Process Monitor

Mateo Šimonović, 0036465116

Mentor: prof. Marin Golub
Akademska godina 2014/2015

SADRŽAJ

1. Uvod

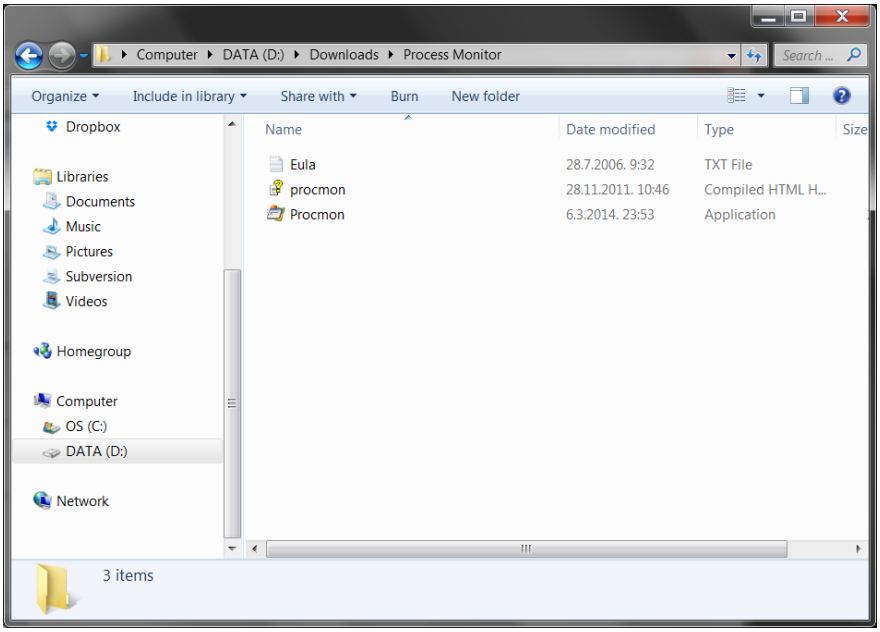
Process Monitor je besplatan alat tvrtke Windows Sysinternals, koja je dio Microsoft TechNet odjela. Program je besplatan, ali tvrtka Sysinternals u ugovoru o licenci strogo zabranjuje dekompajliranje programa, izmjenu bilo kojeg njegovog djela te kopiranje i redistribuciju programa, stoga, ovaj program nije otvorenog koda.

Alat prati i prikazuje sve aktivnosti datotečnog sustava, registara računala, svih aktivnih procesa i mrežnih akcija u stvarnom vremenu. Primjenjiv je isključivo na Microsoft Windows operacijskim sustavima. To je program koji je nastao kao spoj starijih alata FileMon i RegMon te se koristi u sistemskoj administraciji, računalnoj forenzici te prilikom traženja i ispravljanja pogrešaka (engl. *debugging*). Process Monitor prati i bilježi svaki pokušaj dohvaćanja Windows registara, pa čak i neuspjele pokušaje čitanja ili pisanja u iste. Osim što prikazuje stanje sustava na vrlo detaljnoj razini, Process Monitor omogućava sortiranje i filtriranje sadržaja po raznim ključevima, imenima, procesima, dretvama i drugom što je njegova velika prednost jer takve složene analize nemoguće je raditi ručno s obzirom na količinu podataka o kojima se ovdje radi.

Slika 1.1 - Logo programa Process Monitor

2. Instalacija i pokretanje programa

Instalacija programa Process Monitor je vrlo jednostavna. Program je besplatan te je zadnju verziju moguće preuzeti sa Windows Sysinternals web stranice na adresi http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx. Nakon preuzimanja korisnik na računalu ima jednu ZIP datoteku naziva ProcessMonitor.zip. Alat nema klasičnu instalaciju već je dovoljno raspakirati danu ZIP arhivu bilo gdje na računalu. Sadržaj raspakirane arhive prikazan je na slici 2.1.



Slika 2.1 – Sadržaj Process Monitor direktorij nakon preuzimanja i raspakiravanja

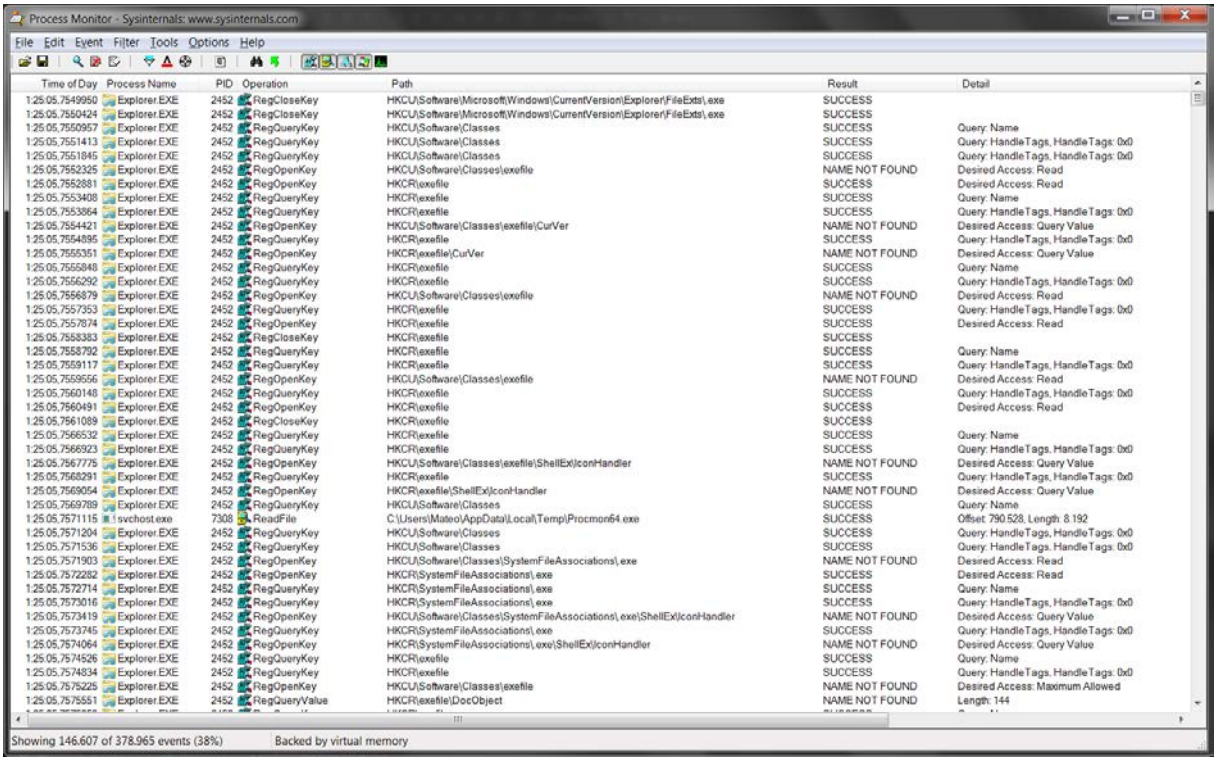
Nakon raspakiranja direktorij Process Monitor sadrži sljedeće datoteke:

- **Eula.txt** – Datoteka koja sadrži ugovor o licenci, potrebno pročitati prije korištenja programa
- **procmon.chm** – HTML datoteka s detaljnim uputama za korištenje programa
- **Procmon.exe** – Izvršna datoteka za pokretanje programa

Nakon raspakiranja preuzete ZIP arhive, program se pokreće jednostavnim pokretanjem izvršne datoteke Procmon.exe.

3. Rad s programom

Početak rada s Process Monitorom počinje njegovim otvaranjem nakon čega se na ekranu pojavljuje prozor poput onog na slici 3.1. Process Monitor je vrlo složen program i ima vrlo napredne funkcionalnosti, a u ovom projektu će biti predstavljene neke od najvažnijih.

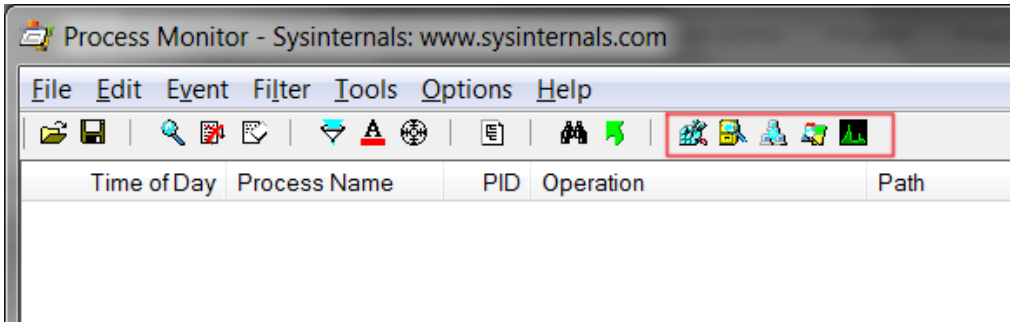


Slika 3.1 – Izgled osnovnog prozora programa

Glavni dio prozora programa zauzima tablica koja prikazuje sve aktivnosti koje se trenutno događaju nad registrima računala, datotečnim sustavom ili mrežnim prometom. Svaku od ovih aktivnosti moguće je uključiti ili isključiti pritiskom na odgovarajući gumb, što će biti predstavljeno u nastavku. Tablica sadrži nekoliko najbitnijih stupaca te veliki broj redova od kojih svaki predstavlja po jedan praćeni zapis. Stupce je moguće reorganizirati na sljedeći način:

1. Klikom i držanjem zaglavlja stupca moguće je promijeniti redoslijed stupaca tako da ga se odvuče ispred ili iza nekog željenog stupca
2. Desnim klikom na bilo koji od stupaca nudi se opcija „Select Columns…“ klikom na koju korisnik može birati između 27 tipova stupaca koje želi uključiti ili maknuti iz glavnog prozora

Sljedeći vrlo važan i efikasan način izbora što će se pratiti nalazi se u alatnoj traci i prikazan je na slici 3.2 označen crvenom bojom. S obzirom da Process Monitor prati sve moguće oblike prometa na računalu, nerijetko je korisniku potreban samo jedan tip događaja (npr. samo promjene nad registrima računala). Objašnjenje što radi svaki od gumbi u crveno označenom dijelu alatne trake dano je u tablici 1.



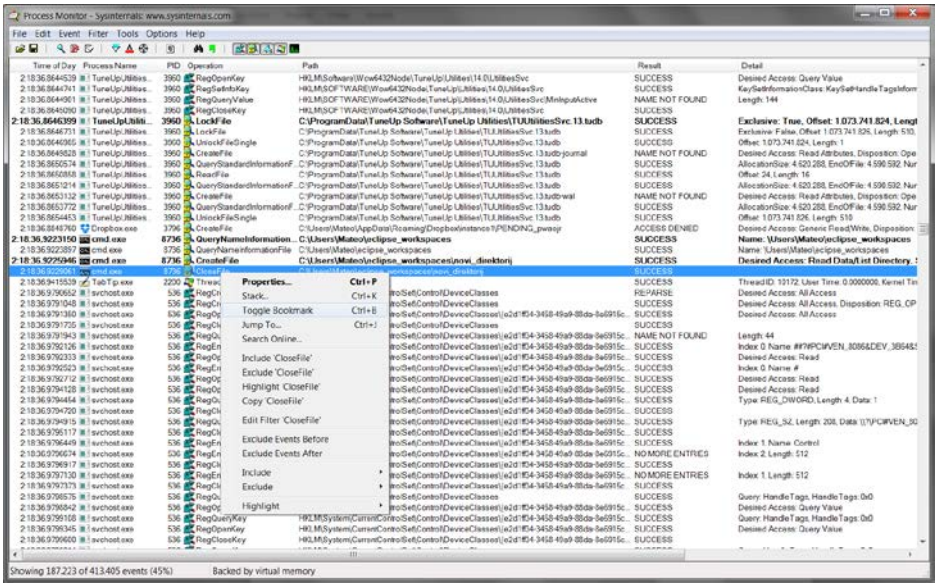
Slika 3.2 - Izbor vrste događaja koji su praćeni

Ikona	Operacija
	Uključuje/isključuje prikaz aktivnosti nad registrima. To su najčešće operacije čitanja određenog registra, upita nad registrima (engl. *query*), stvaranja novih ključeva, upisivanja novih vrijednosti u nove ili postojeće ključeve itd.
	Uključuje/isključuje prikaz aktivnosti nad datotečnim sustavom. U te aktivnosti spadaju operacije čitanja datoteke s diska, stvaranja nove datoteke, zatvaranja datoteke, upita operacijskom sustavu o tipu ili svojstvima neke datoteke itd.
	Uključuje/isključuje prikaz mrežne aktivnosti na računalu. Tu spadaju operacije primanja i slanja TCP i UDP segmenata, ostvarivanja konekcije, retransmisije te ostale mrežne aktivnosti.
	Uključuje/isključuje prikaz aktivnosti procesa i dretvi računala. Tu spadaju operacije stvaranja i uništavanja procesa i dretvi, njihovog učitavanja određenih resursa itd.
	Uključuje/isključuje prikaz aktivnosti vezanih uz sistemske procese. Tu spadaju svi trenutno pokrenuti programi kao i programi koji se podižu prilikom uključivanja računala.

Tablica 1 – Prikaz ikona alatne trake za prikaz određenih tipova događaja

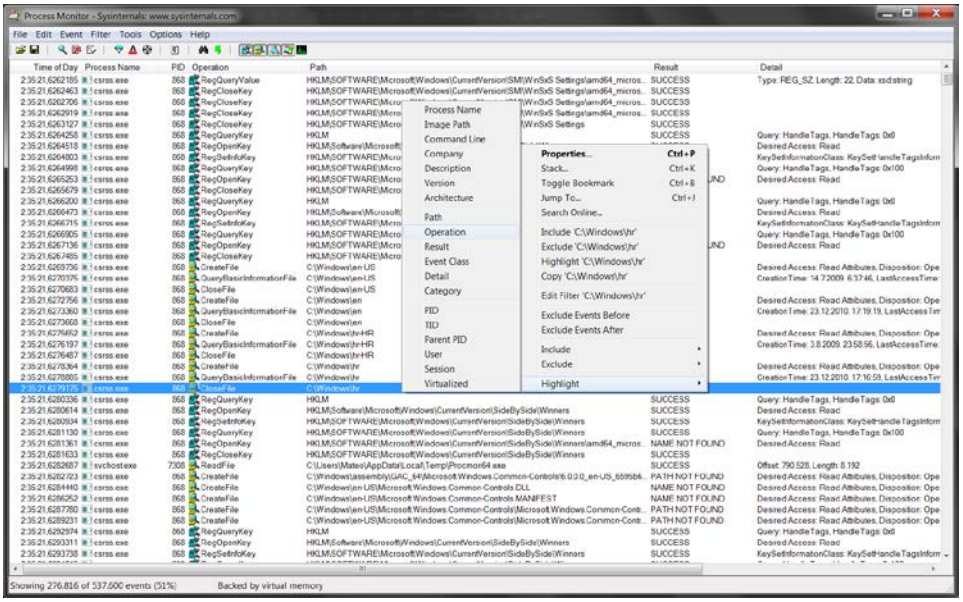
Stručnjaci tvrtke Sysinternals izlažu kao glavnu prednost korištenja Process Monitora sposobnost označavanja određenih zapisa, skakanja među njima te filtriranje svih zapisa po više kriterija paralelno. Operacija filtriranja je u novoj inačici nanovo implementirana i tvorci alata ponosno izjavljuju da je to najmoćniji dio alata i da radi s nevjerojatnom brzinom. Uistinu, Process Monitor filtrira nekoliko stotina tisuća zapisa bez da je to korisniku primjetno i bez da mu uspori ili zasmeta prilikom rada s alatom.

Na sljedećem je primjeru prikazan još jedan vrlo pogodan način izbora skupa podataka koji će se promatrati. Desnim klikom na jedan zapis moguće je izabrati opciju *Toggle Bookmark* (tipkovnička kratica: Ctrl + B) što će sam zapis podebljati (engl. *bold*), ali i ono najbitnije, omogućit će korisniku da pritiskom na tipku F6 skače s jednog označenog zapisa na drugi. To je vrlo korisna opcija ako se želi pratiti samo određene akcije.

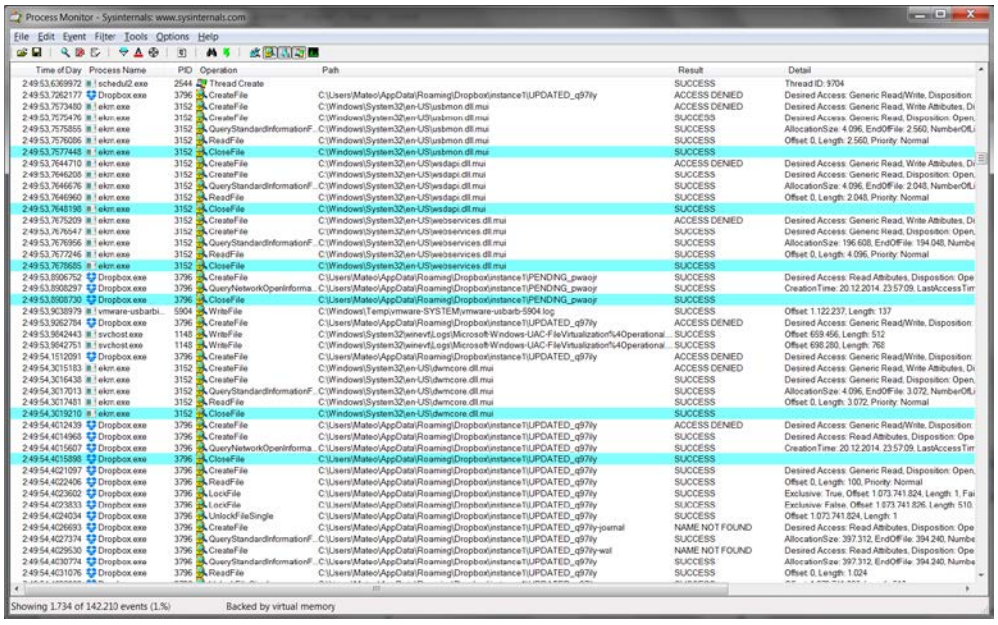


Slika 3.3 - Praćenje određenih aktivnosti označavanjem bookmark-a

Na sljedećem je primjeru prikazan je još jedan vrlo koristan način selektiranja određenih zapisa. Desnim klikom na željni zapis moguće je izabrati meni *Highlight* i nakon njega bilo koji od trenutno aktivnih stupaca koji se želi selektirati. Postupak selektiranja prikazan je na slici 3.4, a rezultat selektiranja na slici 3.5

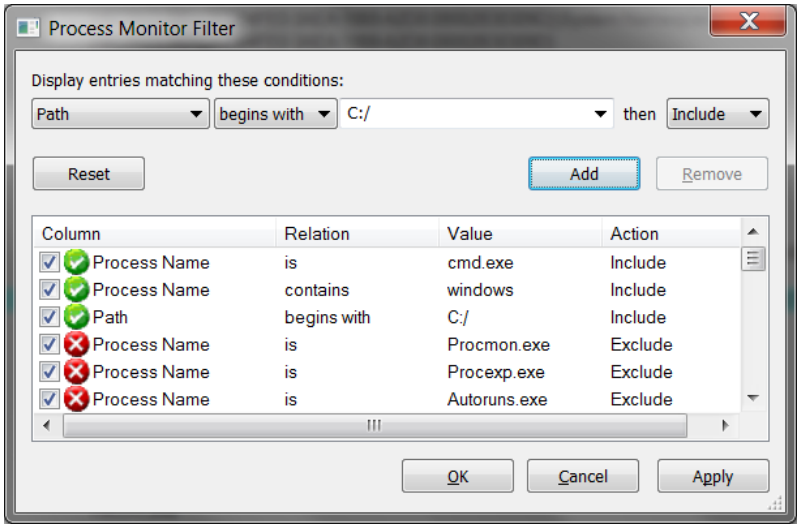


Slika 3.4 – Postupak označavanja zapisa s jednakim opisom operacije



Slika 3.5 – Rezultat označavanja svih zapisa s jednakom operacijom

Zadnji i najvažniji oblik selektiranja podataka je upravo ono u čemu je Process Monitor dobar, zapravo, jako dobar, a to je filtriranje. Do prozora za filtriranje moguće je doći tako da se u izborniku *Filter* izabere podizbornik *Filter…* ili pritiskom na istoimeni gumb na alatnoj traci. Prozor koji se otvara prikazan je na slici 3.6. Taj prozor omogućava naprednije filtriranje dok se do jednostavnog filtriranja može doći i desnim klikom na bilo koji zapis te pomoću podizbornika *Include* i *Exclude* odrediti koji se sve zapisi slični tom odabranom trebaju uključiti ili isključiti iz prikaza.



Slika 3.6 - Primjer naprednog filtriranja

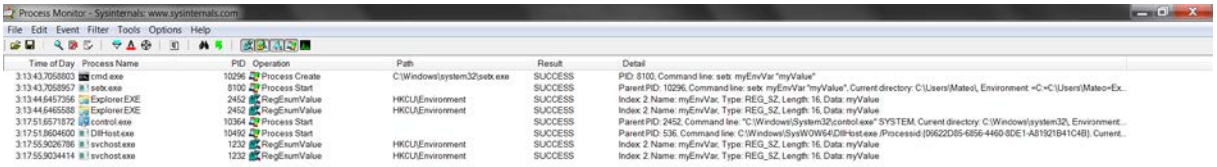
Na slici je dan primjer jednog složenijeg filtera, iako ovisno o primjeni, filteri u radu s Process Monitorom mogu biti daleko složeniji. Trenutni filter će zadržati sve zapise kojima je ima procesa točno jednako „cmd.exe“ ili one kojima ime procesa sadrži tekst „windows“ uz uvjet da putanja s kojom proces radi započinje tekstom „C:/“, odnosno da proces radi nešto na C disku. Treba dobro obratiti pozornost na prednost logičkih operatora prilikom izrade složenijih filtera. Tvorci Process

Monitora su odlučili da su sva filtriranja po istom stupcu odvojena logičkim operatorom I, dok su onda ti zapisi odvojeni filtriranjima po ostalim stupcima operatorom ILI. Upravo zbog toga gore navedeni filter riječima glasi: „(ime procesa je „cmd.exe“ ILI ime procesa sadrži „windows“) I putanja počinje s „C:/“. Pored navedenih mogućnosti (filtriranja po različitim stupcima te po više unosa unutar jednog stupca), filter dozvoljava suprotnu logiku, odnosno odlučivanje koji će zapisi biti odbačeni. Za to je dovoljno padajući izbornik s *Include* promijeniti na *Exclude*. Ovdje također treba dobro pripaziti oko prednosti logičkih operatora jer je sa suprotnom logikom često još teže pratiti što se događa.

Na kraju, proveden je jedan mali eksperiment kako bi se pokazalo kako ovaj program radi. Otvoren je Process Monitor a odmah potom je otvoren novi naredbeni redak i u njemu je izvedena sljedeća naredba:

```
setx myEnvVar ''myValue''
```

Ta naredba operacijskom sustavu postavlja varijablu okruženja *myEnvVar* (ako je nema onda je stvara) za trenutnog korisnika i pridjeljuje joj vrijednost *„myValue“*. U Process Monitoru su najprije filtrirani svi zapisi koji sadrže proces *cmd.exe*. Među tim zapisima bilo je vrlo jasno vidljivo kako računalo traži u svim direktorijima zadanim u sistemskoj varijabli PATH nalazi li se unutra naredba `setx`, te ju na kraju pronađe u sistemskom direktoriju i izvede. Kako se nakon toga uz proces vidio opis „Command line setx myEnvVar 'myValue'“ odlučilo se otići pogledati sve zapise s istim PID-om da se vidi kako je taj proces tekao od početka do kraja. Konačno, kad se vidjelo kada je naredba izvršena napravljeno je zadnje filtriranje u kojem se u polju Detail traži ključna riječ *„myEnvVar“* i rezultat tog filtriranja prikazan je na slici 3.7.



Slika 3.7 – Rezultat izvođenja eksperimenta

Iz ovog malog eksperimenta vidljivo je kako Process Monitor vrlo detaljno radi svoj posao i prati apsolutno sve što se događa na računalu te sekundarno, kako analizirati programe na ovaj način nije niti malo lagano i potrebno je osim jako dobrog poznavanja alata i velika količina iskustva.

4. Process Monitor u analizi zloćudnih programa

Process Monitor vrlo je efikasan i složen program koji omogućuje praćenje svih procesa na računalu, način na koji oni komuniciraju, što rade u datotečnom sustavu, mreži i registrima računala. Stoga, nije čudno što se taj alat našao kao jedan od fundamentalnih alata u analizi zloćudnih programa.

Sama analiza zloćudnih programa vrlo je složen i zahtjevan proces, zahtijeva veliku količinu znanja, iskustva ali i dozu inventivnosti i razmišljanja. Zloćudni programi (engl. *malware*) često sav „prljavi“ posao rade u pozadini, često u zasebnom procesu ili u zasebnoj dretvi, tako da ih običan korisnik nikako ne može primijetiti. Process Monitor ovdje uvelike pomaže. On omogućava da se za svaki proces i svaku dretvu vidi u svakom trenutku što on radi, što pokušava pročitati, gdje nešto zapisuje i da li pokušava određene podatke slati putem mreže. Najveći problem u analizi zloćudih programa je upravo to što ispitivač ne može unaprijed znati što i na koji način program u pozadini radi i radi li se zapravo o zloćudnom programu. Zbog toga mora ispitati apsolutno sve mogućnosti da bi se u to uvjerio. Ovdje svakako uskače mogućnost vrlo složenih izbora skupa podataka te filtriranja istih u Process Monitoru. Moguće je pratiti tijek izvođenja samo jednog programa, samo jedne dretve ili pak tražiti među svim pokrenutim programima one koji pristupaju točno određenim resursima (npr. određenoj datoteci ili određenom registru) i na taj način suziti izbor i u konačnici odrediti je li program zloćudan ili nije.

5. Zaključak

Process Monitor na prvi pogled je vrlo jednostavan program za praćenje svih događanja na jednom računalu, od registara do datotečnog sustava. S druge strane, iako program nema enormnu količinu opcija i značajki, neke od njih su dovoljno složene da treba duže vrijeme kako bi korisnik ovladao njime i naučio u potpunosti raditi s njime.

U ovom projektu su objašnjene samo osnovne značajke koje bi budućem korisniku mogle pomoći započeti rad s ovim ozbiljnim profesionalnim programom. Za dublju analizu čitatelja se upućuje na originalnu knjigu autora ovog programa. U ovom projektu je pokazano kako program radi i jednim manjim dijelom koje su njegove mogućnosti. Pokazano je da, ono što tvorci programa tvrde da su njegove jače strane, to uistinu i jesu. Process Monitor vrlo brzo i efikasno prolazi kroz stotine tisuća zapisa te u njima traži određene podatke, filtrira ih ili označava i različitim bojama prikazuje korisniku. Također, važno je dotaknuti se uloge Process Monitora u analizi zloćudnih programa zbog toga što, iako on nije nastao s tom namjenom, specijalisti ispitivači zloćudnih programa našli su u njemu veliku korist. Nažalost, zbog velikog rizika i nemogućnosti dobivanja zasebnog računala, na ovom projektu nije bilo moguće iz prvog lica probati analizirati zloćudni program ovim alatom te je stoga to učinjeno na jednom vrlom jednostavnom primjeru kako bi se stekao dojam kako je raditi s takvim programom. Zaključno, Process Monitor je vrlo kvalitetan alat koji ima jedan prilično zahtjevan zadatak i ispunjava ga u potpunosti, vrlo brzo, točno i s korisničke strane, vrlo jasno i dobro dizajnirano iako za potpuno savladavanje rada s programom trebaju tjedni, mjeseci, a možda i više od toga.

6. Literatura

[1] Process Monitor Help, Sysinternals

[2] Process Monitor, Wikipedia, http://en.wikipedia.org/wiki/Process_Monitor

[3] Defrag Tools: #3 – Process Monitor (video), Channel 9, http://channel9.msdn.com/Shows/Defrag-Tools/Defrag-Tools-3-Process-Monitor

[4] Using Sysinternals Tools Like a Pro, How-To-Geek, http://www.howtogeek.com/school/sysinternals-pro/lesson5/all/