Zlonamerni programi

DRAGAN RANĐELOVIĆ, BRANKICA POPOVIĆ
Kriminalističko policijska akademija, Beograd

Stručni rad
UDC:519.686:681.067

Danas, u informatičkoj epohi razvoja ljudskog društva, postoji veliki interes za proučavenje zlonamernog programa (malware) i odgovarajućih programa za zaštitu od njega. Zlonamerni ili nepoželjni program je svaki koji poseduje sposobnost useljavanja u računarski sistem korisnika u nameri da na bilo koji način oteža pa i onemogući rad samostalnog ili umreženog korisnika, pri čemu je prirodno stanište nepoželjnog programa Internet. Precizna taksonomija neopoželjnih programa je onemogućena pre svega njihovim svakodnevnim uvećavanjem. Pri tome se, često pogrešno, termin komjuterski virus upotrebljava kao sveobuhvatna fraza koja podrazumeva sve nepoželjne programe uključujući i prave viruse.

Ključne reči: *nepoželnji programi, sistem datoteka, arhive*

1. UVOD

Mada precizna definicija zlonamernog programa (eng. *malware, od* zlonamerni-***mal****icious* i program - *soft****ware***) ne postoji, pod tim pojmom se podrazumeva svaki program koji ima sposobnost useljavanja u računarski sistem korisnika bez njegovog znanja i odobrenja. Autori zlonamernih kodova pišu nove varijante koje se razlikuju od postojećih i tako otežavaju njihovo prepoznavanje pa je iz tih razloga i samu klasifikaciju tih programa jako teško sačiniti. Termin komjuterski virus često se upotrebljava kao sveobuhvatna fraza koja podrazumeva sve nepoželjne programe, a koji su takodje programski kodovi prepoznatljivi po tome što obavljaju dve nekontrolisane funkcije: razmnožavanja i pokretanja. Ponekad se programi koji inače služe u korisne svrhe mogu upotrebiti zlonamerno, što takođe otežava raspoznavanje i zaštitu.

Zlonamerni programi mogu raditi neprimetno u pozadini, i/ili usporiti računar i periodično izazivati kočenje ili obaranje sistema. Zavisno od vrste i namene, zlonamerni program može obavljati jednu ili više aktivnosti: narušavanje performansi sistema, dovođenje sistema u nestabilno stanje, generisanje „neobičnog" ponašanja sistema, preusmeravanje zahteva za otvaranje Web stranica, opsluživanje iskačućih (pop-up*)* prozora ili banera s reklamnim sadržajem, praćenje aktivnosti i *of services*) uznemiravanje korisnika, krađa ili uništavanje poverljivih informacija, DoS tj. odbijanje servisa (*denial of services*) na određenom serveru, preuzimanje dodatnog izvršnog koda sa Interneta i instalacija drugih zlona uznemiravanje korisnika, krađa ili uništavanje poverljivih informacija, DoS tj. odbijanje servisa (*denial of services*) na određenom serveru, preuzimanje dodatnog izvršnog koda sa Interneta i instalacija drugih zlonamernih programa, isključivanje sigurnosnih aplikacija, modifikacija lozinki na sistemu i dodela prava daljinskog pristupa računaru, menjanje podataka i baze Registry i oštećenje hardvera. Iako je najveći broj zlonamernih programa namenjen Windows platformama (Windows XP je omiljena meta), ugroženi su i UNIX, Linux i druge platforme. Zlonamerni programi se distribuiraju na različite i stalno nove načine: preko deljenih direktorijuma na mreži, priloga elektronske pošte, otvorenih TCP i/ili UDP portova koji omogućavaju izvršenje udaljenog koda na žrtvi, peer–topeer (P2P) mreža, Internet Messaging (IM) servisa, drugih *malware* koji će preuzeti zlonamerni kod s neke lokacije na Internetu i instalirati ga na žrtvi.

U računarima su sve informacije memorisane u datotekama kao osnovnoj organizaciji podataka u računaru. Kako je predmet ovog rada malware za čije dejstvo osnovu čine datoteke, to je neophodno poznavati osnovne pojmove o sistemu datoteka i naročito arhivama zbog njihove masovne upotrebe u svrhu ušteda.

2. TAKSONOMIJA MALWARE

Kako se svaki dan pojavljuju nove varijante zlonamernih kodova, razumljivo je da je jako teško sačiniti njihovu klasifikaciju. Jedna od mogućih, verovatno najsveobuhvatnija, bila bi sledeća klasifikacija:

- da postoje zarazni – čiji su tipični primeri virus i worm;
- sakriveni – čiji su tipični primeri trojan horse, rootkit i backdoor;

Adresa autora: Dragan Ranđelović, Kriminalističko policijska akademija, Beograd - Zemun, Srbija, Cara Dušana 196

Rad primljen: 21. 02. 2010.

- koristoljubivi – čiji su tipični primeri spyware, Keyloggers, adware i dialer.

Tehnički posmatrano zlonamerni programi se dele:

- na one kojima **je neophodan nosilac**, tj. program gde su sakriveni (trojanski konji, virusi), i
- samostalne, tj. one kojima nije neophodan nosilac program (crvi, špijunski programi).

Prema drugom takođe tehničkom kriterijumu, zlonamerni programi se dele na one:

- koji se **repliciraju** (virusi, crvi) i
- koji se ne repliciraju (trojanski konji, logičke bombe).

Virus je najstarija vrsta malicioznog koda koji izvršava dve osnovne radnje i to nekontrolisano razmnožavanje i pokretanje, a zavisno od nekog kriterijuma ugrađenog u programski kod virusa (datum, vreme,...). Smatra se da su obavezno i destruktivni, što ne mora biti tačno. Klasifikuju se kao infektori fajlova ili izvršni virusi koji se najčešće infiltriraju u neki izvršni fajl i makro virusi formirani primenom standardnih komandi nekog makro ili script jezika.

Crvi (*worms*) su maliciozni kod koji za svoje "razmnožavanje" (stvaranje većeg broja primeraka) ne koristi fajlove već slabosti i propuste komunikacionih protokola i sistema zaštite računarskih mreža.

Trojanci predstavljaju prave programe, ne samo maliciozni kod u nekom programu. *Rootkits* su maliciozni kod koji modifikuje MBR (*Master Boot Records*) koji je deo na hard disku u kome se nalaze informacije o samom disku u cilju sakrivanja fajlova na kome je smešten ili modifikacije fajlova samog operativnog sistema pa *malware* ostaje sakriven od korisnika. *Backdoor malware* je maliciozni kod kojim se ostvaruje zaobilaženje autentifikacije. *Spyware*, kao često skrivena komponenta sumnjivih *shareware* i *freeware* programa, je maliciozan kod namenjen neovlašćenom prikupljanju podataka sa okupiranih računara. *Adwares* su programi koji se instaliraju na računar zajedno sa nekim drugim programima, uglavnom skinutih sa Interneta, a pre svega služe da prikažu reklamne poruke dok je okupirani korisnik na Internetu. Ponekad su i špijunski nastrojeni. *Keylogger* je program namenjen za krađu personalnih informacija zaraženog korisnika kao lozinke, bankovnih računa, brojeva platnih kartica i njihovu distribuciju na određene e-mail adrese. *Dialers* su programi koji modifukuju i preusmeravaju dial-up konekciju ka Internetu korisnika, a da bi ostvarivao skupe konekcije.

3. DATOTEKE

3.1. Sistem datoteka

Operativni sistem računara je zadužen da obezbedi upravljanje datotekama i on to čini pomoću sistem datoteka (*file system*).

Najpoznatiji file systemi koriste uređaje za skladištenje podataka koji nude pristup blokovima fiksne veličine-sektorima, najčešće 512 bajtova. *File system* je zadužen za organizaciju ovih sektora u datoteke i direktorijume i za vođenje evidencije o tome koji sektor pripada kojoj datoteci i koji sektori nisu u upotrebi. *File system* organizuje pristup i dinamički stvorenim podacima (sa Weba).

File system obično sadrži direktorijume koji povezuju imena datoteka sa datotekama, tako da povežu ime datoteke sa nekim indexom u neku *File Allocation Table*, kao npr. FAT-a u MS-DOS-u ili INODE-a u Unix sistemima. Postoje sledeći tipovi:

- Regularne datoteke – sadrže informacije u binarnom i ASCII obliku (Windows i Unix)
- Direktorijumi – sistemske datoteke koje održavaju strukturu fajl sistema (Windows i Unix)
- Karakter specijalne datoteke – modeliraju serijske U/I uređaje (Unix)
- Blok specijalne datoteke – modeliraju diskove (Unix).

Dakle za održavanje strukture sistema datoteka koriste se direktorijumi (*folder*) koji su najčešće implementirani kao datoteke i imaju strukturu:

* jednonivovsku kada je u sistemu samo jedan osnovni (*root*) direktorijum i sve datoteke se nalaze u okviru njega (kod višekorisničkih sistema može doći do konflikta prilikom imenovanja datoteka),
* dvonivovski u kome postoji jedan *root* direktorijum i po jedan privatni direktorijum za svakog korisnika (problem veliki broj datoteka) i
* sistem sa generalnom hijerarhijom, kao najprirodniji, ima jedan *root* direktorijum od koga se granaju ostali direktorijuma u dubinu stabla.

Kod sistema generalne hijerarhije potrebno je obezbediti pravilno imenovanje datoteka i to

- zadavanjem apsolutne putanje gde je obavezni početak *root* folder i
- relativnom putanjom kada je bitan pojam i tekući direktorijum.

Sistemi daoteteka su smešteni na disku ili drugom spoljašnjem memorijskom medijumu pri čemu oni mogu biti podeljeni na jednu ili više particija i svaka particija može imati nezavisan sistem datoteka. Svaki disk mora sadržatii:

- MBR (*master boot record*) – nalazi se na sektoru 0 i koristi se za podizanje sistema
- Particiona tabela (*partition table*) – nalazi se na kraju MBR-a i sadrži informacije o particijama tj. njihovu početnu i krajnju adresu
- Particije, koje mogu da sadrže - *boot block* koji se koristi za učitavanje operativnog sistema (*loader*), super block koji sadrži informacije o sistemu datoteka, strukture za upravljanje slobodnim prostorom particije, root direktorijum i ostale direktorijume i datoteke.

Kod implementacije file sistema jedna od najvažnijih stvari je način na koji se pamti podatak o tome koji blok diska pripada kojoj datoteci. Raspored prostora diska naziva se alokacija. O pristupu podacima na disku brine sistem datoteka, kojem su performanse i osobine vezane za operativni sistem (OS) koji ga koristi. Npr. Windows koristi FAT i NTFS file sistem.

Postoje:

- Kontinualna alokacija
- Alokacija uz pomoć lančane liste
- Alokacija uz pomoć lančane liste korišćenjem tablice u memoriji
- i-nodes

3.2. Stvaranje, vrste i struktura pakovanih datoteka

Datoteke nastaju iz uredjaja i programa kreatora kao što su respektivno npr. foto-aparati, kamere itd. tj. Editori teksta, programi za obrade crteža, slika, fotografija i multimedije ali i programski jezici itd. U svojoj ekstenziji datoteke nose bližu oznaku vrste (kada je u pitanju Windows, jer npr. Unix nema ekstenzije u imenima datoteka) i npr. EXE označava izvršni fajl, DOC Word, XLS Excel dokument, JPG je jedan od formata slike itd. Datoteke nastaju i postupcima pakovanja i to kao izvršne. Da bi se bitna uloga pakovanih datoteka u radu *malware* razumela neophodno je pravilno razumeti izraze za pojedine tipove pakovanih datoteka i njihovu strukturu:

1. Arhiver je program koji više fajlova smešta u jedan za potrebe arhiviranja. Potreba za takvim tipom programa se pojavila jako davno, u vreme kada su trake bile jedini medij na koji je bilo moguće smestiti veće količine podataka. Kako taj sistem ne sadrži direktorijume već su svi podaci snimani jedan za drugim na traku, bilo je potrebno nekako održati red. Zato su se prvo svi srodni podaci pakovali u jednu arhivu, pa ona na traku. Tako na traci umesto 10.000 zasebnih fajlova ima višestruko manje arhiva. Arhiver koji se zadržao do današnjih dana je TAR – Tape ARchiver.

2. Kompresor je posledica ideje, nakon pojave arhivera, da bi se moglo na te trake da smesti još više podataka ako bi upotrebili kompresiju po nekom od algoritama koji ne degradiraju (nakon dekompresije podaci su istog oblika kao pre) podatke. Danas od samostalnih kompresora mogu se sresti u upotrebi još Bzip2 i Gzip.

3. Kompresor – Arhiver (može i obrnut redosled) je danas jako upotrebljavani program, tipa ZIP, RAR..., koji u suštini obavlja posao prethodno opisana dva tipa. Naime, kompresor na svom ulazu ne prima više fajlova od jednom, tako da imate dva rešenja ili prvo arhiverom arhivirate više fajlova u jedan pa arhivu (koja je jedan fajl) ubacite u kompresor ili izkompresujete svaki fajl posebno, pa sve to na kraju arhivirate u jedan fajl.

4. Paker se upotrebljava u dva konteksta, u jednom za rezultat kompresor-arhivera, u drugom za exe-pakere (ili run-time packer). Ovaj zadnji ne treba mešati sa SFX arhivama.

5. SFX je program nastao kao poseledica što svaki kompresor-arhiver ima svoj format arhiva i svoj algoritam za kompresiju (ili više njih). Neko se dosetio da i sam program za otvaranje arhive smesti na početak arhive. Tako primalac tako spremljene poruke ne mora da ima i program za raspakovanje. Pokretanjem SFX arhive startuje se program za raspakovanje sa početka arhive i vrši raspakovanje. SFX arhive na Windows sistemima imaju ekstenziju EXE, kao i svi izvršni programi.

6. EXE-pakeri su nastali u vremenu kada je zbog malih HD (tvrdi diskovi-skraćenica od engleskog *hard disc*) trebalo da fajlovi budu kompresovani da bi zauzeli manje mesta na HD-u. Kako se fajlovi podataka uvek mogu arhivirati po želji, problem je programa i njihovih biblioteka. Struktura ovog tipa datoteka je slična strukturi SFX datoteka tj. Prvo se kompresuje program i na njegov početak doda program za raspakovanje. Razlika je u tome što exe-paker pakovani program raspakuje u memoriji i tamo odmah izvrši. EXE-protektori i EXE-kripteri su nastali kao potreba da se reši problem krađa programa i podataka uopšte jer ih je relativno lako iz binarnog oblika pretvoriti u neki oblik koji je čitljiv. Na principu rada EXE-pakera napravljeni su programi kripteri koji program tj. podatke ispretumbaju pre plasiranja programa na tržište, kriptuju program i na njegov početak stave program koji će da ga vrati u normalu. Na korisnikovom disku je čitljiv samo deo za raspakovanje, ali ne i program. Kada korisnik startuje program, deo za dekriptovanje će preneti program u memoriju, tamo ga pretumbati ponovo da bi ga vratio u normalu, i onda ga startovati. Međutim ova zaštita ima mogućnost da bude razbijena npr. programom koji će kontrolisano da pusti štićeni program, dozvoliće delu za tumbanje da učita štićeni program u memoriju i da ga dekriptuje a onda će da zaustaviti dalji proces i iskopirati štićeni program iz memorije na disk; ti programi se zovu memorijski – dampери i debageri. Zato se mora imati još jedan vid zaštite koji poseduju EXE-protektori koji mogu detektovati da je dekriptor startovan u okruženju memorijskih dampera i debagera, i ne dekriptuju fajl koji poseduju EXE-protektor. Često se EXE-protektori, EXE-kripteri i EXE-pakeri nazivaju imenom EXE-paker. Kod protekcije je najbitnije non-stop proveravati u kom je okruženju startovan protektovani fajl i da to ne bude neki debuger ili virtuelna mašina.

7. Morpheri su grupa programa čija je uloga da pretumbaju izvršni fajl. Kod fajl-infektora (kao što su npr virusi) imaju ulogu da učine da svaka sledeća replikacija izgleda drugačje, a da je i dalje funkcionalna.

8. Instaleri i Setup-rutine su programi koji se mogu posmatrati kao SFX arhive koje osim arhive sa fajlovima koje trebaju da instaliraju, sadrže i program koji vrši instalaciju, skripte po kojima vrši instalaciju, kao i program za deinstalaciju sa njemu pripadajucim fajlovima. Kod pokretanja, on prvo ucita skript u kome je opisano u koje foldere treba da iskopira koji fajl (kod Windowsa i upisivanje podataka u registry bazu ili ekvivalentne baze

eventualno instalirananog nekog drugog operativnog sistema). Obično uz instalirane fajlove jedan instaler iskopira i program ili skriptu koje će kasnije poslužiti za deinstalaciju. Sami programi u instaleru su arhivirani i kompresovani analogno fajlovima kod kompresor-arhivera.

9. Kontejneri su takva vrsta fajlova koji u sebi sadrže druge fajlove, tj. preciznije rečeno, sadrže streamove. Stream je takav vid podatka nad kojim se može vršiti neka operacija bez da imamo ceo podatak, tj. operacija se može vršiti još u toku čitanja streama. Tako npr. poznati AVI fajl. koji može sadržati jedan video stream i dva audio streama (kod stereo signala je svaki kanal poseban stream kada je reč o digitalnom zapisu signala).

Na kraju ovog potpoglavlja posebno ćemo skrenuti pažnju na proces raspakovanja upakovanih datoteka i potencijalnih opasnosti za implementaciju u proces malicioznih programa.

- Arhive, uključujući i kompresovane fajlove, za raspakovanje traže odgovarajući program za raspakovanje; učitava se arhiva i zadaje folder gde se izvrši raspakovanje. Međutim SFX arhive se raspakuju startovanjem, kada njihov ugrađen stub, koji može biti izložen dejstvu *malware*-a, raspakuje arhivu uz mogućnost da nakon raspakovanja odmah startuje neki od fajlova koji je upravo raspakovan; ako je fajl bio trojanac, posledice mogu biti teške po računar.

- Instaleri se raspakuju generalno kao i SFX arhive ali je teže pronaći programe za raspakovanje pošto nije u interesu onog koji je napravio instaler da napiše i program za raspakovanje instalera.

- Pakeri, protektori i kripteri su grupa programa namenjena za zaštitu programa od reverznog inženjeringa, pa su im i načini pakovanja komplikovaniji i teži za inverziju. Interes za pisanje raspakivača imaju kraker (*cracker*) grupe da bi proučile način da razbiju zaštitu, bilo da napišu crackove ili da nadju algoritam po kome bi napisali generatore serijskih brojeva. Interes imaju i pisci antivirus programa.

3.3. Identifikacija datoteka

Pojam magičnih brojeva (*magic numbers*) je uveden u vreme UNIX-a kada fajlovi nisu morali da imaju ekstenzije (na Unixu i naslednicima ni sada to nije obavezno). Da bi se znalo koji fajl je kog tipa, propisani su *magic numbers*. Po originalnom standardu prva dva bajta u fajlu su služila za identifikaciju tipa fajla. Kasnije se odstupilo od cifre od dva bajta.

Primera radi, svi EXE fajlovi pod DOS-om počinju bajtovima 4D5A - ASCII kodove za slova MZ (MZ su inicijali Marka Zbikowskog koji je osmislio DOS format izvršnih fajlova). DOS je imao problem jer je osim EXE-formata izvršnih fajlova dopuštao i izvršavanje bilo kog drugog binarnog fajla ukoliko mu je ekstenzija .COM. COM (skraćeno od engleskog *command*) fajlovi nisu morali da imaju ništa od metadata u sebi, tj. nisu imali nikakva zaglavlja fajla, već je prvi bajt u fajlu već pripadao izvršnom kodu i taj program se učitavao u prvi slobodan segment memorije na adresu 0x0100 i počeo izvršavanje. Danas se programi kompajliraju tako da rade nezavisno na kojoj adresi u memoriji su učitani. Zato služi deo fajla koji se zove *Relocation table*. COM fajlovi nisu imali u sebi podatak sa kojim bi bili identifikovani pa je to činjeno puštanjem u rad.

Windows 3.xx kao Microsoft produkti je imao *New Executable Format* (skraćeno NE) među formatima izvršnih fajlova koji je koristio i IBM, tj. Operaativni sistem OS/2. Novi format omogućava izvršne fajlove veće od 64kb.

LE/LX/PE identifikacija su varijante na temu fajlova koji počinju MZ magic numberom i PE je trenutno aktuelni format izvršnih fajlova za Windows pri čemu je MZ još uvek prisutno kao i u NE formatu i to samo iz razloga da kad neki program za Windows startujemo u DOS-u dobije se poruka:This program must be run under Win32.

Enkodinzi (*encodings*) su programi za prevođenje podataka iz formata u format. Nastali su još u vreme DOS za potrebe mrežnog prenosa binarnih fajlova samo ASCII set karakterima, koji je 7-bitan (u jednom bajtu prenose samo vrednosti od 0 do 127 a bajtovi binarnog fajla sadrže vrednosti od 0 do 255). Enkodinzi Base64, UUE, XXE itd. se i danas koriste za prenos priloga uz elektronsku pruku (eng. *attachment*). Struktura enkodinga je slična današnjim exe-pakerima jer je na početku programa deo za raspakovanje i nakon njega 7-bitno spakovan fajl. Postavlja se pitanje kako je mogao deo za raspakovanje da se prenese mrežom u vreme DOS-a ako je on bio programski kod a odgovor je da su napisali program koji je upotrebljavao samo one procesorske instrukcije koje su bile ispod broja 127 tj. 7-bitni raspakivač koji je raspakovao 8-bitni kod iz 7-bitne arhive i onda ga izvršio.

3.4. Zaštita podataka u datotekama

Zaštita podataka se obično sastoji od enkripcije podataka koji se nalaze u datoteci. Osim enkripcije, može se samo ograničiti pristup šifrom, a da sami podaci ne budu kriptovani. U drugom slučaju je moguće zaobići zaštitu i pristupiti podacima a kod kriptovanih podataka se mora znati lozinka da bi se podaci dekriptovali. Osnovne pojmove ovih metoda zaštite objasnićemo na primeru *InnoSetup* instalera koji omogućava oba navedena načina zaštite. *InnoSetup* instaler, pri postupku pravljenja instalacionog fajla za program koji će se distribuirati, nudi obe opcije. Kod izbora ograničenja pristupa lozinkom:

- inicira se MD5 hash rutina
- u bafer za računanje hasha se prvo ubacuje reč „Password CheckHash“

- u bafer se ubacuje salt (slučajno generisan broj)
- u bafer se ubacuje lozinka koju je autor odabrao
- na kraju se generiše MD5 hash svega ovoga, i upisuje se u zaglavlje budućeg instalacionog fajla

Ako se autor odluči i za enkripciju podataka, tada se dešava sledeće:

- prvo se uradi opisana procedura za upis hasha
- nakon toga se ponovo inicira MD5 hash rutina
- u bafer se ubacuje isti salt koji je već korišćen
- u bafer se ubacuje lozinka
- generiše se hash koji služi kao ključ za enkripciju
- enkriptuju se svi fajlovi generisanim ključem
- fajlovi se kompresuju i u zaglavlje se upišu CRC.

Inače hash funkcija je takva funkcija koja će od ulaznih podataka generisati nešto što se može nazvati njihovim opisom. Generalno, dva različita podatka nikada nebi trebalo da daju isti hash, ali se to u praksi dešava, i naziva se kolizijom. Kao jednosmerna operacija ne omogućava da se od generisanog hasha sazna podatak od koga je taj hash generisan. Nebitno od veličine ulaznog podatka, hash generisan jednom hash-rutinom uvek daje rezultat iste veličine.

CRC je vid hasha, ali se ne upotrebljava za enkripciju jer je 16-bitan (iako postoji i CRC32) čime je mogućnost kolizije jako velika. Upotrebljava se kao brza provera ispravnosti jer se brzo izračunava i zato sve vrste arhiva koje se danas upotrebljavaju, u samom zaglavlju arhive imaju upisani CRC (ili CRC32) fajlova koji se nalaze u arhivi, tako da se nakon raspakovanja može videti da li su fajlovi ispravno raspakovani. Hash se koristi za proveru lozinke na sledeći način:

- kada korisnik prvi put odabere svoju lozinku, generiše se njen hash koji se negde zapamti
- kada korisnik sledeći put treba da upotrebi svoju lozinku, generiše se hash unetog i upoređuje da li je isti sa onim koji je zapamćen što znači da sama lozinka nije nigde zapamćena.

Dakle sada je jasnije kako je *InnoSetup* podatke kriptovao generisanim hashom, i takođe uočavamo da je sam hash upisan i u zaglavlje fajla. Pošto jednostavno čitanje hash koji je upisan u zaglavlje fajla za dekripciju podataka nije moguće jer se u prvom postupku u bafer prvo ubacuje reč „PasswordCheckHash“, a menjanje samo jednog bita daje potpuno drugi hash to se uloga tog hash najbolje može razumeti iz opisa procedure raspakovanja podataka pri instalaciji, a ona je:

- korisnik pokreće instalaciju
- instaler traži lozinku
- korisnik unosi lozinku
- inicira se MD5 hash rutina
- u bafer se ubacuje reč „PasswordCheckHash“
- u bafer se ubacuje salt, koji je takođe u zaglavlju
- ubacuje se lozinka koju je korisnik uneo
- izračunava se hash i poredi sa onim koji je upisan u zaglavlje i postupak do ovog koraka traje par μs
- ako je izračunati hash jednak upisanom postupak se nastavlja u suprotnom se obustavlja instalacija
- inicira se MD5 hahs rutina
- u bafer se ubacuje salt koji iz zaglavlja fajla
- u bafer se ubacuje lozinka koju je korisnik uneo
- generiše se hash koji služi kao ključ za dekripciju
- počinje dekompresija i dekripcija prvog fajla
- računa se CRC fajla i poredi se sa upisanim u zaglavlje arhive
- ukoliko je CRC isti, fajl je ispravno raspakovan
- ukoliko CRC ne odgovara, onda je fajl ili oštećen ili je ključ za dekripciju pogrešan
- postupak dekompresije, dekripcije i provere CRC traje zavisno od veličine fajla koji je u arhivi.

Upisani hash se koristi za proveru lozinka pre dugog procesa dekompresije i dekripcije koji zavisno od veličine fajla, traje i desetak minuta. Sličan sistem je kod svih fajlova zaštićenih lozinkama, a većina nema prvu proveru pa se ispravnost lozinke vidi tek kod provere CRC-a.

Za nalaženje lozinke kod enkritpovanih fajlova jedina je mogućnost isprobavati sve moguće lozinke redom. To se naziva „*brute force attack*“ (BF) koji može da potraje dugo, naročito kod onih vrsta arhiva koje nemaju primarnu proveru lozinke, već se čeka provera CRC-a, pri čemu trajanje BF-a takođe zavisi i od vrste hasha koji se koristi jer npr. MD5 generiše 128-bitni hash, a koriste se i 512-bitni hashevi a što je duži hash duže traje i dekompresija/dekripcija.

4. ZAKLJUČAK

Malware je realnost računarskog i naročito mrežnog okruženja sa kojom obavezno treba računati u danas svakodnevnom i masovnom korišćenju različitih mrežnih okruženja počev od nezaobilaznog Interneta.

Za efikasnu zaštitu od dejstva malicioznih programa potreno je kvalitetno poznavanje novina i nauke koje se bave ovom problematikom. Sistem datoteka operativnih sistema na kojima radi naš računar tj. mreža ima u tome osnovnu ulogu. Sve više ljudi na razne načine i iz različitih razloga napadaju Internet ali i druge mreže, neki od njih to čine radi zarade, pojedini da bi se osvetili društvu, dok postoji i oni, koji prosto žele da demonstriraju svoje sposobnosti i talenat. Prema nepotpunim podacima, širom sveta danas postoji i preko 100000 vrsta samo virusa, a taj broj se godišnje povećava za čak 20000 što ukazuje da je i poznavanje taksonomija *malware-a* bitno za njihovo suzbijanje.

LITERATURA

[1] Bishop, M. (2003). Computer Security: Art and Science, Addison-Wesley Professional.

[2] Jones, K. J., Shema, M., & Jonhson, B. C. (2003). Антихакерски алати, Чачак, компјутер библиотека

[3] Microsoft, Web page , http://www.microsoft.com/ technet/security

[4] Pastore, M., & Dulaney E.(2007). *Security* + (prevod na hrvatski), Miš d.o.o.+

[5] Wikipedia, Web page, http://en.wikipedia.org/ wiki/ malware

SUMMARY

MALICIOUS SOFTWARE

Today, during the epoch of informatics and human progress, there is a big interest for malware programs as well as for the programs used for protection against them. Malware is each program which has ability for moving into someone's computer system with intention to disable, or at least make difficult, work of this independent or network user. Natural residence of malware is Internet. It is impossible to give precise taxonomy of malware because their number is increased each day. The term computer virus is often wrongly used as universal phrase for all malware, including and real viruses.

Key words: *malware, file system, archives*