Pregled korištenih metoda lova na kibernetičke prijetnje

Mirković, Nikša

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Nikša Mirković

PREGLED KORIŠTENIH METODA LOVA NA KIBERNETIČKE PRIJETNJE

ZAVRŠNI RAD

Varaždin, 2022.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Nikša Mirković

Matični broj: 41210/12-IZV

Studij: Primjena informacijske tehnologije u poslovanju

PREGLED KORIŠTENIH METODA LOVA NA KIBERNETIČKE PRIJETNJE

ZAVRŠNI RAD

Mentor/Mentorica:

Doc. dr. sc. Igor Tomičić

Varaždin, srpanj 2022.

Nikša Mirković

Izjava o izvornosti

Izjavljujem da je moj završni/diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

U radu će se opisati i objasniti temeljni okvir za pristupanje lovu kibernetičkih prijetnji. Opisati će se struktura lova, razine lova te će biti objašnjeno na koje načine timovi mogu pristupiti lovu na kibernetičke prijetnje. Rad će obuhvatiti osnovne metode lova na kibernetičke prijetnje upotrebom alata iz Sysinternals skupa programskih rješenja za analizu računala. Opisat će se kako koristiti Windows alate, event viewer i registry editor, za lov na kibernetičke prijetnje. Pregledat će se ključni zapisi događaja i registarski zapisi koji mogu upućivati na postojanje kibernetičke prijetnje. Naposljetku opisati će se postupak kreacije Yara pravila koje služe za pronalazak specifičnih kibernetičkih prijetnji na računalu.

Ključne riječi: kibernetička prijetnja; računalni virus; sigurnost; Sysinternals; dnevnik događaja; registri; Yara;

Sadržaj

1. Uvod

Lov na kibernetičke prijetnje odnosi se na gotovo neiscrpan spektar znanja jer sadrži sve metode i tehnike pronalaska i uklanjanja eventualnih kibernetičkih prijetnji koje svakoga dana rastu u broju kako se tehnologije mijenjaju, a broj kriminalnih aktivnosti iz dana u dan je sve veći. SecurityInteligence portal navodi kako kibernetički kriminalci u prosjeku provedu 191 dan na mreži na kojoj čine kriminalne radnje prije nego što budu primijećeni [1]. Svaki lovac na kibernetičke prijetnje osim adekvatnog znanja o korištenim tehnologijama treba poznavati i svog klijenta. Ovisno o sustavu koji će osiguravati lovac mora prepoznati navike pojedinaca koji koriste sustav kao i razinu njihove informatičke pismenosti. Mogućnost lovca da upozna svog klijenta dolazi s iskustvom i čini razliku između početnika i profesionalca jer će profesionalac znati da će shvaćanjem navika klijenata znati kako započeti lov i na što se fokusirati što kao posljedicu ima smanjenje utrošenog vremena i novca.

Lov na kibernetičke prijetnje može se podijeliti na tri pristupa koji se isprepliću i dijele poneke metode i tehnike lova, ali imaju objektivno drugačiji pristup problematici.

Prvi pristup odnosi se na lov kibernetičkih prijetnji unutar specifične organizacije i iscrpan je proces sakupljanja informacija o organizaciji i pronalaska načina kako zaustaviti svaki pokušaj kibernetičkog kriminala. Ovaj princip obuhvaća metode forenzičke analize poput analiziranja pokrenutih procesa, registara i procesa koji se pokreću prilikom pokretanja sustava kao i mnoge druge metode [2].

Drugi pristup odnosi se na proaktivni lov odnosno neprestano nastojanje očuvanja sigurnosti kroz pristup učenja na tuđim greškama. Obuhvaća konstantno praćenje drugih organizacija tj. žrtava kriminalnih radnji, trenutno poznatih i aktivnih prijetnji, trendova i drugih vanjskih čimbenika [3].

Treći pristup odnosi se na svojevrsno postavljanje zamki tj. kreaciju izoliranih (*eng. sandbox*) sistema limitiranih resursa koji se koriste kao mete napada nakon čega se sakupljaju informacije o korištenim metodama i tehnikama napada u svrhu zaštite sistema koji sadrže bitne resurse. Ovaj pristup gubi na značaju jer noviji zlonamjerni programi detektiraju procese karakteristične za virtualno pokrenute sustave i ne aktiviraju se [4], [5].

2. Metode i tehnike rada

U radu će se najprije objasniti kako pristupiti lovu. Obradit će se struktura lova koja objašnjava od procesa i postupaka je sačinjen lov na kibernetičke prijetnje. Ovisno o veličini sustava koji se pokušava zaštiti zadatci lovaca su drugačiji. Utvrđivanjem razine pristupa lovu obradit će se metode lova sa skupom alata Sysinternals i to specifično ProcessExplorer, Autoruns, RamMap i TCPView. Alati Autoruns i ProcessExplorer korist će se za analizu procesa sustava. RamMap koristit će se za analizu RAM memorije, a alat TCPView za analizu mrežne aktivnosti procesa. Nakon analize mrežne aktivnosti računalnih procesa pomoću preglednika događaja utvrdit će se kako pronaći dokaz da je računalo bilo meta računalnog kibernetičkog napada. Za sličnu funkciju koristit će se i alata uređivač registara gdje će se na primjeru pokazati kako ustvrditi da su registarski zapisi bili meta zlonamjerne radnje te kako istu ukloniti. Na koncu će se pokazati kako automatizirati proces pronalaska kibernetičkih prijetnji izradom skripte u svojevrsnom programskom jeziku Yara tvrtke VirusTotal koja pronalazi tražene prijetnje upotrebom zadanih parametara. Istražuje se kako adekvatno koristi Yara pravila radi analize e-mail poruka i memorije računala.

3. Struktura lova na kibernetičke prijetnje

Pokazalo se kako svim velikim kompanijama koje raspolažu s velikim brojem podataka, koji su od ključne važnosti za njihovo poslovanje ili svoje poslovanje temelje na digitalnim tehnologijama, veliki problem predstavlja sigurnost tih podataka. Kao rješenje unutar tih kompanija postoje posebni odjeli za informacijsku i obavještajnu sigurnost čiji zadatak je loviti potencijalne prijetnje tj. prepoznati i ukloniti eventualne prijetnje prije nego što eskaliraju u problem koji bi kompromitirao podatke koje pokušavaju zaštititi. Stručnjaci u tim odjeljenjima uvidjeli su da započeti lov i kvantificirati uspješnosti trenutačnog stanja nije lako stoga je Američka firma SQRLL osmislila dokument koji služi kao okvir za lov kibernetičkih prijetnji. Firmu su osnovali stručnjaci koji su prethodno radili za Nacionalnu Sigurnosnu Agenciju Sjedinjenih Američkih Država. Sam okvir pruža smjernice za sistematičan pristup lovu na kibernetičke prijetnje te predlaže dobru praksu u okviru definiranja zrelosti odnosno razine cjelokupnog lova na prijetnje unutar organizacije. Unutar okvira lov na kibernetičke prijetnje definiran je kao proces proaktivne i iterativne pretrage kroz mreže kako bi se otkrile i izolirale napredne prijetnje koje zaobilaze postojeća sigurnosna rješenja. Iako je lov na kibernetičke prijetnje specifičan za svaku firmu, odnosno njezin informacijski sustav, ipak se određene prakse mogu univerzalno primjenjivati [6].

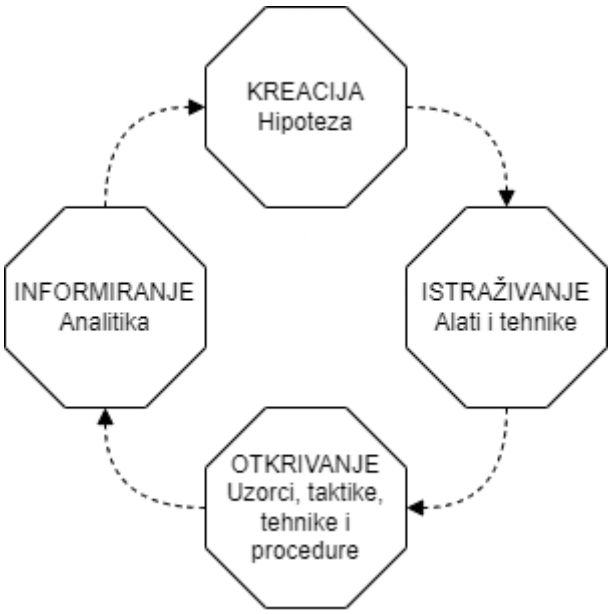
3.1. Razine lova

Ovisno o veličini organizacije i njezinoj željenoj razini zaštite ovisit će i njezine sposobnosti lova kibernetičkih prijetnji. Glavni lovac u SQRLL organizaciji David J. Bianco prepoznao je pet razina na kojima djeluju organizacije koje se pokušavaju zaštiti. Shvatio je glavne karakteristike pristupa lovu koje su na posljetku definirale i razinu uspješnosti tih organizacija u lovu na prijetnje. Razine se kreću od nulte tj. inicijalne pa sve do četvrte razine koju implementiraju organizacije vodeće na području lova na kibernetičke prijetnje navodi [6].

0. Inicijalna razina – organizacija se oslanja na software za automatsku detekciju zlonamjernih programa i antivirusne programe koji služe funkciju upozoravanja. Ne sakuplja se baza znanja i zbog toga mogućnost proaktivnog pronalaska prijetnji je nepostojeća.
1. Minimalna razina – organizacije se i dalje služe programima za automatsku detekciju zlonamjernih programa i radnji, ali evidentiraju i proširuju bazu znanja što otvara mogućnost bržeg pronalaska sličnih prijetnji u budućnosti. Zbog postojanja timova koji sakupljaju podatke o prijetnjama ovo je zapravo prva, minimalna razina lova na prijetnje.
2. Proceduralna razina – organizacije ovog tipa koriste i mijenjaju procedure za lov koje su razvile druge kompanije, ali nisu u stanju razvijati svoje vlastite procedure. Shodno tome koriste procedure koje primaju očekivani tip podatka i koriste tehnike analize specifične za te tipove podataka. Ovo je najčešća razina lova na kibernetičke prijetnje jer malim i srednjim poduzećima nije isplativo financirati veliki broj stručnjaka.
3. Inovativna razina – za razliku od prijašnje razine na ovoj razini organizacije zapošljavaju timove stručnjaka koji aktivno smišljaju nove procedure lova. Nerijetko zapošljavaju stručnjake koji koriste naprednije tehnologije poput strojnog učenja, vizualizacije velikih podataka i povezane analize podataka.
4. Vodeća razina – na ovoj razini nalaze se organizacije koje su vodeće na području lova na kibernetičke prijetnje, a od organizacija inovativne razine razlikuje ih automatizacija lova. Procedure svakog uspješnog lova trebaju se analizirati i automatizirati što ostavlja analitičarima vremena za izradu novih procedura ili unaprjeđenje postojećih. Upravo u mogućnosti fokusiranja na stalno promjenjive zahtjeve na području sigurnosti omogućavaju neometan rad organizacije.

3.2. Ciklus lova kibernetičkih prijetnji

Kako bi organizacije i lovci znali kako pristupiti samom lovu, a kasnije znali koje procese automatizirati, moraju se držati formalnog procesa kibernetičkog lova. Sqrll je razvio ciklus lova kibernetičkih prijetnji koji opisuje faze u izvođenju lova i ukazuje kako je lov na kibernetičke prijetnje neprekidan proces koji se stalno ponavlja. Ciklus lova sastoji se od četiri faze kako opisuje [6]. Prva je faza kreacije, a slijede ju faza istraživanja, otkrivanja, informiranja tj. prikazivanja rezultata.



Slika 1: Ciklus lova na kibernetičke prijetnje (Izvor: SQRLL organizacija, 2022)

Proces lova započinje hipotezom o eventualnom problemu. Za formiranje hipoteze u obzir se ne uzimaju samo problemi vezani direktno uz informacijsko komunikacijske tehnologije već se može formirati ovisno o događanjima unutar organizacije, karakteristikama ciljanih grupa i drugih čimbenika. Ako organizacija zaposli određeni broj novih zaposlenika koji nisu upoznati sa sigurnosnim standardima za očekivati je da bi netko od tih zaposlenika mogao kompromitirati sigurnost informacijskog sustava, može se postaviti hipoteza koja bi tražila dokaz da prijetnja mreži dolazi sa sustava koji takvi zaposlenici koriste. Ovaj proces može biti automatiziran na višim razinama upotrebom algoritama za procjenu rizika koji označavaju korisnike na mreži sumnjivima ovisno o njihovim akcijama. Ako algoritam detektira povećano slanje podataka s određenog računala što može indicirati na takozvani *beaconing* koji je vrsta maliciozne komunikacije sa serverom koja ima svrhu zagušivanja kako bi se kasnije izveo napad uskraćivanja usluge.

Nakon što je postavljena hipoteza analitičari koriste različite alate i tehnike kako bi analizirali kompletnu mrežu u svrhu pronalaska sigurnosnih manjkavosti ili propusta. Koriste se alati za analizu pojedinih računala na mreži poput alata Autoruns koji ustupa detaljan prikaz pokretačkih programa, pokrenutih procesa, instaliranih drivera i mnoštva drugih informacija o stanju računala što može ukazati da je analizirano računalo zaraženo malicioznim programom. Prilikom analize velikih količina podataka koji kolaju mrežom koriste se alati koji analiziraju količinu poslanih podataka unutar mreže te detekcijom anomalija može se primijetiti da postoji propust na mreži tj. da postoji kompromitirano računalo ili mreža. Nerijetko se koriste metode statističke analize kako bi se utvrdio standardna vrijednost parametara poput prosječne veličine datoteka koje cirkuliraju mrežom, a kasnije se pronašao uzorak odstupanja od tih veličina. Sve tehnike i alati korišteni u ovom koraku služe svrsi upoznavanja napadača odnosno njegovih taktika, tehnika i korištenih procedura.

Nakon pronalaska žrtve, odnosno kompromitiranog korisnika, zadatak lovaca je shvatiti uzorak napada. Nakon što se utvrde korištene tehnike, taktike i procedure lovci su dužni poduzeti mjere zaštite odnosno zaštiti organizaciju od eskalacije incidenta u problem provodeći analizu povezan podataka. Primjerice, ako je ustvrđeno da je određeni element mreže, korisnik, žrtva programa za iskorištavanje tada se treba zabilježiti taktike, tehnike i procedure koje su ga učinile žrtvom i zabilježiti ih i podijeliti kako bi se mogao izvesti adekvatna istraga pronalaska počinitelja.

Posljednji korak uspješnog lova je pohraniti slučaj zbog automatizacije lova u buduće svrhe. Korištene tehnike i metode koje su bile uspješne automatiziraju se pomoću raznih alata. Kompletan proces lova može se automatizirati kao skripta napisana u nekom programskom jeziku ili ustupiti podatke programu baziranom na strojnom učenju kako bi on u budućnosti mogao automatski prepoznati slične ili iste prijetnje.

3.3. Matrica lova

Nakon što smo shvatili kako različite organizacije pristupaju lovu na kibernetičke prijetnje i kako izgleda ciklus lova treba konstatirati kako se pojedinačne faze ciklusa izvode u organizacijama različitih razina spremnosti. SQRLL je kreirao matricu lova koja udružuje aktivnosti ciklusa lova s razinama različitih organizacija [6]. Tablica 1. u svojim redcima sadrži faze ciklusa lova, a u stupcima prethodno definiranih pet razina pristupa lovu u organizacijama.

Tablica 1: Matrica lova

	Inicijalna	Minimalna	Proceduralna	Inovativna	Vodeća
Prikupljanje podataka	Nepostojeća ili niska razina prikupljanja podataka	Osrednja razina prikupljanja nekih tipova podataka s ponekog ključnog izvora u IT okruženju	Visoka razina prikupljanja određenih tipova podataka u IT okruženju	Visoka razina prikupljanja određenih tipova podataka u IT okruženju	Visoka razina prikupljanja svih tipova podataka u IT okruženju
Kreacija hipoteze	Odaziv na postojeće automatizirane sisteme upozoravanja (Firewall, antivirusni programi)	Pregled obavještajnih podataka o prijetnjama za razvoj novih hipoteza	Pregled obavještajnih podataka o prijetnjama i prijateljskih obavještajnih podataka za razvoj novih hipoteza	Pregled obavještajnih podataka o prijetnjama, prijateljskih obavještajnih podataka i ručno ocjenjivanih kibernetičkih rizika za razvoj novih hipoteza	Pregled obavještajnih podataka o prijetnjama, prijateljskih obavještajnih podataka i automatski ocjenjivanih kibernetičkih rizika za razvoj novih hipoteza

Alati i tehnike za testiranje hipoteze	Konzole za uzbunjivanje; SIEM pretrage; Nema proaktivne istrage	Koristi SIEM ili alate za analizu zapisa za provođenje osnovne pretrage pomoću SQL upita ili teksa	Koristi jednostavne alate i histograme za pronalazak i analizu podataka temeljem postojećih procedura lova	Koristi vizualizacijske tehnike i grafikone. Razvija nove procedure lova	Koristi naprednu vizualizaciju i grafikone. Objavljuje i automatizira nove procedure lova.
Detekcija uzoraka i TTP	Nepostojeća	Identifikacija indikatora kompromisa na najnižim razinama mreže poput domena, URLa, i hasheva	Identifikacija indikatora kompromisa na najnižim i srednjim razinama mreže i mapiranje trendova za te indikatore kompromisa kroz vrijeme	U mogućnosti je detektirati napadačevih TTP-a i drugih indikatora kompromisa na svim razinama mreže	Automatizirano kompleksno otkrivanje TTP-a i kampanjski lov. Aktivno dijeljenje indikatora kompromisa s organizacijama za dijeljenje informacija
Analitička automatizacija	Nepostojeća	Integrira podatke o prijetnjama u automatizirano uzbunjivanje za osnovno podudaranje	Izgradnja biblioteke učinkovitih procedura lova i izvodi ih po redovitom rasporedu	U mogućnosti je detektirati napadačevih TTP-a i drugih indikatora kompromisa na svim razinama mreže	Automatizacija efikasnih procedura lova kako bi se konstantno unapređivao sistem uzbunjivanja; Napredna razina znanja o podatcima (strojno učenje)

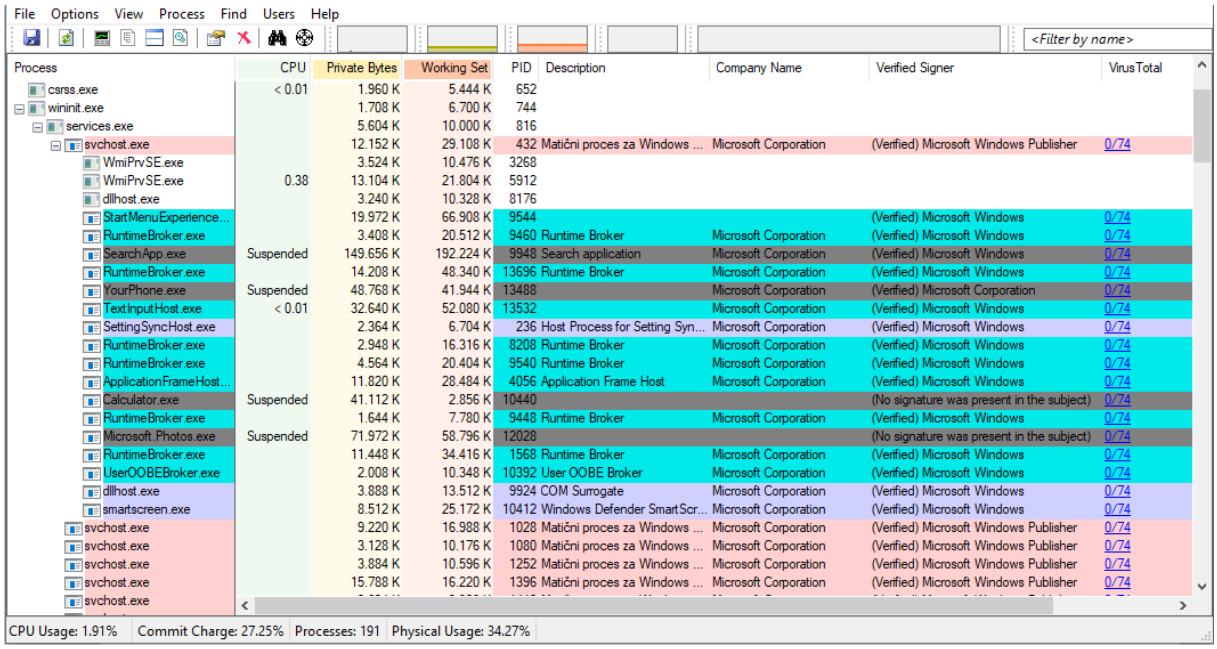
(Izvor: SQRLL, 2022)

4. Sysinternals, alati za lov na prijetnje

Sysinternals je skupina alata koju je razvio Mark Russinovich pod okriljem Microsofta 1996. godine za kompletnu tehničku analizu sustava. Alati su raznih namjena i funkcionalnosti kao što je analiza pokrenutih i pokretačkih programa, stanja memorije i mrežnih aktivnosti te alata za opterećivanje sustava u svrhu pronalaska oštećenja. U ovom radu koristi se alat Autoruns za analizu pokretačkih i pokrenutih programa i registara. Alat Autoruns koristi se u kombinaciji s Process Explorer alatom koji prikazuje sve pokrenute procese kao i količinu korištenih resursa. Alat RamMap koristi se za analizu rada RAM memorije odnosno memorije s nasumičnim pristupom, a alat TCPView koristi se za analizu mrežnog prometa. Svi od navedenih alata koriste se u prepoznavanju i lovu na prijetnje računalnim sustavima. Sysinternals sadrži još mnoštvo drugih alata koji nisu od velikog značaja za lov na kibernetičke prijetnje [7].

4.1. Process Explorer alat za analizu pokrenutih procesa

Programsko rješenje Process Explorer prikazuje sve pokrenute procese i njihove dretve s numeričkim vrijednostima potrošnje procesorske snage. Alat pokrenute procese označava bojama radi provođenja lakše analize. Na slici 2. prikazan je alat Process Explorer. Roza bojom označeni su procesi koji su usluge tj. pokrenuo ih je operacijski sustav, dok su ljubičastom označeni procesi koje je pokrenuo korisnik. Sivom bojom se označavaju suspendirani procesi, crvenom bojom procesi koji se gase, a zelenom nedavno započeti procesi.



Slika 2.: Prikaz alata ProcessExplorer (Izvor: Nikša Mirković, 2022)

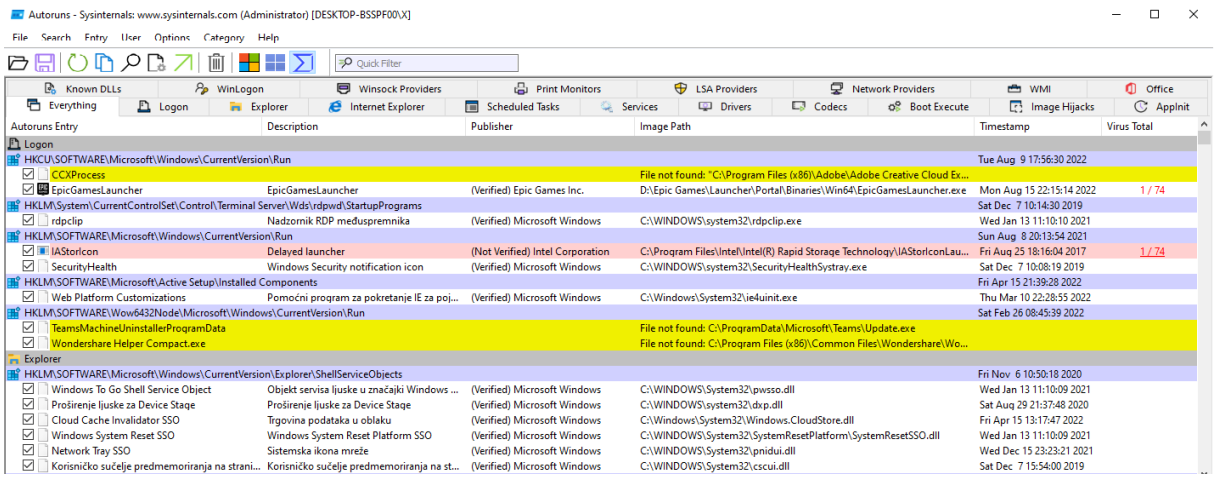
Prilikom analize procesa u svrhu pronalaska prijetnje treba obratiti pozornost na potrošnju resursa centralne procesorske jedinice. Ustvrdi li se da određeni proces troši previše resursa to može biti indikator zamaskiranog malicioznog programa. Alat prikazuje da li je pokrenuti proces verificiran. Zlonamjerni programi neće imati verificiran digitalni potpis i kao takvi će se jasno razlikovati od drugih verificiranih programa. Ako se pronađe sumnjivi proces duplim klikom na njega otvara se prozor za detaljan pregled karakteristika tog procesa. Unutar kategorije Strings i označavanjem kućice Memory otvorit će se prozor sa svim tekstualnim zapisima tog procesa. Na ovaj način mogu se pronaći svi meta podatci o kreatoru procesa i najčešće će se analizom tih zapisa utvrditi da li je riječ o zlonamjernom programu koji se predstavlja kao legitiman program jer meta podatci neće upućivati na službene stranice proizvođača legitimnog programa navodi Mark Russinovich u svome predavanju [8]. ProcessExplorer ima i funkcionalan prikaz aktualnih prijetnji vezanih uz specifični proces provjerom baze prijetnji VirusTotal kompanije.

Nakon pronalaska procesa koji je potencijalno opasan preporuka je da se najprije suspendira isti prije terminiranja kako bi se spriječilo repliciranje ili ponovno pokretanje.

4.2. Autoruns alat za izmjenu pokretačkih programa

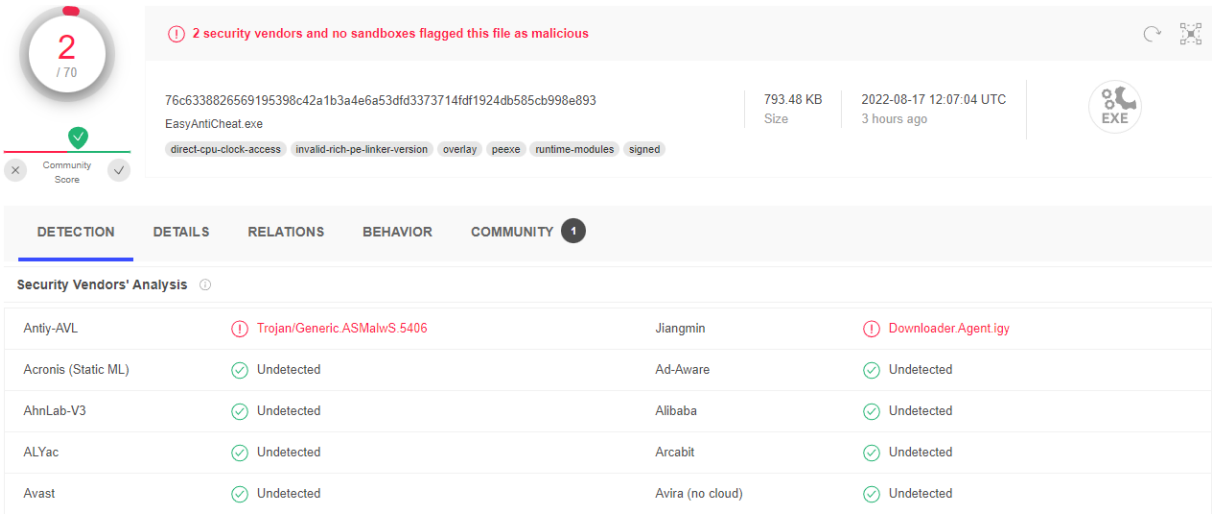
Jedan od alata kojim se lovci svakodnevno koriste zove se Autoruns. Ovaj alat vrši provjeru svih pokretačkih i pokrenutih programa njihovih procesa, usluga i popratnih dinamički povezanih biblioteka. Alat prikazuje sve zapise registra. Alat nakon provjere spomenutih

elemenata vrši provjeru sigurnosti koja je povezana s bazom podataka tvrtke Virus Total. Nakon provjere prikazuje rezultate i označava eventualne prijetnje crvenom i žutom bojom. Žutom bojom označeni su zapisi koji nemaju unesene valjanje putanje. Ako alat pronađe registarski zapis koji se odnosi na program koji je uklonjen s računala tada će taj zapis u alatu biti označen žutom bojom i takvi zapisi predstavljaju nisku razinu opasnosti od prijetnje. Zapisi označeni crvenom bojom označavaju zapise koje predstavljaju značajan problem ili propust jer nije uspješno izvršena verifikacija zapisa ili autora, kompanije koja je kreirala zapis i ukazuju na mogućnost izvora prijetnje. Dobra praksa nalaže da se u takvim slučajevima provjeri autentičnost autora procesa, dinamički povezanih biblioteka ili registarskog zapisa kao i sami zapis te se utvrdi kolika je razina opasnog utjecaja u budućnosti [9].



Slika 3: Rad u alatu Autoruns (Izvor: Nikša Mirković, 2022)

Prilikom provjere alat svaki od pronađenih zapisa uspoređuje s bazom svih prijetnji i traži podudaranja, a ako prijetnju i pronađe tada se pokraj zapisa brojčanom oznakom prikaže koliko je istih pronađeno. Klikom na brojčanu oznaku otvara se web stranica Virus Total servisa za specifičnu prijetnju. Virus Total je kompanija koja se bavi širokim spektrom aktivnosti u sferi kibernetičke sigurnosti. Jedan od njihovih servisa je i baza podataka prijetnji koja nastaje slanjem izvješća raznih kompanija koje se bave kibernetičkom sigurnošću. Na slici 4 prikazana je analiza sigurnosnih kompanija i njihovih alata za pokrenuti proces EasyAntiCheat.exe jer je alat Autoruns pronašao dvije sigurnosne prijetnje za spomenuti proces.

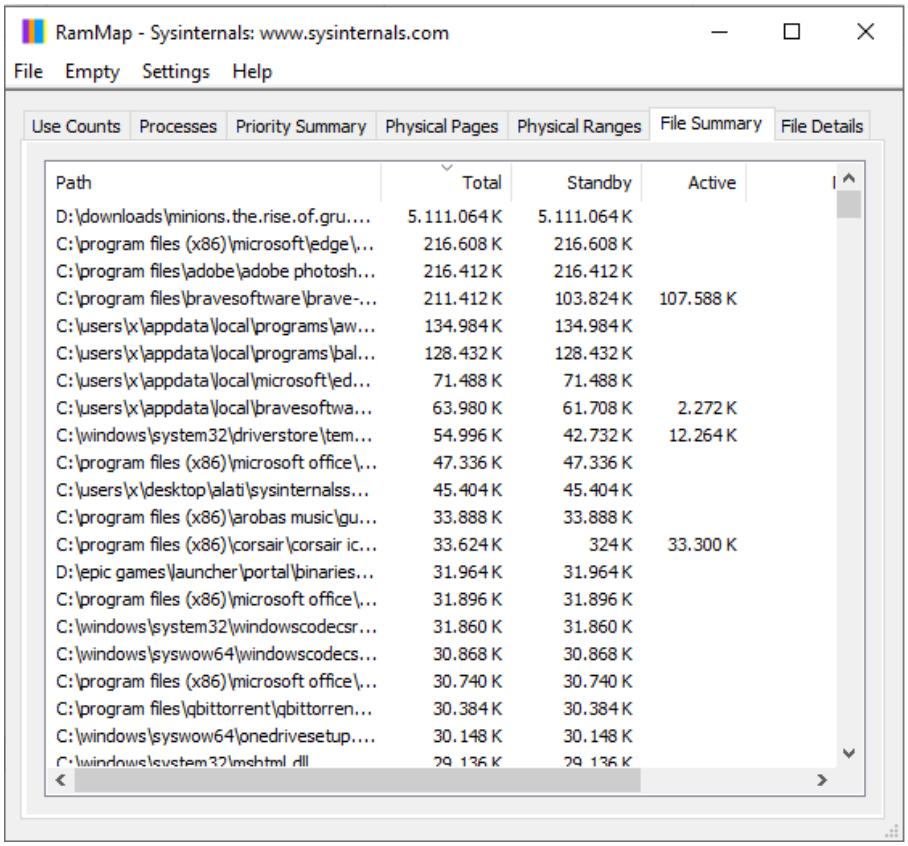


Slika 4: Virus Total analiza EasyAntiCheat.exe procesa (Izvor: TotalVirus, 2022)

Na slici je vidljivo da je alat kompanije Antiy-AVL nad spomenutim procesom pronašao računalni virus Trojan/Generic.ASMalwS.5406 i Downloader.Agent.igy zlonamjerni program koji neovlašteno šalje podatke iz memorije. Ovaj pronalazak ne mora nužno biti alarmantan jer postoji mogućnost i lažno pozitivnih prijetnji. Prije donošenja zaključka trebalo bi utvrditi kredibilitet kompanije koja je proizvela pokrenuti proces. EasyAntiCheat je program za pronalazak igrača koji varaju, renomiranog proizvođača, čije usluge se često koriste u industriji video igara. Samim time može se pretpostaviti kako je korisnik želeći zaobići program protiv varanja ubacujući eksterne dll datoteke koje su bile zaražene računalnim virusom i zlonamjernim programom pokrenuo vlastiti antivirusni program koji je poslao izvješće VirusTotal bazi podataka da je proces EasyAntiCheat kompromitirajući. Na ovom primjeru može se vidjeti i važnost poznavanja žrtve i njezinih navika. Najčešće mete hakera, izuzev starijih osoba, su i pojedinci koji uživaju u natjecateljskim video igrama jer često pokušavaju ostvariti prednost nad konkurencijom pomoću programa za varanje. Upravo takvi programi često prenose viruse koji mogu biti prijetnje sustavima. Kratkom analizom pronađenih prijetnji također potvrđuje prijašnje navedeni scenarij. Računalni virus Trojanskog konja odnosi se na karakteristiku skupine virusa koji su sakriveni unutar naizgled bezazlenih programa i podataka a imaju mogućnost preuzimanja kontrole nad računalom poput kontrole perifernih uređaja pa sve do kontrole podataka s diska zaraženog računala. Zlonamjerni program Downloader.Agent, iz velike familije računalnih virusa tipa trojanski konj [10], zadužen je za skriveno slanje podataka počinitelju bez žrtvinog znanja. Upravo zbog kombinacije navedenih prijetnji shvaćamo širu sliku kako je došlo do ovog zapisa tj. pronalaska prijetnji u inače sigurnom programu.

4.3. RamMap alat za analizu RAM memorije

RamMap je alat koji analizira stanje RAM memorije. Osim pregleda integriteta RAM memorije alat prikazuje koliko su resursa specifični procesi koristili. Alat pruža uvid u trenutno korištenje memorije za svaki pojedini proces kao i ukupno dodijeljene resurse od početka sesije [11]. Na slici 5 prikazano je koji program odnosno datoteka koristila najviše memorije kao i koliko trenutno koriste memorije.



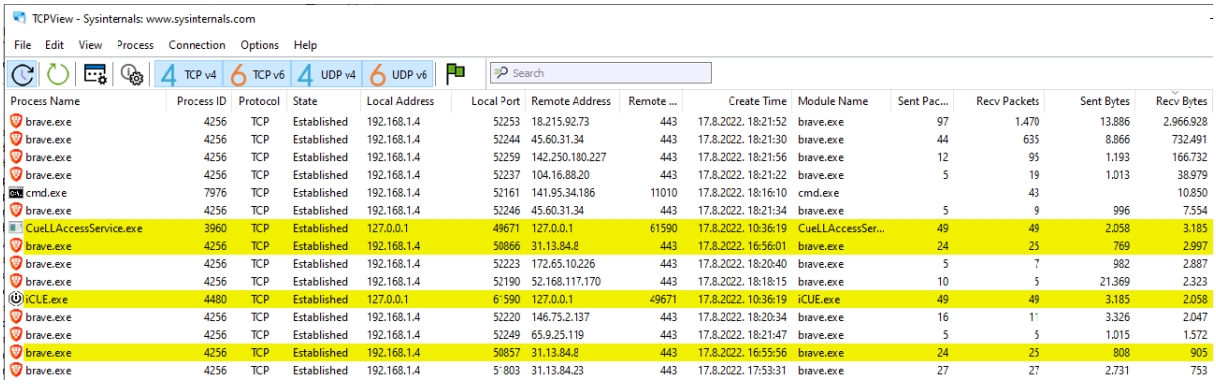
Slika 5: RamMap prikaz korištenja RAM memorije (Izvor: Nikša Mirković, 2022)

Vidljivo je da u ovoj sesiji RAM memorije najviše konzumirala video datoteka naziva minions.the.rise.of.gru koja iznosi nešto više od 5GB memorije. Ovaj alat se može koristiti za pronalazak prijetnji tako da se pronađe program ili datoteka koji konzumiraju velike količine RAM memorije što može ukazati na neovlašteno korištenje računalnih resursa što je karakteristično za programe koji rudare kripto valute. U posljednje vrijeme svjedoci smo kako su upravo napadi bazirani na memoriji najopasniji i najteže ih je detektirati jer se mogu izvesti bez računalnim virusom zaraženih datoteka. SecurityIntelligence navodi kako greške u programskom kodu mogu uzrokovati prekoračenje međuspremnika i tako izazvati kritičnu grešku koja zaobilazi autentikaciju korisnika i napadaču ustupa povjerljive podatke [12]. Slično

kako napad SQL injekcije nad bazom ustupa napadaču podatke zbog upita nad bazom tako i preopterećenje memorije uruši modul za prijavu korisnika koji napadaču omogućuje neovlašteni pristup podatcima.

4.4. TCPView alat za mrežnu analizu

Alat TCPView prikazuje količinu poslanih i primljenih podataka s mreže za svaki od procesa koji komunicira na mreži [13]. Alat ispisuje odredišne IP adrese, lokalne i udaljene portove te količinu poslanih i primljenih paketa kao što je vidljivo na slici 6.



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote ...	Create Time	Module Name	Sent Pac...	Recv Packets	Sent Bytes	Recv Bytes
brave.exe	4256	TCP	Established	192.168.1.4	52253	18.215.92.73	443	17.8.2022. 18:21:52	brave.exe	97	1.470	13.886	2.966.928
brave.exe	4256	TCP	Established	192.168.1.4	52244	45.60.31.34	443	17.8.2022. 18:21:30	brave.exe	44	635	8.866	732.491
brave.exe	4256	TCP	Established	192.168.1.4	52259	142.250.180.227	443	17.8.2022. 18:21:56	brave.exe	12	95	1.193	166.732
brave.exe	4256	TCP	Established	192.168.1.4	52237	104.16.88.20	443	17.8.2022. 18:21:22	brave.exe	5	19	1.013	38.979
cmd.exe	7976	TCP	Established	192.168.1.4	52161	141.95.34.186	11010	17.8.2022. 18:16:10	cmd.exe		43		10.850
brave.exe	4256	TCP	Established	192.168.1.4	52246	45.60.31.34	443	17.8.2022. 18:21:34	brave.exe	5	9	996	7.554
CueLLAccessService.exe	3960	TCP	Established	127.0.0.1	49671	127.0.0.1	61590	17.8.2022. 10:36:19	CueLLAccessSer...	49	49	2.058	3.185
brave.exe	4256	TCP	Established	192.168.1.4	50866	31.13.84.8	443	17.8.2022. 16:56:01	brave.exe	24	25	769	2.997
brave.exe	4256	TCP	Established	192.168.1.4	52223	172.65.10.226	443	17.8.2022. 18:20:40	brave.exe	5	7	982	2.887
brave.exe	4256	TCP	Established	192.168.1.4	52190	52.168.117.170	443	17.8.2022. 18:18:15	brave.exe	10	5	21.369	2.323
iCUE.exe	4480	TCP	Established	127.0.0.1	6`590	127.0.0.1	49671	17.8.2022. 10:36:19	iCUE.exe	49	49	3.185	2.058
brave.exe	4256	TCP	Established	192.168.1.4	52220	146.75.2.137	443	17.8.2022. 18:20:34	brave.exe	16	11	3.326	2.047
brave.exe	4256	TCP	Established	192.168.1.4	52249	65.9.25.119	443	17.8.2022. 18:21:47	brave.exe	5	5	1.015	1.572
brave.exe	4256	TCP	Established	192.168.1.4	50857	31.13.84.8	443	17.8.2022. 16:55:56	brave.exe	24	25	808	905
brave.exe	4256	TCP	Established	192.168.1.4	5`803	31.13.84.23	443	17.8.2022. 17:53:31	brave.exe	27	27	2.731	753

Slika 6: TCPView alat (Izvor: Nikša Mirković, 2022)

Korištenjem ovog alata možemo doznati da li neki od pokrenutih programa šalje ili prima više podataka od očekivanog. Ako se ustvrdi da određeni proces šalje iznadprosječno više podataka nego što je to uobičajeno tada se treba provjeriti na koju destinaciju se šalju ti podatci i koji podatci se točno šalju. Kako bi se doznalo koji podatci se šalju tada se za analizu paketa koji se šalju preko mreže treba koristiti neki od alata za analizu paketa poput WireSharka. Ako počinitelj kibernetičkog napada nije vješt tada pomoću TCPView alata možemo doznati na koju se IP adresu šalju podatci te doznati lokaciju počinitelja.

5. Windows alati kao alati uspješnog lova

Operacijski sustavi Windows sadrži dva alata koja se mogu koristiti za lov na kibernetičke prijetnje. Prvi alat je dnevnik događaja koji bilježi razne događaje koji su se dogodili nad sustavom prilikom korištenja. Drugi alat je uređivač registara koji prikazuje i pruža mogućnost mijenjanja registara za pripadne im programe. Registri sadrže niz uputa za izvođenje programa i analizom tih registara može se pronaći prijetnja sustavu.

5.1. Dnevnik događaja

Gotovo svaka promjena, akcija i njezin rezultat na računalu koja komunicira s operacijskim sustavom bilježi se kao zasebni događaj u dnevniku događaja. U dnevnik događaja bilježe se informacije o operacijama bitnima za pokretanje sustava kao što su manipulacije nad korisnicima te same prijave korisnika u sustav. Tu se nalaze zapisi o instalaciji, brisanju programa kao i akcijama provedenima nad sustavom od strane tih programa. U logovima se mogu naći i ključne sigurnosne promjene učinjene nad sustavom kao i greške sustava prilikom rada. Iako su zapisi prvenstveno osmišljeni kao alat za dijagnostiku pogrešaka pokazalo se kao jedan od ključnih alata računalnih analitičara.

Zapisi se pohranjuju u %SystemRoot%\System32\winevt\logs datoteci i prepoznaju se po „.evtx“ ekstenziji koja označava binarni XML format Windows prijave događaja [14].

Za pregled logova tvrtka Microsoft proizvela je alat preglednik događaja koji je ugrađen u sustav prilikom instalacije. U prethodnim verzijama Windows operacijskih sustava, sve do verzije Windows 8, broj dnevnika bio je znatno manji nego u novijim inačicama operacijskog sustava Windows koji broje preko 320 dnevnika. Alat je podijeljen u tri panela. Lijevi panel sadrži hijerarhijski ispisane dnevnike, središnji panel unose u dnevnik kao i informacije o njima, a desni panel sadrži razne funkcijske gumbe koji služe lakšoj navigaciji i uređivanju dnevnika. Svaki događaj zabilježen u dnevnik sadrži entitet razine koja ukazuje kakav je tip događaja. Događaj može biti informacija, pogreška ili upozorenje. Sadrži još entitete vremena i nadnevka u kojemu se događaj zbio, izvora koji je događaj generirao, identifikacijskog broja događaja te kategorije događaja koja pobliže opisuje sami događaj.

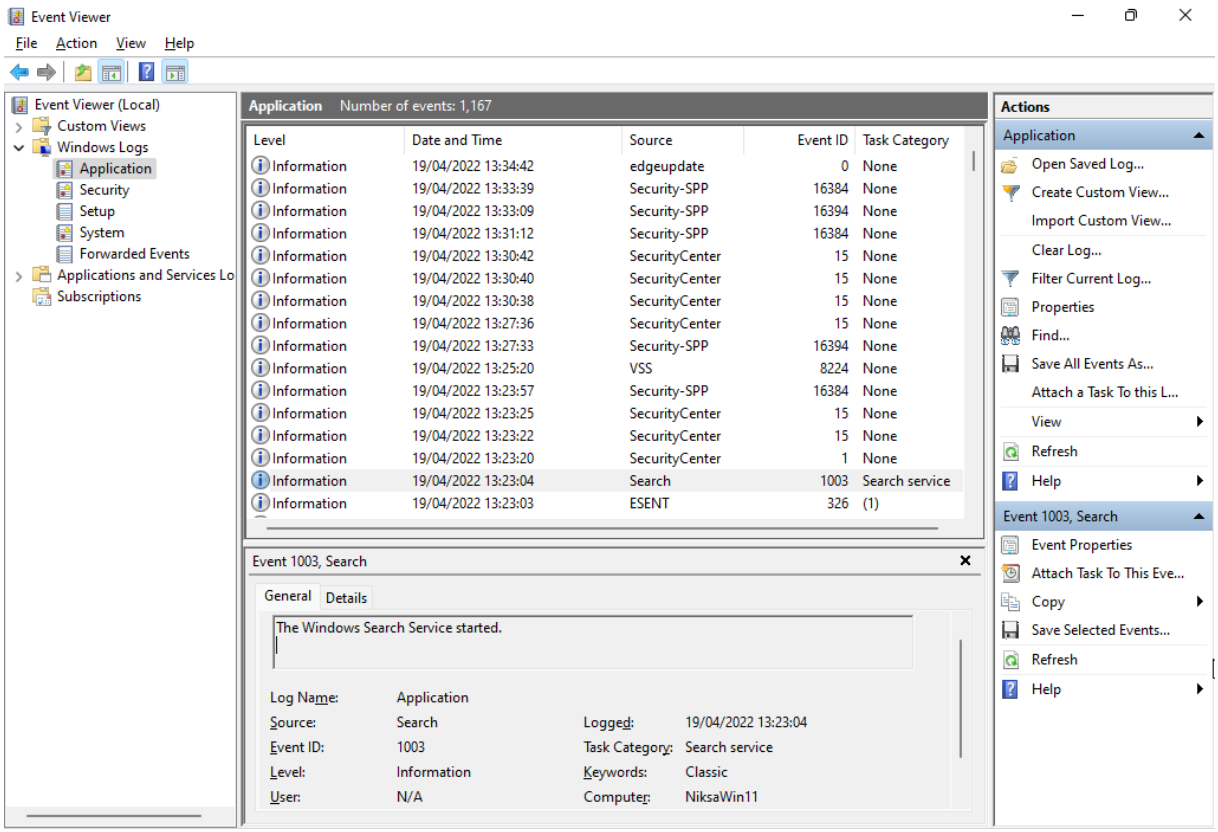
Za potrebe analize sigurnosti sustava i lova na prijetnje dnevnici koji sadrže najviše informacija tj. artefakata bitnih za pronalazak prijetnje su dnevnik Windows logova koji sadrži artefakte o radnjama operacijskog sustava i sastoji se od dnevnika aplikacija, sigurnosti i sustava. Zapisi Windows vatrozida, Windows Defender aktivnosti, posljednji događaji, aktivnost bežičnih uređaja, zapisnik vanjskih uređaja, planer zadataka, udaljenog desktopa te brisanja zapisa događaja sadržani su u kategoriji zapisa aplikacija i usluga.

5.1.1. Windows zapisi visoke važnosti za sigurnost računala

Unutar Windows zapisa nalaze se informacije o događajima koje je kreirao operacijski sustav ili korisnik i vezani su uz sam operacijski sustav.

U dnevnik aplikacija bilježe se događaji koji sadrže informacije o programima koji su u sklopu operacijskog sustava ili potprogrami operacijskog sustava. Unutar ovih dnevnika može se doznati da li je i kada korisnik koristio specifične programe i radnje i u koje vrijeme ih je

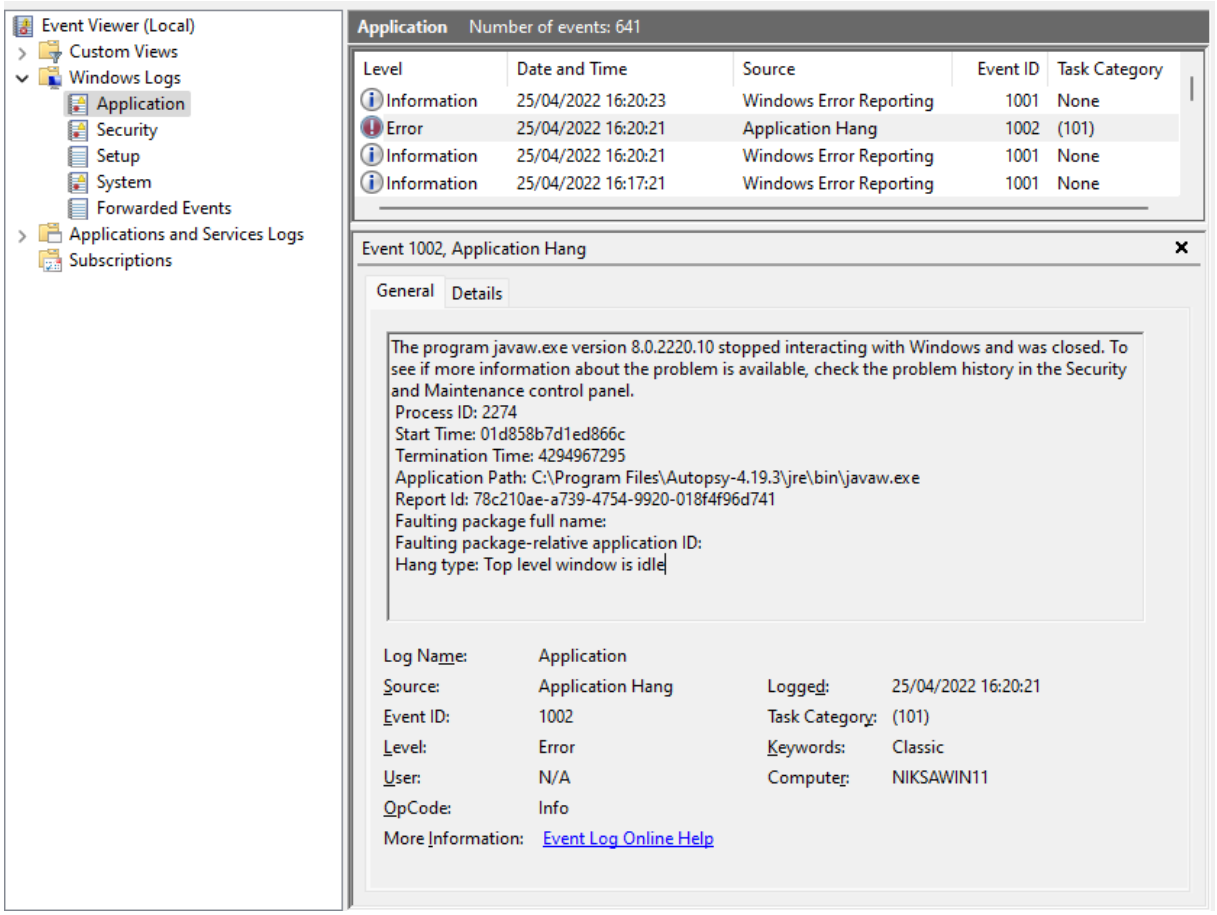
učinio. Na sljedećoj slici, slika 7., prikazan je događaj pokretanja tražilice sustava te pokretanja potprograma zaduženog za sigurnost operacijskog sustava sigurnosnog centra. Sigurnosni centar i tražilica su potprogrami operacijskog sustava, stoga su akcije učinjene nad i unutar njih zabilježene pripadajućim identifikacijskim oznakama i vremenskim zapisima i opisima. Na slici je vidljivo da se je 19.04.2022. godine u 13:23:04 sati zbio događaj pokretanja Windows Search Service koji sadrži identifikacijski kod 1003 izvorište Search te kategoriju zadatka Search service. U opisu je pobliže opisan sami događaj kao i prijavljeni korisnik koji je pokrenuo događaj.



Slika 7.: Događaj pokretanja tražilice sustava (Izvor: Nikša Mirković, 2022)

Nakon ovog događaja, u 13:23:20 sati pokrenut je potprogram Windows sigurnosni centar koji sadrži identifikacijsku oznaku 1 koja označava pokretanje potprograma za kojim slijede potvrde uspješnog pokretanja označene oznakom 15. U ovom primjeru može se vidjeti kako se pomoću zapisa događaja mogu potvrditi, dokazati, određene radnje učinjene nad sustavom. Unutar aplikacijske kategorije mogu se vidjeti i greške i upozorenja koja mogu ukazivati upotrebu zabranjenih programa ili zabranjenih radnji. U sljedećem primjeru, slika 8., vidi se kako se programa javaw.exe, program za pokretanje aplikacija napisanih u programskom jeziku Java kao što je Autopsy, prisilno zaustavio. U ovom primjeru pomoću

upravitelja zadataka prisilno se zaustavio rad programa Autopsy što je zabilježeno unutar aplikacijskih dnevnika. Na slici se vidi kako se dogodila pogreška, točnije Application Hang identifikacijske oznake 1002 u kojemu je program javaw.exe iznenada prekinuo s radom u koje vrijeme te koji je bio identifikacijski broj samog procesa.



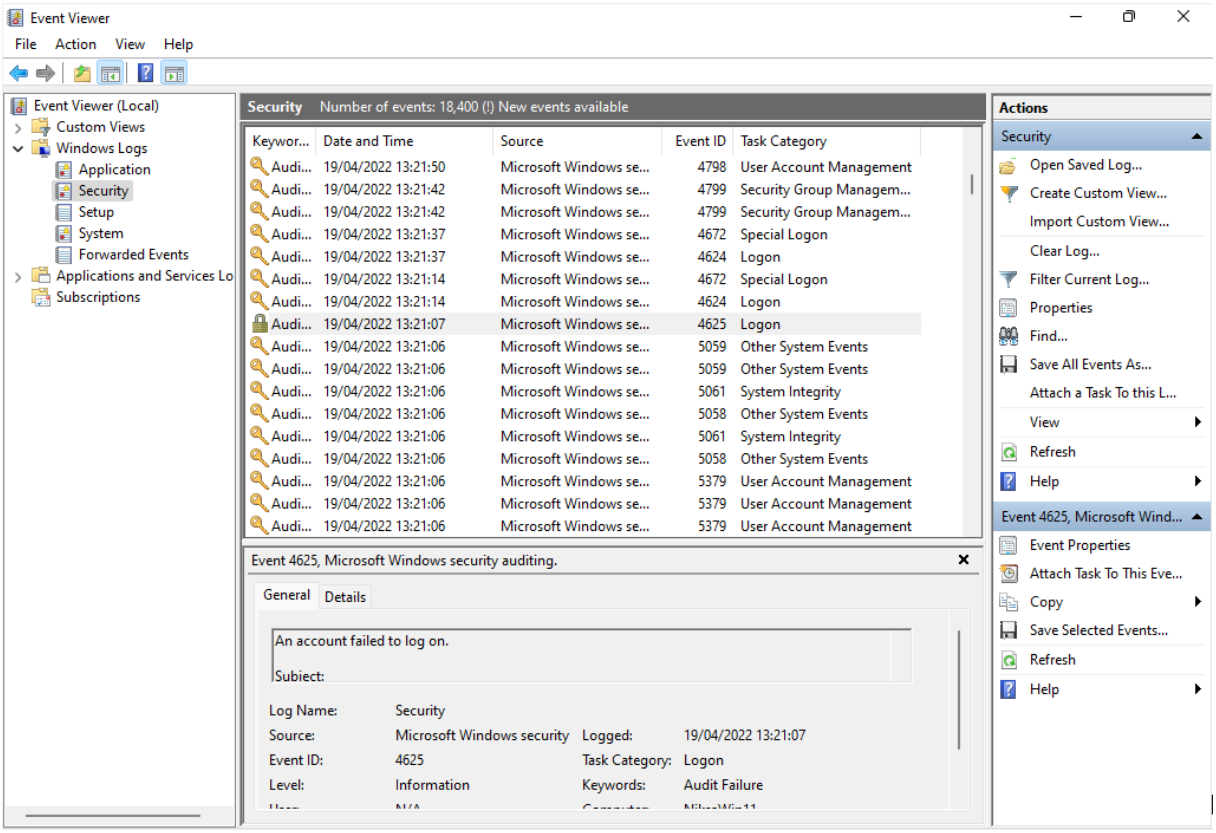
Slika 8.: Slika prisilnog gašenja programa javaw.exe (Izvor: Nikša Mirković, 2022)

Aplikacijski dnevnici sadrže nekoliko ključnih oznaka koje mogu ukazivati na nedozvoljene aktivnosti. Neke od tih oznaka su:

- 1000 – Greška aplikacije
- 1002 – Prestanak rada aplikacije
- 1001 – Plavi ekran smrti; izvještaj Windows pogrešaka

Unutar kategorije sigurnost nalaze se dnevnici u koje su zapisani događaji vezani uz korisnike tj. kreacije i promjene učinjene nad korisničkim računima. Ovi zapisi sadrže informacije o uspješnim i neuspješnim prijavama u sustav koje mogu ukazivati na krađu identiteta odnosno dokazati da je računalo koristila druga osoba ili da je korištena takozvana

metoda sirove snage za prijavu na korisnički račun. Na slici 9. prikazan je događaj koji bilježi pokušaj prijave u sustav s pogrešnom lozinkom nakon kojega slijedi prijava u sustav s ispravnom lozinkom.



Slika 9.: Događaj neuspjele prijave u sustav (Izvor: Nikša Mirković, 2022)

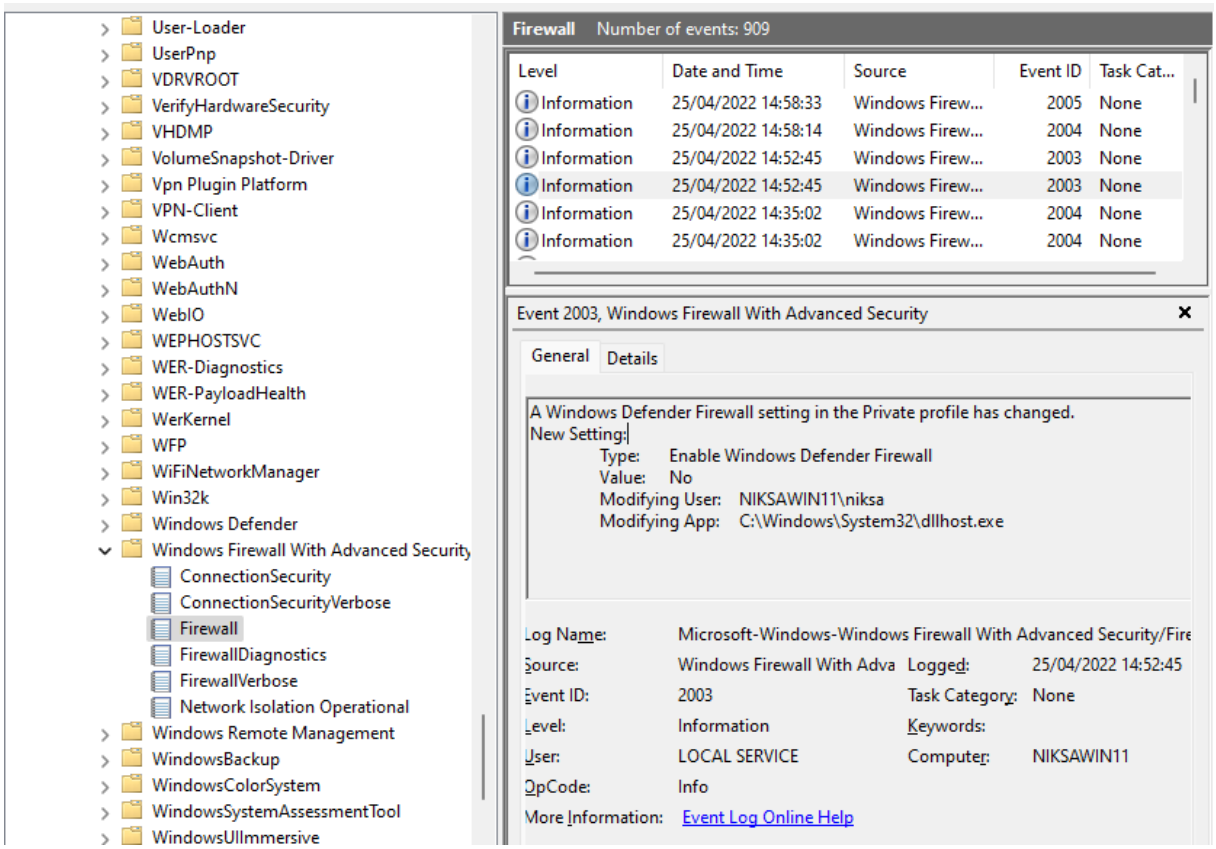
Slika prikazuje događaj oznake 4625 koji se dogodio u 13:21:07 sati i u opisu piše da je došlo do neuspješne prijave u sustav. Iznad ovog događaja nalazi se događaj 4624 koji označava uspješnu prijavu u sustav. Opis događaja sadrži informacije koje pobliže označavaju događaj poput informacije da li je pokušaj prijave bio proveden s mreže i ako je s kojim ovlastima je korisnik pristupio. Unutar sigurnosnih dnevnika bitno je znati nekoliko vrsta oznaka:

- 4740 – Račun zaključan
- 4728, 4732, 4756 – Korisnik dodan u grupu s privilegijama
- 4735 – Omogućene sigurnosne modifikacije grupe
- 4624 – Uspješna prijava korisnika na račun
- 4648 – Prijava na račun s eksplicitnim podatcima

Kategorija dnevnika sustava sadrži zapise o promjenama i akcijama nad operacijskim sustavom i bitnim mu značajkama. Ovdje se mogu pronaći zapisi o stanjima ažuriranja operacijskog sustava, statusu promjena u radu centralne procesorske jedinice kao i informacije o promjenama na mrežnim uređajima. U ovim logovima može se pronaći u koje vrijeme i s kojim parametrima su pokrenuti razni mrežni protokoli poput DHCPv6 (*eng. Dynamic Host Configuration Protocol version 6*) što ukazuje da je računalo bilo domaćin ili gost pripadajuće mreže. Sukladno tome mogu se pronaći zapisi o uspostavi ili isteku DNS-a (*eng. Domain Name System*) imena što može dokazivati postojanje korisnika na određenoj mreži. Unutar sistemske kategorije nalaze se zapisi o zahtjevima za resetiranjem sustava. Unutar opisa takvog događaja opisan je razlog za zahtjevom resetiranja sustava kao i izvor zahtjeva koji može biti korisnički ili aplikacijski. Aplikacijski zahtjev za resetiranjem sustava može ukazivati na neovlašteno korištenje računala ili krađu identiteta.

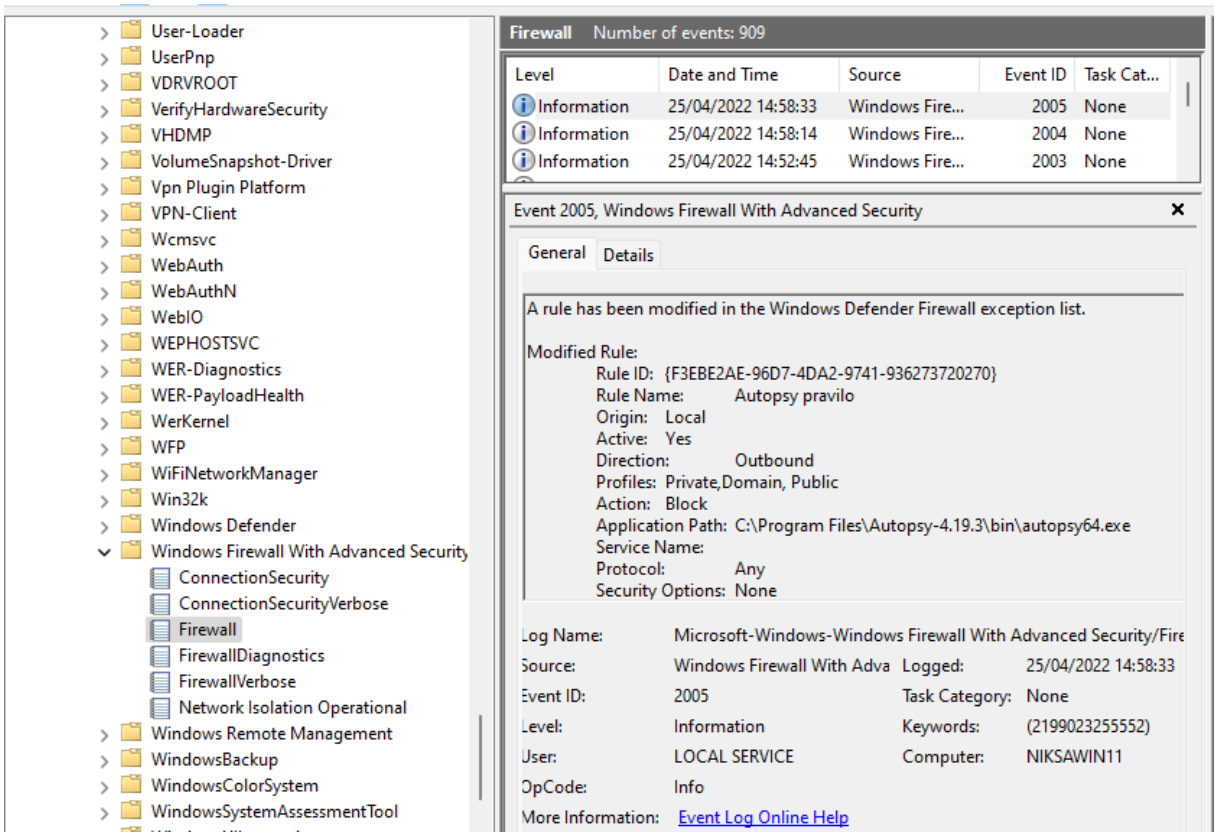
5.1.2. Zapisi aplikacija i usluga

Unutar kategorije zapisa o aplikacijama i uslugama nalaze se dnevnici koji ukazuju na aktivnosti Windows potprograma i usluga. Unutar potkategorije Microsoft, zatim potkategorije Windows, nalazi se pozamašan popis svih usluga i potprograma operacijskog sustava koji nisu od ključne važnosti za rad samog operacijskog sustava, ali mogu sadržavati mnoštvo informacija tj. artefakata potrebnih za pronalazak prijetnje. Jedan od važnijih je skup dnevnika udaljenog pristupa u kojemu se mogu naći artefakti koji mogu ukazivati na kibernetički napad mrežne krađe identiteta. Ako VPN-Client direktori sadrži zapise o postojanju virtualne privatne mreže što može ukazivati na potrebu maskiranja identiteta počinitelja. Skup dnevnika izrazite važnosti su zapisi o aktivnostima Windows vatrozida. U ovim dnevnicima mogu se naći artefakti koji ukazuju na promjene u načinu rada vatrozida čija je primarna funkcija zaštita korisnika od malicioznih radnji na mrežama i od lokalno instaliranih programa. Na sljedećoj slici prikazan je događaj isključivanja Windows vatrozida označen identifikacijskom oznakom 2003 i promjenom vrijednosti u „ne“ što označuje isključivanje privatnih postavki vatrozida.



Slika 10.: Događaj promjene postavki Windows vatrozida (Izvor: Nikša Mirković, 2022)

Događaj nakon isključivanja privatnih postavki odnosi se na događaj isključivanja vatrozida javnih postavki i sadrži identičan identifikacijski broj. Događajem oznake 2004 označeno je dodavanje iznimke za program Autopsy koja uključuje vatrozid za spomenuti program, a događajem 2005 vrši se promjena nad tom iznimkom tj. isključuje se provjera vatrozida nad programom Autopsy kao što je prikazano na slici 11. akcijom blokiranja.



Slika 11.: Događaj izmjene postavki vatrozida za aplikaciju Autopsy (Izvor: Nikša Mirković, 2022)

Najvažnije identifikacijske oznake unutar Windows vatrozid dnevnika koje mogu ukazivati na kriminalne radnje su:

- 2004 – Dodavanje pravila u Windows vatrozid
- 2005 – Promjena pravila u Windows vatrozidu
- 2006, 2033 – Brisanje pravila u Windows vatrozidu
- 2009 – Vatrozid nije uspio učitati grupnu politiku

Windows Defender kategorija sadrži zapise o provedenim aktivnostima potprograma Windows Defender koji je svojevrsni antivirusni program ugrađen u operacijske sustave Windows. Ovi zapisi mogu sadržavati informacije ako je Windows Defender detektirao određenu prijetnju ili računalni virus.

5.2. Manipulacije zapisima događaja

Iako su zapisi događaja provedenim nad računalom dobar izvor informacija o malicioznim radnjama provedenim na računalu one ipak nisu finalni korak lova na kibernetičke prijetnje. Zapisi se mogu mijenjati i sofisticirani računalni virusi iznimno lako mogu izmijeniti vrijednosti zapisa pa čak ih i brisati i tako prikriti svoju prisutnost na računalu.

Osim brisanja i mijenjanja zapisa događaja računalni virusi mogu na razne načine onemogućiti zapisivanje novih događaja. Najjednostavniji način blokiranja zapisivanja novih događaja je kreacijom novog registarskog unosa HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\MiniNt [15]. Iako je ovo računalna greška operacijskog sustava koja još nije ispravljena računalni virusi mogu pokrenuti skriptu koja bi otvorila naredbeni redak i kreirala spomenuti registarski zapis pomoću „reg add“ naredbe brže nego što korisnik može primijetiti što se dogodilo. Drugi način blokiranja kreacije novih zapisa događaja podrazumijeva blokiranjem dretvi zaduženih za pravilan rad zapisa događaja unutar svchost.exe procesa. Iako je druga metoda kompliciranija zbog terminiranja ključnih dretvi otvorena je mogućnost brisanja postojećih zapisa događaja bez generiranja sigurnosnog indikatora 1102 koji označava brisanje zapisa. Izvor [15] navodi da se pomoću PhantOm skripte za PowerShell naredbeni redak može terminirati dretve 1616, 1780, 1784, 1788 i 1808 te tako onesposobiti rad zapisnika događaja i zaobići generiranje 1102 indikatora.

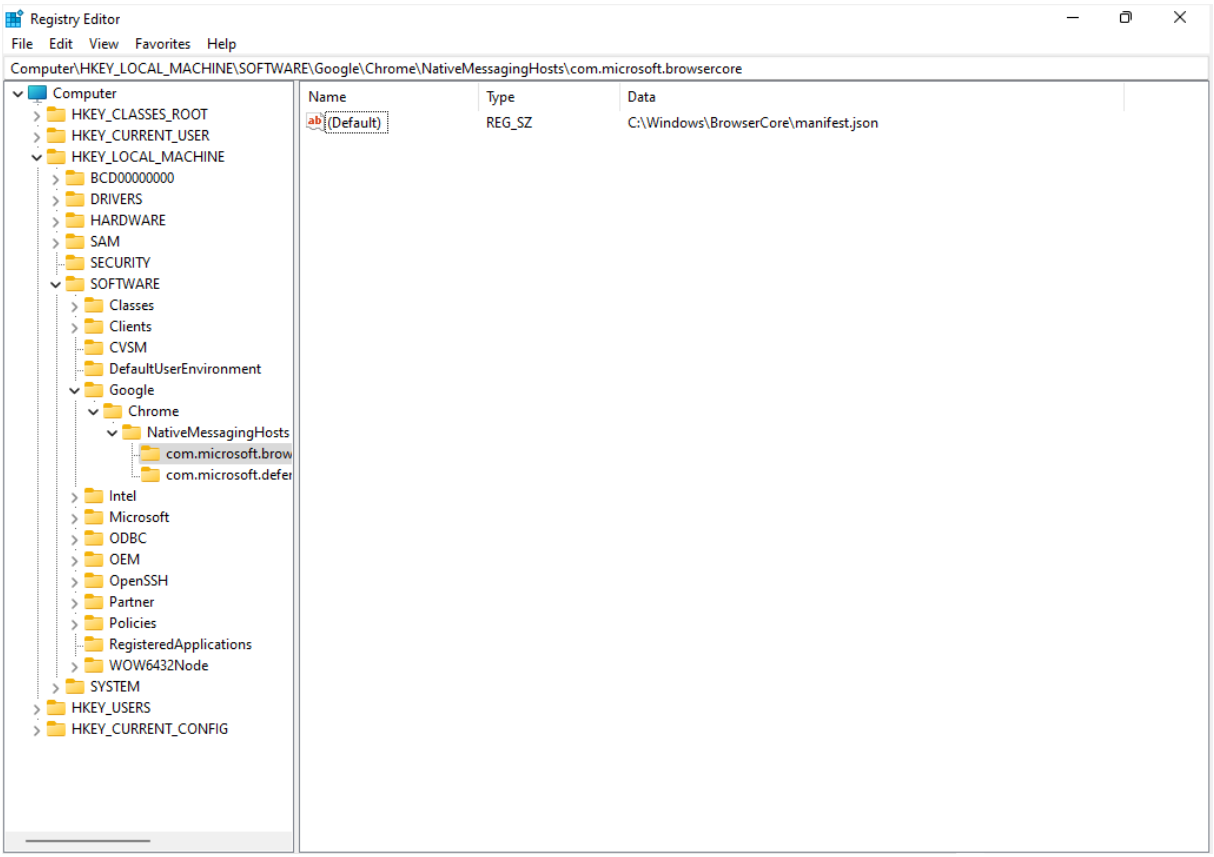
Kako bi se napravile izmjene nad postojećim zapisima događaja potrebno je razumjeti kako se zapisi pohranjuju. Svaki zapis događaja sastoji se od kontrolnog polja zaglavlja datoteke, zaglavlja bloka te zapisa događaja. Kontrolna polja postoje kako bi se osigurao integritet samih zapisa ali i otežale izmjene zapisa događaja [16]. Najprije je potrebno onesposobiti već spomenute dretve kako bi se izbjegao indikator izmjene zapisa. Upotrebom alata za manipulaciju heksadecimalnog zapisa datoteke poput WinHex ili HxD prave se izmjene nad zapisom događaja. Potrebno je napraviti adekvatne izmjene nad sva tri kontrolna polja kako bi se izbjegla korupcija izmijenjenog događaja. Kao primjer izmjene autor [16] napravi izmjenu vrijednosti imena računala na kojemu se događaj dogodio. Izmjene ovog tipa mogu se dokazati pomoću provjere registarskog zapisa na lokaciji HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\IPSec\Policy\Local. Ako je vrijednost tog zapisa nije prazna tada znamo da su mijenjani zapisi događaja [16].

5.3. Windows registri kao sredstvo pronalaska prijetnje

Windows registar je hijerarhijska baza podataka koja sadrži podatke koji su kritični za rad operacijskog sustava, aplikacija i svih ostalih usluga koje se koriste na Windows sustavu [17]. Svaki operacijski sustav Windows, od verzije 3.1, sadrži registre u koje se pohranjuju informacije bitne za pravilan rad programa. Informacije mogu opisivati korisničke postavke ili rad uređaja koji komuniciraju s računalom poput periferijskih uređaja ili USB uređaja. U svrhu personalizacije rada na računalu koja bi trebala olakšati korisnički rad, u registre se pohranjuje dosta informacija koje nam mogu ukazivati na eventualne kibernetičke prijetnje sustavu.

Registriraju se i informacije poput učestalosti upotrebe programa i posjećivanja internetskih stranica.

Windows uređivač registara je alat koji se sastoji od dva panela. U lijevom panelu prikazani su korijenski ključevi, a u desnom panelu zapisi registra odabranog korijenskog ključa. Kao i u prijašnjim verzijama operacijskog sustava Windows operacijski sustav Windows 11 sadrži pet korijenskih ključeva i to su HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS i HKEY_CURRENT_CONFIG. Ključevi i njihovi potključevi koji tvore košnice (eng. Hives) koje su logički povezane vrijednosti u registru i imaju skup pratećih datoteka učitanih u memoriju [18]. Prateće datoteke učitavaju se u memoriju prilikom pokretanja operacijskog sustava ili prijave korisnika u sustav. Na slici 12. prikazan je alat uređivač registara i na njoj se mogu vidjeti ključevi na lijevoj paneli, na desnoj potključ te vrijednost, vrsta i podatak zapisan unutar potključa.



Slika 12.: Uređivač registara (Izvor: Nikša Mirković, 2022)

Podatci zapisani u registre mogu sadržavati vrijednosti binarnih zapisa te poveznice na lokaciju [19].

Mnogi ransomware zlonamjerni programi kao i računalni virusi trojanskog tipa prilikom izvršenja izmjene vrijednosti postojećih registara i kreirati nove registre bez korisničkog dopuštenja. Ransomware zlonamjerni programi preuzimaju kontrolu nad zaraženim računalom i blokiraju korištenje računala dok se počiniteljima ne uplati novac na račun odnosno otkupnina. Ovaj tip prijetnje funkcionira tako što izmjeni vrijednosti registara ključnih za pravilan rad operacijskog sustava. Ransom.Win32.LOCKBIT.YXCGD zlonamjerni program promjeni vrijednosti unutar četiri postojeća Windows registara i kreira tri nova registarska zapisa. Tvrtka Trend Micro kao rješenje predlaže brisanje izmijenjenih i novo kreiranih registarskih unosa uz brisanje datoteka koje je virus kreirao na disku [20]. Važno je primijetiti kako su svi izmijenjeni registri na lokaciji HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft što ukazuje da je program izmijenio vrijednosti registara bitnih za funkcioniranje operacijskog sustava. Zlonamjerni program mijenja vrijednost registarskog zapisa HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce na putanju na kojoj se nalazi što osigurava da će biti pokrenut prilikom paljenja računala [21]. Druge izmjene registarskih zapisa omogućavaju da se program pokrene s administratorskim ovlastima što osigurava da program funkcionira neometano.

6. Upotreba Yara pravila za automatizaciju pronalaska kibernetičkih prijetnji

Yara je alat otvorenog koda koji automatizira proces pronalaska prijetnji. Alat je razvila Virus Total organizacija i funkcionira kao svojevrsni programski jezik. Alat se može koristiti kao Phyton skripta s posebnim Phyton modulom ili kao ekstenzija naredbenom retku. Yara se može koristiti i unutar web aplikacija koje analiziraju prijetnje na oblaku. Skup instrukcija za specifičnu prijetnju naziva se pravilom [22]. Svako pravilo sastoji se od naziva pravila, meta podataka koji opisuju pravilo i autora pravila, string sekcije u kojoj se nalaze varijable kojima se dodjeljuje vrijednost string ili heksadecimalan niz. Posljednji dio pravila su uvjeti s kima se opisuje način pretrage ili odnosi između prethodno deklariranih varijabli. Na primjeru sljedećeg programskog koda prikazano je pravilo koje je kreirao Florian Roth, korisnik Github platforme, a služi za pronalazak BlackEnergy 2 malwarea [23]:

```
Rule BlackEnergy_BE_2
{
   Meta:
         Description = „Detects BlackEnergy 2 Malware“
         Author = „Florian Roth“
         Reference = „http://goo.gl/DThzLz“
```

```
        Date = „2015/02/19“
        Hash = „983cfcf3aaaeff1ad82eb70f77088ad6ccedee77“

    Strings:
        $s0 = „<description> Windows system utility service
</description>“ fullword ascii
        $s1 = „WindowsSysUtility – Unicode“ fullword wide
        $s2 = „msiexec.exe“ fullword wide
        $s3 = „WinHelpW“ fullword ascii
        $s4 = „ReadProcessMemory“ fullword ascii

    Condition:
        Unit16(0) == 0x5a4d and filesize < 250KB and all of ($s*)
}
```

Standardna sintaksa pisanja pravila sadrži naziv pravila koje slijedi nakon instrukcije „rule“. Unutar sekcije „meta“ zapisuju se meta podatci poput opisa pravila, datuma, imena autora te hash vrijednosti pravila. Unutar „string“ sekcije deklariraju se varijable čija se vrijednost postavlja na vrijednost tipa string tj. tekstualni zapis koji se traži. Nakon svakog „stringa“ opisnom riječi „fullword“ označavamo da se mora pronaći cjelokupan identičan string kako bi se izvršilo podudaranje. Osim „fullword“ modifikatora postoje „wide“, „ascii“ i „nocase“ modifikatori. Wide modifikator traži unicode podudaranje stringa npr. $a=“primjer“ će pronaći podudaranje i ako pronađe zapis poput „p.r.i.m.j.e.r“. Ascii modifikator traži podudaranja prema ASCII tablici znakova dok će nocase modifkator pronaći podudaranja bez obzira o načinu podudaranja. Osim stringa u varijable se može pohranjivati i niz heksadecimalnih vrijednosti koje se umjesto u navodnike navode unutar vitičastih zagrada. Uvjet Unit16(0) == 0x5a4d označava da se pretražuje windows datoteka jer je norma svih windows datoteka da početna dva heksadecimalna zapisa budu 5a i 4d što označava slova M i Z. Ovaj korak se mogao izvesti deklaracijom nove varijable, $mz = {5a 4d}, te zamijeniti Unit16(0) uvjet s $mz. Uvjet filesize < 250KB uvjetuje da se pretražuju datoteke manje od 250KB dok uvjet „all of ($s*)“ označava da se traže podudaranje sa svim navedenim varijablama $s.

BlackEnergy 2 je malware prepoznat 2007 godine a širio se pomoću word i powerpoint dokumenata koji su slani e-mailovima. Malware je kreirao mrežu botova koji su se kasnije koristili u izvršavanju napada distribuiranog uskraćivanja usluge [24].

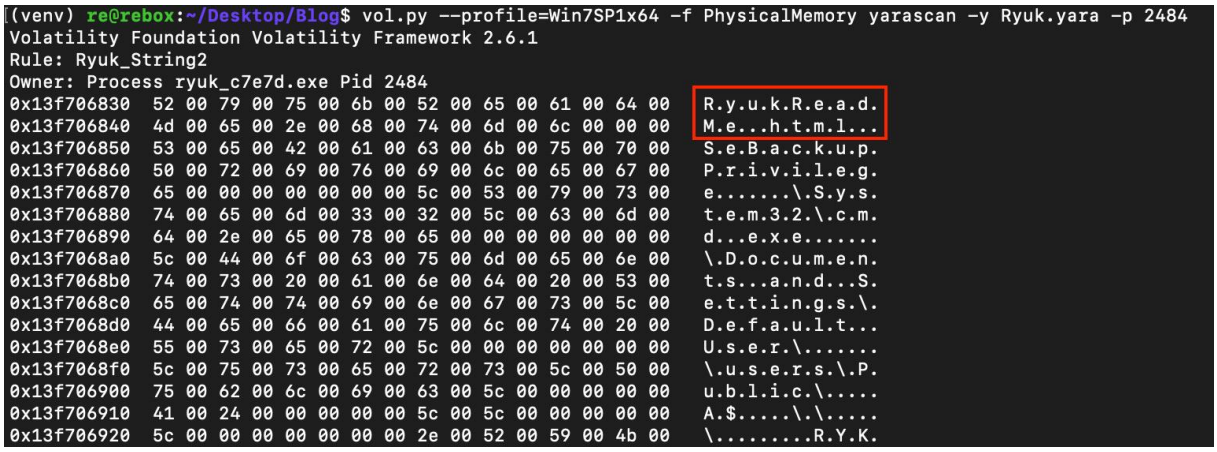
Za adekvatno korištenje Yara pravila potrebno je koristiti i alate za heksadecimalnu analizu datoteka poput WinHex ili HxD alata koji prikazuju kompletan heksadecimalan zapis odabrane datoteke. Slijed zapisa u heksadecimalnom obliku karakterističan za neku prijetnju koristi se kao vrijednost koja se pohranjuje u varijablu za pronalazak prijetnje.

6.1. Načini upotrebe Yara pravila

U općenitom smislu Yara se koristi za filtriranje datoteka navođenjem traženih vrijednosti u varijable. Primarna svrha upotrebe Yara pravila je ubrzavanje procesa lova odbacujući sigurne datoteke koje se ne trebaju pregledavati. Tako se štedi vrijeme i novac. Osim općenite upotrebe Yara pravila postoji i niz specifičnih upotreba poput analize e-mailova, memorije i retro lova navodi [25].

Prilikom korištenja Yara pravila za analizu malicioznih e-mailova nailazi se na specifičan problem. Sadržaj e-maila poruke prije analize treba pretvoriti u tekst i zbog limita duljine tekstualnog zapisa u pojedinoj liniji MIME protokola sadržaj može biti raspoređen u više redaka. Pretvorbom se sadržaj poruke pretvara iz Quoted-Printable kodiranja u Base64 način kodiranja [26], [27]. Podatci poput adrese koja vodi do maliciozne lokacije, IP adresa ili imena domaćina rasporede se prilikom pretvorbe u dva retka. Korištenjem alat poput CyberChef web aplikacije parsira se sadržaj poruke u format upotrebljiv za pronalazak prijetnje pomoću Yara pravila [25]. Tako obrađen sadržaj pohranjuje se kao vrijednost varijable koja se koristi u svrhu pronalaska prijetnje. Preporuka autora [25] za dekodiranje priloga e-mail poruke je korištenje Titanium platforme koju je razvila Reversing Labs organizacija čiji rezultat se može uključiti unutar Yara pravila.

Analizom memorije i provođenjem pretrage nad prijetnjom s Yara pravilom mogu se pronaći kibernetičke prijetnje. Upotrebom WimPmem alata analizira se memorija, a rezultat analize pohranjuje se u naprednom forenzičkom formatu datoteka ekstenzije „AFF4“ [25]. Nakon analize memorije potrebno je odvojiti fizičku memoriju iz rezultata analize i pohraniti sliku dobivene memorije. Upotrebom Yara pravila s Volatility alatom nad slikom fizičke memorije vršimo pretraživanje željene prijetnje [25]. Na slici 13. prikazano je kako pomoću alata Volatility provesti analizu slike fizičke memorije s „Ryuk_String2“ pravilom.



Slika 13.: Upotreba Yara pravila s Volatility alatom za analizu memorije (Izvor: Reversing Labs, 2022)

Yara pravilo u varijablu pohranjuje vrijednost „RyukReadMe.html“ koja se traži u slici fizičke memorije [25]. Na slici 13. crvenom je bojom označen sektor u kojemu je pronađena tražena vrijednost s Yara pravilom.

Upotreba Yara pravila kao sredstvo retro lova odnosi se na korištenje pravila unutar web servisa za analizu prijetnji koji sakupljaju podatke u bazu znanja o prijetnjama [25]. Glavna karakteristika retro lova je proces obrnutog inženjeringa. Proces lova započinje pronalaskom prijetnje te analizom iste lovac istražuje prijetnju i njezine karakteristike. Proučavanjem kako prijetnja šteti računalu, kako se prenosi i kako je nastala lovac shvaća širu sliku o samoj prijetnji. Svrha retro lova je identifikacija karakteristika prijetnje kako bi se slične prijetnje u mogle brže pronaći i brže sanirala eventualna šteta koju su prouzročile. Pomoću web servisa, poput Reversing Labs servisa za pronalazak prijetnji, lovac pravi izvješće o prijetnji i navodi pomoću kojeg Yara pravila se prijetnja može pronaći [28]. Takvim djelovanjem pridonosi se zajednici te podiže se kolektivna razina sigurnosti.

7. Zaključak

U ovom radu prikazano je kako lov na kibernetičke prijetnje izuzetno kompliciran skup aktivnosti jer od pojedinca zahtjeva poznavanje širokog spektra znanja o informacijskim tehnologijama i načinu rada računala. Kao proces, lov na kibernetičke prijetnje izuzetno je dugačak jer zahtjeva konstantno provjeravanje i analizu sustava. Isto tako od lovca zahtjeva konstantno napredovanje u kontekstu sveobuhvatnog znanja jer se broj prijetnji povećava iz dana u dan, a vrijeme je pokazalo da antivirusni programi nisu adekvatno rješenje za sprečavanje eskalacije prijetnje u problem, a naročito unutar velikih kompanija. Svaki tim koji lovi kibernetičke prijetnje trebao bi prepoznati svoje mogućnosti i potencijale kako bi se adekvatno pripremili za lov tj. znali koje tehnike i metode koristiti i u kojem rasponu kako ne bi trošili vrijeme i novac. Svaki lov na kibernetičke prijetnje započinje analizom sustava tako smo obradili skup alata za tehničku analizu računalnih sustava Sysinternals koji pružaju lovcima mogućnost razumijevanja kako promatrani računalni sustavi funkcioniraju i pruža im mogućnost izolacije prijetnje radi boljeg razumijevanja, a kasnije osiguravanja sustava od sličnih prijetnji u budućnosti. Pomoću dnevnika događaja utvrdili smo kako se može utvrditi da je računalna sigurnost kompromitirana obrativši pozornost na zapise koji opisuju sigurnosne promjene na računalu. Uređivač registra koristili smo kako bi se dokazalo da je računalo zaraženo i razumjeli kako računalni virus funkcionira. Brisanjem malicioznih registarskih zapisa uklonili smo mogućnost samopokretanja računalnog virusa prilikom paljenja sustava što je omogućilo brisanje kompletnog računalnog virusa s računala. Na koncu pokazali smo kako djelomično automatizirati proces lova na kibernetičke prijetnje izradom Yara skripte koja pretražujući zadane vrijednosti analizira da li je računalo zaraženo računalnim virusom. Potpuna korisnost Yara skripti prikazana je na primjeru analize e-mail poruka i memorije računala. Razumijevanjem retro lova primjećuje se kako su Yara pravila postala sredstvo komunikacije između lovaca ali i moćno oružje čijoj snazi lovci kolektivno pridonose.

Iako je umijeće detekcije, izolacije i uklanjanja računalnih virusa postoji od kada postoje računalni virusi tek u posljednje vrijeme pojavila se potreba da velike korporacije zapošljavaju sigurnosne stručnjake koje formiraju u timove zadužene za konstantan lov na prijetnje. Antivirusni programi nisu dovoljna mjera zaštite od prijetnji jer se razina informatičke pismenosti na globalnoj razini drastično povećala, a samim time broj novih prijetnji proporcionalno raste. Kompanije koje se bave izradom antivirusnih programa za detekciju prijetnje relativno su male usporedivši ih s brojem novih prijetnji koje se pojavljuju u svijetu svakodnevno stoga će potreba za stručnim lovcima na kibernetičke prijetnje biti sve veća.

Popis literature

[1] Security Intelligence: A Beginner's Guide to Threat Hunting. Dostuno 5.8.2022. na: https://securityintelligence.com/a-beginners-guide-to-threat-hunting/

[2] Infosec institut: Ultimate guide to threat hunting. Dostupno 5.8.2022. na: https://resources.infosecinstitute.com/topic/the-ultimate-guide-to-threat-hunting/

[3] Security Intelligence: Threat Hunting Techniques: A Quick Guide. Dostupno 5.8.2022. na: https://securityintelligence.com/posts/threat-hunting-guide/

[4] Guidepoint Security; Threat Hunting: Tips and Tools. Dostupno 5.8.2022. na: https://www.guidepointsecurity.com/education-center/threat-hunting-tips-and-tools-2/

[5] The Cyphere, Threat Hunting: Process, Methodologies, Tools and Tips. Dostuno 5.8.2022. na: https://thecyphere.com/blog/threat-hunting/

[6] SQRLL; A framework for Cyber Threat Hunting. Dostupno 5.8.2022. na: https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper.pdf

[7] Službena Microsoft dokumentacija za skup alata Sysinternals; Dostupno 15.8.2022. na: https://docs.microsoft.com/hr-hr/sysinternals/

[8] Malware Hunting with Mark Russinovich and the Sysinternals Tools; Predavanje Marka Russovicha dostupno 12.8.2022. na: https://www.youtube.com/watch?v=vW8eAqZyWeo

[9] Nasreddine Bencherchali, Hunting Malware With Windowns Sysinternals – Autoruns. Dostupno 5.8.2022. na: https://nasbench.medium.com/hunting-malware-with-windows-sysinternals-autoruns-19cbfe4103c2

[10] F-Secure; O računalnom virusu Trojan-Downloader:W32/Agent. Dostupno 15.8.2022. na: https://www.f-secure.com/v-descs/trojan-downloader_w32_agent.shtml

[11] Službena Microsoft dokumentacija za alat RamMap; Dostupno 15.8.2022. na: https://docs.microsoft.com/hr-hr/sysinternals/downloads/rammap

[12] SecurityIntelligence; Inside the Mind of a Hacker: Attacking the Memory. Dostupno na:https://securityintelligence.com/inside-the-mind-of-a-hacker-attacking-the-memory/

[13] Službena Microsoft dokumentacije za alat TCPView; Dostupno 15.8.2022. na: https://docs.microsoft.com/hr-hr/sysinternals/downloads/tcpview

[14] Steve Anson (2019). Analyst Reference. Windows Event Log Analysis. Applied Incident Response. Dostupno 4.3.2022. na: https://secureservercdn.net/160.153.138.53/x27.24e.myftpupload.com/download/Windows-Event-Log-Analyst-Reference.pdf?time=1649840585

[15] Event Log Tampering Part 1: Disrupting the EventLog Service; Osobni blog autora svch0st. Dostupno 30.8.2022. na: https://svch0st.medium.com/event-log-tampering-part-1-disrupting-the-eventlog-service-8d4b7d67335c

[16] Event Log Tampering Part 2: Disrupting the EventLog Service; Osobni blog autora svch0st. Dostupno 30.8.2022. na: https://svch0st.medium.com/event-log-tampering-part-2-manipulating-individual-event-logs-3de37f7e3a85

[17] Forensic Analysis of Windows Registry Against Intrusion, International Journal of Network Security & Its Applications. Vol.4, No.2, Ožujak 2012. Haoyang Xie, Keyu Jiang, Xiaohong Yuan i Hongbiao Zeng. Dostuno 4.3.2022. na: https://www.researchgate.net/publication/267261942_Forensic_Analysis_of_Windows_Registry_Against_Intrusion

[18] Anson, S., & Bunting, S. (2007). Mastering Windows Network Forensics and Investigation. Indianapolis: Sybex. Dostupno 4.3.2022. na: https://vdoc.pub/download/mastering-windows-network-forensics-3mbsqas3vr60

[19] Structure of the Registry, Microsoft. Dostupno 5.3.2022. na: https://docs.microsoft.com/hr-hr/windows/win32/sysinfo/structure-of-the-registry

[20] Nathaniel Gregory Ragasa; Trend Micro; Izvještaj o Ransom.Win32.LOCKBIT.YXCGD malicioznom programu. Dostupno 15.8.2022. na: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom.win32.lockbit.yxcgd

[21] Run and Run Once Registry Keys; Microsoft; Dostupno 16.8.2022. na: https://docs.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys

[22] Virustotal; Yara; Dostupno 15.8.2022. na: https://support.virustotal.com/hc/en-us/articles/115002178945-YARA

[23] Yara rule Github repozitorija za pronalazak BlackEnergy 2 malwera; Florian Roth; Dostupno 19.8.2022. na: https://github.com/Yara-Rules/rules/blob/master/malware/APT_Blackenergy.yar

[24] Jose Nazario (2007). BlackEnergy DDoS Bot Analysis. Arbor Networks. Dostupno 19.8.2022. na: https://web.archive.org/web/20200221013253/http://atlas-public.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.pdf

[25] Rober Simmons (2020). Five Uses of Yara. Reversinglabs. Dostupno 31.8.2022. na: https://blog.reversinglabs.com/blog/five-uses-of-yara#_ftn8

[26] Quoted-printable. Wikipedia članak. Dostupno 31.8.2022. na: https://en.wikipedia.org/wiki/Quoted-printable

[27] Base64. Wikipedia članak. Dostupno 31.8.2022. na: https://en.wikipedia.org/wiki/Base64

[28] How to Hunt for Threats Using YARA Rules. Youtube video zapis kanala ReversingLabs. Dostupno 31.8.2022. na: https://www.youtube.com/watch?v=T8utVmUbxlk

Popis slika

Popis tablica