssadmin.exe* će biti detaljnije analizirani.

Svaki proces ima svoj jedinstveni identifikator – PID (od eng. *process id*) pomoću kojeg se može jedinstveno identificirati taj proces iz liste pokrenutih procesa na računalu. Identifikatori procesa *ngwksdp.exe* i *vssadmin.exe* su 3224 i 3527, što je korisno zabilježiti za sljedeće naredbe čiji je rad moguće ograničiti na određene procese kako bi se smanjila količina ispisanih rezultata i ubrzao rad alata Volatility.



3.2 Argumenti naredbene linije

Kako bi znali što je učinjeno pomoću alata *vssadmin.exe*, potrebno je saznati s kojim argumentima naredbene linije je program pozvan, a upravo to je moguće saznati naredbom **cmdline**. Argumentom **--pid=3224,3527** moguće je ograničiti njen rad samo na prethodno navedene procese koje želimo detaljnije istražiti, kako bi se smanjila količina ispisanih podataka. Potpuna naredba izgleda ovako:

volatility -f infected_teslacrypt.elf --profile=Win7SP1x86 cmdline
--pid=3224,3572

Command Prompt	—	×
C:\volatility>volatility -f infected_teslacrypt.elfprofile=Win7SP1x86 cmdlinepid=3224,3572 Volatility Foundation Volatility Framework 2.6 ************************************		Â
ngwksdp.exe pid: 3224 Command line : C:\Users\IEUser\AppData\Roaming\ngwksdp.exe ***********************************		
vssadmin.exe pid: 3572 Command line : vssadmin delete shadows /all		~

Slika 4 – Informacije o argumentima naredbene linije procesa dobivene pokretanjem naredbe *cmdline*

U ispisu naredbe moguće je vidjeti da je puni poziv alata *vssadmin* bio:

```
vssadmin delete shadows /all
```

Kratkim istraživanjem moguće je saznati da se takvim pozivom brišu sigurnosne kopije datoteka stvorene *Volume Shadow Copy* sustavom. Istražiteljima koji su se prethodno susretali s *ransomwareom* će već ovo biti izrazito sumnjivo – ovo je uobičajena tehnika *ransomwarea* za brisanje sigurnosnih kopija kako se ne bi lako mogle povratiti šifrirane datoteke.

Također, u alatu Volatility postoji i naredba **consoles**, kojom se mogu vidjeti upisane naredbe i njihov ispis, kao i neki dodatni detalji o pokrenutom naredbenom retku. U ovom slučaju pomoću naredbe *consoles* se ne dolazi do novih tragova, no pri kraju ispisa naredbe može se potvrditi kako su zaista alatom *vssadmin* brisane sigurnosne kopije.

volatility -f infected_teslacrypt.elf --profile=Win7SP1x86 consoles



Command Prompt



Slika 5 - Ispis sadržaja naredbenog retka dobiven poretanjem naredbe consoles

3.3 Ručke (eng. handles) procesa

Ručke (eng. handles) su apstrakcija operacijskog sustava Windows – to su identifikatori pomoću kojih proces pristupa objektima operacijskog sustava. Primjeri takvih objekata su datoteke, ključevi registra i sinkronizacijski mehanizmi. Tablice ručki procesa su zapisane u memoriji računala te ih se može pročitati Volatility naredbom handles. Proučavanjem objekata operacijskog sustava koje proces koristi obično se može dobiti šira slika njegova rada.

Sada kada je poznato što je radio proces *vssadmin.exe*, potrebno je detaljnije istražiti proces ngwksdp.exe. Pokretanjem sljedeće naredbe dobiva se popis ručki procesa ngwksdp.exe (s identifikatorom 3224):

```
volatility -f infected teslacrypt.elf --profile=Win7SP1x86 handles
--pid=3224
```

Kako proces tipično koristi velik broj ručki, ovakav ispis naredbe je velik, te je korisnije ciljano gledati objekte po vrsti. To je moguće ostvariti kroz prosljeđivanje ispisa alata Volatility alatu za filtriranje teksta. Na Unix sustavima i sustavima izvedenim iz Unixa, u tu svrhu se najčešće koristi alat *grep*, dok se u ovom dokumentu koristi alat *findstr*, koji je dostupan iz naredbenog retka sustava Windows.

Kako bi ispisali samo ručke koje služe za datoteke moguće je koristiti sljedeću naredbu:

```
volatility -f infected teslacrypt.elf --profile=Win7SP1x86 handles
--pid=3224 | findstr File
```



💽 Comman	d Prompt				- 🗆 X
C:\volatili	ity>volat	ility -f in	nfected_tes	lacrypt.e	lfprofile=Win7SP1x86 handlespid=3224 findstr File
volatility	Foundatio	on volatili	ity Framewo	rK 2.6	
0x83Taa040	3224	8X0	0x100020	File	\Device\Harddiskvolumei\Users\lEUser\Desktop
0x84063960	3224	0x98	0x100001	F11e	VDevice/KSecOU
0X84008970	3224	0x00	0x120089	File	\Device\NeredDirelsesterus
0x03177000	2224	0x150	0x120191	File	\Device\Wanderight\Device\Tellson\AnnData\Lasa\Microsoft\Uindevc\Temponany,Internet Files\
ountons dat	5224	0X134	0X120191	FILE	(Device (narouiskyoiume) (Sers (Teoser (Appbaca (Eocal (Airrosof C Windows (Temporary Internet Files (
00000001001 S.0000	2004	0-101	0-100020	Filo	\Device\Handdick\alume1\Windows\winsxs\x86 microsoft windows common-controls 6595664144ccf1df 6
0 7601 189	227 none	41e855142bc	15705d	1116	
0x83ffb1a8	3224	0x1d8	0x100080	File	\Device\Nsi
0x849fa7f8	3224	0x260	0x16019f	File	\Device\Afd\Endpoint
0x84ad83d8	3224	0x298	0x120089	File	\Device\HarddiskVolume1\Windows\Fonts\StaticCache.dat
0x83f8d258	3224	0x308	0x100020	File	\Device\HarddiskVolume1\Windows\winsxs\x86 microsoft.windows.common-controls 6595b64144ccf1df 6
.0.7601.188	337 none	41e855142bo	d5705d		
0x83ebce30	3224	0x31c	0x120089	File	\Device\HarddiskVolume1\Windows\System32\en-US\wshtcpip.dll.mui
0x84079d38	3224	0x320	0x16019f	File	\Device\Afd\Endpoint
0x84048910	3224	0x324	0x16019f	File	\Device\Afd\Endpoint
0x83f0a7a0	3224	0x32c	0x120089	File	\Device\HarddiskVolume1\Windows\System32\en-US\wship6.dll.mui
0x840c5220	3224	0x388	0x100001	File	\Device\HarddiskVolume1\Users\IEUser\AppData\Roaming\Microsoft\SystemCertificates\My
0x83f27588	3224	0x3a8	0x100003	File	\Device\KsecDD
0x841278b0	3224	0x4cc	0x100001	File	\Device\HarddiskVolume1\Users\IEUser\AppData\Roaming\Microsoft\SystemCertificates\My
0x841f5210	3224	0x514	0x120089	File	\Device\HarddiskVolume1\Windows\System32\en-US\crypt32.dll.mui
0x84de0828	3224	0x540	0x120089	File	\Device\HarddiskVolume1\Windows\System32\en-US\KernelBase.dll.mui
0x841bcf80	3224	0x550	0x100001	File	\Device\KsecDD
0x841bdeb8	3224	0x560	0x16019f	File	\Device\Afd\Endpoint
0x84ed31e0	3224	0x580	0x16019f	File	\Device\Afd\Endpoint
0x84ad5538	3224	0x588	0x16019f	File	\Device\Afd\Endpoint
0x84a81e50	3224	0x5cc	0x120089	File	\Device\HarddiskVolume1\Windows\System32\en-US\setupapi.dll.mui
0x84a81b30	3224	0x624	0x16019f	File	\Device\Afd\Endpoint
0x83ebe760	3224	0x650	0x16019f	File	\Device\Afd\Endpoint

Slika 6 – Ispis ručki otvorenih datoteka dobivenih pokretanjem naredbe *handles* i filtriranjem po ključnoj riječi "File"

U ovom slučaju, u trenutku snimanja slike memorije ovaj proces nije imao nikakve posebno zanimljive otvorene datoteke. Sada, moguće je filtrirati ispis i po drugom tipu objekta – ključevima registra:

volatility -f infected_teslacrypt.elf --profile=Win7SP1x86 handles --pid=3224 | findstr Key

C:\WIND	OWS\system32	\cmd.exe				- 🗆	×	
C:\volatili	ity>volatili	ity -f inf	ected_te	slacrypt.elfpr	ofile=Win7SP1x86 handlespid=3224 findstr Key			
Volatility	Foundation	Volatilit	y Framew	ork 2.6				
0x996e3180	3224	0xc	0x1	Key	MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER			
0x9f850228	3224	0x28	0xf003f	Key	MACHINE			
0x9970e938	3224	0x2c	0x20019	Key	MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS			
0x935c48a0	3224	0xa0	0x1	Key	USER\S-1-5-21-3583694148-1414552638-2922671848-1000\SOFTWARE\MICROSOFT\WINDOWS	CURRENTVE	RSION	
\EXPLORER								
0x8a4a2420	3224	0xa4	0xf003f	Key	USER\S-1-5-21-3583694148-1414552638-2922671848-1000			
0x96e2f0f8	3224	0xac	0x20019	Key	MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\FOLDERDESCRIPTIONS\	B4BFCC3A-	-DB2C-	
424C-B029-7	7FE99A87C641	L}\PROPERT	YBAG					
0x94a64828	3224	0xbc	0x9	Key	MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIC	ONS		
0x8a46c7f0	3224	0xc8	0x2001f	Key	USER\S-1-5-21-3583694148-1414552638-2922671848-1000\CONTROL PANEL\DESKTOP			
0xa1d4ca78	3224	0xd0	0x20019	Key	MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE\ALTERNATE SORTS			
0x9fb86be8	3224	0xd4	0x20019	Key	MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE			
0x99783030	3224	0x108	0xf0003	KeyedEvent				
0x8a1fe628	3224	0x13c	0x20019	Key	MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\FOLDERDESCRIPTIONS\	{F38BF404-	1D43-	
42F2-9305-6	57DE0B28FC23	<pre>3}\PROPERT</pre>	YBAG					
0x9f84c9b0	3224	0x140	0x20019	Key	MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\FOLDERDESCRIPTIONS\	[18989B1D-	99B5-	
455B-841C-A	AB7C74E4DDFC	C}\PROPERT	YBAG					
0xa1c7cb00	3224	0x148	0x2001f	Key	USER\S-1-5-21-3583694148-1414552638-2922671848-1000\SOFTWARE\MICROSOFT\WINDOWS	CURRENTVE	RSION	
\INTERNET S	SETTINGS							
0x94bf84f8	3224	0x150	0xf003f	Key	USER			
0x9a204650	3224	0x164	0x1	Key	MACHINE\SOFTWARE\MICROSOFT\INTERNET EXPLORER\MAIN\FEATURECONTROL			
0xa03b9358	3224	0x168	0x20019	Key	MACHINE\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS			
0x9ca288c8	3224	0x16c	0x20019	Key	USER\S-1-5-21-3583694148-1414552638-2922671848-1000\SOFTWARE\POLICIES\MICROSOF	<pre>F\WINDOWS\</pre>	CURRE	
NTVERSION \]	INTERNET SET	TTINGS						
0x984e34d0	3224	0x170	0x20019	Key	USER\S-1-5-21-3583694148-1414552638-2922671848-1000\SOFTWARE\MICROSOFT\WINDOWS	CURRENTVE	RSION	
\INTERNET S	SETTINGS							
0x9fb9d178	3224	0x174	0x20019	Key	MACHINE\SOFTWARE\POLICIES			
0x94a617d8	3224	0x178	0x20019	Key	USER\S-1-5-21-3583694148-1414552638-2922671848-1000\SOFTWARE\POLICIES			
0x99732638	3224	0x17c	0x20019	Key	USER\S-1-5-21-3583694148-1414552638-2922671848-1000\SOFTWARE			
0x985906c0	3224	0x180	0x20019	Key	MACHINE\SOFTWARE			
								~

Slika 7 – Ispis ručki otvorenih registarskih ključeva dobivenih pokretanjem naredbe *handles* i filtriranjem po ključnoj riječi "Key"

Nažalost, ni u slučaju ključeva registra nema zanimljivih tragova.



No, ima još jedan zanimljivi tip ručke u ovom kontekstu, a to su mehanizmi međusobnog isključivanja, takozvani *mutexi* (skraćeno od eng. *mutual exclusion*). Zlonamjerni softver često stvara *mutex* kako se ne bi više instanca zlonamjernog programa pokrenulo i međusobno si smetalo, npr. više puta šifriralo istu datoteku. Unutar jezgre operacijskog sustava Windows, *mutex* objekti se ne zovu *Mutex*, već *Mutant*. Zato, kako bi se iz ispisa filtrirale ručke *mutex* objekata potrebno je pokrenuti sljedeću naredbu:

volatility -f infected_teslacrypt.elf --profile=Win7SP1x86 handles --pid=3224 | findstr Mutant

Comman	d Prompt				-	×
C:\volatili	ty>volati	lity -f i	nfected_teslacrypt.elf	profile=Win7SP1x86 handlespid=3224 findstr Mutant		~
Volatility	Foundatio	n Volatil	ity Framework 2.6			
0x84c5f0c8	3224	0x38	0x1f0001 Mutant			
0x84457af8	3224	0x3c	0x1f0001 Mutant			
0x84dae700	3224	0xb8	0x1f0001 Mutant	System1230123		
0x84cd80a8	3224	0x2e0	0x1f0001 Mutant	ZonesCacheCounterMutex		
0x84cdf140	3224	0x2e4	0x1f0001 Mutant	ZonesLockedCacheCounterMutex		
0x84a05108	3224	0x3b4	0x1f0001 Mutant			
0x8423b8c8	3224	0x3bc	0x1f0001 Mutant			
0x8402b410	3224	0x5d4	0x1f0001 Mutant			
0x84036560	3224	0x5dc	0x1f0001 Mutant			
	_					\sim

Slika 8 – Ispis ručki *mutex* objekata dobivenih pokretanjem naredbe *handles* i filtriranjem po ključnoj riječi "Mutant"

Mutex objekti koji nemaju ime koriste se lokalno, unutar jednog procesa, dok se za sinkronizaciju više procesa koriste *mutex* objekti s imenom. Upravo ti *mutex* objekti s imenom su zanimljivi u ovom kontekstu – u ovom slučaju to su:

- System1230123
- ZonesLockedCacheCounterMutex
- ZonesCacheCounterMutex

Iako na prvi pogled imena možda i ne izgledaju sumnjivo, korisno je internetskim tražilicama pretražiti jesu li se ta imena pojavljivala kod drugih zlonamjernih softvera. Kratkim istraživanjem moguće je otkriti da se prvi *mutex*, imena *System1230123*, pojavljuje kod *ransomwarea* zvanog TeslaCrypt, dok se druga dva imena *mutexa* pojavljuju kod TeslaCrypta, ali i kod nekih drugih zlonamjernih programa.

3.4 Rekonstrukcija izvršne (.exe) datoteke

Naredbom *procdump*, Volatility može iz procesa pokušati rekonstruirati izvršnu (*.exe*) datoteku. Rezultat rekonstrukcije gotovo nikada neće savršeno odgovarati izvornoj izvršnoj datoteci. Primjerice, sadržaj podatkovnih sekcija datoteke će gotovo zasigurno biti promijenjen, no sadržaj samog strojnog koda često će biti isti kao i u izvršnoj datoteci.

Naredbi *procdump* je, uz identifikator procesa za rekonstrukciju, potrebno zadati i argument –*dump-dir=<direktorij>*, gdje je *<direktorij>* putanja do direktorija u koji će biti spremljena datoteka. Potrebno je stvoriti taj direktorij, primjerice naredbom *mkdir* ili uobičajenim stvaranjem direktorija u grafičkom sučelju, te pokrenuti naredbu:

volatility -f infected_teslacrypt.elf --profile=Win7SP1x86 procdump --dump-dir=dump --pid=3224





Slika 9 - Stvaranje direktorija i rekonstrukcija izvršne datoteke procesa pomoću naredbe *procdump*

Na ovaj način ponekada je moguće dobiti izvršnu datoteku i u korisnijem obliku za analizu od izvornog oblika, primjerice ako je izvorna datoteka bila zapakirana (eng. *packed*). Tzv. pakiranje izvršnih datoteka je česta tehnika zlonamjernog softvera u kojem je sadržaj izvršne datoteke komprimiran i/ili šifriran te se tek prilikom pokretanja programa dešifrira i/ili dekomprimira unutar radne memorije računala.

Kako rekonstruirana datoteka potencijalno sadrži zlonamjeran kod, moguće je da na računalu istražitelja antivirusni alat to prepozna i automatski obriše datoteku.

Rekonstruiranu izvršnu datoteku moguće je otvoriti u drugim alatima za analizu izvršnih datoteka, primjerice u alatu za reverzni inženjering IDA, kao što je prikazano na slici 10.



Slika 10 - Rekonstruirana izvršna datoteka otvorena u alatu IDA

Također, rekonstruiranu izvršnu datoteku moguće je učitati na <u>VirusTotal</u> – Web stranicu koja učitane datoteke predaje na analizu većem broju antivirusnih alata te korisniku prikazuje rezultat analize. Na taj način moguće je lako saznati što razni antivirusni alati misle o toj datoteci – smatraju li da ta datoteka sadržava zlonamjerni softver, i ako da, što misle koji konkretno zlonamjerni softver sadržava.



VirusTotal	×	+									- 0	×
€ → C	۵	(i) A https://www.vir	ustotal.com/	#/file/b1832eac285653c2e2b02979270d9a7	28b7c66881a5266551864	e5146ed3882	B/de 🕢 🏠	Ŧ		¢¶ 🔤	B 🗗 🛙	
Σ	Search or scan a U	RL, IP address, domain, or file	hash					Q	(†		Sign in	Â
		55/67 Detection Details	55 engin SHA-256 File name File size Last analysis Behavio	es detected this file b1832aac285532c2b02979270d9a7 executable.3224.exe 284 KB 2018-02-19 16:56:57 UTC	28b7c66881a526655186-	4e5146ed388	128					
		Ad-Aware	A	Gen:Variant_Zusy.128574	AegisLab	A	Troj.Ransom.W32.Bitman.tngH					
		AhnLab-V3	A	Trojan/Win32.Tescrypt.R137618	ALYac	A	Gen:Variant.Zusy.128574					
		Antiy-AVL	A	Trojan[Downloader]/Win32.Dapato	Arcabit	4	Trojan.Zusy.D1F63E					
		Avast	A	Win32:CryptoLocker-C [Trj]	AVG	A	Win32:CryptoLocker-C [Trj]					
		Baidu	A	Win32.Trojan.WisdomEyes.16070401	BitDefender	A	Gen:Variant.Zusy.128574					
		Bkav	A	W32.RansomwareEnvyF.Trojan	CAT-QuickHeal	A	Ransom.Tescrypt.AG4					
		ClamAV	A	Win, Trojan, TeslaCrypt-3	Comodo	A	Backdoor.Win32.Androm.GML					
		CrowdStrike Falcon	A	malicious_confidence_100% (D)	Cybereason	A	malicious.6ac310					
		Cylance		Unsafe	Cyren	4	W32/Trojan.BWDR-8762					
		DrWeb	A	Trojan.PWS.Siggen1.30341	Emsisoft	A	Gen:Variant.Zusy.128574 (B)					

Slika 11 – Dio rezultata analize rekonstruirane izvršne datoteke na Web stranici VirusTotal

U ovom slučaju, moguće je vidjeti kako brojni antivirusni alati svojim detekcijama upućuju na **TeslaCrypt** (imena *tescrypt, teslacrypt*), no ima i alata koji upućuju na druge zlonamjerne programe (*cryptolocker, zusy*).

3.5 Mrežne veze

Još jedan bitan korak u forenzici radne memorije je analiza mrežnih veza. Kako je na računalu bio pokrenut operacijski sustav Windows 7, potrebno je koristiti naredbu *netscan* za analizu mrežnih veza. Format naredbe je:

Command Pror	npt						- 0	×
0x3f141958	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	320	wininit.exe		^
0x3f141958	TCPv6	:::49152	:::0	LISTENING	320	wininit.exe		
0x3f144398	TCPv4	0.0.0.0:49152	0.0.0.0:0	LISTENING	320	wininit.exe		
0x3f160840	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	752	<pre>svchost.exe</pre>		
0x3f162138	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	752	svchost.exe		
0x3f162138	TCPv6	:::49153	:::0	LISTENING	752	<pre>svchost.exe</pre>		
0x3ec38288	TCPv4	10.0.2.15:49480	23.51.123.27:80	ESTABLISHED	-1			
0x3ec5c008	TCPv4	10.0.2.15:49483	23.51.123.27:80	ESTABLISHED				
0x3ec5e578	TCPv4	10.0.2.15:49481	23.51.123.27:80	ESTABLISHED				
0x3ee1db08	TCPv4	10.0.2.15:49471	185.100.85.150:443	ESTABLISHED	-1			
0x3eec7088	TCPv4	10.0.2.15:49476	23.6.112.138:80	ESTABLISHED				
0x3f082008	TCPv4	10.0.2.15:49479	194.150.168.74:443	CLOSE WAIT				
0x3f10f4c8	TCPv4	10.0.2.15:49482	23.51.123.27:80	ESTABLISHED	-1			
0x3f777b38	UDPv6	::1:53785	*:*		1552	svchost.exe	2018-02-19 14:14:12 UTC+0000	
0x3f777ca8	UDPv4	127.0.0.1:53786	* *		1552	svchost.exe	2018-02-19 14:14:12 UTC+0000	
0x3f777e18	UDPv6	fe80::80ac:4126:fa58:1b81:1900			1552	svchost.exe	2018-02-19 14:14:12 UTC+0000	
0x3fa85278	UDPv6	fe80::80ac:4126:fa58:1b81:546	*:*		752	svchost.exe	2018-02-19 14:19:29 UTC+0000	
0x3f384bc0	TCPv4	10.0.2.15:49469	23.6.112.178:80	ESTABLISHED	-1			
0x3f398818	TCPv4	10.0.2.15:49474	194.150.168.74:443	CLOSE WAIT	-1			
0x3f759660	TCPv4	10.0.2.15:49472	104.31.75.124:80	ESTABLISHED	-1			
0x3f76ede8	TCPv4	10.0.2.15:49473	104.31.74.124:80	ESTABLISHED				
0x3fafdde8	TCPv4	10.0.2.15:49464	23.6.112.138:80	ESTABLISHED				
0x3fb2dde8	TCPv4	10.0.2.15:49478	185.100.85.150:443	ESTABLISHED	-1			
0x3fc6ebe0	UDPv4	0.0.0.0:0			1708	svchost.exe	2018-02-19 14:12:13 UTC+0000	
0x3fd5b510	TCPv4	10.0.2.15:49477	40.77.226.250:443	ESTABLISHED				
0x3fd97828	TCPv4	10.0.2.15:49475	23.6.112.121:80	ESTABLISHED	-1			
0x3fdef008	TCPv4	10.0.2.15:49463	40.77.226.249:443	ESTABLISHED				
0x3ff0c438	TCPv4	10.0.2.15:49470	23.7.206.117:80	ESTABLISHED				
C:\volatilitv>								~

volatility -f infected_teslacrypt.elf --profile=Win7SP1x86 netscan

Slika 12 - Popis mrežnih veza dobiven pokretanjem naredbe netscan



Iz navedenog popisa, računalo je bilo spojeno na sljedeće IP adrese i odgovarajuće TCP priključke (eng. *port*):

- 104.31.74.124:80
- 104.31.75.124:80
- 185.100.85.150:443
- 194.150.168.74:443
- 23.51.123.27:80
- 23.6.112.121:80
- 23.6.112.138:80
- 23.6.112.178:80
- 23.7.206.117:80
- 40.77.226.249:443
- 40.77.226.250:443

Korišteni TCP priključci 80 i 443 upućuju na HTTP i HTTPS protokole, odnosno spajanje na Web servise. Volatility nije uspio povezati mrežne veze s procesom (PID = -1), no već i ovakav popis je korisna informacija. Navedene IP adrese moguće je dalje istražiti na nekoliko načina, opisanih u narednim potpoglavljima. Bit će opisani primjeri istraživanja pojedinih IP adresa s popisa, no u sklopu sveukupne analize je korisno proučiti sve IP adrese.

3.5.1 Obrnuti DNS (eng. reverse DNS)

DNS (eng. *Domain Name System*) sustav je koji povezuje simbolička imena s numeričkim IP adresama. Pomoću DNS-a korisnik može primjerice koristiti simboličko ime *carnet.hr* umjesto IP adrese *161.53.160.25* koju je teško zapamtiti.

Manje je poznato da je pomoću DNS-a moguće napraviti i obrnuti postupak, tj. povezati IP adresu sa simboličkim imenom. Taj postupak naziva se obrnuta DNS pretraga (eng. *reverse DNS lookup*) te ga je moguće napraviti pomoću alata *nslookup*, dostupnog na Windows i Unix računalima ili korištenjem besplatno dostupnih Web alata, primjerice <u>MxToolbox Reverse Lookup alata</u>.

Kako bi se izvršila obrnuta DNS pretraga pomoću alata *nslookup*, potrebno mu je kao argument dati IP adresu za koju se traži simboličko ime, u ovom primjeru jedna od IP adresa iz popisa veza dobivenih naredbom *netscan*:

nslookup 194.150.168.74

command Prompt	—	×
		^
C:\volatility>nslookup 194.150.168./4		
Server: rdns1.bnet.hr		
Address: 83.139.103.3		
Name: www.tor2web.org		
Address: 194.150.168.74		
		\sim





U ispisu naredbe vidi se kako postoji obrnuti DNS zapis za tu IP adresu, te je on jednak <u>www.tor2web.org</u>. Kratkim istraživanjem moguće je saznati da je ta stranica zapravo most koji omogućava pristup skrivenim servisima Tor mreže. U ovom kontekstu, iz toga je moguće posumnjati da je zlonamjerni softver kontaktirao poslužitelje unutar Tor mreže, na Tor skrivenim servisima.

Problem s obrnutim DNS zapisima je to što:

- oni ne moraju uvijek postojati,
- ne moraju čak biti ni točni,
- a i jednostavno više simboličkih imena može pokazivati na istu IP adresu u tom slučaju obrnuti DNS zapis može dati informacije o samo jednom imenu.

3.5.2 WHOIS servis

WHOIS je servis pomoću kojega je moguće saznati informacije o organizaciji koja je registrirala određenu domenu ili blok IP adresa. Za slanje WHOIS upita, na Unix sustavima obično je dostupan alat *whois* koji se pokreće iz naredbenog retka, dok je na Windows sustavima potrebno dodatno instalirati takav alat, dostupan <u>ovdje</u>. Alternativno, moguće je koristiti neki od Web alata za slanje WHOIS upita, primjerice <u>ovaj alat</u>.

Na slici 14 prikazan je ispis rezultata WHOIS upita na navedenom Web alatu za jednu od IP adresa s popisa naredbe *netscan* – 40.77.226.249. IP adresa je registrirana na tvrtku Microsoft, te se zbog toga ne čini sumnjivom – vjerojatno ju je kontaktirao neki dio operacijskog sustava Windows, primjerice servis za ažuriranje.



Whois-RWS	× +						—	
← → ♂ ଢ	(i) 🔒 https://whois.arin.ne	et/rest/net/NET-40-74-0-0		<u>↓</u>	III\ 🗉	10	🖬 <mark>S</mark>	
ARIN American Registry for Internet Numbers	NUMBER RESOURCES P	ARTICIPATE POLICIES	FEES & INVOICES	SEARCH all requests KNOWLEDGE	WhoisRWS subject to term ABOUT US	ns of use	advanced	Search ^
ARIN Online enter								
	You searched for: 40.77.226.249							
	Network					RELEVAN	IT LINKS	
	Net Range	40.74.0.0 - 40.125.127.255				> ARIN W	hois/Whois-F	RWS
	CIDR	40.112.0.0/13 40.120.0.0/14 40.124.0.0/16 40.125.0.0/17 40.74.0.0/15 40.76.0.0/14 40.80.0.0/12 40.96.0.0/12	Terms of Report V > Whois-F docume > ARIN Ter Mailing L > Sample	Terms of Service Report Whois Inaccuracy Whois-RWS API documentation ARIN Technical Discussion Mailing List Sample stylesheet (xsl)				
	Name	MSFT						
	Handle	NET-40-74-0-0-1						
	Parent	NET40 (NET-40-0-0-0)						
	Net Type	Direct Assignment						
	Origin AS							
	Organization	Microsoft Corporation (MSFT)						
	Registration Date	2015-02-23						
	Last Updated	2015-05-27						
	Comments							
	RESTful Link	https://whois.arin.net/rest/net/N	IET-40-74-0-0-1					
	See Also	Related organization's POC re-	cords.					
	See Also	Related delegations.						

Slika 14 - WHOIS zapis za IP adresu 40.77.226.249 na vanjskom Web alatu

3.5.3 Ostale baze informacija o IP adresama

Od ostalih baza informacija o IP adresama korisno je znati za servise s tzv. pasivnim DNS bazama. U takvim bazama zapisane su povijesne informacije o povezanosti IP adresa i simbolička imena. Upitom na takve servise moguće je otkriti i druge domene koje su bile povezane s određenom IP adresom. Jedna od takvih javno dostupnih baza s mogućnošću pretraživanja nalazi se na <u>ovoj poveznici</u>.

Još jedna korisna baza u ovom kontekstu je baza servisa VirusTotal, koje se može pretraživati <u>ovdje</u>. VirusTotal kao cijeli servis specijaliziran je za zlonamjerni softver, tako da je u njegovoj bazi moguće naći informacije o datotekama koje su preuzete s tražene IP adrese te informacije o izvršnim datotekama koje, jednom kada su pokrenute, komuniciraju s tom IP adresom. U primjeru na slici 15 u tražilicu alata VirusTotal upisana je adresa 194.150.168.74, za koju je ranije ustanovljeno da odgovara Web stranici *www.tor2web.com*. Na slici je moguće vidjeti kako je veći broj zlonamjernog softvera komunicirao s tim poslužiteljem.



VirusTotal	×										×
€ → œ	ŵ	(i) A https://www.	w.virustotal.com/#	/ip-address/194.1	50.168.74	··· ☆	Ŧ		•	1	≡
Σ	Search or scan a UR	L, IP address, domain, c	or file hash				Q	F		Sign in	^
Care I		2018-01-09	(2/66) http	is://tor2web.org/b	itcoin.html						
		2018-01-07	wee http	s://www.tor2web	.org/antanistaticmap/tor2web.png						
		2017-12-21	aves http	://tor2web.org/m	irror/						
				.,							
		More									
		Downloaded F	iles 🛛				×				
		Date scanned	Detections	File type	Name						
		2016-06-20	0/56	HTML	gate.php						
		2018-03-05	0/59	HTML	favicon.ico						1
		Communicatir	ng Files 🛛				×				
		Date scanned	Detections	File type	Name						
		2018-01-25	47/66	Win32 EXE	01780000.exe						
		2017-12-14	60/68	Win32 EXE	16865687.exe						
		2017-02-16	53/59	Win32 EXE	calc						1
		2016-07-21	\$1/55	Win32 EXE	calc						
		2016-01-11	20/54	Win32 EXE	dropper.exd						
		2016-05-04	48/57	Win32 EXE	calc						
		2016-04-17	(49/57)	Win32 EXE	calc						~

Slika 15 - Pretraživanje informacija o IP adresi u bazi Web stranice VirusTotal

3.6 Windows registar (eng. registry)

Zlonamjerni softver često koristi Windows registar u sklopu svojih mehanizama trajnosti (eng. *persistence mechanisms*). U Windows registar moguće je zapisati određene ključeve na temelju kojih će se program pokretati prilikom pokretanja računala. Te ključeve koriste i zlonamjerni programi kako ih se ne bi moglo riješiti jednostavnim ponovnim pokretanjem računala. Jedan izvor za popis takvih registarskih ključeva nalazi se <u>ovdje</u>.

Kao primjer, sadržaj jednog od tih ključeva Windows registra moguće je provjeriti pokretanjem sljedeće naredbe:

```
volatility -f infected_teslacrypt.elf --profile=Win7SP1x86 printkey
--key="Software\Microsoft\Windows\CurrentVersion\Run"
```

Command Prompt	_	×
Values: REG_SZ crypto13 : (S) C:\Users\IEUser\AppData\Roaming\ngwksdp.exe		
Registry: \??\C:\Users\sshd_server\ntuser.dat Key name: Run (S) Last updated: 2018-01-03 05:01:34 UTC+0000		
Subkeys:		
Values: REG_EXPAND_SZ Sidebar : (S) %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun		
C:\volatility>		~

Slika 16 – Ispisivanje vrijednosti ključa registra pomoću naredbe printkey



U ispisu naredbe moguće je vidjeti vrijednost povezanu sa sumnjivim *ngwksdp.exe* procesom. Konkretnije, moguće je vidjeti ime ključa (*crypto13*) te putanju do izvršne datoteke (*C:\Users\IEUser\AppData\Roaming\ngwksdp.exe*).

3.7 Datotečni sustav

Datotečni sustav opisuje na koji način se pohranjuju datoteke u trajnu memoriju te opisuje njihovu hijerarhiju, tj. u kojem se direktoriju nalazi koja datoteka. Operacijski sustav Windows koristi datotečni sustav pod nazivom NTFS. Datotečni sustav NTFS koristi datotečnu tablicu zvanu MFT (eng. *Master File Table*) u koju su zapisani detalji svake od datoteka u sustavu. Naredba *mftparser* potražit će datotečne tablice u slici memorije te ispisati neke od informacija sadržanih u njoj:

volatility -f infected_teslacrypt.elf --profile=Win7SP1x86 mftparser

Select Command Prompt				– 🗆 ×		
Birth Volume ID: 5b030000-000 Birth Object ID: 31010dad-000 Birth Domain ID: 00000000-000	00-0000-5b03-0000000000000 00-0000- fff-fff8 2794711 00-0000-0000-0000000000000			^		
MFT entry found at offset 0x4 Attribute: In Use & File Record Number: 42261 Link count: 2		*****				
\$STANDARD_INFORMATION Creation	Modified	MFT Altered	Access Date	Туре		
2018-01-03 02:31:15 UTC+0000	2018-02-19 14:20:33 UTC+0000	2018-02-19 14:20:33 UTC+0000	2018-01-03 02:31:15 UTC+0000	Archive & Content not indexed		
\$FILE_NAME Creation	Modified	MFT Altered	Access Date	Name/Path		
2018-01-03 02:31:15 UTC+0000 p\KB2533~1.ECC	2018-02-19 14:20:33 UTC+0000	2018-02-19 14:20:33 UTC+0000	2018-01-03 02:31:15 UTC+0000	Users\IEUser\AppData\Local\Tem		
\$FILE_NAME Creation	Modified	MFT Altered	Access Date	Name/Path		
2018-01-03 02:31:15 UTC+0000 2018-02-19 14:20:33 UTC+0000 2018-02-19 14:20:33 UTC+0000 2018-01-03 02:31:15 UTC+0000 Users\IEUser\AppData\Local\Tem p\K82533523_20180102_183114542-Microsoft .NET Framework 4 Client Profile-MSP0.txt.ecc						
\$DATA						
\$OBJECT_ID				~		

Slika 17 – Informacije iz datotečne tablice dobivene naredbom mftparser

U ispisu naredbe moguće je vidjeti kako primjerice druga datoteka u tablici ima nastavak od dva dijela: *.txt.ecc*. Neobično je vidjeti takav oblik nastavka, te je istraživanjem moguće saznati da neke inačice *ransomwarea* TeslaCrypt koriste taj nastavak za označavanje šifriranih datoteka. U ovom slučaju, šifrirana je tekstualna datoteka s originalnim nastavkom *.txt*. U ispisu naredbe je moguće pronaći veći broj datoteka s nastavkom *.ecc* te je tako moguće i saznati koje su datoteke šifrirane.



4 Zaključak

U ovom dokumentu opisano je kako alatom Volatility forenzički analizirati sliku radne memorije računala zahvaćenog stvarnim zlonamjernim softverom. Znanja usvojena kroz ovaj primjer moguće je općenito primijeniti za detaljniju analizu procesa, mrežnih veza, Windows registra i podataka o datotečnom sustavu koji se nalaze u radnoj memoriji.

U kontekstu forenzičke analize računala zahvaćenog zlonamjernim softverom, bitno je imati na umu da je forenzikom radne memorije moguće otkriti neke tragove koje druge grane računalne forenzike jednostavno ne mogu otkriti. Primjerice, neki podaci nikada neće biti zapisani na disk ili poslani preko mreže ili ako i hoće, tada će biti šifrirani. U tom slučaju, jedino mjesto gdje ih je moguće pronaći u otvorenom, nešifriranom obliku će biti radna memorija.

No i dalje, forenzika radne memorije je samo jedna grana forenzike, tako da daljnji koraci u ovakvoj analizi bi svakako uključivali i forenziku diska, snimke mrežnog prometa (ako je ona dostupna) te po potrebi i detaljan reverzni inženjering zlonamjernog programa.



5 Literatura

1. **Martinez, Emiliano.** VirusTotal += Passive DNS replication . [Mrežno] 1. 4 2013. [Citirano: 7. 3 2018.] http://blog.virustotal.com/2013/04/virustotal-passive-dns-replication.html.

2. Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters. *The Art of Memory Forensics.* s.l. : Willey, 2014.

3. **Microsoft.** *MSDN* - *Handles and Objects.* [Mrežno] [Citirano: 8. 3 2018.] https://msdn.microsoft.com/en-

us/library/windows/desktop/ms724457(v=vs.85).aspx.

4. -. Command Reference. *Volatility Wiki.* [Mrežno] [Citirano: 8. 3 2018.]

https://github.com/volatilityfoundation/volatility/wiki/Command-Reference.

5. **Russinovich, Mark.** Pushing the Limits of Windows: Handles. [Mrežno] 29. 9 2009. [Citirano: 8. 3 2018.]

https://blogs.technet.microsoft.com/markrussinovich/2009/09/29/pushing-the-limits-of-windows-handles/.

6. **Roussey, Benjamin.** What is passive DNS? [Mrežno] 8. 7 2017. [Citirano: 8. 3 2018.] http://techgenix.com/what-passive-dns/.

7. -. DNS and WHOIS - How it Works. [Mrežno] ICANN, 7 2017. [Citirano: 8. 3 2018.] https://whois.icann.org/en/dns-and-whois-how-it-works.

8. **Seals, Tara.** Anti-Forensic Malware Widens Cyber-Skills Gap. [Mrežno] 9. 8 2015. [Citirano: 8. 3 2018.] https://www.infosecurity-magazine.com/news/antiforensic-malware-widens/.