Centar Informacijske Sigurnosti

Analiza alata Sysinternals Suite

studeni 2011.

CIS-DOC-2011-11-032

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

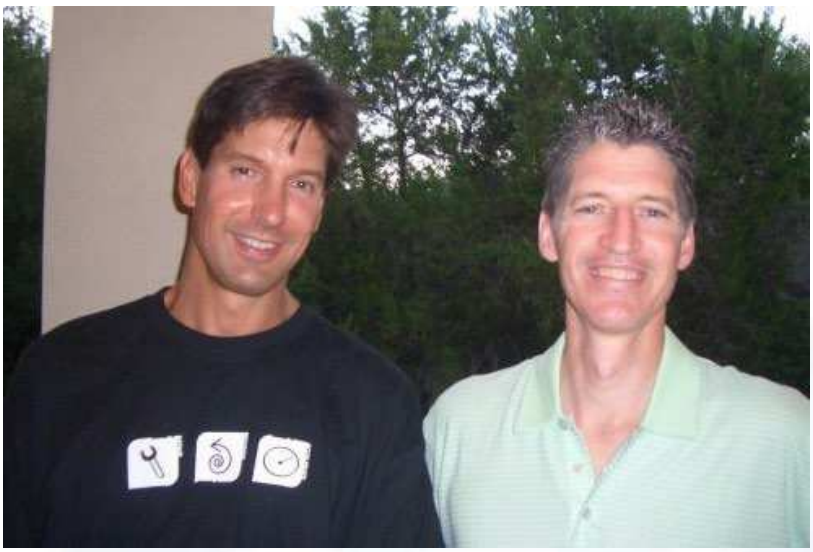
1. Uvod

Sysinternals Suite predstavlja skup uslužnih programa koji se koriste za dobivanje informacija o sustavu, upravljanje sustavom i otklanjanje problema u sustavu temeljenom na Microsoft Windows platformi. Prije svega, ovi alati služe za bolje razumijevanje rada operacijskog sustava Windows, a naročito njegove jezgre. Stoga su namijenjeni prvenstveno naprednijim korisnicima koji su upoznati s principima rada jezgre operacijskog sustava Windows. Općenito bi se moglo reći da su ovi alati korisniku tim korisniji što je veće njegovo znanje o dotičnoj tematici (što nikako ne znači da korisnici koji ne vladaju potrebnim znanjima trebaju zaobilaziti ove alate). Sysinternals alati međusobno se poprilično razlikuju po svojoj složenosti, opsegu te funkcionalnosti koju pružaju, ali im je zajednička korisnost koju osiguravaju svojim korisnicima.

U nastavku dokumenta ukratko je opisan razvoj i namjena Sysinternals Suite alata te je opisano kako ih je moguće preuzeti. Nadalje, dokument ukratko objašnjava koncepte jezgre operacijskog sustava Windows koji su bitni za razumijevanja rada i funkcionalnosti Sysinternals Suite alata. Objašnjeni su neki temeljni pojmovi poput korisničkih prava, procesa, dretvi, poslova, korisničkog i jezgrenog načina rada, stoga poziva, simbola i sl. U ovom dokumentu objašnjeni su najznačajniji Sysinternals alata, a za pojedine programe dane su i kratke upute za njihovo korištenje. Navedena je podjela Sysinternals alata prema području njihove namjene. Programi Process Explorer, Autoruns i Process Monitor iznimno su opsežni. Njihova funkcionalnost detaljno je opisana u [1], a u dokumentu je dan samo njezin kratki pregled. Ostali programi koji su opisani (RootkitRevealer, AcessChk, SigCheck, TCPView, BgInfo, BlueScreen) spadaju među najpopularnije Sysinternals, odnosno sigurnosne alate. U zadnjem, petom poglavlju opisane su smjernice budućeg razvoja Sysinternals alata. U poveznici [5] moguće je pogledati intervju s jednim od osnivača Sysinternals alata, Markom Russinovichem.

2. Razvoj i namjena alata Sysinternals Suite

Sysinternals Suite je skup od 70 naprednih uslužnih programa za Microsoft Windows okruženje koji služe za dijagnostiku, otklanjanje problema (eng. *troubleshooting*) i upravljanje. Njegovi autori su Mark Russinovich i Bryce Cogswell (Slika 1).



Slika 1. *Mark Russinovich (lijevo) i Bryce Cogswell*
Izvor: *Windows Sysinternals Administrator's Reference*

Početak razvoja Sysinternals alata seže u 1995. godinu, kada je Mark Russinovich napisao prvi Sysinternals uslužni program (eng. *utility*) – „Ctrl2Cap". Riječ je o pogonskom programu (eng. *driver*) koji pritisak tipke Caps Lock na tipkovnici pretvara i prosljeđuje u računalo kao pritisak tipke Ctrl. Nastanak ovog programa bio je potaknut autorovim početkom korištenja operacijskog sustava Windows NT. Zajedno s Bryceom Cogswellom, njegovim kolegom sa studija na Carnegie Mellon University, razvija sljedeća tri alata: NTFSDOS, Filemon i Regmon te time postavlja temelje Sysinternals alata. Svoje alate odlučili su omogućiti dostupnima za upotrebu drugima pa su ih prvotno objavili na stranici njihovog prijatelja Andrewa Schulmana. U rujnu 1996. pokreću vlastitu stranicu NTinternals.com na kojoj objavljuju alate i članke vezane uz njih. U isto vrijeme osnivaju i komercijalnu softversku tvrtku Winternals Software. Prvi uslužni program koji je nova tvrtka objavila bio je NTRecover. U samo nekoliko mjeseci njihova stranica postala je jedna od najpopularnijih uslužnih stranica za Windowse s preko 1 500 posjetitelja dnevno. 1998. godine mijenjaju ime stranice u Sysinternals.com. Kroz idućih nekoliko godina nastavljaju razvoj alata te 2006. njihova tvrtka Winternals broji stotinjak zaposlenika, a Sysinternals broji milijune preuzimanja. 18. srpnja iste godine Microsoft preuzima tvrtku Winternals Sofware te Sysinternals stranicu. Windows Systernals danas su dio Microsoft TechNet stranice te su ujedno i jedan od njezinih najposjećenijih dijelova s prosječno 50 000 posjetitelja dnevno i tri milijuna preuzimanja mjesečno. Kao što je i bila želja njezinih osnivača, Sysinternals alati besplatno su dostupni za korištenje. U listopadu 2010. godine umirovljen je Bryce Cogswell.

Osnovna obilježja svih Sysinternals alata (koji ocrtavaju i filozofiju rada njihovih autora) su:

1. Intuitivnost i jednostavnost za uporabu.
2. Ispunjavanje specifičnih potreba IT profesionalaca i razvojnih inženjera.
3. Dolaze kao zasebne izvršne datoteke koje ne zahtijevaju instalaciju i mogu se pokrenuti s bilo koje lokacije, uključujući mrežne lokacije i prijenosne medije.
4. Nakon izvođenja ne ostavljaju nikakve značajne slučajne podatke.

Sysinternals alate moguće je preuzeti sa sljedeće poveznice:

http://technet.microsoft.com/en-us/sysinternals/bb545027

Tamo je moguće preuzeti pojedini program zasebno ili pak čitav skup programa u jednoj komprimiranoj datoteci nazvanoj Sysinternals Suite. Nakon raspakiravanja, pojedini program se pokreće pokretanjem izvršne datoteke (.exe) ili više njih, ako ih ima. Osim na ovaj način, programe je moguće pokrenuti izravno s weba pomoću usluge Sysinternals Live. U tom slučaju nije ih potrebno preuzimati niti raspakiravati, a dodatna je prednost Sysinternals Live u tome što osigurava izvođenje najnovije inačice traženog programa.

3. Jezgra operacijskog sustava Windows

Razumijevanje koncepta jezgre operacijskog sustava vrlo je važno prilikom korištenja Sysinternals Suite alata. Što je korisnik bolje upoznat s načinom rada i konceptima jezgre operacijskog sustava Windows, to će mu Sysinternals alati biti od veće koristi. U nastavku je ukratko opisan koncept jezgre operacijskog sustava Windows kako bi bilo lakše razumjeti rad i namjenu Sysinternals alata. U knjizi [2] može se pronaći opsežan i detaljan opis rada jezgre operacijskog sustava Windows.

3.1. Upravljačka prava

U operacijskim sustavima Windows korisničkim računima su najčešće dodijeljena administratorska ili korisnička prava. Administratorska prava omogućuju potpun i neograničen pristup računalu i svim njegovim resursima, dok korisnička prava nose sa sobom zabrane izmjene konfiguracije operacijskog sustava, kao i zabranu pristupanja podacima koji pripadaju drugim korisnicima. Jedan dio Sysinternals programa zahtijeva administratorska prava, dok drugi dio ima punu funkcionalnost i bez njih. Ipak, postoje i neki programi koji mogu raditi s korisničkim pravima, ali su im za neka svojstva potrebna administratorska prava pa stoga djeluju u svojevrsnom 'degradiranom načinu rada' ako su pokrenuti s korisničkim pravima. Kod operacijskog sustava Windows XP korisnik iz skupine administratora ne treba ništa dodatno napraviti kako bi pokrenuo Sysinternals programe koji zahtijevaju administratorska prava. Svaki program kojeg taj korisnik pokrene automatski ima puna administratorska prava. Korisnik koji nema administratorska prava ne može pokrenuti takav program bez dobivanja administratorskih prava od nekog drugog korisnika. Za razliku od toga, kod operacijskih sustava Windows Vista i novijih, korisnički programi zadano se pokreću s korisničkim pravima, čak i ako korisnik posjeduje administratorska prava. Stoga, ako neki program zahtijeva administratorska prava potrebno ga je pokrenuti kao administrator (eng. *Run as administrator*).

3.2. Procesi, dretve i poslovi

Na početku je potrebno objasniti razliku između programa i procesa, koji se na prvi pogled čine jednakima, no u suštini se bitno razlikuju. Program je statični niz instrukcija, dok proces predstavlja skup računalnih resursa koji omogućuju izvođenje programa. Na najvišem stupnju apstrakcije procesi operacijskog sustava Windows obuhvaćaju:

- jedinstveni identifikator procesa koji se naziva *process ID (PID)*,
- najmanje jednu dretvu izvođenja, pri čemu svaka dretva u procesu ima potpuni pristup svim resursima koje proces obuhvaća,
- privatni virtualni adresni prostor, koji predstavlja skup virtualnih memorijskih adresa koje su na raspolaganju procesu za pohranjivanje i referenciranje podataka i naredaba,
- izvršni program, koji određuje početne naredbe i podatke koji se preslikavaju u virtualni adresni prostor procesa,
- popis otvorenih ručica (eng. *handles*) prema raznim sustavskim resursima te
- sigurnosni kontekst koji se naziva pristupni znak (eng. *access token*).

Operacijski sustav Windows nudi proširenje navedenog modela procesa, koji se naziva posao (eng. *job*). Njegova glavna zadaća je omogućiti rukovanje i upravljanje skupinom procesa kao cjelinom. Posao također omogućuje ispitivanje pojedinih atributa i daje granice za proces ili više njih koji su povezani u isti posao.

Dretva (eng. *thread*) je entitet unutar procesa koji je raspoređen za izvođenje. Svaki proces ima barem jednu dretvu izvođenja. Svaka dretva sadrži vlastito programsko brojilo, registre procesora, jedinstveni identifikator dretve (eng. *thread ID, TID*) i dva stoga (po jedan za izvođenje u korisničkom i jezgrinom načinu rada). Premda svaka dretva ima vlastiti kontekst izvođenja, svaka dretva unutar procesa dijeli virtualni adresni prostor procesa, pa na taj način dretve mogu međusobno komunicirati.

3.3. Korisnički i jezgrin način rada

Kako bi se korisničke aplikacije spriječile od pristupanja ili mijenjanja kritičnih podataka operacijskog sustava, operacijski sustav Windows koristi dva procesorska pristupna načina rada: korisnički (eng. *user mode*) i jezgrin (eng. *kernel mode*) način rada. Svi procesi, osim onih sustavskih, izvode se u korisničkom načinu rada. Za razliku od njih, pogonski programi uređaja te komponente operacijskog sustava izvode se samo u jezgrinom načinu rada. Jezgrin način rada odnosi se na način izvođenja u procesoru u kojem je omogućen pristup cjelokupnoj memoriji sustava kao i svim procesorskim naredbama. Dretve procesa u korisničkom načinu rada prebacuju se iz korisničkog u jezgrin način rada prilikom obavljanja sustavskih poziva. Stoga je za dretvu procesa u korisničkom načinu rada potpuno normalno da dio svog vremena izvođenja provede u korisničkom, a dio u jezgrinom načinu rada.

3.4. Handles

Jezgreni način rada operacijskog sustava Windows sastoji se od različitih podsustava kao što su: upravitelj memorije (eng. *Memory Manager*), upravitelj procesa (eng. *Process Manager*), upravitelj ulazno-izlaznih podataka (eng. *I/O Manager*) te upravitelj konfiguracije (eng. *Configuration Manager*). Svaki od ovih podsustava definira s upraviteljem objekata (eng. *Object Manager*) jedan ili više tipova za predstavljanje resursa koje izlažu aplikaciji. Kada aplikacija želi koristiti jedan od tih resursa, prvo mora pozvati odgovarajuće programsko sučelje, (eng. *Application Programming Interafce, API*) kako bi stvorila ili otvorila resurs. Nakon što je to uspješno napravljeno, operacijski sustav Windows alocira referencu na objekt u *handle* tablici procesa i vraća aplikaciji indeks novog unosa u *handle* tablicu. Aplikacija koristi *handle* vrijednost (eng. *hendlers*) za sljedeće operacije na resursu. Kada proces više ne treba pristup objektu, može osloboditi svoje *handle* vrijednosti prema tom objektu. Prilikom završetka procesa sve *handle* vrijednosti koje tada posjeduje se zatvaraju.

3.5. Stog poziva i simboli

Izvršni kod u procesu tipično je organiziran kao zbirka diskretnih funkcija. Kako bi izvela svoje zadatke funkcija može pozivati i druge funkcije (podfunkcije). Kada pozvana funkcija završi s radom vraća natrag kontrolu funkciji koja ju je pozvala. Stog poziva (eng. *call stack*) je stogovna struktura podataka koja omogućuje sustavu poznavanje kome treba vratiti kontrolu nakon niza poziva, te omogućuje prenošenje parametara između funkcija i pohranjivanje lokalnih varijabli pozvanih funkcija.

Prilikom stvaranja izvršnih datoteka mogu se stvoriti odgovarajuće datoteke simbola (eng. *symbol files*). One sadrže različite podatke koji nisu potrebni prilikom pokretanja izvršnog koda, ali koji mogu biti korisni za vrijeme *debuggiranja*, uključujući imena i pomake ulaznih točaka funkcija u modulu. Pomoću ove informacije *debugger* može uzeti adresu u memoriji i lako identificirati funkciju s najbližom prethodnom adresom. Bez simbola *debugger* je ograničen u korištenju izlaznih funkcija koje vjerojatno nemaju veze s kodom koji se izvodi. Da bi bila valjana, datoteka simbola mora biti izgrađena istovremeno s odgovarajućom izvršnom datotekom.

4. Sysinternals Suite alati

Sysinternals uslužni programi pokrivaju široki raspon funkcionalnosti koje uključuju brojne aspekte operacijskog sustava Windows. Neki programi, kao što su primjerice Process Explorer i Process Monitor, zbog svoje opsežnosti spadaju u više kategorija, dok se većina ostalih programa može svrstati u pojedinu kategoriju. Kategorije u koje se programi dijele (prema [1]) su:

- **procesni i dijagnostički uslužni programi** (eng. *Process and Diagnostic Utilities*),
- **sigurnosni uslužni programi** (eng. *Security Utilities*),
- **uslužni programi za aktivni direktorij** (eng. *Active Directory Utilities*),
- **uslužni programi za radnu površinu** (eng. *Desktop Utilities*),
- **datotečni uslužni programi** (eng. *File Utilities*),
- **uslužni programi za disk** (eng. *Disk Utilities*),
- **mrežni i komunikacijski uslužni programi** (eng. *Network and Communication Utilities*),
- **uslužni programi za sustavske informacije** (eng. *System Information Utilities*),
- **razni uslužni programi** (eng. *Miscellaneous Utilities*).

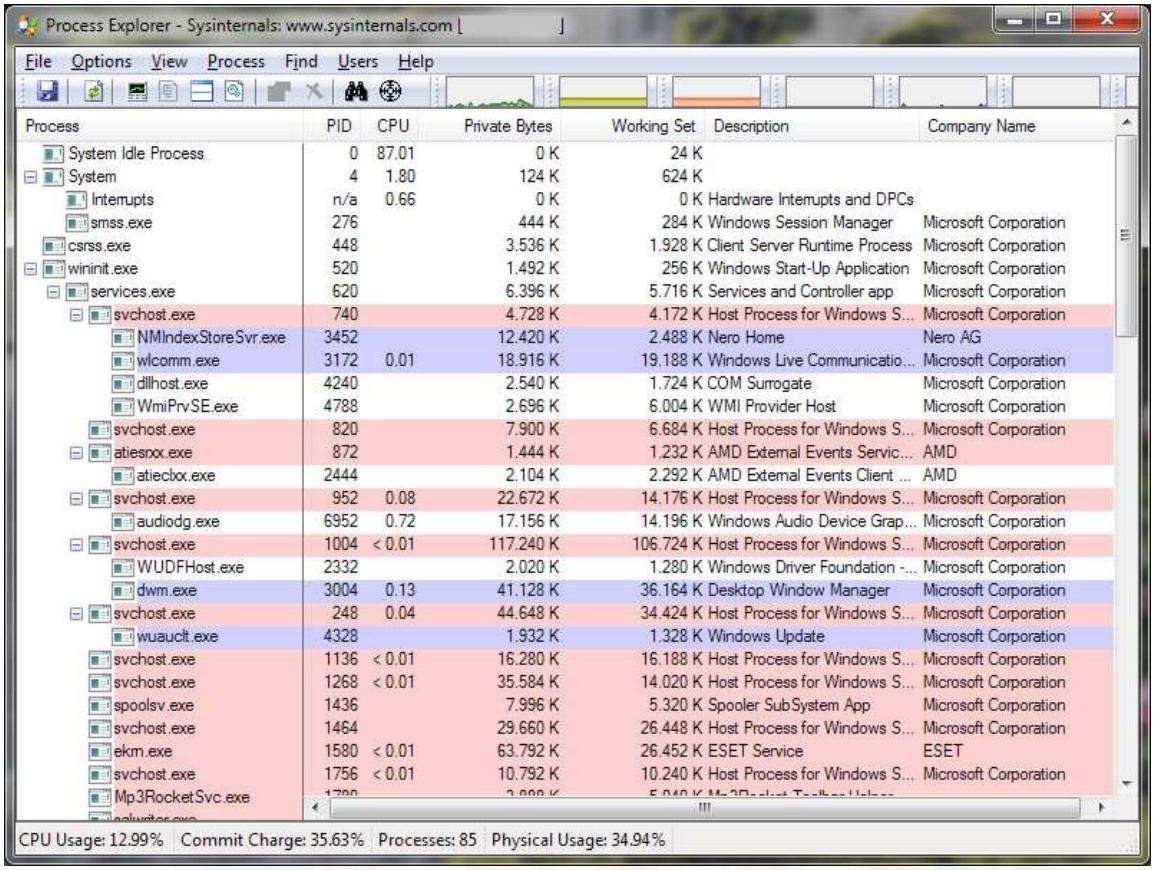
Mnogi od uslužnih programa imaju grafičko korisničko sučelje (eng. *Graphical User Interface, GUI*), dok su ostali konzolni uslužni programi s naredbenim sučeljem (eng. *Command Line Interface*). U narednim poglavljima dan je pregled funkcionalnosti te primjeri korištenja za neke od najznačajnijih Sysinternals programa. Informacije o ostalim programima te njihovim funkcionalnostima, kao i njihov cjelokupan popis mogu se pronaći u [1], odnosno na poveznici [4].

4.1. Process Explorer

Procesi su središte svakog Microsoft Windows operacijskog sustava. Njihovo poznavanje, odnosno znanje o trenutno aktivnim procesima može pomoći oko shvaćanja na koji se način koriste procesor i resursi, a jednako može biti koristan i za identificiranje problema. Upravo Process Explorer daje iscrpne i detaljne informacije o procesima u sustavu. Spada u više kategorija, a naročito je značajan za kategoriju sigurnosnih uslužnih programa. Process Explorer je najpopularniji program iz skupa Sysinternals alata. To je ujedno i program najbogatiji mogućnostima i funkcijama koje nudi. Samo neke od njegovih glavnih značajki su:

- pogled u obliku stabla prikazuje odnose procesa roditelj/dijete,
- kodiranje u boji identificira tip procesa,
- isticanje novih i netom završenih procesa,
- detaljniji prikaz procesa omogućuje prikaz procesa koji troše manje od 1% procesorskog vremena,
- točniji prikaz potrošnje procesora,
- potpuno zamjenjuje upravitelja zadataka (eng. *Task Manager*),
- identificira koji procesi posjeduju prozore vidljive na radnoj površini,
- grafički prikazi aktivnosti procesora, korištenja memorije, ulazno-izlaznih aktivnosti, za cjelokupni sustav ili pak za pojedini proces,
- detaljne mjere korištenja memorije i ulazno-izlaznih aktivnosti,
- i još mnoge druge detaljne i korisne informacije o procesima i svemu vezanom uz njih.

Process Explorer omogućuje nekoliko pogleda za prikaz informacija o procesima. Glavni prozor Process Explorera prikazan je na slici u nastavku.



Slika 3. *Glavni prozor Process Explorera*
Izvor: *LSS*

Lista procesa je tablica u kojoj svaki redak predstavlja proces u sustavu, a stupci predstavljaju trajno osvježene atribute tih procesa. Moguće je promijeniti koji atributi će biti prikazani, kao i njihov redoslijed i veličinu stupaca. Alatna traka sadrži gumbe za izvođenje čestih akcija i grafičku prezentaciju sustavskih mjerenja. Statusna traka prikazuje sustavske mjere.

4.1.1. Isticanje procesa

Jedna od prvih stvari koja se može zapaziti u glavnom prozoru je uporaba različitih boja za isticanje i razlikovanje različitih tipova procesa. Moguće je je podesiti koji tip procesa će biti istaknut kojom bojom, no zadane su sljedeće boje:

- **svijetlo plava** - označava procese koji se izvode u istom korisničkom računu kao i Process Explorer,
- **ružičasta** - označava procese koji sadrže Windows usluge,
- **ljubičasta** - označava 'upakirane datoteke',
- **smeđa** - označava poslove, odnosno više procesa kojima se upravlja kao cjelinom,
- **žuta** - označava procese koji koriste Microsoft .NET Framework
- **tamno siva** - označava suspendirane procese, odnosno one procese u kojima su sve dretve suspendirane i ne mogu biti raspoređene za izvođenje.

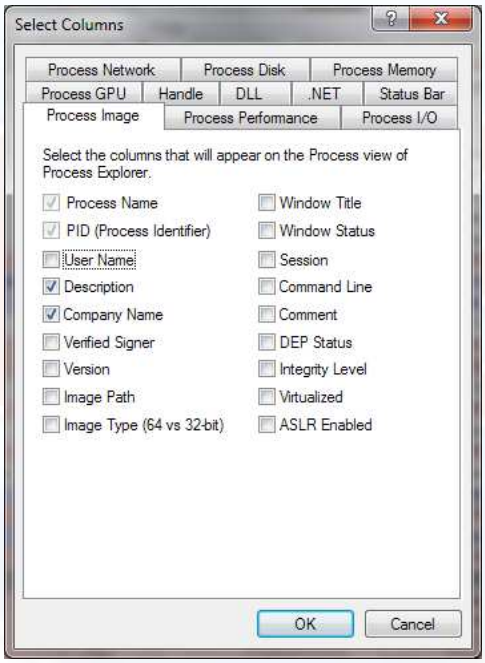
Ako proces spada u više od jedne kategorije označava se u prvu skupinu prema poretku: suspendirani, upakirani, .NET, poslovi, usluge, vlasnički procesi. Osim isticanja vrste procesa, Process Explorer ističe i nove procese (zelena pozadina koja traje jednu sekundu) te procese koji su upravo završili (crvena pozadina koja traje jednu sekundu).

4.1.2. Zadani stupci

Svaki stupac u listi procesa predstavlja neki statični ili dinamični atribut procesa. Dinamički atributi osvježavaju se jednom u svakom intervalu osvježavanja, a zadana vrijednost je jedna sekunda. Stupci u zadanoj konfiguraciji Process Explorera su:

- **Process** - stupac prikazuje ime izvršne datoteke, a ako može identificirati i put do te izvršne datoteke prikazuje i ikonu,
- **PID** - identifikacijski broj procesa,
- **CPU** - postotak procesorskog vremena, zaokružen na dvije decimale, koji je procesor zauzeo unutar posljednjeg intervala osvježavanja,
- **Private Bytes** - broj bitova koje je proces alocirao i koristi za svoju uporabu, a koje ne dijeli s drugim procesima,
- **Working Set** - količina fizičke memorije pridružena procesu od strane upravitelja memorije,
- **Description and Company Name** - opis i ime prikazuju se jedino ako Process Explorer može identificirati put do datoteke i pročitati iz nje.

Navedeni stupci predstavljaju tek malen dio od ukupnog broja stupaca koje je moguće odabrati. Odabir stupaca koji će biti prikazani obavlja se odabirom naredbe *Select Columns* iz izbornika *View*. Izgled prozora *Select Columns* prikazan je na Slici 4.



Slika 4. *Prozor Select Columns*
Izvor: *LSS*

4.1.3. Ostale mogućnosti

Process Explorer nudi beskrajne mogućnosti podešavanja i odabira različitih atributa, načina prikaza, akcija koje je moguće izvesti s procesom i brojnih drugih stvari vezanih uz procese. Sve prikazane podatke moguće je spremiti u tekstualnu datoteku. Moguće je također vidjeti detaljne informacije o *DLL* datotekama[1] i *handle*-ovima[2], kao i o dretvama. Budući da sadrži mnogo više informacija, koje su pritom mnogo detaljnije, od Task Managera, Process Explorer može ga u potpunosti zamijeniti. Iscrpan opis svih mogućnosti i podešenja koje nudi Process Explorer može se pronaći u dodatnoj literaturi pod [1].

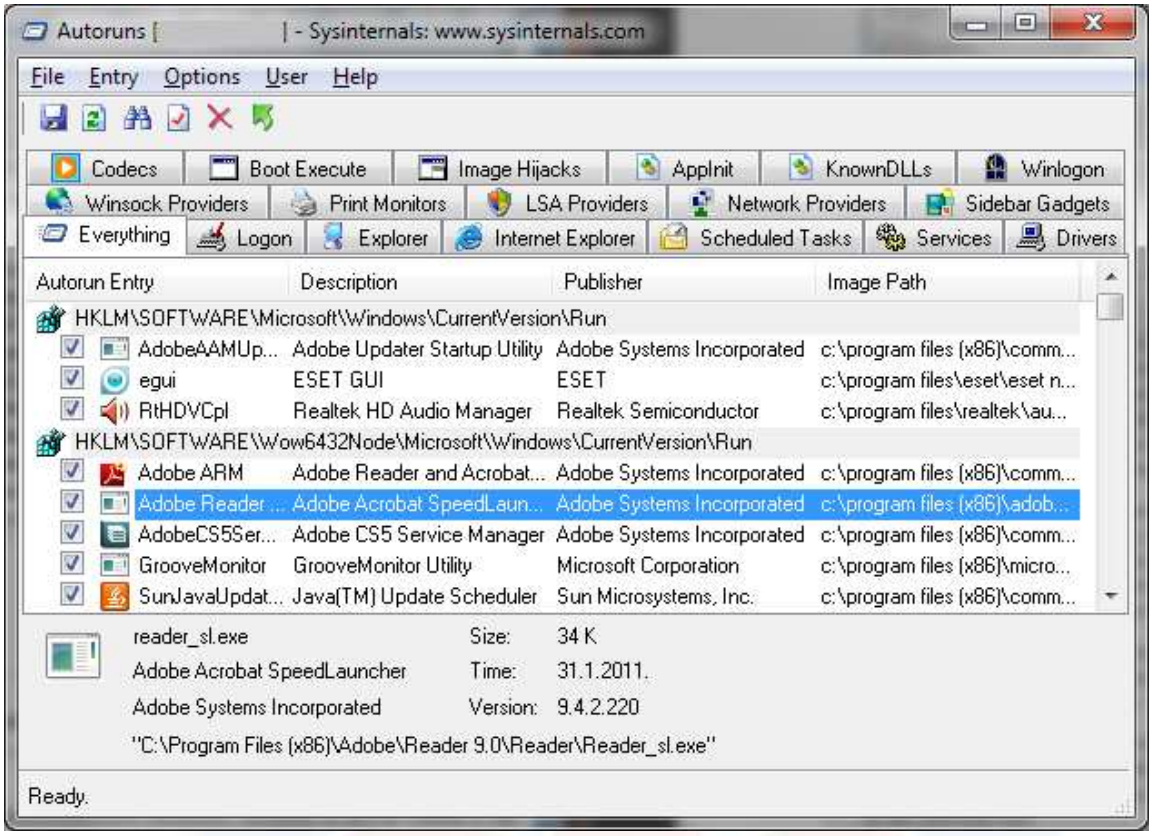
4.2. Autoruns

Još jedan od programa značajnih u kontekstu sigurnosti je program Autoruns. Uslužni program Autoruns stvoren je za otkrivanje što više programa koji se pokreću automatski, bez da ih je korisnik namjerno započeo (eng. *autostarts*), te za olakšavanje njihovog onemogućavanja ili uklanjanja. Informacije koje otkriva Autoruns mogu se otkriti i ručno, ako se zna gdje u registarskom i datotečnom sustavu treba tražiti takve programe. No Autoruns automatizira taj posao, izvodeći ga u nekoliko sekundi. Postoji više od stotinu adresa u datotečnom sustavu i registrima koje omogućuju konfiguriranje programa koji se pokreću automatski. Takve adrese često se nazivaju točke proširenja automatskog pokretanja (eng. *AutoStart Extensibility Points, AESP*).

Pokretanjem programa Autoruns odmah započinje punjenje prozora s unosima sakupljenim iz poznatih ASEP-ova. Na Slici 5. prikazan je glavni prozor programa Autoruns.

[1] DLL datoteka (eng. *Dynamic-link library file, DLL file*) je vrsta izvršne datoteke koja omogućuje programima dijeljenje koda i ostalih resursa potrebnih za izvođenje pojedinih zadataka. Operacijski sustav Microsoft Windows nudi DLL datoteke koje sadrže funkcije i resurse koji omogućavaju programima zasnovanim na operacijskom sustavu Windows izvođenje u Windows okruženju.

[2] *Handle* je referenca na neki podatak, slično kao pokazivač. No za razliku od pokazivača, *handle* se ne može dereferencirati. Većini objekata se pristupa preko *handleova*.



Slika 5. *Glavni prozor programa Autoruns*
Izvor: *LSS*

Svaki osjenčani red predstavlja ASEP adresu s pripadajućom ikonom, ovisno o tome nalazi li se ASEP u registarskoj adresi ili u datotečnom sustavu. Redovi ispod osjenčanog retka označavaju unose konfigurirane u tom ASEP-u. Svaki redak sadrži ime automatskog programa, opis i ime njegovog izdavača te put do datoteke. Uz to, u svakom retku nalazi se i kvadratić za označavanje kojim je moguće privremeno onemogućiti entitet iz tog retka. U prostoru na dnu prozora prikazuju se detalji o odabranom unosu. Za vrijeme dok Autoruns pretražuje sustav izbornik Options je onemogućen.

Autoruns omogućuje brisanje ili onemogućavanje pronađenih automatskih programa. Brisanje pojedinog unosa u nekom retku ga trajno briše. Kako bi se provelo brisanje potrebno je označiti redak i pritisnuti tipku Del. Za razliku od brisanja, za onemogućavanje unosa u nekom retku potrebno je označiti kvadratić za odabir u tom retku. O svakom unosu moguće je dobiti više informacija desnim klikom miša na željeni unos i odabirom željene funkcije. Za pregledniji prikaz moguće je unose podijeliti u kategorije. Postoji 17 takvih kategorija, a njihov pregled dan je u [1].

4.2.1. Autoruns i *malware*

Jedan od glavnih ciljeva većine zlonamjernih programa (eng. *malware*) je ostati aktivan na zaraženom sustavu što je dulje moguće. Zlonamjerni programi su stoga uvijek koristili ASEP. S vremenom su postali sve profinjeniji i teži za otkrivanje. Ipak, postoje određeni znakovi koji otkrivaju prisutnost zlonamjernih programa:

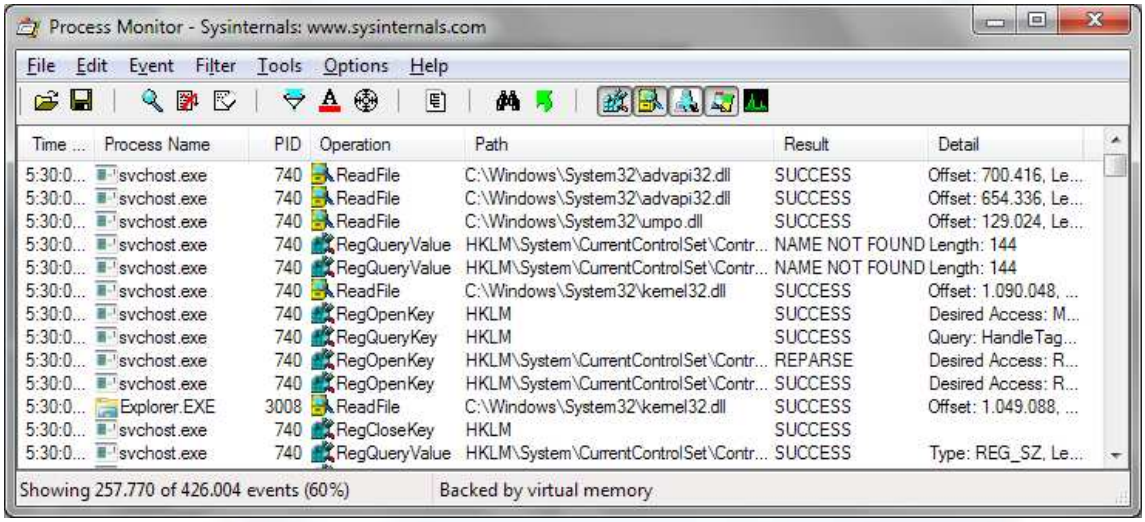
- unosi s dobro poznatim izdavačem, kao što je primjerice Microsoft, koji nisu prošli ovjeru potpisa,
- unosi čiji put ukazuje na DLL ili EXE datoteku za koju nedostaje opis i informacije o izdavaču,
- česta Windows komponenta koja je pokrenuta iz neobične ili nestandardne adrese,
- unosi za koje datum i vrijeme pokretanja programa odgovaraju vremenu kada su se pojavili problemi ili je otkrivena povreda,

- onemogućavanje ili brisanje unosa koji se nakon osvježavanja ponovno pojavljuju prisutni i omogućeni. Zlonamjerni program često nadzire svoje ASEP-e i vraća ih natrag ako se uklone.

U nastavku je ukratko opisana funkcionalnost nekih od najpopularnijih Sysinternals programa s posebnim naglaskom na one koji spadaju u kategoriju sigurnosnih programa.

4.3. Process Monitor

Process Monitor spada među najpopularnije Sysinternals alate. To je napredan alat za operacijski sustav Windows koji u stvarnom vremenu prikazuje aktivnosti datotečnog sustava, registara te procesa i dretvi. Kombinira svojstva dva bivša Sysinternals programa, Filemona i Regmona, te dodaje opsežnu listu poboljšanja koja uključuju bogato i nedestruktivno filtriranje, opsežna svojstva događaja kao što su identifikator sjednice i korisnička imena, pouzdane procesne informacije, stog dretve s ugrađenom podrškom za simbole za svaku operaciju, istovremeno prijavljivanje u datoteku. Process Monitor zahtijeva pokretanje s administratorskim pravima. Na Slici 6. prikazan je izgled glavnog prozora Process Monitora.



Slika 6. *Glavni prozor Process Monitora*
Izvor: *LSS*

4.4. RootkitRevealer

RootkitRevealer je napredan program za otkrivanje *rootkita*. *Rootkitovi* su zlonamjerni programi koji su napravljeni kako bi preuzeli nadzor nad operacijskim sustavom tako da nadomjeste sustavske procese i podatke bez dopuštenja korisnika. Postoji nekoliko klasifikacija *rootkitova* ovisno o tome preživi li zlonamjerni program ponovno pokretanje računala te izvodi li se u korisničkom ili jezgrinom načinu rada:

- **Trajni rootkit** je povezan sa zlonamjernim programom koji se aktivira svaki put prilikom podizanja sustava. Budući da takav zlonamjerni program sadrži kod koji se mora automatski izvesti prilikom svakog pokretanja sustava ili kada se korisnik prijavi u sustav, potrebno ga je pohraniti u registar ili datotečni sustav te konfigurirati metodu kojom će se izvoditi bez sudjelovanja korisnika.
- **Rootkit temeljen na memoriji** je zlonamjerni program koji nema trajnog koda i stoga neće biti aktivan nakon ponovnog pokretanja računala.
- **Rootkit korisničkog načina rada** može prekinuti sve pozive prema programskim sučeljima koje koriste programi za istraživanje datotečnog sustava kako bi pobrojali sadržaj direktorija datotečnog sustava.

- **Rootkit jezgrinog načina rada** može biti još opasniji budući da može ne samo prekidati izvorno korisničko sučelje u jezgrinom načinu rada, već može izravno upravljati sa strukturama podataka jezgrinog načina rada.

4.5. AccessChk

AccessChk je program s naredbenim sučeljem koji daje informacije o postojećim dozvolama pristupa resursima, kao što su datoteke, direktoriji, registarski ključevi, procesi, globalni objekti ili Windows usluge, koje imaju pojedini korisnici ili skupine korisnika. Spada u skupinu sigurnosnih uslužnih programa. Jedno od najjačih obilježja programa AccessChk jest mogućnost preteživanja objekata koji dodjeljuju dozvole pristupa pojedinim korisnicima ili skupinama. Osnovna sintaksa programa AccessChk je sljedeća:

```
accesschk [opcije] [korisnik-ili-skupina] imeobjekta
```

Parametar *imeobjekta* predstavlja objekt koji se analizira. Ako se zada opcionalni parametar *korisnik-ili-skupina* program će izvijestiti o važećim dozvolama samo za te korisnike ili skupinu, inače će prikazati važeće dozvole za sve račune iz liste kontrole pristupa objekta. Parametar *opcije* omogućuje odabir tipova dozvola, količine detalja u izvješću, odabir tipa objekta i još mnoge druge opcije.

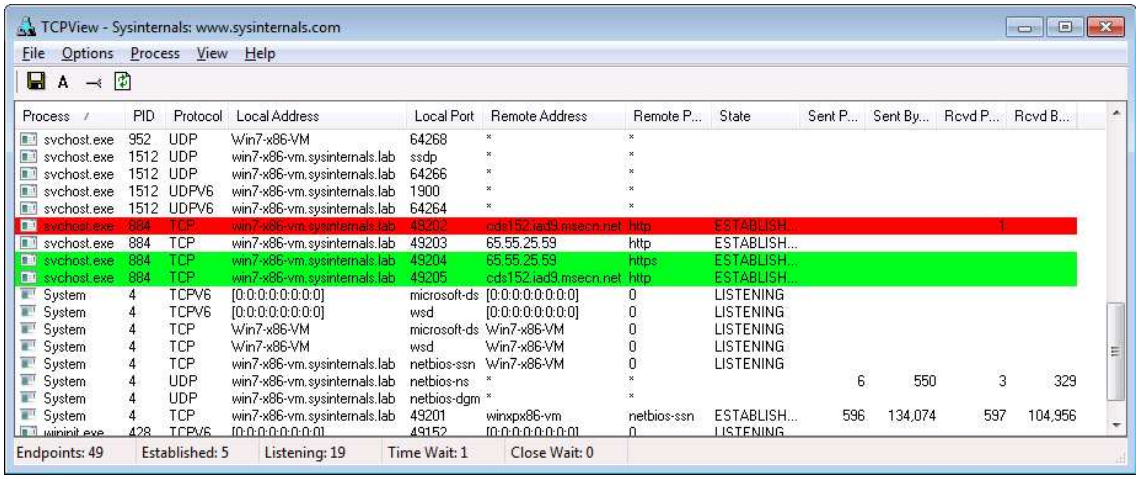
4.6. SigCheck

SigCheck je višenamjenski program s naredbenim sučeljem za provođenje funkcija vezanih uz sigurnost nad jednom ili više datoteka (ili u hijerarhiji mapa). Njegova primarna namjena je potvrda jesu li datoteke digitalno potpisane s valjanim certifikatom. Ovjereni potpis potvrđuje dolaženje datoteke od vlasnika kodnog certifikata te ostajanje datoteke u izvornom obliku (od trenutka kad je potpisana). Parametri naredbene linije procesa SigCheck omogućuju odabir brojnih mogućnosti za provođenje ovjere, određivanje koje datoteke će se analizirati te format izlaznih podataka.

4.7. TCPView

TCPView je program s grafičkim korisničkim sučeljem koji pokazuje ažurirane detaljne popise svih TCP (eng. *Transfer Control Protocol*) i UDP (eng. *User Datagram Protocol*) krajnjih točaka na korisnikovom sustavu, bilo da se radi krajnjim točkama u protokolima IPv4 ili IPv6. Za svaku krajnju točku prikazuje ime vlasničkog procesa, ID procesa, lokalne i udaljene adrese i vrata te stanja TCP veza. Prilikom preuzimanja programa TCPView uključeno je preuzimanje programa Tcpvcon, koji predstavlja inačicu jednake funkcionalnosti kao i TCPView, ali s naredbenim sučeljem. TCPView spada među najpopularnije Sysinternals alate.

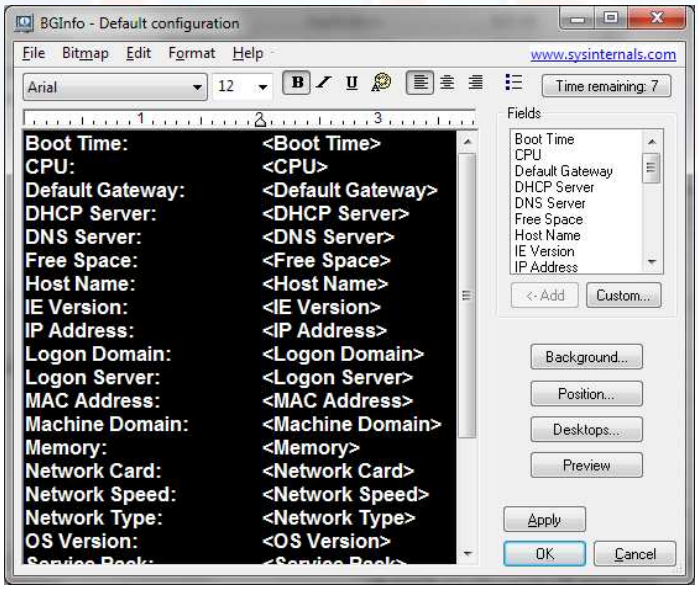
Nakon što se pokrene, TCPView će pobrojati sve aktivne TCP ili UDP krajnje točke, razrješujući sve IP adrese u njihove inačice s domenskim imenom. TCPView se osvježava svaku sekundu, no to je moguće promijeniti. Krajnje točke koje mijenjaju stanje između dva osvježavanja istaknute su žutom bojom, one izbrisane su istaknute crvenom bojom, dok će nove krajnje točke biti istaknute zelenom bojom. Na Slici 7. prikazan je izgled glavnog prozora programa TCPView.



Slika 7. *Glavni prozor programa TCPView*
Izvor: *LSS*

4.8. BgInfo

BgInfo je jedan od najpopularnijih Sysinternals alata. Spada u skupinu uslužnih alata za radnu površinu. Automatski prikazuje na radnoj površini relevantne informacije o računalu, kao što su primjerice naziv računala, IP adresa, inačica operacijskog sustava, količina radne memorije i ostale korisne informacije. Prilikom pokretanja programa BgInfo otvara se *editor* u kojem se odabire koji će podaci biti prikazani na radnoj površini. Uz to, moguće je mijenjati i veličinu, izgled te boju slova prikaza. Moguće je i smjestiti ga u *startup* mapu kako bi se pokrenuo prilikom svakog započinjanja sustava. Na Slici 8. prikazan je izgled BgInfo *editora*.

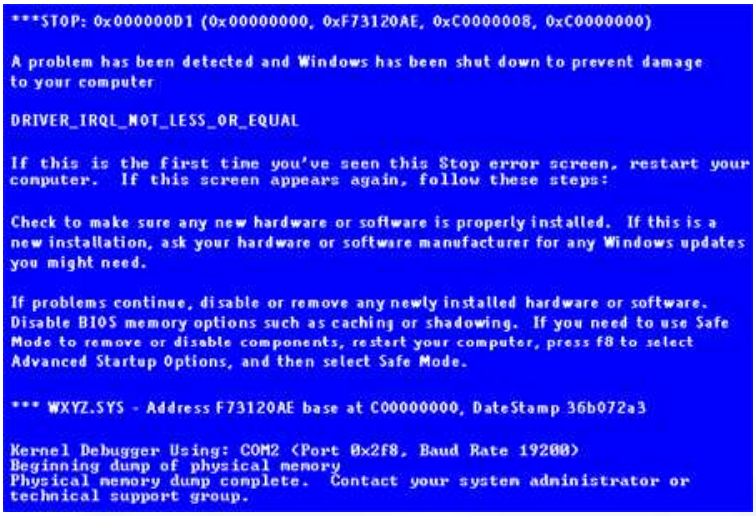


Slika 8. *Izgled BgInfo editora*
Izvor: *LSS*

4.9. BlueScreen

Bluescreen Screen Saver nije uključen u Sysinternals Suite, već ga je moguće preuzeti sa Sysinternals web stranice. Ovdje nije riječ o nekom 'korisnom' programu, nego se radi od čuvaru zaslona (eng. Screen Saver) koji simulira tzv „*beskonačni ciklus plavog ekrana smrti*“ (eng. Blue

Screen of Death, BSOD) i restartanja sustava (Slika 9). Radi se o jednom od najpopularnijih Sysinternals programa.



Slika 9. BSD
Izvor: google.com

5. Budućnost alata Sysinternals Suite

Premda je prošlo petnaestak godina od nastanka Sysinternals Suite alata i premda su doživjeli brojne dopune i poboljšanja, njihov razvoj tu ne završava. Dokle god njihovi autori imaju ideja za poboljšanja i dodatke, dotle će se i Sysinternals Suite alati nastaviti razvijati. Njihova bliža budućnost usko je vezana uz nadogradnju i poboljšanja postojećih programa. To se prvenstveno odnosi na najpopularnije programe: Process Explorer i Process Monitor. Na nadogradnji ovih programa već se radi pa je realno očekivati objavljivanje novih inačica u narednih nekoliko mjeseci. Veća pažnja zasigurno će se posvetiti sigurnosnim aspektima uz koje su vezane teme za pristup te dozvole pristupa.

Ovisno o razvoju novih inačica operacijskog sustava Windows, u skoroj budućnosti vjerojatno će se pojaviti potreba za nekim novim programima ili će biti potrebno napraviti izmjene u već postojećim programima. Korisnost ovih alata u budućnosti može samo rasti, posebno stoga što će se oni nastaviti razvijati, a i sami njihovi korisnici će proširivanjem svojih znanja o jezgri operacijskih sustava imati više koristi od postojećih i budućih alata. Ono što možda krajnje korisnike ovog skupa alata najviše brine je hoće li alati i dalje biti dostupni za besplatno preuzimanje. Iz Microsofta odgovaraju kako nemaju namjere ukloniti ili početi naplaćivati Sysinternals Suite alate. Dakle, pred Sysinternals Suite alatima i svim njihovim korisnicima je zasigurno svijetla budućnost.

6. Zaključak

„Sysinternals suite“ predstavlja skup od 70-ak vrlo korisnih uslužnih programa za Microsoft Windows okruženje. Njihova temeljna namjena je upravljanje, dijagnostika te za prikaz podataka o dijelovima sustava, kao i o sustavu u cjelini. Dobiveni podaci su vrlo korisni za razumijevanje rada sustava te za potencijalno pronalaženje i otklanjanje grešaka u sustavu. Za korisnika Sysinternals Suite alata važno je poznavanje načina rada operacijskog sustava Windows te razumijevanje koncepata jezgre operacijskog sustava. Korisnik s većim znanjima iz ovih područja moći će i iskoristiti više mogućnosti koje mu pružaju ovo alati.

Vjerojatno najznačajniji i najopsežniji Sysinternals alat je *Process Explorer*. Njegove brojne mogućnosti vezane uz prikaz podataka o procesima te upravljanje njima daleko nadmašuju mogućnosti *Task Manager-a* pa ga Process Explorer može u potpunosti zamijeniti. Pored Process Explorera, skup od tri najznačajnija programa čine još i Process Monitor te Autoruns. Važno je naglasiti da se funkcionalnosti svih Sysinternals programa međusobno nadopunjuju, odnosno da svaki program usmjerava svoj rad na neku drugu značajku ili komponentu operacijskog sustava Microsoft Windows. Važna skupina Sysinternals alata su sigurnosni programi, čija namjena je usmjerena na kritične dijelove sustava s pogleda sigurnosti.

U budućnosti će se nastaviti poboljšavanje postojećih alata, dodavanje novih funkcionalnosti te razvoj novih alata. Nove poboljšane inačice postojećih programa već su najavljene te se u narednim mjesecima očekuje njihovo objavljivanje, a korisnicima se svakako preporuča korištenje ovih alata.

Leksikon pojmova

AccessChk

AccessChk je uslužni program s naredbenim sučeljem iz skupine sigurnosnih programa koji daje informacije o postojećim dozvolama pristupa resursima, kao što su datoteke, direktoriji, registarski ključevi, procesi, globalni objekti ili Windows usluge, koje imaju pojedini korisnici ili skupine korisnika.

http://technet.microsoft.com/en-us/sysinternals/bb664922

TCP (Transmission Control Protocol)

Jedan od dva protokola usmjeravanja koja se koriste u Internetu, uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos. TCP se nalazi na transportnom sloju OSI modela. - Jedan od dva protokola usmjeravanja koja se koriste u Internetu. Uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos.

Reference: http://www.webopedia.com/TERM/T/TCP.html

IP protokol (Internet Protocol)

IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanja paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža.

Reference: http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm

Rootkit

Rootkit-ovi su zlonamjerni programi koji su napravljeni da bi preuzeli kontrolu nad operacijskim sustavom tako da nadomjeste sustavske procese i podatke bez dopuštenja korisnika.

Reference: http://os2.zemris.fer.hr/ns/2008_Mackovic/rootkit.htm, http://searchmidmarketsecurity.techtarget.com/definition/rootkit

***Payload* - Koristan teret**

Na području informacijske sigurnosti, koristan teret označava odsječak koda pomoću kojeg se iskorištava određeni propust računala mete. Na primjer, koristan teret računalnog crva može sadržati modul za širenje vlastite kopije putem globalne mreže Internet.

Reference: http://searchsecurity.techtarget.com/definition/payload

IPv6 (Internet Protocol version 6)

IPv6 je nova inačica IP protokola. Trenutna inačica (IPv4) koristi 32 bita za IP adrese, dok IPv6 koristi IP adrese od 128 bita. Time se uvelike povećao adresni prostor što je jedan od glavnih problema IPv4 inačice. IPv6 također unosi bolju podršku za mobilnost i višeodredišne adrese, kao i neke dodatne mogućnosti koje nisu dostupne u trenutnoj inačici.
Reference: http://www.networkworld.com/news/2011/082911-ipv6-250196.html

Reference

[1] Russniovich, M., Margois, A. Windows Sysinternals Administrator's Reference, Microsoft Press, 2011. http://technet.microsoft.com/en-us/sysinternals/hh290819, studeni 2011.

[2] Russniovich, M., Solomon, D., Ionescu, A. Windows internals, Microsoft Press, 2009. http://technet.microsoft.com/en-us/sysinternals/bb963901, studeni 2011.

[3] Winternals - Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Winternals, studeni 2011.

[4] Sysinternals Utilities Index, Windows Sysinternals, http://technet.microsoft.com/en-us/sysinternals/bb545027, studeni 2011.

[5] Interview with Mark Russinovich: The future of Sysinternals, Security, Windows, http://technet.microsoft.com/en-us/edge/Video/ff710550, studeni 2011.

[6] Sysinternals Learning Resources, Windows Sysinternals, http://technet.microsoft.com/en-us/sysinternals/bb469930, studeni 2011.