CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Anti-rootkit programi

NCERT-PUBDOC-2010-01-287

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Korisnici osobnih računala često nisu svjesni svih prijetnji koje dolaze s Interneta. Većina korisnika upotrebljava neki antivirusni program kojem prepušta svu zaštitu sustava. Problem se javlja kada sustav napadne neki od zlonamjernih programa koje antivirusni alati ne mogu detektirati. Jedna od takvih prijetnji je *rootkit* program.

Spomenuti zlonamjerni program ima svrhu skrivanja nedopuštenih aktivnosti na sustavu. Cilj toga je osiguravanje kontrole nad ugroženim sustavom, skrivanje zlonamjernih programa ili stvaranje tzv. *zombie* računala. Svoju neprimjetnost na ugroženom sustavu osiguravaju lažiranjem rezultata skeniranja antivirusnim programima ili nekim naprednijim metodama zaobilaženja detekcije (prekid rada u slučaju pokretanja skeniranja). Ovisno o sektoru na koji su usmjereni (jezgra, datoteke, aplikacija i sl.) postoje razne inačice ovih zlonamjernih programa.

Iako su tehnike koje *rootkit* programi koriste da sakriju svoje zlonamjerne radnje vrlo napredne, poznate su neke metode koje osiguravaju njihovu detekciju. Među prvim razvijenim metodama su one zasnovane na praćenju potpisa *rootkit* programa koji se pohranjuju u bazama podataka te metode zasnovane na praćenju aktivnosti na sustavu. Budući da su autori *rootkit* programa ubrzo pronašli učinkovite načine zaobilaženja detekcije putem spomenutih metoda, razvijena je tzv. „cross-view" tehnika. Radi se o naprednoj tehnici detekcije koja se koristi usporedbom rezultata dobivenih od funkcija za dohvat popisa procesa, datoteka i sl,. s rezultatima koji se dobiju izravnim pregledom sadržaja diska. Osim spomenutih metoda postoje još i metode zasnovane na provjeri integriteta i sklopovski izvedena rješenja. Većinom se u jednom anti-rootkit programu koristi kombinacija više metoda kako bi se postigla pouzdanija detekcija.

Ovaj dokument donosi kratki pregled rada i oblika *rootkit* programa. Zatim su opisani svi spomenuti načini detekcije koji se primjenjuju u anti-rootkit programima. Slijedi ih kratki opis poznatijih anti-rootkit programa, kao i njihova usporedba. Dan je i opis dodatnih mogućnosti za detekciju i uklanjanje ovih zlonamjernih programa, kao i uvid u očekivani razvoj u budućnosti.

2. Rootkit programi

Rootkit čini jedan ili više programa dizajniranih za skrivanje dokaza da je napadnuti sustav ugrožen. Napadači ga koriste kako bi zamijenili osnovne izvršne datoteke (datoteke koje se uobičajeno koriste za izvođenje određenih radnji na računalu) u svrhu skrivanja zlonamjernih procesa i instaliranih, zlonamjernih datoteka. Obično svoje postojanje na sustavu skrivaju izbjegavanjem standardnog sigurnosnog skeniranja ili mehanizama poput anti-virusnih i anti-spyware alata. Oni su često i trojanski konji (eng. trojan) koji uvjeravaju korisnike kako ih je sigurno pokrenuti na njihovom sustavu. Tehnike koje se za to koriste uključuju prikrivanje pokrenutih procesa upravljačkih programa ili skrivanje datoteka i sistemskih podataka (eng. system data) na operacijskom sustavu. Također mogu instalirati i stražnja vrata (eng. back door) zamjenom mehanizma za prijavu (npr. /bin/login) s izvršnom datotekom koja napadaču otkriva tajne kombinacije za pristup.

Ovi programi mogu postojati i kao legalne aplikacije koje nisu namijenjene preuzimanju kontrole nad ugroženim sustavom. Ipak zadnjih godina pojavljuju se kao programi koji pomažu napadačima ostvariti pristup sustavu izbjegavajući detekciju. *Rootkit* programi postoje za razne operacijske sustave poput „Microsoft Windows“, „Linux“, „Mac OS“ i „Solaris“. Ovisno o vrsti operacijskog sustava, *rootkit* programi pojavljuju se kao upravljački programi (eng. drivers) ili jezgreni moduli.

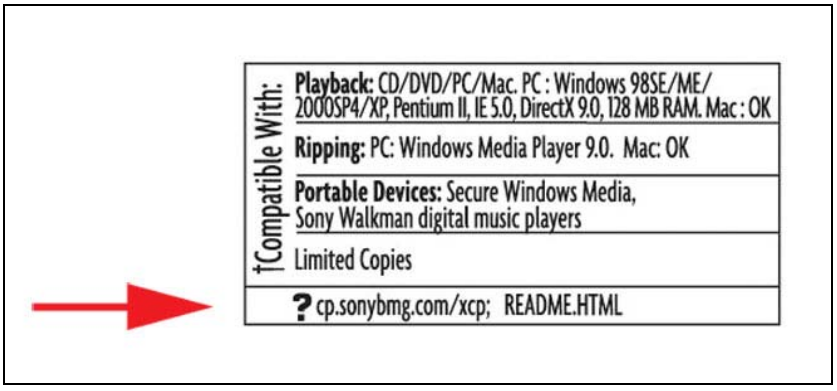
2.1. Značajniji događaji u razvoju rootkit programa

Rootkit tehnologija nije novina, nego postoji već više od desetljeća. Izraz *rootkit* je originalno označavao zlonamjerno oblikovanu skupinu alata za operacijske sustave, temeljene na platformi „Unix“, koji su služili za neovlašteno dobivanje administratorskih ovlasti. Ako napadač ima mogućnost zamjene standardnih administratorskih alata s *rootkit* programom, modificirani alati omogućuju mu upravljanje administratorskim pristupom.

Današnji *rootkit* programi ne mogu povećati prava napadača prije nego su instalirani na ciljani sustav. Kako bi uspješno instalirao *rootkit* program na računalo, napadač mora imati ostvaren administratorski pristup. To može postići iskorištavanjem sigurnosnih nedostataka koji dovode do povećanja prava na računalnom sustavu.

Prvi poznati *rootkit* program stvorili su 1990. godine istraživači Lane Davis i Steve Dake za platformu „SunOS“ inačice 4.1.1. Raniji primjer programa sličnog *rootkit*-u napravio je Ken Thompson iz laboratorija Bell Labs. 1996. godine razvijen je prvi *rootkit* za operacijske sustave „Linux“, a dvije godine kasnije i za operacijske sustave „Windows“ (stvorio ga je sigurnosni stručnjak Greg Hoglund). Značajniji napredak ovih programa dogodio se tek 2002. godine kada su napadači u svoje *rootkit* programe počeli uključivati mogućnost stvaranja stražnjih vrata i snimanja prometa.

Jedan od većih napada *rootkit* programom dogodio se 2005. godine. Tada je tvrtka Sony BMG izazvala skandal ugradnjom *rootkit* programa na CD (eng. Compact Disc) uređaje s glazbom. Razlog ugradnje tog programa bio je upravljanje digitalnim pravima ili DRM (eng. Digital Rights Management), ali on je omogućio stvaranje stražnjih vrata kod korisnika CD-a. Spomenuti program, pod nazivom „XCP“, instalirao se na računala korisnika nakon prihvata poruke u *pop-up* prozoru prilikom učitavanja CD-a. Tvrtka je ubrzo izdala programsko rješenje za uklanjanje ovog *rootkit* programa te upozorila korisnike na provjeru CD-a prije njihove uporabe. Svaki CD koji je sadržavao zlonamjerni *rootkit* program imao je posebnu oznaku na poleđini, prikazanu na slici 1.



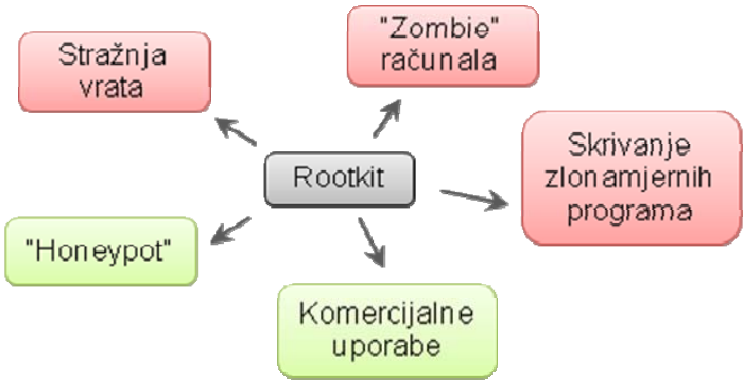
Slika 1. Oznaka CD-a ugroženog rootkit programom

Izvor: Sony BMG

Ranije opisani događaj ukazao je na to kako *rootkit* programima treba posvetiti posebnu pažnju pa su mnogi sigurnosni stručnjaci počeli razvijati tehnike kojima bi spriječili njihovo štetno djelovanje. Opasnosti od *rootkit* programa postali su svjesni i stručnjaci tvrtke Microsoft kada su u prosincu 2006. godine otkrili kako više od 20% zlonamjernih programa usmjerenih na operacijski sustav „Windows XP" pripada tipu *rootkit* programa. Oni su ovu prijetnju ozbiljno shvatili te su ugradili funkcionalnost detekcije i uklanjanja *rootkit* programa u alat „MSRT" (eng. *Malicious Software Removal Tool*).

2.2. Namjena

Uspješno instaliran *rootkit* program omogućava neautoriziranim korisnicima preuzimanje i zadržavanje potpune kontrole nad ugroženim sustavima. Najčešće skrivaju zlonamjerne datoteke, procese, mrežne veze, blokove memorije ili vrijednosti registra od drugih programa koje administratori sustava koriste za detekciju posebno privilegiranog pristupa resursima računala. Neki *rootkit* programi mogu se prikazivati kao da su isprepleteni s drugim datotekama, programima ili bibliotekama. To znači da se umeću među oktete drugih programa kako bi zavarali skenere. Ipak, ne mora svaki *rootkit* program biti zlonamjeran pa mogu biti korišteni za konstruktivne i destruktivne namjene kako je prikazano na slici 2.



Slika 2. Namjene rootkit programa

Mnogi *rootkit* programi skrivaju programe kako bi zlouporabili ugroženi sustav te obično uključuju stvaranje stražnjih vrata kako bi napadač imao pristup sustavu. Jednostavan primjer je *rootkit* program koji skriva aplikacije koje koriste sučelje za obradu naredbi (eng. command processing shell) kada se napadač pokuša spojiti na određeni mrežni priključak. Stražnja vrata omogućuju korisniku koji nema ovlasti pokretanje procesa s ovlastima privilegiranog korisnika, kao i obavljanje administratorskih funkcija.

Još jedna od čestih namjena *rootkit* programa je skrivanje mnogih drugih zlonamjernih programa poput alata za snimanje mrežnog prometa (eng. sniffer) ili alata za bilježenje korisničkih unosa preko tipkovnice (eng. *keylogger*).

Mogući način zlouporabe je i preuzimanje potpune kontrole nad nekim računalom (eng. *zombie computer*) kako bi se lažirao izvor nekog drugog napada. Alati za izvođenje takvih napada mogu uključivati funkcije uskraćivanja usluga (eng. *Denial of Service*), slanje neželjenih poruka elektroničke pošte (eng. spam) i sl.

Velik broj autora zlonamjernih programa odlučuje se za uporabu *rootkit* tehnologija kako bi skrili djelovanje svojih programa na napadnutom sustavu. Razlog tome je široka dostupnost izvornih kodova *rootkit* programa na Internetu.

Međutim, *rootkit* programi nisu uvijek korišteni za stjecanje kontrole nad sustavom. Neki programi koriste *rootkit* tehnologije kako bi trećoj strani skrili svoje postojanje. Najjednostavniji primjer je postavljanje računala kojem je uloga otkrivanje zlonamjernih pokušaja pristupa sustavu (eng. honeypot). Komercijalni programi koji koriste *rootkit* tehnologije su, primjerice, alati za rukovanje slikom diska (eng. disk image): „Alcohol 120%" i „Daemon Tools". Razlog uporabe *rootkit* tehnologije kod navedenih alata je zavaravanje operacijskog sustava kako bi se datoteka mogla prikazati kao CD disk. Neki antivirusni programi (npr. „Kaspersky") također koriste slične tehnologije kako bi se zaštitili od djelovanja zlonamjernih programa.

2.3. Način rada

Jedan način na koji je moguće otkriti zlonamjerne programe je skeniranje direktorija tvrdog diska kako bi se usporedio sadržaj datoteka s potpisima zlonamjernih programa sadržanima u bazama podataka skenera. *Rootkit* program djeluje tako da presreće sve zahtjeve te uklanja imena vlastitih datoteka s liste koja se dobije kao odgovor.

Na primjer, ako postoji neki direktorij sa sljedećim datotekama:

Ispravna_datoteka1.exe
Ispravna_datoteka2.exe
Zlonamjerni_Program.exe
Ispravna_datoteka3.exe

Kada korisnik pokuša otkriti popis datoteka u direktoriju pomoću neke od naredbi, pregledom sadržaja u prozoru „Windows Explorer" ili skeniranjem sadržaja antivirusnim programom, rootkit program presreće zahtjev te vraća sljedeći rezultat:

Ispravna_datoteka1.exe
Ispravna_datoteka2.exe
Ispravna_datoteka3.exe

Budući da skener ne vidi postojanje datoteke, ne može provesti njeno skeniranje.

Kako bi se zlonamjerni program ili neka aplikacija automatski pokrenula s operacijskim sustavom, mora postojati odgovarajući zapis u registrima operacijskog sustava. Skeneri zlonamjernih programa pretražuju registre kako bi otkrili nevaljane vrijednosti koje osiguravaju pokretanje zlonamjernih programa.

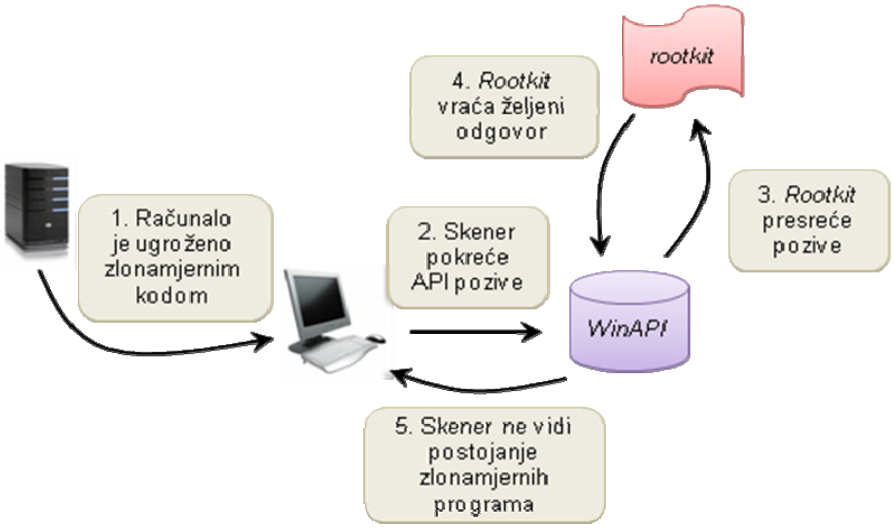
Na primjer, da bi se pokrenuli svaki put kada i operacijski sustav Windows, legitimni programi koriste sljedeći registarski ključ:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run_registry_key

Skeneri antivirusnih programa koriste razne funkcije za skeniranje navedenog sektora. *Rootkit* programi presreću takve funkcije te vraćaju vrijednosti kakve one očekuju kao ispravne, što omogućuje skrivanje njihova postojanja.

Prilikom skeniranja koriste se funkcije za otkrivanje liste pokrenutih procesa na računalu, poput ispisa komponente „Task Manager" na operacijskom sustavu „Windows". Tada se ispita svaki proces i usporedi ga se s poznatim potpisima iz baza podataka. *Rootkit* programi takve funkcije mijenjaju zlonamjernim inačicama kako bi se kao rezultat dobio ispis koji ne sadrži zlonamjerne procese.

Presretanje opisanih poziva i funkcija obavlja se na način prikazan na slici 3. Kada se pokrene postupak skeniranja nekim antivirusnim programom, skener radi API (eng. Application Programming Interface) pozive. Riječ je o skupini standarda preko koje programi mogu pozvati posebnu uslugu operacijskog sustava ili mreže. Nakon što se pokrene takav poziv, *rootkit* program ga otima ponašajući se kao neki oblik filtra te kao rezultat pruža samo one rezultate koje korisnik i očekuje. Znači, zlonamjerni procesi, datoteke ili druge vrijednosti nisu detektirane te ostaju i dalje skrivene na korisnikovom računalu.



Slika 3. Djelovanje rootkit programa

2.4. Tipovi rootkit programa

Postoji šest vrsta *rootkit* programa, a to su:

1. **Sklopovski *rootkit* programi** – obično su vezani uz male programe koji se koriste za kontrolu raznih elektroničkih uređaja (eng. firmware). Moguće ih je jednostavno sakriti u takve programe jer se često ne provjerava integritet njihovog koda, a koriste ih kako bi stvorili trajnu sliku zlonamjernog programa (uklanjanje nije moguće nikakvim alatima). Primjer ovakvih programa je napad na kreditne kartice koji se dogodio u listopadu 2008. godine. Tada su kriminalci umetnuli zlonamjerni kod u mehanizam za očitavanje kreditnih kartica kako bi dobili informacije o korisnicima. Takve su informacije zatim slane kriminalcima preko mreže mobilnih uređaja.
2. **VMM (eng. virtual machine monitor) *rootkit*** – funkcioniraju izmjenom *boot* niza računala (inicijalni skup operacija koje se izvode kada se pokrene računalo) kako bi se učitale kao virtualni stoj. Također imaju mogućnost pokretanja originalnog operacijskog sustava kao virtualnog stroja kako bi presreli sve sustavne pozive. Jedan od primjera ovakvih *rootkit* programa je „SubVirt" koji su razvili istražitelji iz tvrtke Microsoft i fakulteta Michigan.
3. ***Rootkit* programi boot sektora ili *bootkit*** – zamjenjuju legitimni pokretač operacijskog sustava (eng. boot loader) s nekim koji kontrolira napadač. Obično on ima mogućnost pristupiti zaštićenom modu kada se pokrene jezgra. Kao primjer ovog programa najčešće se navodi „Stoned Bootkit" koji je omogućavao rušenje sustava te otkrivanje povjerljivih informacija o korisniku sustava.
4. **Jezgreni *rootkit*** – dodaju kod ili zamjenjuju dijelove operacijskog sustava uključujući jezgru i pridružene upravljačke programe. Mnogi operacijski sustavi podržavaju upravljačke uređaje koji se pokreću s istim pravima kao i operacijski sustav (eng. kernel-mode device drivers). Prema tome, ovakvi su *rootkit* programi najčešće razvijeni kao jezgreni moduli kod operacijskog sustava „Linux" te upravljački programi kod operacijskog sustava „Microsoft Windows". Smatraju se vrlo opasnima zbog neograničenog pristupa sustavu. Jedan od prvih široko poznatih jezgrenih *rootkit* programa razvio je Greg Hoglund za operacijski sustav „Windows NT 4.0" te objavio u elektroničkom časopisu „Phrack".
5. **Bibliotečni *rootkit*** – dopunjuju ili zamjenjuju sustavne pozive s inačicama koje skrivaju informacije o napadaču.
6. **Aplikacijski *rootkit*** – zamjenjuju legalne aplikacije s trojanskim konjima. Također mogu izmijeniti ponašanje aplikacija dodacima, umetnutim kodom i sl. Primjer takvih programa je *rootkit* koji preusmjerava korisnika s popularnih web stranica (poput www.google.com) na napadačeve stranice.

2.5. Usporedba s drugim zloćudnim programima

Računalni virus je program kojem je glavni cilj promijeniti način rada računala, bez znanja i dopuštenja korisnika. Jednom kada je pokrenut, on ugrožava druge datoteke na računalu s ciljem da se na neki način proširi na druga računala. Ugrožavanje se provodi umetanjem vlastitog programskog koda u legitimne datoteke, a pokretanje pristupom istoj datoteci. Kao i računalni virusi, *rootkit* programi mijenjaju programske komponente sustava kodom koji ima ulogu skrivanja zlonamjernih radnji. Svaki virus uzrokuje neki događaj s više ili manje štetnim posljedicama (od prikaza poruke na zaslonu računala do onesposobljavanja računalne mreže). Širenje virusa obavlja se prenošenjem (preko prijenosnih medija, poruka elektroničke pošte i sl.) i pokretanjem ugroženih datoteka na drugim računalima.

Poput virusa, i crvi se mogu samostalno umnožavati. Ipak za širenje im nisu potrebni drugi programi, već se šire sami iskorištavanjem nedostataka u prijenosu podataka. Prije širenja automatski skeniraju mrežu da bi otkrili ranjivosti sustava i iskoristili ih za ugrožavanje operacijskog sustava. Zatim stvaraju kopije koje zatim šalju mrežom blokirajući ostali promet. Ovim crvi djeluju na cjelokupnu mrežu, dok su virusi usmjereni na skupinu računala. Za razliku od toga, *rootkit* se koristi u napadu na jedno računalo.

Virusi i crvi mogu imati bilo koji oblik korisnog tereta (eng. payload) kako bi imali mogućnost samostalnog umnožavanja. Kod *rootkit* programa korisni teret može upravljati njegovim integritetom (prikazivati ga korisnim programom, skrivati zlonamjerne procese i sl.) kako bi ugrozio sustav. Na primjer, svaki put kad se pokrene *rootkit* inačica naredbe ps (status procesa), pretražuju se kopije *init* (stvaranje procesa) i *inetd* (upravljanje Internet uslugama) kako bi se osiguralo zadržavanje ugroženih inačica. Ostatak korisnog tereta osigurava napadaču zadržavanje kontrole nad sustavom. Ovo obično uključuje posjedovanje stražnjih vrata u obliku ugrađenih (eng. hard-coded) kombinacija „korisničko ime/lozinka".

Svi ovi programi na neki način imaju funkcije koje se preklapaju, a usporedba je vidljiva u tablici 1. Također postoje i hibridni oblici programa tj. crvi s uključenom instalacijom *rootkit* programa. Isto tako *rootkit* program može uključivati kopiju jednog ili više crva ili programa za snimanje prometa.

Obilježje	Rootkit program	Računalni virus	Računalni crv
Samostalno umnožavanje	NE	DA	DA
Samostalno širenje	NE	NE	DA
Izmjena stanja na sustavu	DA	DA	DA
Usmjerenost napada	Jedno računalo	Više računala	Cjelokupna mreža
Korisni teret	Upravljanje integritetom/zadržavanje kontrole;	Umnožavanje/štetno djelovanje	Umnožavanje/štetno djelovanje

Tablica 1. Usporedba rootkit-a s virusima i crvima

3. Anti-rootkit programi

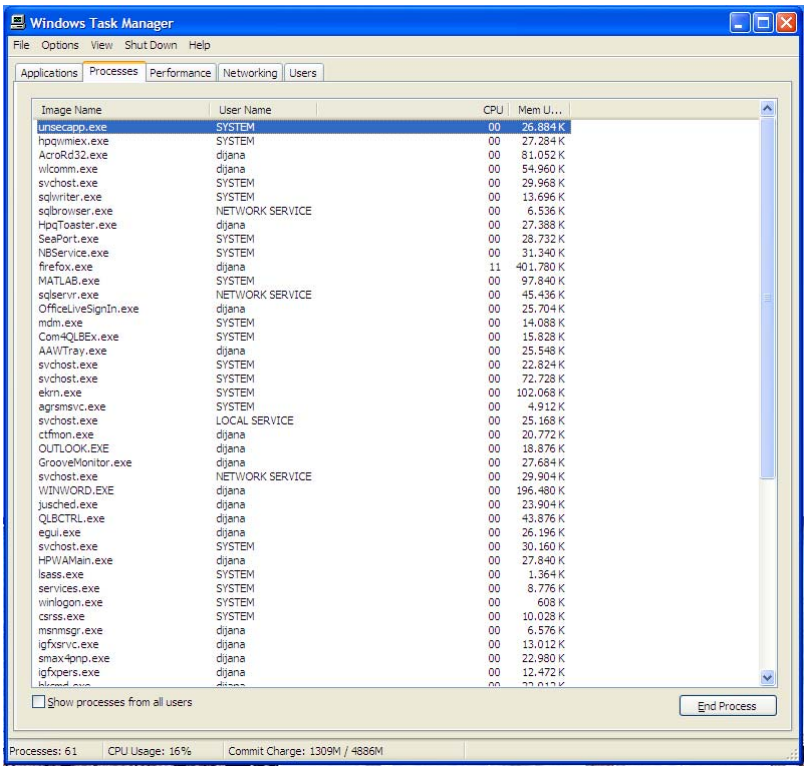
Kao jedna od osnovnih zaštita od opisanih prijetnji *rootkit* tehnologija razvijeni su razni anti-rootkit programi. Njihov se rad zasniva na skupu sigurnosnih alata koji omogućuju otkrivanje skrivenih datoteka, mrežnih priključaka, procesa i sl.

3.1. Problemi prilikom skeniranja

3.1.1. Skrivanje djelovanja

Skeniranjem liste procesa moguće je lako uočiti koji od njih zauzima ogromne količine resursa računala što je jedno od osnovnih obilježja većine zlonamjernih programa.

Jedna od komponenti koje se nalaze ugrađene u operacijski sustav, a omogućuju ispis liste aktivnih procesa je „Task Manager“. Njenim pokretanjem korisnik može vidjeti aktivne procese na računalu te količinu memorije i CPU (eng. Central Processing Unit) jedinica koje zauzimaju. Također, uključuje mogućnost zaustavljanja svakog od procesa ukoliko korisnik prepozna da se radi o zlonamjernom programu. Nedostatak ovog programa je nepostojanje zapisa o smještaju programa na disku pa je u te svrhe pogodnije koristiti naprednije programe (poput „Process Explorer“).



Slika 4. Popis aktivnih procesa u „Task Manager-u“

Ipak, uporaba spomenute komponente ne osigurava prikaz pouzdanih rezultata o pokrenutim procesima. Razlog tome je što gotovo svi *rootkit* programi koriste presretanje API poziva koje stvara „Task Manager“ te vraćaju rezultate koji ne uključuju skrivene procese. Ovo predstavlja veliko ograničenje u otkrivanju zlonamjernih procesa na sustavu.

Na sličan način *rootkit* programi djeluju kako bi sakrili:

- zlonamjerne zapise u registrima – „Regedit“ ne prikazuje zapise *rootkit* programa u registrima,
- instalirane datoteke – „Windows Explorer“ ne prikazuje skrivene datoteke,
- mrežne konekcije – „Netstat“ ne prikazuje *rootkit* priključke,
- zapise u memoriji,

- ostale učinke zlonamjernih programa (npr. blokiranje pristupa određenim web stranicama, prekid rada skenera i sl.).

3.1.2. Tehnike skrivanja

Jedna od tehnika koju koriste *rootkit* programi koriste kako bi sakrili svoje djelovanje je presretanje poziva funkcija sustava (eng. *hooking*). Radi se o preusmjeravanju normalnog programskog toka s legitimnih programskih funkcija na one kojima upravlja *rootkit*. Tehnike uključuju filtriranje rezultata funkcija za skeniranje i analizu sustava. Uspješnost ovih tehnika leži u tome što se rad funkcija temelji na podacima koje dobiju od operacijskog sustava.

Operacijski sustav Windows koristi mnoge podatkovne strukture (tablice) za pohranu kritičnih informacija sustava. *Rootkit* programi napadaju takve strukture te presreću njihov dohvat ili ih zamjenjuju generiranjem novih.

Postoje *rootkit* programi koji uključuju neku vrstu „radara" te privremeno prekidaju svoje djelovanje ako se na računalu pojavi neki skener. Također, mogu uključivati i tehnike koje blokiraju pristup web stranicama koje sadrže alate za njihovo uklanjanje, kao i preuzimanje takvih alata i njihovo pokretanje.

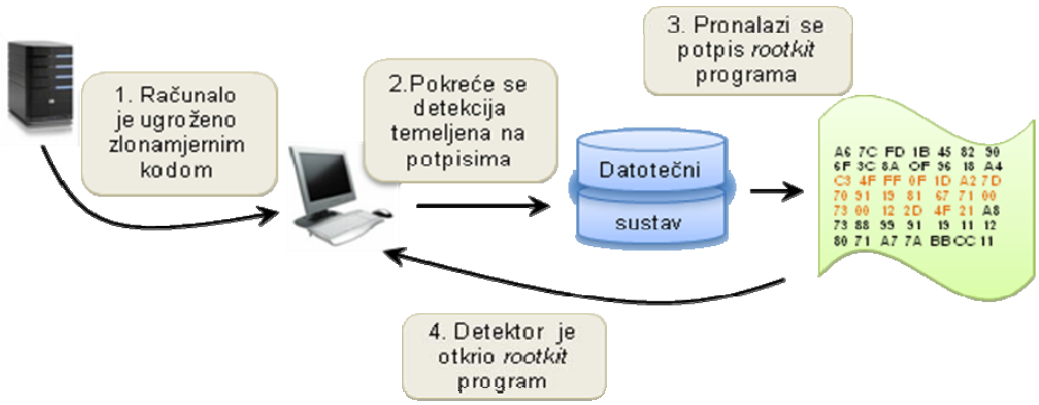
Postoje brojne tehnike skrivanja koje koriste *rootkit* programi, a razlikuju se u ovisnosti o njihovom tipu i namjeni. Svaka od njih predstavlja prepreku u otkrivanju njihova zlonamjernog djelovanja.

3.2. Rad anti-rootkit programa

Usporedno s razvojem brojnih tehnika skrivanja rada *rootkit* programa razvijane su i tehnike koje omogućuju njihovo pouzdanije otkrivanje. Osnovne tehnike koje su uključene u popularnije anti-*rootkit* programe ukratko su opisane u nastavku.

3.2.1. Detekcija temeljena na potpisima

Metode detekcije temeljene na potpisima (eng. signatures) godinama se već koriste kod antivirusnih programa. Koncept je vrlo jednostavan, a uključuje skeniranje datoteka kako bi se otkrio niz koji predstavlja tzv. otisak (eng. fingerprint) jedinstven za neki određeni *rootkit* program. Postupak detekcije prikazan je na slici 5.



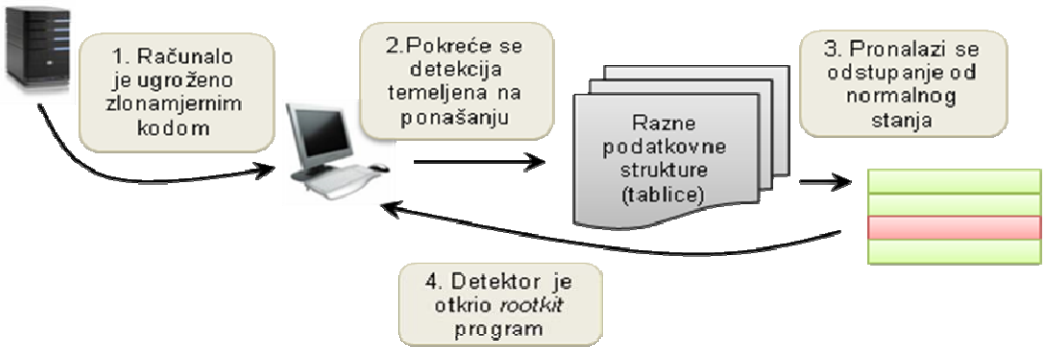
Slika 5. Detekcija temeljena na potpisima

U slučaju da je pronađen takav potpis na nekoj datoteci, ona se označava kao ugrožena. Budući da se ovakvo skeniranje obično primjenjuje na datotečni sustav, za otkrivanje *rootkit* programa je obično nepouzdano (osim u kombinaciji s drugim tehnikama). Razlog neuspješnosti navedene tehnike je skrivanje datoteka koje provodi gotovo svaki *rootkit* program.

Ipak, ova se tehnika može uspješno primijeniti na skeniranje memorije sustava. Mnogi popularni i poznati jezgreni *rootkit* programi mogu se otkriti ovakvim skeniranjem jer obično postoji zapis o njihovu djelovanju u memoriji jezgre. Osnovni nedostatak je mogućnost detekcije samo javno poznatih tj. ranije otkrivenih *rootkit* programa čiji potpis postoji u bazi podataka.

3.2.2. Detekcija temeljena na ponašanju

Ukoliko detekcija temeljena na potpisima nije uspješno otkrila postojanje *rootkit* programa, moguće je iskoristiti detekciju temeljenu na ponašanju (eng. heuristic detections). Rad ovih metoda zasniva se na prepoznavanju odstupanja u uobičajenom ponašanju sustava, kao i u provjeravanju uzoraka iz sustava (eng. system patterns). Postupak detekcije dan je na slici 6. Njihova glavna snaga je mogućnost identificiranja novih, prethodno neotkrivenih *rootkit* programa.



Slika 6. Detekcija temeljena na ponašanju

Postoje razni načini na koji se provodi detekcija temeljena na ponašanju poput:

- Provjera SSDT (eng. System Service Descriptor Table) tablice s pokazivačima funkcija – radi se o skupini tablica koje održava jezgra. Svaki sustavni poziv iz korisničkog programa preko API sučelja prikazuje se kao ulaz u podatkovnu strukturu SSDT koji jezgra koristi kako bi locirala funkcije koje treba izvesti.
- Provjera IRP (eng. I/O Request Packet) tablica individualnog upravljačkog programa. Svaki operacijski sustav i korisničke aplikacije koriste IRP tablice kako bi komunicirale s upravljačkim programima kada trebaju izvesti neku posebnu funkciju koju on podržava. IRP tablicu posjeduje i jezgreni upravljački program.
- Provjera IAT (eng. Import Address Table) tablica u svim DLL (eng. Dynamic Link Library) bibliotekama koje obično predstavljaju dio nekog programa. IAT tablice sadrže pokazivače koji omogućuju aplikacijama lociranje i pokretanje sustavnih funkcija. Mogu također sadržavati i pokazivače na DDL biblioteke.
- Provjera postojanja dodanog programskog koda na određenim putanjama (npr. do filtra koji vraća izmijenjene rezultate nakon presretanja funkcija). Ove se provjere mogu provoditi određivanjem broja naredbi koje se izvode prilikom provjera. U slučaju postojanja *rootkit* programa taj će broj biti znatno veći.

Primjeri programskih alata koji koriste opisanu tehniku detekcije su:

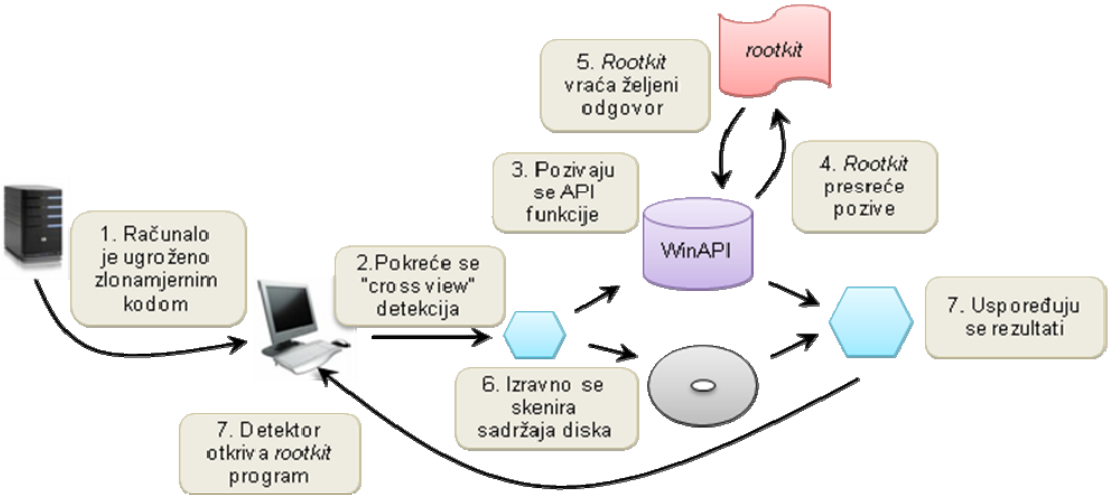
- „VICE" – detekcija na temelju statičke analize koda i podatkovnih struktura,
- „Patchfinder" – detekcija na temelju analize putanje izvođenja.

3.2.3. „Cross view" detekcija

„Cross view" detekcija predstavlja metodu koja je vođena pretpostavkom da je sustav ugrožen. Funkcioniranje se zasniva na sljedećem:

1. Pozivaju se API funkcije kako bi se dobili rezultati o pokrenutim procesima, skrivenim datotekama i sl.
2. Posebnim postupkom radi se provjera istih podataka na nižem sloju, ne koristeći API funkcije.
3. Rezultati se uspoređuju kako bi se otkrila odstupanja, tj. moguće postojanje *rootkit* programa.

Opisani postupak detekcije prikazan je i na slici 7.



Slika 7. „Cross view" detekcija

Kako je vidljivo iz načina rada, ove se metoda zasniva na činjenici da će *rootkit* programi (i sve njegove komponente) biti skriveni u rezultatima API funkcija koje oni presreću. Postupak je uspješan jer su metode koje se koriste za dohvat istih podataka kao i API funkcije, dizajnirane na način da nisu podložne presretanju *rootkit* programa.

Način na koji se obavlja detektiranje prikazan je u nastavku kroz primjere pronalaženja skrivenih datoteka na operacijskom sustavu „Microsoft Windows".

Kako bi se otkrio sadržaj nekog direktorija potrebno je pregledati odgovarajući sektor diska te obraditi podatke. Detektori to obično obavljaju preko funkcija:

1. „CreateFile("\\.\C")" – kreiranje ili otvaranje određenog objekta kako bi se s njim moglo rukovati,
2. „ReadFile()" – pregled nekog dijela diska.

Alternativno tome, detektori mogu pokušati pristupiti pseudo-datoteci „\\.\PHYSICALDRIVE0„ te zatim iskoristiti funkciju „ReadFile()".

Obje opisane metode mogu biti vrlo jednostavno narušene djelovanjem *rootkit* programa. Potrebno je samo presresti poziv funkcije „ReadFile()" te izmijeniti rezultate o sadržaju na disku. Ipak, implementacija ovakvog postupka je dosta zahtjevna pa se rijetko nalazi u *rootkit* programima.

Ipak, pouzdanije rezultate moguće je dobiti ako se u jezgru umetne „agent" koji bi omogućio zaobilaženje API poziva te koristio funkcije „ZwCreateFile()"/"ZwReadFile()" u jezgrenom modulu. Ova je tehnika uspješna u većini slučajeva, osim ako *rootkit* koristi presretanje putem SST (eng. System Service Table) ili IAT tablica.

U slučaju da prethodne provjere ne daju zadovoljavajuće rezultate, moguće je koristiti IRP(eng. I/O Request Packet) zahtjeve za čitanje nekog dijela diska i funkciju „IoCallDriver()" za njihovo slanje izravno disku. Kao i prethodne metode, *rootkit* programi mogu zaobići i ovu detekciju. Potrebno je samo presresti korištene IRP zahtjeve te izmijeniti rezultate.

Najdublja razina skeniranja koju je moguće postići je uporaba samih naredbi „in" i „out" kako bi se komuniciralo izravno s upravljačkim sklopom (eng. controller) tvrdog diska. Ovakvu detekciju bilo bi nemoguće presresti, ali njena je implementacija vrlo složena.

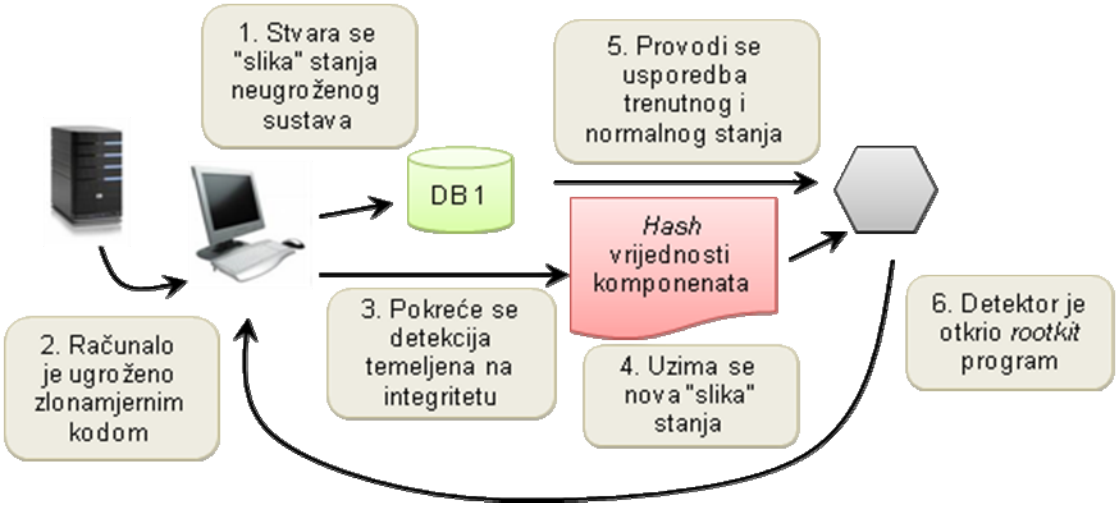
Kako je vidljivo iz opisanih primjera detekcije, da bi ovaj postupak bio uspješan potrebno je implementirati metode za dobivanje informacija o sustavu. Pri tome se javlja jedan od nedostataka, a to je složenost postupka implementacije. Drugi nedostatak metode leži u tome što, i nakon uspješne implementacije svih metoda, ostaje mogućnost njihovog presretanja.

Programski alati koji koriste opisanu metodu su:

- „Rootkit Revealer",
- „Klister",
- „Blacklight",
- „Strider GhostBuster".

3.2.4. Detekcija temeljena na integritetu

Detekcija temeljena na integritetu pruža alternativu detekciji putem potpisa i ponašanja. Obavlja se usporedbom trenutne slike datotečnog sustava ili memorije s već poznatom povjerljivom inačicom. Svaka razlika među njima uzima se kao moguća zlonamjerna radnja. Međutim, koliko god da je ovo pouzdana metoda detekcije (jer može ukazati na svaku promjenu), osnovni je nedostatak nemogućnost specificiranja uzroka te promjene.



Slika 8. Detekcija temeljena na integritetu

Neki od načina na koje je moguće provoditi ovakvu detekciju su:

1. Stvaranje baze podataka s jedinstvenim *hash* vrijednostima datoteka na sustavu. Kada se pokrene skeniranje, detektor obavlja identično računanje *hash* vrijednosti te ih uspoređuje sa zapisima u bazi podataka. Temelji se na pretpostavci da se sistemske datoteke ne bi trebale mijenjati (osim u slučaju kada se nadograđuju novim inačicama, ali tada su razlike očekivane). Ova je metoda bila vrlo uspješna u borbi protiv prvih *rootkit* programa koji su obavljali jednostavnu zamjenu datoteka na disku s trojanskim konjima. Na žalost, moderniji *rootkit* programi adaptirali su se premještanjem njihovih modifikacija s diska u memoriju što je učinilo ovu metodu gotovo beskorisnom pri njihovoj detekciji.
2. Provjera integriteta podatkovnih struktura operacijskog sustava (IAT, SSDT, IRP tablica i dr.) te memorije. Provodi se usporedba dijelova koda za važnije biblioteke i upravljačke programe na disku s njihovim odgovarajućim, valjanim slikama u memoriji.

Programski alati koji sadrže ovakve metode detekcije su:

- „Tripwire“,
- „System Virginity Verifier“.

3.2.5. Sklopovska detekcija

Jedini alat razvijen na temelju metoda sklopovske detekcije je „Copilot“. Radi se o obliku PCI kartice koja je umetnuta u poslužitelj na kojem se prati aktivnost *rootkit* programa. Cilj je zadržati neovisnost kartice o operacijskom sustavu koji bi morao biti ugrožen. Kako bi se to osiguralo, kartica ima vlastite CPU resurse i koristi DMA (eng. Direct Memory Access) za skeniranje fizičke memorije računala. Obavlja se pretraživanje ponašanja koje ukazuje na postojanje *rootkit* programa, poput:

- presretanja u SSDT tablicama,
- promjena u jezgrenim funkcijama (provjerom integriteta),
- izmjena ključnih podatkovnih struktura.

Spomenuti alat također ima vlastito mrežno sučelje za komunikaciju.

Budući da se radi o sklopovski izvedenom rješenju, alat pruža visok stupanj sigurnosti. Osnovni nedostatak kod ove metode su visoki troškovi prilikom implementacije i održavanja.

4. Poznati anti-rootkit programi

4.1. Besplatni programi

4.1.1. Program „Sophos Anti-Rootkit“

„Sophos Anti-Rootkit“ omogućuje otkrivanje i uklanjanje *rootkit* programa koji mogu postojati na računalu. Sučelje navedenog programa vidljivo je na slici 9.

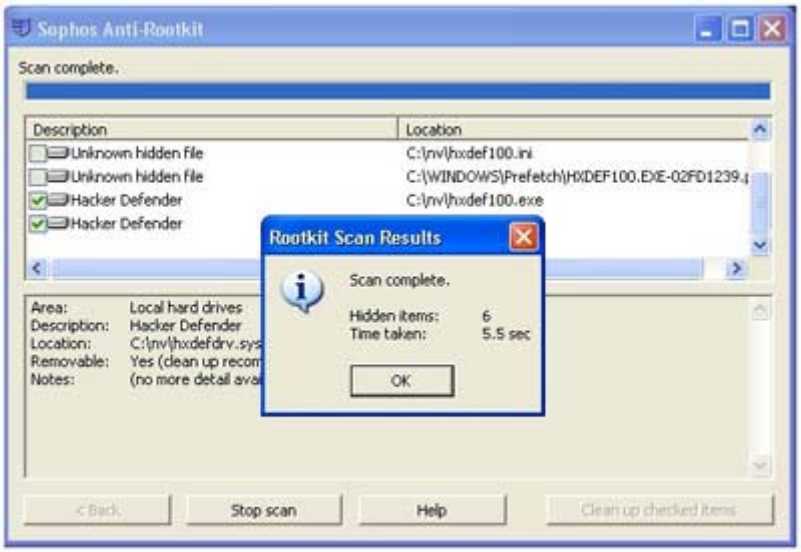
Postoje dvije inačice ovog programa:

1. inačica sa korisničkim sučeljem,
2. inačica s prozorom za naredbe.

Dostupan je za operacijske sustave „Windows“ inačica 2000, XP, 7 te Vista Server 2003 i Server 2008. Instalacija i uklanjanje ovog programa vrlo je jednostavna i ne zahtjeva puno vremena. Jedan od nedostataka je nepostojanje automatskog ažuriranja inačica programa pa korisnik mora samostalno preuzeti posljednju, valjanju inačicu.

Ovisno o računalu koje se skenira, proces može potrajati od 5 minuta do više od jednog sata. Općenito, skeniranje traje nešto dulje ako se provodi skeniranje poslužitelja. Također, proces je moguće prekinuti u bilo kojem trenutku te naknadno ponovno pokrenuti.

Rezultat skeniranja je popis sumnjivih datoteka, a može uključivati i vrijednosti ili ključeve registra. Nakon uklanjanja nekog od *rootkit* programa, njegovo ime nestaje s popisa.



Slika 9. Program Sophos Anti-Rootkit

4.1.2. Program „chkrootkit“

Program „chkrootkit“ služi za otkrivanje zlonamjernih *rootkit* programa , a sadrži sljedeće komponente:

- „chkrootkit“ – skriptu koja provjerava da li sustav sadrži *rootkit* modifikacije,
- „ifpromisc.c“ – provjerava da li je neko mrežno sučelje u promiskuitetnom načinu rada (mrežna kartica prihvaća propušta sav promet),
- „chklastlog.c“ – provjera za promjenom vrijednosti datoteke „lastlog“ (zapis o zadnjoj prijavi na sustav),
- „chkwtmp.c“ – provjera za promjenom vrijednosti datoteke „wtmp“ (zapisi o svim prijavama i odjavama sa sustava),

- „check_wtmpx.c“ – provjera za promjenom vrijednosti datoteke „wtmpx“ (samo na operacijskim sustavima „Solaris“),
- „chkproc.c“ – provjera da li postoje skrivene „/proc“ vrijednosti,
- „chkdirs.c“ – provjera za znakovima „LKM“ trojanskih konja,
- „strings.c“ – brza zamjena nizova,
- „chkutmp.c“ – provjera za promjenama vrijednosti u datoteci „utmp“ (poput datoteke „wtmp“ sadrži zapise o svim prijavama i odjavama na sustavu).

Navedeni program je dostupan za platforme „Linux“, „MAC“, „BSD“, „Solarix“ te ostale temeljene na operacijskom sustavu „Unix“. Instalacija i uklanjanje programa je vrlo jednostavno.

Prednost programa je detekcija velikog broja poznatih *rootkit* programa. Proces skeniranja obavlja se s administratorskim ovlastima, a moguće ga je obaviti s raznim opcijama. Prije samog postupka skeniranja komponentom „chkrootkit“, preporuča se provjera komponentom „ifpromisc.c“ kako bi se otkrilo da li je neko od sučelja u ugroženom načinu rada. Primjer ispisa dan je na slici 10 prikazanoj u nastavku.

```
[root chkrootkit-0.34]# ./ifpromisc
eth0 is not promisc
eth0:0 is not promisc
eth0:1 is not promisc
eth0:2 is not promisc
eth0:3 is not promisc
eth0:4 is not promisc
eth0:5 is not promisc
eth0:6 is not promisc
eth0:7 is not promisc
eth0:8 is not promisc
[root chkrootkit-0.34]#
```

Slika 10. Rezultat skeniranja naredbom „ifpromisc“

Izvor: LinuxDevCenter

Zatim se pokreće naredba „chkrootkit“, a kao rezultat dobije se popis datoteka s oznakom valjanosti. Slika 11 daje primjer detekcije rootkit programa na navedeni način.

```
[root chkrootkit-0.34]# ./chkrootkit
ROOTDIR is `/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not found
Checking `gpm'... not infected
Checking `grep'... not infected
Checking `hdparm'... not infected
Checking `su'... not infected
Checking `ifconfig'... not infected
Checking `inetd'... not infected
Checking `inetdconf'... INFECTED <--
Checking `identd'... not found
Checking `killall'... not infected
Checking `login'... not infected
```

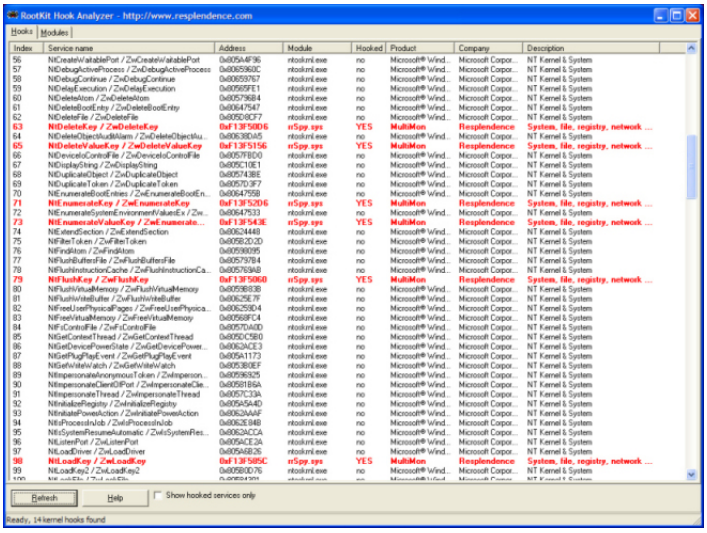
Slika 11. Detekcija rootkit programa

Izvor: LinuxDevCenter

4.1.3. Program „RootKit Hook Analyzer“

Program „RootKit Hook Analyzer“ je sigurnosni alat koji provjerava postojanje instaliranih *rootkit* programa na računalu. Rad se temelji na prikazu svih jezgrenih usluga zajedno s nazivom, adresom, modulom te opisom. Također omogućuje prikaz instaliranih modula i upravljačkih programa. Razvijen je za uporabu na operacijskim sustavima „Windows“ inačice Vista, XP, 2003 i 2000 (samo izdanje x86).

Ako se na sustavu pronađu neke nepravilnosti (slika 12), spomenuti program pruža mogućnost provjere da li se radi o dijelu legitimnog programa.

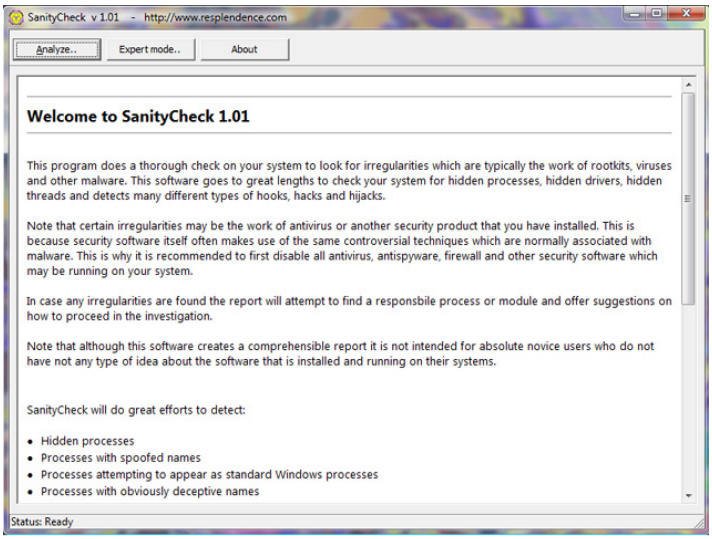


Slika 12. Program „RootKit Hook Analyzer“

Izvor: Resplendence

Razvijena je i napredna inačica programa „RootKit Hook Analyzer“ pod nazivom „SanityCheck“ (slika 13). Dostupan je za operacijske sustave: „Windows XP“, „Windows Vista“, „Windows 2003“ i „2008 Server“.

Posebno obilježje ovog programa je posebna tehnika nazvana *„deep inventory“*. Radi se o postupku koji omogućava dubinsko skeniranje upravljačkih programa, procesa i mnogih drugih informacija na sustavu. Također, program može otkriti skrivene i lažirane procese, upravljačke programe i veliki broj *rootkit* programa.



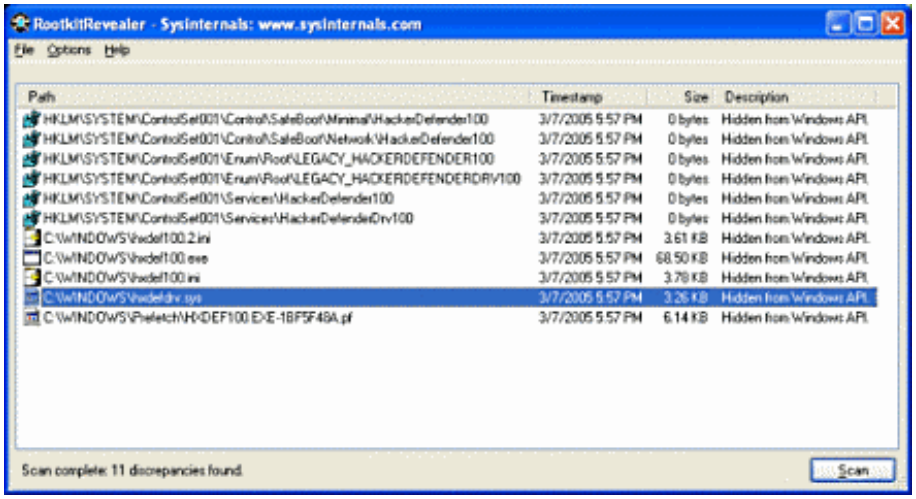
Slika 13. Program SanityCheck

Izvor: Resplendence

4.1.4. Program „RootkitRevealer“

Program „RootkitRevealer“ je napredni alat za detekciju rootkit programa namijenjen operacijskom sustavu „Windows“ inačice NT4 i novije. Ima mogućnost otkrivanja mnogih *rootkit* programa uključujući: „AFX“, „Vanquish“ i „HackerDefender“.

Postoje dva načina pokretanja skeniranja - ručno i automatski. Rezultat skeniranja računala je popis registara koji ukazuju na prisutnost nekog *rootkit* programa. Primjer ispisa skeniranja dan je u nastavku na slici 14, a prikazuje otkrivanje jednog *rootkit* programa „HackerDefender“.



Slika 14. Program RootkitRevealer

Izvor: Microsoft TehNet

Potrebno je ispitati sve rezultate koji mogu ukazati na postojanje *rootkit* programa. Nedostatak ovog programa je što ne sadrži mogućnost uklanjanja pronađenih zlonamjernih programa.

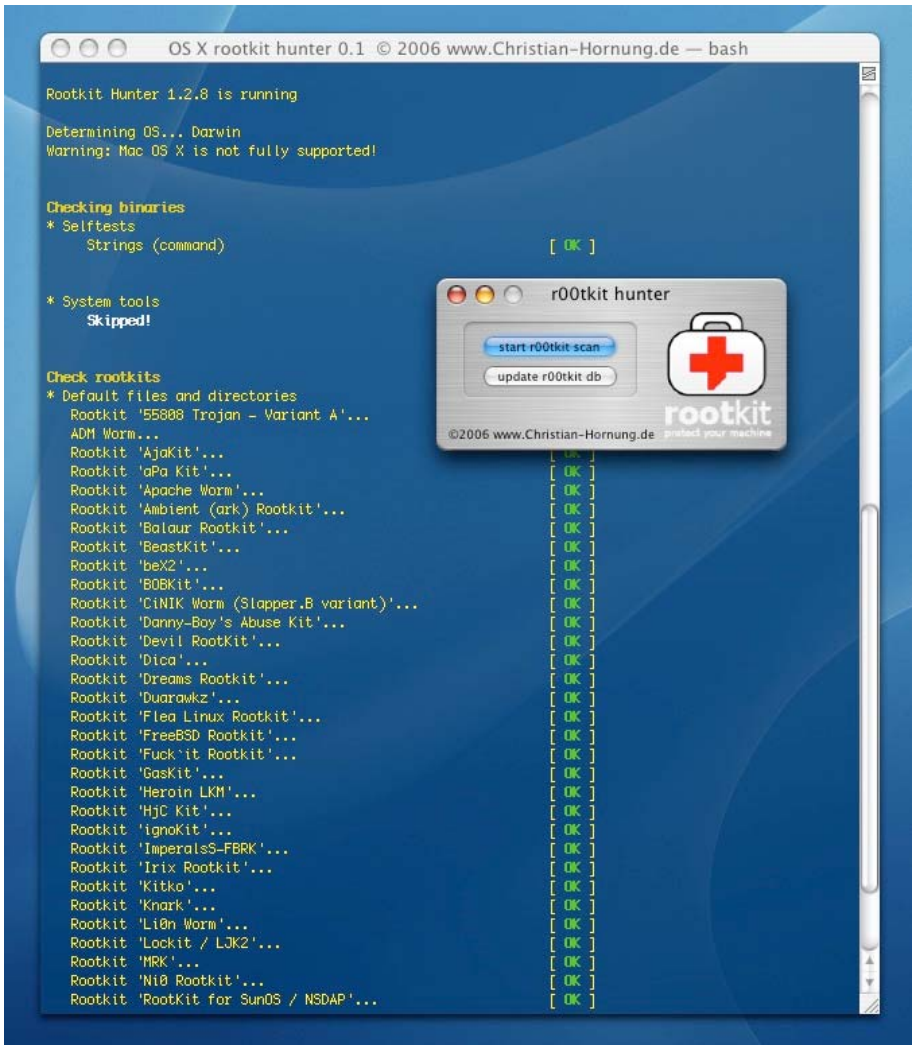
4.1.5. Program „Rootkit Hunter“

Program „Rootkit Hunter“ služi za skeniranje računala u svrhu pronalaženja *rootkit* programa, ali i postojanja stražnjih vrata.

Provodi više vrsta ispitivanja poput:

- usporedbe MD5 *hash* vrijednosti,
- pregledom postojanja datoteka koje koriste *rootkit* programi,
- provjerom prava pristupa datotekama,
- pregledom nizova u modulu LKM (eng. *Loadable Kernel Module*),
- pretraživanjem skrivenih datoteka.

Sadrži podršku za većinu distribucija operacijskih sustava „Linux“ i „*BSD“, iako nije razvijena inačica za platformu „NetBSD“. Detekcija zlonamjernih *rootkit* programa opisanim alatom prikazana je na slici 15.



Slika 15. Program „Rootkit Hunter“

Izvor: Antirootkit.com

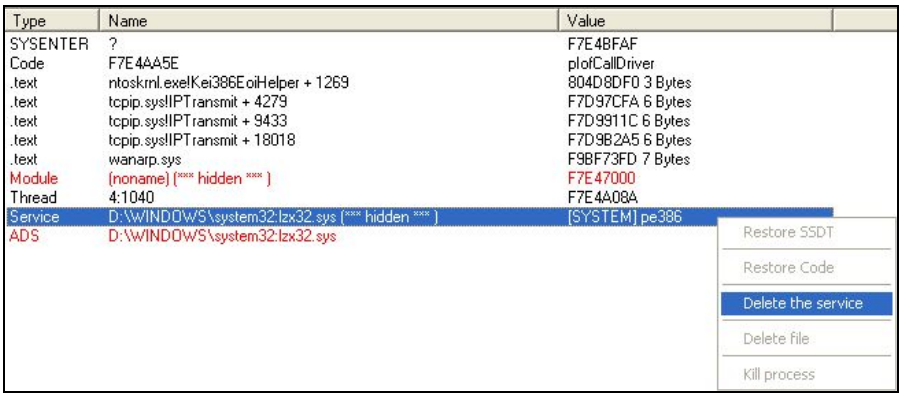
4.1.6. Program „GMER“

Program „GMER“ je aplikacija za detekciju i uklanjanje *rootkit* programa na operacijskim sustavima „Windows“ inačica NT/W2K/XP/VISTA.

Ovaj program obavlja provjeru skrivenih:

- procesa,
- dretva,
- modula,
- usluga,
- datoteka,
- vrijednosti registra.

Sadrži vrlo razvijeno korisničko sučelje te mnoge funkcije za jednostavnu pretragu i uklanjanje pronađenih prijetnji. Kako bi se uklonio *rootkit* program, nakon njegova pronalaska, korisnik treba samo odabrati odgovarajuću opciju za brisanje zlonamjernih sadržaja. Ovaj je postupak prikazan na slici 16.



Slika 16. Program „GMER“ – uklanjanje rootkit-a

Izvor: GMER.com

4.2. Komercijalni programi

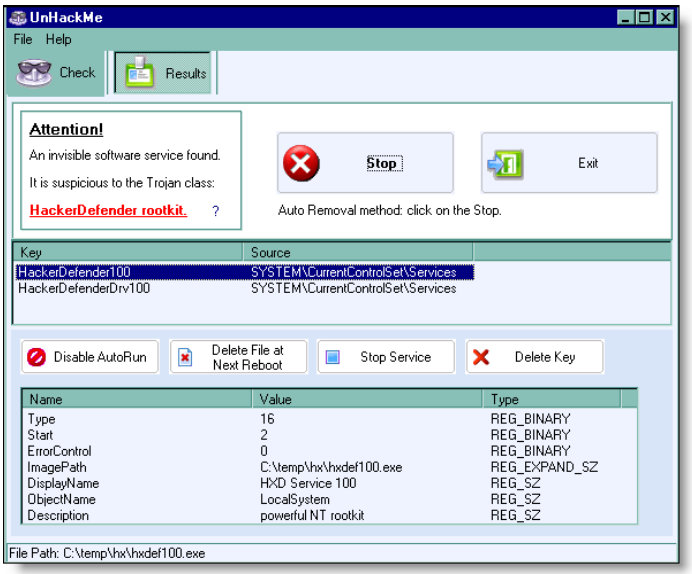
4.2.1. Program „UnHackMe“

Program „UnHackMe“ služi za detekciju i uklanjanje *rootkit* programa, a razvijen je za operacijske sustave „WinXP“, „Win7 x32“, „Win2000“, „Windows2000“, „Windows2003“, „Windows Vista“, „WinNT 4.x“, „Windows Vista“ i „Windows Vista Enterprise“.

Program je moguće besplatno isprobati u vremenskom razdoblju od 30 dana, ili kupiti licencu za trajnu uporabu za $19.95. Sučelje programa vidljivo je na slici 17.

Osnovna obilježja navedenog programa uključuju:

1. jedinstvenu metodu otkrivanja zlonamjernih programa – praćenje procesa prilikom samog pokretanja računala.
2. visoka razina sigurnosti jer se jezgreni upravljački programi koriste samo za stvaranje slike stanja sustava (pa ne može doći do rušenja rada sustava prilikom skeniranja),
3. automatsko detektiranje *rootkit*-a prilikom pokretanja (u roku 5-7 sekundi),
4. kompatibilnost s mnogim antivirusnim i anti-rootkit alatima,
5. mogućnost uklanjanja drugih zlonamjernih programa (trojanski konji, *adware*, *spyware* i sl).



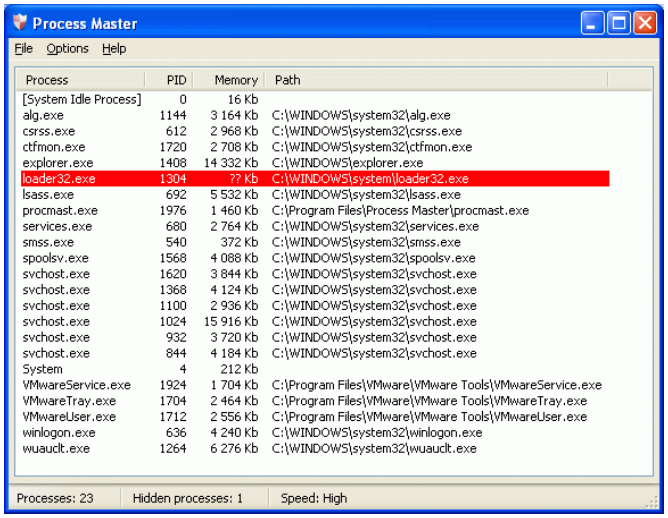
Slika 17. Program „UnHackMe“

Izvor: Greatis

4.2.2. Program „Proces Master“

Program „Proces Master“ (slika 18) omogućuje detekciju i uništavanje skrivenih procesa zlonamjernih programa poput *rootkit*-a, virusa i *spyware*-a. Uspješno otkriva većinu *rootkit* programa i njihove modificirane inačice. Njegov rad se zasniva na usporedbi rezultata koje dobiva pregledom komponenti poput „Task Manager“-a i rezultata koje dobije skeniranjem samog računala na razini sustava.

Razvijen je za operacijske sustave „Windows“ inačica 2000, XP i 2003, s tim da je besplatna inačica dostupna na korištenje samo 30 dana, a licenca košta $19.95.



Slika 18. Program „Process Master“

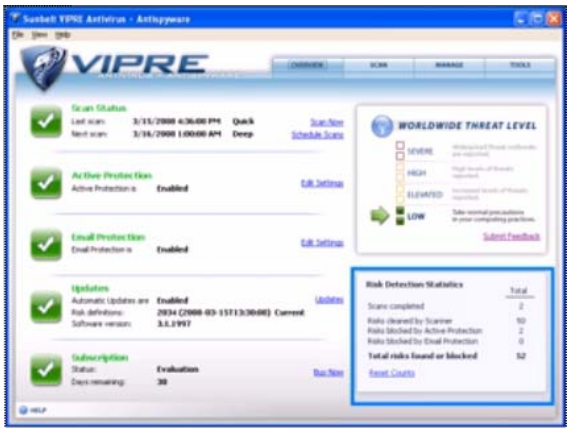
Izvor: Backfaces

4.2.3. Program „Vipre“

Program „Vipre“ je antivirusni alat koji uključuje zaštitu od *spyware* i *rootkit* programa. Sadrži podršku za operacijske sustave: „Windows 2000 SP4 RU1“, „Windows XP“ i novije (32 i 64-bitne) te „Windows Vista“. Slika 19 prikazuje sučelje ovog programa.

Osnovna obilježja spomenutog programa su:

- visoka razina zaštite od prijetnji s malim učinkom na resurse računala,
- napredna tehnologija detekcije *rootkit* programa,
- zaštita u stvarnom vremenu.



Slika 19 Program „VIPRE“

Izvor: VIPRE

4.3. Usporedba anti-rootkit programa

Na stranicama portala „WhenSecurityMatters“ objavljeni su rezultati usporedbe raznih anti-rootkrit programa prilikom detekcije nekoliko poznatijih rootkit programa. Njihov je rad također uspoređen s mogućnostima detekcije pojedinih antivirusnih alata. Istraživanje je provedeno na računalu s operacijskim sustavom „Windows XP SP2“. Popis svih ispitanih alata, kao i *rootkit* programa dan je u tablici 2.

Anti-virusni programi	Anti-rootkit programi	Rootkit programi
„BitDefender Antivirus 2008“	„AVG Anti-Rootkit 1.1“	„Trojan-Spy.Win32.Goldun.hn“
„Dr.Web 4.44“	„Avira Rootkit Detection 1.00.01.1“	„Trojan-Proxy.Win32.Wopla.ag“
„F-Secure Anti-Virus 2008“	„GMER 1.0.13“	„SpamTool.Win32.Mailbot.bd“
„Kaspersky Anti-Virus 7.0“	„McAfee Rootkit Detective 1.1“	„Monitor.Win32.EliteKeylogger.21“
„McAfee VirusScan Plus 200“	„Panda AntiRootkit 1.0“	„Rootkit.Win32.Agent.ea“
„Eset Nod32 Anti-Virus 3.0“	„RkU 3.7“	„Rootkit.Win32.Podnuha.a“
„Symantec Anti-Virus 2008“	„Sophos Anti-Rootkit 1.3“	
„Trend Micro Antivirus plus Antispyware 2008“	„Trend Micro RootkitBuster 1.6.“	

Tablica 2. Popis programa korištenih u ispitivanju

Rezultati ispitivanja (slika 20) pokazuju da su najbolju detekciju među antivirusnim programima ostvarili:

1. „Dr.Web 4.44“,
2. „Kaspersky Anti-Virus 7.0“,
3. „Symantec Anti-Virus 2008“.

Antivirus\Virus	Rootkit.Win32.Agent.ea	Rootkit.Win32.Podnuha.a	Ukupno
BitDefender Antivirus 2008	-/-	-/-	3
Dr.Web 4.44	+/+	+/+	5
F-Secure Anti-Virus 2008	-/-	-/-	2.5
Kaspersky Anti-Virus 7.0	+/-	-/-	4.5
Eset Nod32 Anti-Virus 3.0	-/-	-/-	1
McAfee VirusScan Plus 2008	-/-	-/-	1.5
Symantec Anti-Virus 2008	-/-	-/-	4
Trend Micro Antivirus plus Antispyware 2008	-/-	-/-	1

Slika 20. Rezultati usporedbe antivirusnih programa

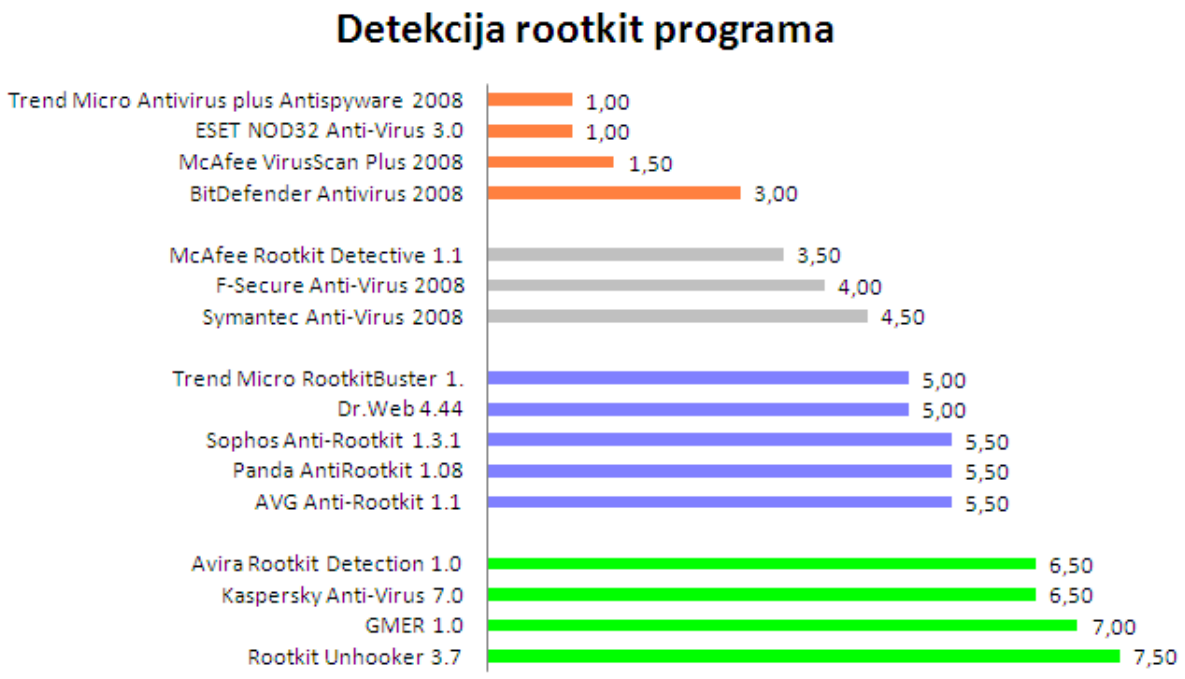
Izvor: portal „WhenSecurityMatters“

Gotovi svi anti-rootkit program osim programa „McAfee Rootkit Detective“i dali su dobre rezultate tijekom ispitivanja,. Svi rezultati prikazani su na slici 21.

Anti-rootkit specialized software	Rootkit.Win32.Agent.ea	Rootkit.Win32.Podnuha.a	Ukupno
AVG Anti-Rootkit 1.1	-/-	-/-	4
Avira Rootkit Detection 1.0	+/+	-/-	5
GMER 1.0.13	+/+	+/+	5.5
McAfee Rootkit Detective 1.1	-/-	-/-	3
Panda AntiRootkit 1.08	+/-	-/-	4
Rootkit Unhooker 3.7.300	+/+	+/-	5.5
Sophos Anti-Rootkit 1.3.1	+/-	-/-	4.5
TrendMicro RootkitBuster 1.6	+/-	-/-	4

Slika 21. Rezultati usporedbe anti-rootkit programa
Izvor: portal „WhenSecurityMatters“

Sličnu usporedbu programa prilikom detekcije rootkit prijetnji napravio je portal „Anti-Malware.ru“. Cilj je bio određivanje koji je program najučinkovitiji prilikom detekcije i uklanjanja rootkit programa. Rezultati su pokazali kako je antivirusni alat „Kasperski Anti-Virus 7.0“ najbolji među trenutno popularnijim alatima prilikom otkrivanja rootkit programa. Među ostalim rezultatima izdvajaju se anti-rootkit alati „Rootkit Unhooker 3.7“, „GMER 1.0“ te „Avira Rootkit Detection 1.0“ s također odličnim rezultatima uklanjanja *rootkit* programa. Ostali rezultati prikazani su na slici 22.



Slika 22. Rezultati istraživanja portala „Anti-Malware.ru“
Izvor: Anti-Malware.ru

5. Zaštita

5.1. Detekcija

Rootkit programe moguće je detektirati antivirusnim programima koji se temelje na potpisima ili praćenju ponašanja dok ih korisnik ne pokrene (pa nemaju mogućnost prikrivanja radnji). Nakon što je *rootkit* pokrenut postoje razna ograničenja za njegovu detekciju jer oni izmjenjuju mnoge jezgrene komponente. Osnovni problem kod detekcije *rootkit* programa je nemogućnost vjerovanja analizama sustava, kao i otkrivanju neautoriziranih modifikacija. Drugim riječima, akcije poput pregleda svih pokrenutih procesa ili popisa datoteka u direktoriju ne moraju davati pouzdanu sliku stanja. Razlog tome je izmjena pokrenutih procesa ili prekid aktivnost do prestanka skeniranja. U takvoj situaciji pouzdani način detekcije je isključivanje ugroženog računala te njegovo pokretanje s alternativnog povjerljivog medija (npr. CD ili USB uređaj). Nepokrenuti *rootkit* ne može aktivno sakriti svoje postojanje pa ih može otkriti bilo koji antivirusni program. Proizvođači antivirusnih proizvoda žele uključiti detekciju *rootkit* programa u tradicionalne antivirusne programe. U slučaju kada *rootkit* prikrije svoje ponašanje za vrijeme skeniranja, antivirusni program identificirat će ga pomoću potpisa. Ipak, neki tvorci *rootkit* programa stvaraju programe koji imaju mogućnost uklanjanja procesa antivirusnih programa iz memorije te time onemogućuju rad antivirusnih programa.

Najučinkovitiji način detekcije *rootkit* programa je uporaba posebnih alata popu:

1. za sustave temeljene na platformi „Unix“ to su: „chkrootkit“, „rkhunter“, „Zeppoo“ ili „OSSEC“,
2. za operacijske sustave „Windows“: „avast! Antivirus“, „RootkitRevealer“, „Sophos Anti-Rootkit“, „F-Secure Blacklight“ i „Radix“.

Još jedna od metoda detekcije je usporedba sadržaja prisutnog na disku sa kopijom u memoriji kako bi se otkrile promjene koje je načinio *rootkit* program. U tu svrhu moguće je koristiti neke od metoda kriptografije (npr. hash funkcije). Nakon prvotne instalacije operacijskog sustava potrebno je napraviti otisak (eng. fingerprint) te isti postupak ponoviti nakon svake nove instalacije nekog programa. Na taj način administrator sustava bit će upoznat sa svakom zlonamjernom izmjenom usporedbom novog i starog otiska.

5.2. Uklanjanje

Izravno uklanjanje *rootkit* programa moglo bi biti dosta nepraktično. Iako je poznat tip i ponašanje *rootkit* programa, potrebno je puno više napora i vremena za uklanjanje tih programa nego za jednostavno ponovno instaliranje operacijskog sustava. Posao reinstalacije može biti jednostavniji uz uporabu programa za stvaranje slike diska.

Budući da mnogi *rootkit* programi ugrožavaju datoteke na najnižoj razini operacijskog sustava, njegovo pokretanje u sigurnom načinu rada (eng. Safe Mode) ne omogućuje uklanjanje tog zlonamjernog programa. Ipak postoje alati, poput „BartPE“ ili „Live Distros“, koji omogućuju korisniku pokretanje valjane kopije operacijskog sustava na ugroženom računalu. Tada korisnik ima mogućnost pregleda sadržaja na disku te može zamijeniti ili obrisati zlonamjerne dijelove.

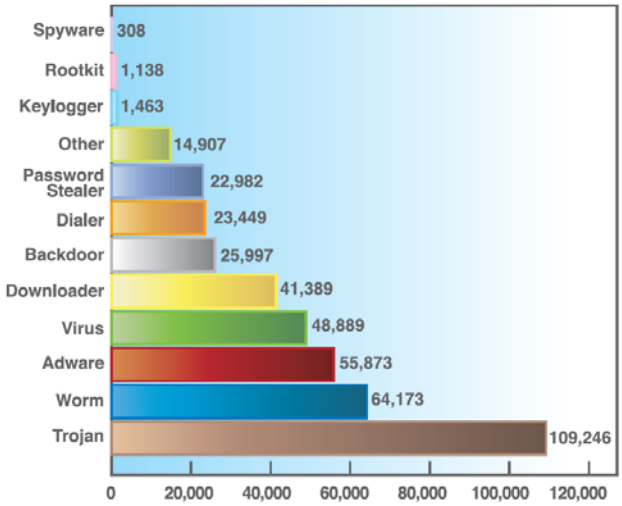
Druga vrsta alata, poput „Symantec Veritas VxMS“, omogućuje antivirusnim skenerima zaobilaženje API (eng. application programming interface) sučelja datotečnog sustava (eng. File System) operacijskog sustava „Windows“. Navedena sučelja kontrolira operacijski sustav pa su ranjiva na manipulaciju s *rootkit* programima. „VxMS“ izravno pristupa osjetljivim datotekama datotečnog sustava pa može izolirati svaku nepravilnost.

6. Očekivanja u budućnosti

6.1. Zastupljenost rootkit programa

Napadi *rootkit* programima čine mali dio zlonamjernih aktivnosti. Prema analizi tvrtke IBM s početka 2008. godine, prijavljeno je 1138 napada *rootkit* programima (slika 22). To je u usporedbi s napadom trojanskim konjima (oko 100 000), računalnim crvima (oko 60 000) te virusima i adware programima (oko 45 000) gotovo neznatan udio u ukupnim prijetnjama.

Ipak, potrebno je obratiti pozornost na prijetnje koje donosi i taj tip zlonamjernih programa zbog posljedica koje mogu uzrokovati na ugroženim računalima. Neke od najozbiljnijih su potpuno preuzimanje kontrole nad ugroženim računalom u svrhu pokretanja napada na druga računala (npr. *spam*), zatim, mogućnost prikrivanja raznih zloćudnih radnji i programa i otvaranje stražnjih vrata na napadnutom računalu.



Slika 23. Udio pojedinih zlonamjernih programa u ukupnim prijetnjama
Izvor: IBM

Sigurnosni stručnjaci koji sudjeluju u razvijanju anti-rootkit programa „Panda Anti-Rootkit“, izdali su u lipnju 2007. godine izvješće o *rootkit* programima. Tvrde kako *rootkit* programi koriste razne tehnike kako bi skrili svoje postojanje na sustavu (datoteke, procese i vrijednosti registra). One sežu od jednostavnijih metoda koje uključuju presretanje IAT funkcija, do naprednijih tehnika koje se javljaju kod jezgrenih *rootkita*. Radi se o modifikaciji SDT (eng. Service Description Table) ili IDT (eng. Interrupt Description Table) tablica te omogućuju filtriranje poziva upravljačkim programima.

Također navode kako su otkrili neke *rootkit* programe koji koriste naprednije metode za zaobilaženje detekcije anti-rootkit programom. Neke od njih su instalacija unutar područja NTFS ADS (eng. *New Technology File System Alternate Data Streams*) tokova, što čini detekciju i postupak uklanjanja vrlo otežanima. Radi se o komponenti datotečnog sustava NFTS koja omogućuje pridruživanje više podatkovnih tokova jednom imenu datoteke.

Primjeri programa koji su koristili takve metode su:

- „Oddysee.B“ – instalirao se u ADS datoteke „NTOSKRNL.EXE“,
- „Rustock.A“ – instalirao se u ADS direktorija „C:\Windows\System32“.
- „Unreal“ – instalirao se u ADS diska sustava.

Iako mnogi anti-rootkit programi koriste napredne tehnike detekcije poznate pod nazivom „cross view“, oni nisu u mogućnosti detektirati *rootkit* programe skrivene u ADS području.

Osim navedenih funkcionalnosti rootkit programa, istražitelji su otkrili neke nove:

1. Skrivanje izvođenja umetanjem u jezgrene dretve,
2. Uništavanje vlastite strukture u slučaju pokretanja nekog anti-rootkit alata,

3. Pretraga za trenutno dostupnim sigurnosnim programima kako bi se otkrio pokušaj detekcije,
4. Instalacija skrivenih posredničkih poslužitelja (eng. proxy) za slanje neželjenih poruka elektroničke pošte (eng. spam).

6.2. Budući razvoj

Od prve pojave *rootkit* programa, njihov razvoj tekao je velikom brzinom. Napadači neprestano razvijaju nove metode skrivanja zlonamjernih radnji koje su uključene u te programe kako bi se zaobišla detekcija. Njihov razvoj potaknut je i činjenicom da je programski kod većine *rootkit* programa dostupan za besplatno preuzimanje na Internetskim stranicama. To omogućuje neograničenu izmjenu funkcionalnosti ili korištenje već postojećih *rootkit* programa za napade. Sigurnosni stručnjaci uporno rade na otkrivanju metoda koje će pružiti pouzdanu detekciju *rootkit* programa i uključuju ih u svoje anti-rootkit proizvode. Ipak, ni danas ne postoji jedinstveni anti-rootkit program koji može otkriti djelovanje bilo kojeg *rootkit*-a. Zbog toga, da bi se osigurala veća razina sigurnosti, potrebno je provesti skeniranje pomoću više anti-rootkit alata.

Razvojem tehnologije i računala može se očekivati daljnji napredak tehnika koje *rootkit* programi koriste za skrivanje svojih datoteka, procesa i sl. Već su poznate inačice tih programa koje mogu prekinuti svoje djelovanje tijekom skeniranja nekim alatom, instalirati datoteke u područja koja nije moguće skenirati ili koji mogu onemogućiti rad antivirusnih programa. U budućnosti se mogu očekivati samo još naprednije metode.

Paralelno s razvojem *rootkit* programa, očekuje se povećanje svijesti o opasnostima koje oni donose. To bi trebalo potaknuti proizvođače anti-rootkit programa na pronalaženje načina detekcije naprednih tehnika koje koriste *rootkit* programi. Očekuje se uključivanje brojnih metoda detekcije u jedinstvene alate kako bi se osigurala detekcija bar jednom do njih. Ipak, nije moguće predvidjeti, niti očekivati, razvoj alata koji će imati mogućnost detekcije svih postojećih inačice *rootkit* programa. Isto tako, moguće je da neke inačice *rootkit* programa toliko napreduju da ih neće biti moguće ukloniti sa sustava nikakvim dostupnim alatima. U takvim slučajevima jedina opcija koja će ostati korisnicima je ponovna instalacija operacijskog sustava.

7. Zaključak

Rootkit programi su tip zlonamjernih programa koji se koriste za skrivanje određenih datoteka ili aktivnosti na sustavima na kojima su instalirani. Iako neki od njih imaju korisnu namjenu, najčešće su usmjereni na ugrožavanje sustava kako bi se sakrilo djelovanje nekog zlonamjernog programa ili napadaču omogućila kontrola sustava.

Prve inačice tih programa koristile su vrlo primitivne metode pa je njihove radnje bilo lako detektirati. Međutim, te primitivne metode velikom su brzinom prerasle u napredne mehanizme skrivanja prisutnosti zlonamjernih sadržaja na računalima. Uključivale su skrivanje procesa, prodor u nove dijelove operacijskog sustava, onesposobljavanje skeniranja i sl.

Sigurnosni stručnjaci trude se razviti alate kojima mogu detektirati postojanje *rootkit* programa na računalu u obliku anti-rootkit alata. Koriste tehnike detekcije koje se zasnivaju na pretraživanjima baza podataka s ranije otkrivenim *rootkit* programima ili praćenju ponašanja programa. Budući da ove tehnike često nisu davale pouzdane rezultate, razvijene su naprednije metode koje se oslanjaju na vlastite postupke skeniranja podataka na disku. Riječ je o „cross view" tehnikama koje koriste mnogi anti-rootkit programi, zajedno s provjerom integriteta datoteka i memorije.

Iako su dostupni razni besplatni i komercijalni anti-rootkit alati, ne postoji niti jedan koji jamči sigurno detektiranje i uklanjanje svih vrsta *rootkit* programa. Razlog tome je njihova česta izmjena te veliki broj raznih *rootkit* programa koji koriste neke posebne metode skrivanja. Kako bi se osigurala određena razina sigurnosti sustava, korisnicima se preporuča stalna primjena nekog od anti-rootkit alata s mogućnošću detekcije i uklanjanja tih zlonamjernih programa. Također dodatnu sigurnost donosi savjesno ponašanje, što se odnosi na izbjegavanje pregleda sumnjivih web stranica i posjećivanja nesigurnih poveznica.

8. Reference

[1] Rootkit, http://en.wikipedia.org/wiki/Rootkit, siječanj, 2010.

[2] L. Stevenson, N. Altholtz, „Rootkit for Dummies“, Wiley Publising, Inc, 2007.,

[3] R. B. Blunder, „The rootkit arsenal“, Wordware Publishing, Inc, 2009.,

[4] Windows rootkits of 2005, part three, http://www.securityfocus.com/infocus/1854, 2005.,

[5] Rootkit Analytics, http://www.rootkitanalytics.com/, siječanj 2010.,

[6] Rootkit Analyse, http://www.omninerd.com/articles/r00tkit_Analysis_What_Is_A_Rootkit, studeni, 2005.,

[7] Anti.rootkit, http://www.antirootkit.com/, siječanj 2010.,

[8] Anti-rootkit, http://www.antirootkit.com/software/index.htm, siječanj 2010.,

[9] Sony rootkit, http://cp.sonybmg.com/xcp/english/titles.html, siječanj 2010.,

[10] Sophos anti-rootkit http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html, siječanj 2010.,

[11] Sophos anti-rootkit, http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html, siječanj 2010.,

[12] Chrootkit - http://www.chkrootkit.org/, siječanj 2010.,

[13] RootKit Hook Analyzer, http://www.resplendence.com/hookanalyzer, siječanj 2010.,

[14] Sanity - http://www.resplendence.com/sanity, siječanj 2010.,

[15] RootkitRevealer, http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx, siječanj 2010.,

[16] Rootkit Hunter, http://www.rootkit.nl/projects/rootkit_hunter.html, siječanj 2010.,

[17] Gmer, http://www.gmer.net/, siječanj 2010.,

[18] UnHackMe, http://www.greatis.com/unhackme/, siječanj 2010.,

[19] Proces Master, http://www.backfaces.com/, siječanj 2010.,

[20] Vipre, http://www.vipreantivirus.com/, siječanj 2010.,

[21] Popis antirootkit programa, http://www.antirootkit.com/software/index.htm, siječanj 2010.,

[22] Usporedba anit-rootkit alata, http://whensecuritymatters.com/index.php/Comparative-tests/Anti-Rootkit-Detection-and-Treatment-Test.html, siječanj, 2010.,

[23] Rootkit in the mist, http://research.pandasecurity.com/rootkits-in-the-mist/, lipanj, 2007.,

[24] IBM Internet Security Systems, X-Force® 2007 Trend Statistics, http://www-935.ibm.com/services/us/iss/pdf/etr_xforce-2007-annual-report.pdf, siječanj, 2008.,

[25] Anti-rootkit tests, http://www.anti-malware-test.com/?q=taxonomy/term/7, siječanj, 2001.