Malware

Izvor: **http://www.cert.hr/malver/virusi**

- **Malver** (malware je skraćeno od malicious software) je zlоćudni (zlonamjerni) softver namijenjen infiltraciji računala bez znanje njegovog vlasnika, odnosno korisnika. Softver se klasificira kao malver ovisno o njegovoj (štetnoj) namjeni. Prema tome, u malver spadaju:

- virusi
- crvi
- trojanski konji
- spyware
- zloćudni adware
- crimeware
- scareware
- keyloggeri
- rootkitovi

Općenito virus

- Računalni virus je računalni program koji svojom reprodukcijom može zaraziti računala na način da bez dopuštenja ili znanja samog korisnika računala kopira samog sebe u datotečni sustav ili memoriju ciljanog računalnog sustava.
- Izraz "virus" često se povezuje i s malicioznim programima poput adware-a (program za oglašavanje) i spyware-a (program za prikupljanje podataka), koji nemaju sposobnost reprodukcije kao virus.

- **Računalni crv** ima za namjeru iskorištavanje sigurnosne ranjivosti sustava kako bi se proširio na druga računala, umnožavajući sam sebe koristeći Internet bez sudjelovanja druge fizičke osobe, dok je **trojanski konj** program, koji se pretvara da izgleda bezopasno, predstavljajući se kao neka igra ili sadržaj koji se šalje u e-mail poruci, no najčešće ima skrivenu štetnu funkcionalnost koja može dovesti do npr. formatiranja cijelog diska ili instalacije programa za udaljenu kontrolu, koja omogućava nekoj trećoj zlonamjernoj osobi potpunu ili djelomičnu kontrolu nad vašim pohranjenim podacima i računalom.

- Također je važno napomenuti da na taj način zaražena računala mogu biti član „**botneta**“, odnosno infrastrukture sastavljene od mnogo zaraženih računala koja imaju uspostavljenu vezu sa komandnim centrom. Na taj način treće osoba imaju kontrolu nad računalima korisnika koja su izvršioci kod slanja spama ili masivnih DDoS napada. Isto tako veliki broj virusa ima i drigih zlućudnih funkcija, kao što su na primjer praćenje aktivnosti tipkovnice što omogućuje krađu privatnih podataka, lozinka, brojeva kreditnih kartica i ostalo.

Načini zaraze i izvršenja malicioznog koda

- Da bi se virus replicirao pokretanjem izvršenja malicioznog koda, virusi se vežu za izvršne datoteke legitimnih programa. Tako se u slučaju pokretanja zaraženog legitimnog programa, istovremeno pokreće izvršavanje i virusnog koda.

- Prema svom načinu djelovanja, virusi se dijele se na dvije vrste, **nerezidentne i rezidentne**.
- **Nerezidentni virusi** se nalaze u RAM memoriji samo u vrijeme njihovog izvršenja, odnosno od njihovog pokretanja pa do završetka rada. Njihovo širenje se svodi na princip da dio njihovog koda pronalazi datoteke koje mogu biti zaražene na sustavu(npr. .exe., .doc i slično), a drugi dio koda kopira virusni kod u pronađenu datoteku.

- **Rezidentni virusi** se prilikom njihovog izvršenja učitaju u memoriju i njihov kod ostaje u memoriji cijelo vrijeme rada računala. Rezidentni virusi koriste tehnike TSR („terminate and stay resident“) i manipulaciju memorijskim blokovima (MBC) kako bi se zadržali cijelo vrijeme u memoriji računala. Maliciozni kod rezidentnih virusa koristi mehanizme operativnog sustava za svoje aktiviranje, na primjer, pokretanje koda pri svakom pokretanju bilo koje aplikacije. Na taj način se postiže efekt zaraze i nad novim instaliranim aplikacijama.

Osnovne vrste virusa

- boot sektor virusi – kopiraju svoj maliciozni kod u Master boot sektor i na taj način osiguravaju izvršenje malicioznog koda pri svakom startu računalnog sustava
- programski virusi – aktiviraju se pri izvršenju zaražene izvršne datoteke, najčešćom s ekstenzijom .exe ili .com
- makro virusi – virusi koji su napisani višim programskim makro jezikom imaju mogućnost da sami sebe kopiraju, brišu i mijenjaju dokumente
-

Tehnike skrivanja

- „Potpis virusa“ je uzorak sastavljen od niza okteta koji je dio malicioznog koda određenog virusa ili skupine virusa. Ukoliko antivirusni program pronađe takav uzorak u datoteci, obavještava korisnika da je datoteka inficirana. U svrhu težeg otkrivanja, virusi koriste razne tehnike pomoću kojih mijenjaju virusne potpise, dok se njihov kod modificira prilikom svake infekcije što znatno otežava antivirusnom alatu detektiranje virusa.
-

Stealth tehnika

- Sakriveni virus leži u pozadini, presreće zahtjeve koje šalje antivirusni alat prema operativnom sustavu, kako bi ih analizirao računalni sustav te na taj način obmanjuje korisnika i antivirusni program da je sve u redu. Virusi koji koriste „stealth“ tehnike su obično rezidentni u RAM memoriji računala i koriste se podacima, odnosno, dijelom koda koji se nalazi sakriven na nezauzetim sektorima diska, a često se koriste i druge metode sakrivanja kao što je sakrivanje promjene dužine pojedinih datoteka i foldera.

Polimorfni kod

- Svaki puta pri novoj zarazi, odnosno repliciranju, virus mijenja svoj kod i dužinu te ga je teško prepoznati standardnim metodama prepoznavanja potpisa, jer se isti mijenja.

Metamorfni kod

- U svrhu izbjegavanja od detekcije neki se virusi samostalno na novo reprogramiraju te na taj način promjene svoj kod i potpis. Razlika između polimorfnog i metamorfnog koda je ta, što polimorfni virus koristi tehnike enkripcije za promjenu potpisa, dok metamorfni virus mijenja svoj kod i pri tome zadržava istu funkcionalnost. Metamorfni virus je u većini slučajeva velik i kompleksan.

Najčešći oblici hoaxeva

- Hoaxi kao upozorenja o štetnim programima
- Lanci sreće i zarade
- Lažne peticije
- …
- CILJ:
- pošiljatelji žele vidjeti kako daleko poruka može stići i koliko dugo može egzistirati
- zavaravanje korisnika
- uništavanje ugleda neke organizacije, tvrtke ili osobe

Crvi

- **Računalni crvi** su programi koji sami sebe umnožavaju i šire se putem računalne mreže. Za razliku od računalnih virusa, crvi ne zahtjevaju postojanje domaćinske datoteke za svoj radi. Oni su samostalni programi koji se u većini slučajeva šire bez interakcije korisnika. Iako je moguće pronaći računalne crve koji nisu štetni, većina sigurnosnih stručnjaka sve crve smatra zlonamjernim i nepoželjnim programima.

- Crvi koriste računalnu mrežu kako bi s jednog računala zarazili drugo. Većina crva programirana je tako da u što kraćem vremenskom roku zarazi što veći broj računala
- Dva su osnovna načina na koji se računalni crvi mogu širiti:

1. **Bez interakcije korisnika**
2. **Putem socijalnog inženjeringa**

Trojan horse

- **Trojanski konj** je oblik malvera koji se korisniku lažno predstavlja kao neki korisni softver kako bi ga korisnik izvršio, odnosno dozvolio mu instalaciju. Termin je, zbog analogije, preuzet iz grčke mitologije. Trojanski konj može izmijeniti operacijski sustav na zaraženom računalu kako bi on prikazivao oglase (pop-up prozori) u svrhu ostvarivanja novčane koristi od strane napadača. Opasniji je slučaj kada trojanski konj omogući napadaču potpunu kontrolu nad zaraženim računalom.

Šire se

- preuzimanjem zaraženog softvera
- kao dio softvera
- kao e-mail privitci
- putem zloćudnih web stranica sa dinamičkim sadržajem (npr. ActiveX)
- preko ranjivosti softvera

Spyware

- **Spyware** je vrsta malicioznog programa čija je namjena sakupljanje informacija te preuzimanje kontrole rada na računalu korisnika bez njegova znanja ili dozvole. Ono što ga razlikuje od virusa i crva je u tome što se obično ne replicira. Dizajniran je da iskorištava zaražena računala za komercijalnu dobit, poput prikazivanja pop-up reklama (to je onda **adware**), krađu osobnih informacija (uključujući i financijske informacije kao što su brojevi kreditnih kartica i lozinke) ili preusmjeravanjem HTTP zahtjeva na reklamne stranice.

Lažni anti-spayware programi

- Važno je naglasiti da se Internetom distribuira veći broj web reklama koje ukazuju korisnicima da su im računala zaražena malicioznim programom te ih navode da kupe lažni program koji ustvari ne uklanja spyware, već ga instalira na korisnikovo računalo. Isto tako se ne preporuča korisnicima instalacija lažnih besplatnih programa, koji su deklarirani kao antivirusna ili anti-spyware zaštita, osim, ako su službeno potvrđeni kao legitiman proizvod.

Keylogger

- **Keylogger** je softver namijenjen tajnom praćenju i snimanju (svih) pritisnutih tipki na računalu. Ovdje se govori o keyloggerima u užem smislu riječi, jer oni inače mogu biti i dijelovi hardvera, odnosno uređaji. Legitimni programi mogu imati funkciju keyloggera i pratiti pritisnute tipke kako bi pozvali specijalne programske funkcije (hotkeys) ili za promjenu rasporeda tipki tipkovnice (keyboard layout). Također, takav softver se može koristiti za kontrolu zaposlenika ili roditeljsku kontrolu djece (radi zabrane pristupa sadržaju za odrasle).

- Što se tiče zlonamjerne upotrebe keyloggera, ona uglavnom podrazumijeva krađu povjerljivih podataka (lozinki za pristup različitim servisima za plaćanje, brojeva kreditnih kartica, PIN brojeva itd.)

Rootkit

- Rootkit je vrsta malicioznog softvera koja napadaču omogućuje udaljenu administrativnu kontrolu nad računalom. Oni su posebno dizajnirani da budu nevidljivi na računalu kojeg zaraze.
- Najčešći današnji rootkitovi su oni koji djeluju na razini operacijskog sustava. Njihov razvoj je dugotrajan i tehnički zahtjevan, ali kada zarazi računalo mogu proći mjeseci pa čak i godine prije nego bude primjećen. Neki sigurnosni stručnjaci idu toliko daleko te ističu da je jedini način otklanjanja takvih rootkitova potpuno brisanje diska i reinstalacija cijelog sustava.

Hoax

- **Hoax** je poruka elektroničke pošte neistinitog sadržaja, poslana s ciljem zastrašivanja ili dezinformiranja primatelja. Želja osobe koja je poslala hoax je njegovo prosljeđivanje na što veći broj adresa. Pri tome ih primatelji doista i prosljeđuju Internetom jer su uvjereni da time pomažu drugima. Hoaxi ne mogu uzrokovati oštećenja računalnih programa i operacijskih sustava, ali zabilježeni su brojni slučajevi gdje su hoaxi svojim sadržajem i vještom psihologijom naveli korisnike da sami oštete svoje programe i sustave. Drugi oblik štete koji hoaxi nanose korisnicima je zavaravanje korisnika te narušavanje njihovog ugleda, kao i ugleda određenih organizacija, tvrtki i poznatih osoba.
- Scam je ozbiljniji oblik hoaxa, često s ozbiljnim financijskim, pravnim ili drugim posljedicama za žrtvu.