CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Ispitivanje antivirusnih alata

CCERT-PUBDOC-2009-07-269

+CERT.hr u suradnji s LSS

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

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

CARNet 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

Naglim razvojem širokopojasnog Interneta posljednjih godina održavanje prihvatljive razine sigurnosti osobnih računala postalo je delikatan zadatak. Pri tome je važno koristiti nekoliko razina sigurnosne zaštite kako bi se rizik od potencijalnog kompromitiranja računala smanjio na minimum. Antivirusni alati tako su postali nezaobilazni dodatak svakom korisničkom računalu. Odabir odgovarajućeg antivirusnog alata od ključne je važnosti za sigurnost svake tvrtke, organizacije, pa i kućnih korisnika. Prilikom donošenja takvih odluka korisnici se obično koriste rezultatima raznih ispitivanja ovih alata kako bi ih usporedili te izabrali rješenje koje ima najviše odgovara. Iako postoje brojne institucije koje se već godinama bave ovakvim ispitivanjima i u tome su postigle zavidnu razinu kvalitete, brojne organizacije i magazini ne provode testove na odgovarajući način. Pogrešna interpretacija rezultata može zavarati korisnike i ozbiljno narušiti njihovu sigurnost.

Potaknuti pojavom sumnjivih ispitivanja stručnjaci su osnovali organizaciju AMTSO (http://www.amtso.org) koja je zadužena za razvoj standarda i smjernica koji se tiču testiranja antivirusnih alata. Ova organizacija u godinu dana svojeg postojanja održala je već nekoliko stručnih konferencija i izdala nekoliko važnih dokumenata. Također, AMSTO će provoditi revizije postupaka ispitivanja za institucije koje to zatraže te time potvrditi kvalitetu i sukladnost ispitivanja sa smjernicama organizacije.

U ovom dokumentu opisani su antivirusni alati i tehnike koje koriste u svom radu te neki problemi s kojima se krajnji korisnici susreću pri njihovom korištenju. Također, navedene su neke poznate organizacije koje su se kroz godine iskazale kvalitetnim i informativnim ispitivanjima te time stekle ugled u struci. Posebno je opisana organizacija AMTSO kao jedan od najvažnijih autoriteta na ovom području, te smjernice iz najvažnijih dokumenata koje je ova organizacija objavila.

2. Antivirusni alati

Iako sama riječ antivirus u sebi sadrži virus, koji predstavlja jedan od prvih oblika zloćudnih programa, antivirusni alati danas se koriste i za uklanjanje drugih vrsta zloćudnih programa poput crva ili trojanskih konja. Neki od ovih alata sprječavaju, pa čak i uklanjaju razne vrste *spyware* programa te programa za reklamiranje raznih (često također zloćudnih) proizvoda (eng. adware).

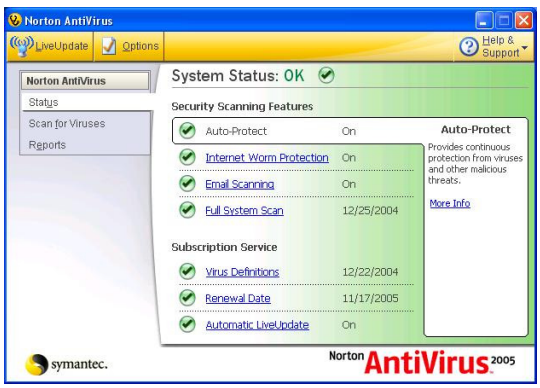
Za prepoznavanje zloćudnih programa antivirusi se koriste raznim tehnikama detekcije. Jedna od najstarijih i još uvijek najučinkovitijih tehnika je ona bazirana na potpisima zloćudnih programa. Problem nastaje u slučajevima kada ne postoji potpis virusa (npr. novi virusi koji još nisu poznati tvorcima antivirusnih programa – još se nazivaju i „*zero day*" virusi). Da bi se obranili od ovih. „*zero day*", virusa, antivirusni alati koriste razne heurističke tehnike detekcije. Jedna od takvih tehnika koristi se općenitim (eng. generic) potpisima zlonamjernih programa za pretragu datoteka na računalu. Na ovaj način antivirusni alati mogu pronaći zloćudne programe koji su manje varijacije već poznatih. O navedenim tehnikama detekcije biti će više riječi u nastavku dokumenta. Neki antivirusi mogu emulirati izvođenje programa pomoću tzv. sandbox mehanizma te tako prepoznati obavljaju li oni nekakve zlonamjerne aktivnosti. Više o sandbox mehanizmu može se pročitati u dokumentu na web adresi:

http://www.cert.hr/documents.php?id=375

Iako je osnovna funkcionalnost antivirusnih alata iznimno korisna i predstavlja jednu od osnovnih linija obrane protiv zlonamjernih programa, oni često znatno utječu na performanse računala na kojem su pokrenuti. Razlog tome najčešće je loš i neučinkovit dizajn antivirusnih programa. Također, neiskusni korisnici često imaju probleme sa razumijevanjem rada antivirusnih alata pa ne reagiraju na odgovarajući način kada se od njih traži interakcija sa alatom (npr. ne odabiru brisanje zloćudnog programa kada ih se to upita, jer ne razumiju o čemu se točno radi). Kada antivirusi pritom još koriste i razne heurističke tehnike detekcije zlonamjernih programa, njihova uspješnost ovisi i o postotku pronalaženja tzv. lažno pozitivnih i lažno negativnih uzoraka. Riječ je o programima koje antivirusni program proglasi opasnim, iako oni to nisu, ili ih proglasi bezopasnim iako oni obavljaju neku zlonamjernu aktivnost. Tako je, primjerice, 2007. godine antivirusni alat tvrtke Symantec, zbog pogreške u potpisu zlonamjernog programa, prepoznao dvije sistemske datoteke operacijskog sustava Windows XP kao trojanske konje i zato ih izbrisao, zbog čega se tisuće računala više nisu mogla pokrenuti [8].

2.1. Povijest

Postoji nekoliko teorija o autoru prvog antivirusnog alata, no ona najvjerojatnija govori o Berntu Fixu koji je izradio prvi dokumentirani alat za uklanjanje virusa Vienna 1987. godine. Neki od prvih pravih antivirusnih proizvoda bili su „Dr. Solomon's Anti-Virus Toolkit", „AIDSTEST" i „AntiVir" izdani tijekom 1988. te antivirus „Vaccine I" koji je izradio Dr. Ahn Chul Soo, jedan od prvih stručnjaka koji su se bavili virusima, sredinom iste godine. Do kraja 1990. godine devetnaest različitih antivirusnih alata bilo je dostupno na svjetskom tržištu uključujući poznate alate Norton AntiVirus i McAfee VirusScan. Neki od najpoznatijih stručnjaka iz područja računalnih virusa u to vrijeme bili su Fred Cohen, Peter Tippett, John McAfee i već spomenuti Ahn Chul Soo.



Slika 1. *Norton AntiVirus – i danas jedan od najpopularnijih antivirusnih alata*

Izvor: Google

Prije nego je Internet postao raširen, virusi su se obično širili putem disketa. Antivirusni alati koji su se tada koristili osvježavali su se vrlo rijetko i provjeravali su samo izvršne datoteke i *boot* sektore (dijelovi diskova koji se prvi učitavaju prilikom paljenja računala) disketa i tvrdih diskova. Međutim, izumom modema i širenjem Interneta, virusi i drugi zlonamjerni programi pronašli su jednostavniji način za svoje širenje i izvođenje zlonamjernih aktivnosti.

Uvođenjem mogućnosti primjene makro naredbi u moćnim uredskim aplikacijama (npr. Microsoft Word), autori zlonamjernih programa iskoristili su još jedan način za ugrožavanje korisničkih računala. Virusi su se sada mogli širiti i putem bezazlenih uredskih dokumenata koji su sadržavali zlonamjerne (skrivene) makro naredbe.

Kasnije, kada su popularni programi za čitanje elektroničke pošte (poput programa Microsoft Outlook) omogućili umetanje programskog koda u tijelo poruka elektroničke pošte, a virusi su se mogli širiti samim čitanjem takve zloćudne poruke, antivirusni alati morali su provjeravati puno veći broj različitih vrsta datoteka i osvježavati bazu potpisa puno češće kako bi zaštitili svoje korisnike na odgovarajući način. Ipak, niti tada korisnici nisu bili sigurni od tzv. „*zero day*" zloćudnih programa.

2.2. Tehnike detekcije zloćudnih programa

Kao što je već spomenuto, postoji nekoliko različitih tehnika detekcije zloćudnih programa:

1. **Detekcija bazirana na potpisima**. Ovo je najčešća metoda detekcije zloćudnih programa, a svodi se na uspoređivanje sadržaja datoteka na računalu sa potpisima već pronađenih virusa pohranjenih u bazi antivirusnog alata. Budući da se virusi mogu ubaciti bilo gdje unutar zaražene datoteke, pretraživanje se obavlja u svim dijelovima ispitivane datoteke.
2. **Detekcija zlonamjernog ponašanja**. Kod ovog pristupa antivirusni alat bilježi sve promjene koje se događaju na sustavu prilikom normalnog rada računala. Ukoliko se neka od aktivnosti raznih programa okarakterizira kao zlonamjerna, antivirus može upotrijebiti neke od drugih tehnika kao bi pobliže ispitao program koji je obavljao takve aktivnosti ili obavijestiti korisnika.
3. **Heuristička detekcija**. Baš kao i detekcija zlonamjernog ponašanja, heuristička detekcija koristi se raznim metodama kako bi otkrila do sada neotkrivene oblike zlonamjernih programa. To se najčešće postiže detaljnom analizom sumnjivih datoteka ili emulacijom rada istih.

Navedene tehnike biti će pobliže opisane u sljedećim poglavljima.

2.2.1. Detekcija bazirana na potpisima zloćudnih programa

Iako je tehnika detekcije potpisima zloćudnih programa najstarija od svih tehnika, antivirusni alati i dalje se u svom radu najviše oslanjaju na nju. Ona je u većini slučajeva vrlo učinkovita, no ne može zaštititi korisnike od zlonamjernih programa čiji potpisi nisu uneseni u bazu. Zbog toga se ovom tehnikom ne mogu detektirati novi, stručnjacima još nepoznati, virusi i drugi zloćudni programi.

Kada antivirus ispituje datoteke, on provjerava sadržaj i traži zloćudni kod. Upravo taj zloćudni kod predstavlja potpis određenog zlonamjernog programa. Ukoliko je taj kod pronađen u nekoj datoteci antivirus obično nudi jednu od tri moguće opcije – brisanje zaražene datoteke, uklanjanje zlonamjernog koda kako bi datoteka i dalje mogla biti korištena ili spremanje datoteke u neku vrstu karantene, odnosno izolacije. Podrazumijevana akcija je obično spremanje datoteke u karantenu. Ovo se najčešće postiže kriptiranjem zaražene datoteke, jer bez poznavanja odgovarajućeg ključa zlonamjerni kod je beskoristan i ne može se dalje širiti.

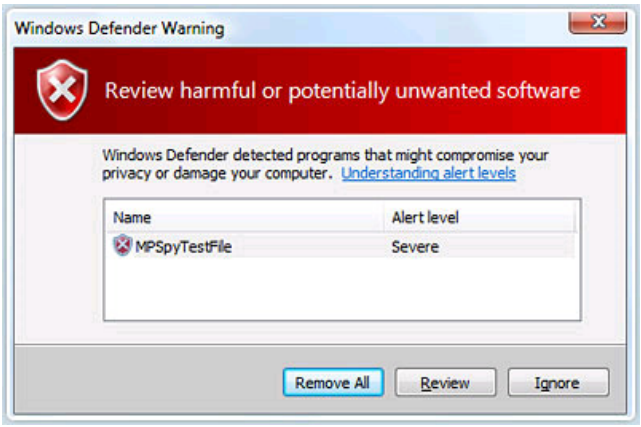
Budući da virusi nerijetko napadaju neke često korištene vrste datoteka (slike, video datoteke, dokumente i dr.), korisnici ih obično ne žele obrisati, već zadržati i nakon napada virusa. Iako većina modernih antivirusnih alata nudi opciju obnavljanja zaraženih datoteka, zbog prirode nekih destruktivnih tipova zlonamjernih programa, obnavljanje datoteka često nije moguće. U takvom slučaju najbolja praksa je brisanje datoteke kako bi se spriječilo daljnje širenje zlonamjernog koda.

Kako se novi virusi pojavljuju svakodnevno, važno je često osvježavati bazu potpisa zlonamjernih programa. Antivirusni programi često omogućavaju korisniku jednostavno slanje novootkrivenih zlonamjernih programa stručnjacima, kako bi se ubrzao proces izrade novih potpisa i zaštite ostalih korisnika antivirusnog proizvoda.

Antivirusi koji koriste ovu tehniku detekcije obično ispituju samo datoteke koje su trenutno korištene na sustavu. Međutim, sistemski administratori mogu konfigurirati antivirusni alat da skenira sve datoteke na računalu u određenim vremenskim trenucima.

2.2.2. Detekcija zlonamjernog ponašanja

Korištenjem tehnike detekcije zlonamjernog ponašanja antivirusni alati ne pokušavaju identificirati samo poznate zloćudne programe već nadgledaju ponašanje svih programa pokrenutih na računalu. Ukoliko neki program, primjerice, pokuša pisati po izvršnoj datoteci (datoteka sa nastavkom „.exe“ na operacijskim sustavima Windows) alat ovo ponašanje može označiti sumnjivim i upozoriti korisnika.



Slika 2. *Primjer upozorenja o sumnjivom programu*

Izvor: microsoft.com

Detekcija zlonamjernog ponašanja pruža zaštitu protiv tzv. *„zero day“* virusa, odnosno onih koji još nisu u bazi proizvođača antivirusnog proizvoda. Međutim, korištenjem ove metode antivirus također prijavljuje veliki broj lažno pozitivnih programa, što korisnika može učiniti neosjetljivim na upozorenja.Zato se često događa da korisnik zbog pojave čestih upozorenja prestane obraćati pozornost na njihov sadržaj i prihvaća sve podrazumijevane opcije, što obično nije najbolji izbor.

Problem lažno pozitivnih prijava postao je iznimno velik u posljednjem desetljeću, jer su mnogi legitimni programi dizajnirani tako da izvode neke osjetljive naredbe (npr. korištenje važnih sistemskih biblioteka) koje antivirusi često prepoznaju kao zlonamjerne. Ipak, nove sofisticirane metode detekcije koriste neke napredne provjere (poput provjera sistemskih poziva i dr.) čijom upotrebom se broj lažno pozitivnih prijava znatno smanjio.

2.2.3. Heuristička detekcija

Najnapredniji antivirusni alati koriste tzv. heurističku analizu kako bi detektirali nove, do sada nepoznate, zloćudne programe, kao i mutirane inačice već poznatih. Postoje tri glavne metode koje se koriste kod ove vrste detekcije, a one su:

1. analiza programa,
2. emulacija rada programa i
3. općeniti potpisi.

Analiza programa je proces kod kojeg antivirus ispituje svaku naredbu programa, te prema ispitanim naredbama odlučuje je li program zloćudan ili nije. Ako program sadrži naredbu koja npr. briše neke važne sistemske datoteke, antivirus će ga vjerojatno okarakterizirati zloćudnim. lako je ova metoda izuzetno korisna za detekciju novih i mutiranih zloćudnih programa, ona, poput drugih heurističkih metoda, prijavljuje veliki broj lažno pozitivnih programa.

Druga metoda heurističke detekcije je emulacija rada programa. Kod ove metode program se pokreće u posebnom virtualnom okruženju koje je odvojeno od stvarnog računalnog sustava. Promjene koje program napravi u tom okruženju se bilježe i analiziraju. Ukoliko antivirus procijeni da su zabilježene promjene rezultat zlonamjerne aktivnosti, prijavljuje ispitivani program korisniku.

Mnogi virusi svoje djelovanje započinju kao jedinstveni primjerak, a naknadno mutiraju u nekoliko različitih inačica. Također, često drugi napadači mijenjaju izvorni program kako bi ga poboljšali i ponovno zloupotrijebili. Korištenjem općenitih potpisa moguće je detektirati npr. cijelu familiju zloćudnih programa. Istraživači izrađuju općenite propuste tako da analiziraju slične zloćudne programe i pronalaze njihove zajedničke točke.

Tehnika	Prednosti	Mane
Potpisi zloćudnih programa	- preciznost detekcije	- ne detektira "*zero day*" viruse - potpise treba redovito osvježavati
Detekcija zlonamjernog ponašanja	- detektira "*zero day*" viruse	- veliki broj lažno pozitivnih - traži interakciju s korisnikom
Heuristička detekcija	- detektira "*zero day*" viruse - koristi više heurističkih metoda	- veliki broj lažno pozitivnih - troši dosta resursa

Tablica 1. *Usporedba tehnika detekcije*

2.3. Problemi

Iako razvoj antivirusnih proizvoda traje već preko dva desetljeća i oni su u svim područjima napredovali, neki osnovni problemi i dalje ih prate:

- **Resursi**

  Mnogi antivirusni alati zbog prevelikog korištenja računalnih resursa značajno utječu na smanjenje performansi sustava na kojem su pokrenuti. Korisnici ih zato često odbijaju koristiti ili ih gase i time povećavaju rizik da se njihov računalni sustav zarazi nekim zloćudnim programom. Da bi bio potpuno učinkovit, antivirusni program mora biti cijelo vrijeme pokrenut, no to često rezultira slabijim performansama zaštićenog računala.

- **Sigurnost**

  Sami antivirusni proizvodi predstavljaju određen sigurnosni rizik jer u svom radu koriste najviše sistemske privilegije. Iako su im one nužne za pravilan rad, u slučaju kompromitiranja alata napadač je u mogućnosti preuzeti potpunu kontrolu nad ranjivim računalom.

- **Privatnost**

  Mnogi antivirusni alati imaju podrazumijevanu konfiguraciju koja dozvoljava slanje zaraženih datoteka na poslužitelj proizvođača kako bi se one detaljnije analizirale. Iako je ovo korisna opcija u borbi protiv zloćudnih programa, potrebno je obratiti pažnju kako se na poslužitelj ne bi poslale datoteke koje sadrže osjetljive informacije.

- **Lažni antivirusi**

  Postoji veliki broj lažnih antivirusnih proizvoda koji se prilično često reklamiraju na raznim internetskim portalima. Ovi programi, iako se predstavljaju kao korisni, u biti sadrže zlonamjeran programski kod i time kompromitiraju korisnika. Neki od poznatijih takvih programa su WinFixer i MS Antivirus.

- **Lažno pozitivni rezultati**

  Kao što je već nekoliko puta spomenuto u ovom poglavlju, lažno pozitivni rezultati ispitivanja datoteka veliki su problem antivirusne industrije. Neiskusni korisnici mogu tako pogreškom obrisati neku važnu datoteku što njihove sustave ili aplikacije može učiniti neupotrebljivima.

3. Vrednovanje antivirusnih alata

Ispitivanja koja danas provode brojne organizacije nad antivirusnim proizvodima većim dijelom ne zadovoljavaju kriterije zasnovane na formalnim metodama. Procese ispitivanja vode različite osobe koje koriste razne alate i metode. Neki od alata i metoda bi svakako trebali biti dio evaluacijskog procesa, no korištenje dijela alata i metoda može dovesti do krivih rezultata i informacija koje u konačnici mogu naštetiti krajnjim korisnicima. Kod odabira antivirusnog alata na nekim područjima prilično je lako uočiti razliku između proizvoda. Tu spada eliminacija proizvoda zbog neodgovarajuće podrške za radno okruženje korisnika, zatim eliminacija zbog cijene ili neodgovarajuće licence. Također, korisnicima je obično važno da se proizvodi mogu koristiti na različitim računalnim sustavima te da se lako primjenjuju i podešavaju.

No, osim ovih osnovnih zahtjeva, postoje i kriteriji prema kojima je teže uočiti razliku među proizvodima različitih proizvođača, a jednako su važni kao i ovi već navedeni. Tu se prvenstveno misli na evaluaciju antivirusa pomoću pravih zloćudnih programa. Ovakva ispitivanja još od nastanka antivirusnih alata provode brojne profitne i neprofitne organizacije, svaka sa različitim kriterijima i metodama. Korisnici se često oslanjaju na rezultate takvih ispitivanja pri odabiru antivirusnog alata, a bez informacija o metodama i alatima koji su korišteni priliko ispitivanja. Brojna ispitivanja provodili su nestručni ljudi što može dovesti do katastrofalnih posljedica za korisnike koji odaberu „krivi“ proizvod. U narednim poglavljima opisane su najpoznatije organizacije koje su obilježile ovo važno područje evaluacije antivirusnih proizvoda kroz povijest i postavile temeljne standarde za postizanje kvalitetnijih rezultata.

3.1. Wildlist

Iako organizacija Wildlist (http://www.wildlist.org) ne provodi ispitivanja antivirusnih alata, ona u njima odigrava jednu od ključnih uloga. Naime, radi se organizaciji koja iz različitih izvora prikuplja informacije o zloćudnim programima „u divljini“ (eng. „in the wild“). Ti izvori su obični sigurnosni stručnjaci i istraživači kojima je borba sa zlonamjernim programima svakodnevica. Periodički, svaki mjesec, ova organizacija objavljuje listu zlonamjernih programa koji su u tom razdoblju uočeni na korisničkim računalima. Radi se o neprofitnoj organizaciji koja postoji isključivo zahvaljujući dobroj volji i žrtvi svojih osnivača i ljudi koji sudjeluju u izradi liste, a s druge strane predstavlja standard koji većina ispitivača koristi u svojim testovima.

Organizaciju TWO (eng. The Wildlist Organization) osnovao je Joe Wells prema terminu „virus u divljini“ koji je uvela organizacija Virus Bulletin. Ideja je bila sastaviti listu najaktualnijih zloćudnih programa kako bi se ona mogla koristiti pri ispitivanju različitih antivirusnih alata. Da bi program dospio na ovu listu mora biti prijavljen iz dva ili više različitih izvora. Iako je ovo najorganiziraniji poduhvat ove vrste, popis ovih programa ne može se smatrati u potpunosti reprezentativnim skupom, već tek podskupom svih zloćudnih programa koji se šire računalima korisnika. Zato, iako je svakako korisno ispitivati antivirusne alate ovim skupom programa, nije preporučljivo osloniti se samo na ovu metodu ispitivanja.

```
                                        List  Reported
Name of Virus           [Alias(es)      ] Date  by:
=============================================================================
W32/Agent!ITW#100.......[..............]  2/09 PaTl
W32/Agent!ITW#101.......[..............]  3/09 AoMtSnWw
W32/Agent!ITW#102.......[..............]  3/09 AoSjTl
W32/Agent!ITW#103.......[..............]  3/09 AoMtPaSt
W32/Agent!ITW#104.......[..............]  3/09 AoMtRsTl
W32/Agent!ITW#105.......[..............]  3/09 AoTl
W32/Agent!ITW#106.......[..............]  4/09 AoStTl
W32/Agent!ITW#107.......[..............]  5/09 PaSjTl
W32/Agent!ITW#108.......[..............]  5/09 MtPa
W32/Agent!ITW#109.......[..............]  5/09 PaSj
W32/Agent!ITW#110.......[..............]  5/09 AoPa
W32/Agent!ITW#111.......[..............]  5/09 PaTl
W32/Agent!ITW#112.......[..............]  5/09 AoMtPa
W32/Agent!ITW#113.......[..............]  5/09 AoMt
W32/Agent!ITW#114.......[..............]  5/09 AoMt
W32/Agent!ITW#115.......[..............]  5/09 AoPa
W32/Agent!ITW#116.......[..............]  5/09 MtPa
W32/Agent!ITW#117.......[..............]  5/09 AoTl
W32/Agent!ITW#118.......[..............]  5/09 PaTl
W32/Agent!ITW#119.......[..............]  5/09 PaRsTl
W32/Agent!ITW#120.......[..............]  5/09 AoTl
W32/Agent!ITW#121.......[..............]  5/09 MtPa
W32/Agent!ITW#122.......[..............]  5/09 AoMt
W32/Agent!ITW#123.......[..............]  5/09 PaTl
```

Slika 3. *Dio skupa zlonamjernih programa objavljenih u lipnju 2009.*

Izvor: Wildlist.org

3.2. ICSA Labs

Organizacija ICSA (eng. International Computer Security Association) provodi ispitivanja antivirusnih alata još od 1992. godine. Mnogi popularni alati prošli su komercijalno certifikacijsko testiranje koje ova organizacija nudi (ICSA 2000). Ovo ispitivanje od samih početaka temeljilo se na tzv. „*on access*" i „*on demand*" skeniranjima. „*On access*" skeniranje se provodi dinamički, odnosno antivirusni alat mora prepoznati zlonamjerni program prilikom njegovog učitavanja u memoriju. Da bi to mogao, antivirus mora cijelo vrijeme u pozadini nadgledati rad računala. Nasuprot tome, „*on demand*" skeniranje se obavlja tako da se antivirusu da lista datoteka koje treba ispitati. Od srpnja 1999. godine ICSA organizacija ispituje i mogućnost uklanjanja već pokrenutih zlonamjernih programa. Zlonamjerni programi kojima se antivirusi testiraju razdvojeni su u dvije osnovne skupine : „*in the wild*" i „*zoo*" zlonamjerni programi. Uz već opisanu „*in the wild*" skupinu zlonamjernih programa, ovdje se pojavljuju i tzv. „*zoo*" zloćudni programi. Riječ je o skupini programa koji se ne pojavljuju na računalima običnih korisnika već se čuvaju u strogim laboratorijskim uvjetima. Stručnjaci iz ICSA organizacije održavaju veliku kolekciju takvih programa koje koriste za opsežna ispitivanja antivirusnih proizvoda. Da bi neki proizvod prošao certifikacijsko ispitivanje potrebno je da otkrije barem 90% programa iz „*zoo*" kolekcije. S druge strane provode se i testiranja programima sa Wildlist popisa, a ispitivani programi moraju detektirati 100% „*in the wild*" zloćudnih programa kako bi zadovoljili postavljene kriterije. ICSA stručnjaci svakodnevno rade na novim metodama i kriterijima ispitivanja, pa je zato njihov certifikat, iako komercijalan, vrlo cijenjen u svom području.

Slika 4. *Logo ICSA certifikata*

Izvor: ICSALabs.com

3.3. Westcoast Labs

Još sredinom devedesetih godina prošlog stoljeća organizacija WestCoast etablirala se kao vodeći centar za ispitivanje i certificiranje antivirusnih proizvoda uvođenjem certifikata „WestCoast Labs Checkmark". Kriteriji koje antivirus mora zadovoljiti ovise o razini certifikacije koja se želi postići. Kod prve razine certificiranja ispituje se mogućnost alata da detektira sve zlonamjerne programe iz Wildlist kolekcije, ne starije od dva mjeseca. Da bi se zadovoljili kriteriji druge razine certificiranja ispitivani proizvod mora imati mogućnost uklanjanja svih programa iz spomenute kolekcije. Kod druge razine koristi se Wildlist kolekcija koja nije starija od jednog mjeseca. Sva ispitivanja se provode nad skupom zlonamjernih programa koje su replicirali stručnjaci iz WestCoast laboratorija prema Wildlist popisu, pa se time mjeri sposobnost ispitivanog alata u borbi protiv realnih prijetnji. Mnogi popularni antivirusni alati (McAfee, Sophos, Symntec i dr.) redovno se podvrgavaju ispitivanjima za dobivanje certifikata ove organizacije, a rezultati se objavljuju javno.

Slika 5. *Neki od popularnih alata koji posjeduju WestCoast certifikat*

Izvor: WestCoastLabs.com

3.4. Virus Bulletin

Virus Bulletin je svakako jedna od najpoznatijih institucija na području ispitivanja antivirusnih proizvoda. Osim izdavanja magazina i drugih brojnih publikacija posvećenih ovoj tematici, kao i organiziranja VB konferencije, ova institucija na redovnoj bazi objavljuje komparativne rezultate ispitivanja mogućnosti antivirusnih alata. Njihovi testovi provode se nad bogatom kolekcijom *„zoo"* zloćudnih programa, kao i nad repliciranim skupom programa sa Wildlist popisa. Skup Wildlist programa za svako ispitivanje ne smije biti stariji od dva tjedna s obzirom na rok prijave alata za ispitivanje.

U siječnju 1998. godine ova organizacija uvela je certifikat **VB100%**. Riječ je o ispitivanju koje se provodi na mjesečnoj bazi nad velikim skupom komercijalnih i besplatnih antivirusnih alata, a za dobivanje certifikata potrebno je zadovoljiti sljedeće kriterije:

- program mora detektirati sve zlonamjerne programe iz Wildlist kolekcije te
- mora uspješno detektirati sve viruse tijekom tzv. *„on demand"* ispitivanja.

Tijekom godina ova shema ispitivanja proširena je zahtjevom da ispitivani program mora uspješno detektirati sve Wildlist programe tijekom *„on demand"* i *„on access"* skeniranja. Osim ovih testova detekcije Virus Bulletin također provodi ispitivanja brzine skeniranja te razine lažno pozitivnih i negativnih prijava. Nakon 2000. godine kao uvjet za dobivanje VB100% certifikata dodan je kriterij koji zahtjeva da alat ne prijavi niti jedan lažno pozitivan program.

Slika 6. *Logo certifikata VB100%*

Izvor: VirusBtn.com

3.5. AV-Comparatives

Tim koji stoji iza organizacije AV-Comparatives predvođen je cijenjenim sigurnosnim stručnjakom Andreasom Clementijem. Oni se bave ispitivanjem antivirusnih alata već dugi niz godina, no tek od 2004. javno su objavili rezultate svojih istraživanja. Njihovi testovi poznati su po vrlo strogim pravilima, a odvijaju se na kvartalnoj bazi (svaka tri mjeseca). Antivirusni alati koje podvrgavaju svojim ispitivanjima spadaju među najbolje alate, koji detektiraju preko 85% zlonamjernih programa u svim njihovim testovima i to na operacijskom sustavu koji je u datom trenutku najviše korišten u svijetu. Metodologija ispitivanja kao i detaljni opisi i rezultati javno su dostupni na njihovim web stranicama (http://www.av-comparatives.org). Detaljni testovi koje ova organizacija provodi uključuju:

- „*on demand*" testove na velikoj bazi pronađenih zlonamjernih programa,
- proaktivne testove za ispitivanje mogućnosti programa da prepozna nove, još nepoznate, zloćudne programe,
- testove koji koriste polimorfne viruse (virusi koji mijenjaju oblik),
- testove na lažno pozitivne prijave,
- testove brzine skeniranja i dr.

Rezultati ovih ispitivanja objavljuju se neposredno nakon završetka testova (bez vremenskog razmaka), a ovisno o uspješnosti pojedinih antivirusnih alata dodjeljuju se sljedeće nagrade:

- Standard – nagrada za programe čiji rezultati zadovoljavaju minimalne kriterije.
- Advanced – nagrada za programe kod kojih rezultati ispitivanja ukazuju na naprednu razinu detekcije.
- Advanced+ - najveća nagrada za programe koji su se posebno istaknuli prilikom izvršavanja testova.

Company		AVIRA		Alwil Software		AVG Technologies		BitDefender	
Product		**AntiVir Premium**		**avast! Professional**		**AVG Anti-Virus**		**BitDefender AV**	
Program version		8.2.0.374		4.8.1335		8.0.234		12.0.11.4	
Engine / signature version		8.02.00.76/7.01.01.248		090209-0		270.10.19/1941		*N/A*	
Certification level reached		**ADVANCED**		**STANDARD**		**STANDARD**		**ADVANCED**	
Number of false positives		*many*		*many*		*many*		*many*	
ProActive detection of "NEW" samples									
Windows viruses	188	161	86%	65	35%	89	47%	87	46%
Worms	1.738	626	36%	349	20%	330	19%	562	32%
Backdoors	4.966	3.737	75%	2.677	54%	2.656	53%	3.087	62%
Trojans	13.555	9.523	70%	5.288	39%	5.823	43%	6.607	49%
other malware (incl. script+macro)	2.238	1.698	76%	1.156	52%	1.287	58%	1.105	49%
TOTAL	**22.685**	15.745	**69%**	9.535	**42%**	10.185	**45%**	11.448	**50%**

Slika 7. *Primjer rezultata iz izvještaja organizacije AV-Comparatives*

Izvor: AV-Comparatives.org

3.6. AV-test

Iza organizacije AV-test stoji skup stručnjaka predvođen Andreasom Marxom. Riječ je o organizaciji koja se bavi ispitivanjem kvalitete antivirusnih proizvoda već dugi niz godina. Osim antivirusa provode i testiranja drugih sigurnosnih proizvoda poput vatrozidova i sl. Rezultate svojih ispitivanja periodički objavljuju u raznim stručnim magazinima na zahtjev proizvođača antivirusnih alata ili samih magazina. AV-test se smatra jednom od vodećih organizacija na svojem području, a opsežni testovi koje provode nad antivirusnim proizvodima uključuju:

- „*on demand*" testove,
- „*on access*" testove,
- „*in the wild*" testove,
- ispitivanja utjecaja alata na performanse sustava i dr.

Rezultati njihovih ispitivanja ne objavljuju se besplatno na njihovima web stranicama već isključivo u komercijalnim stručnim časopisima i magazinima.

Slika 8. *Logo organizacije AV-test*

Izvor: AV-test.org

3.7. Virus Test Center

Pod paskom sigurnosnog i antivirusnog stručnjaka Dr. Klausa Brunnsteina, studenti iz VTC centra sa sveučilišta u Hamburgu oblikuju i izvode ispitivanja antivirusnih alata još od 1994. godine. Rezultati ovih testiranja javno su dostupni na stranicama centra (http://agn-www.informatik.uni-hamburg.de/vtc/). Ova ispitivanja razvila su se od jednostavnih testova „*boot*" virusa i detekcije virusa u datotekama do opsežnih ispitivanja koje ova institucija provodi danas. Kao dodatak bogatoj „*zoo*" kolekciji zlonamjernih programa, stručnjaci iz VTC centra od 1999. godine koriste u svojim ispitivanjima i replicirane primjerke iz Wildlist kolekcije. Time je osigurano da ispitivanja pružaju realno okruženje za vrednovanje antivirusnih alata. Osim navedenih uzoraka ispitivanja koja provodi, VTC koristi i neke generičke oblike zlonamjernih programa koji prema njihovim tvrdnjama realno simuliraju situacije u kojima se obični korisnici mogu naći. Njihova testiranja besplatna su za proizvođače antivirusnih programa, a rezultati se redovno dostupni široj javnosti. Neke proizvode VTC ipak odbija testirati zbog raznih kontroverzi i konflikata oko namještanja rezultata drugih testiranja.

Slika 9. *Logo VTC centra*

Izvor: agn-www.informatik.uni-hamburg.de

4. Organizacija AMTSO

Veliki broj ispitivanja antivirusnih alata koje danas provode brojne institucije, magazini i neki pojedinci ne zadovoljavaju niti minimalne kriterije kvalitete, te su time ne samo beskorisni, već i štetni za krajnje korisnike. Rezultati takvih ispitivanja mogu krajnje korisnike, pri odabiru svojeg antivirusnog rješenja, navesti na krive zaključke i time naštetiti njihovoj sigurnosti. Ovakva ispitivanja često su produkt zlonamjernih marketinških kampanji, pa je nekoliko puta otkriveno i da su financirana od samih proizvođača antivirusnih alata. Mnoga takva ispitivanja rezultirala su burnim medijskim diskusijama i raspravama između najvećih sigurnosnih stručnjaka današnjice. Jedno od takvih kontroverznih ispitivanja je ono magazina Consumer Reports [7]. Stručnjaci koji su obavljali ovo ispitivanje odlučili su stvoriti 5500 primjeraka novih zloćudnih programa te pomoću njih testirati najpopularnije antivirusne alate danas. Ovo je izazvalo buru reakcija stručnjaka iz svih značajnih antivirusnih kompanija koji su smatrali kako, s obzirom na veliki broj zlonamjernih programa koji ionako kruže Internetom, nema potrebe za stvaranjem još primjeraka (jer oni u slučaju neodgovarajućeg tretiranja mogu ugroziti globalnu sigurnost).

Upravo iz tih razloga, sigurnosni stručnjaci sastali su se u svibnju 2008. godine u Bilbau i dogovorili osnivanje nove internacionalne neprofitne organizacije - Anti-Malware Testing Standards Organization (u daljnjem tekstu AMTSO). Riječ je o organizaciji koja se bavi stvaranjem standarda na području ispitivanja antivirusnih proizvoda. Članstvo u organizaciji otvoreno je za sve ispitivače, proizvođače, akademske i druge komercijalne entitete. Organizacije i pojedinci koji su danas članovi ove udruge navedeni su u tablici 2.

AhnLab	Kaspersky Lab
Alwil Software	KingSoft
ARCABIT	K7 Computing Private Ltd
AV-Comparatives	Lavasoft AB
AVG Technologies	Mario Vuksan
AVIRA	McAfee
AV-TEST.org	Norman
Bit9	NSS Labs
BitDefender	Panda Security
CA, Inc.	PC Security Labs
Cascadia Labs	Sophos Plc
Comodo Security, Inc.	Symantec Corporation
Dennis Technology Lab	TrendMicro
ESET	Vesselin Bontchev
F-Secure	Veszprog Ltd.
Hispasec	Virus Bulletin
IBM	VirusBuster
ICSA Labs	Webroot Software Inc.
Ikarus Security Software	West Coast Labs

Tablica 2. *Članovi organizacije AMTSO*

Izvor: AMTSO.org

Osnovna područja rada AMTSO organizacije su sljedeća:

- organiziranje foruma za diskusije vezane uz antivirusne alate i ispitivanja istih,
- razvoj i objavljivanje objektivnih standarda i najboljih praksi za ispitivanje antivirusnih proizvoda,
- promoviranje edukacije i svijesti o problemima vezanim uz ispitivanja antivirusnih alata,
- promoviranje korisnih alata i drugih materijala nužnih za provođenje ispitivanja prema standardima,
- provođenje revizija sadašnjih i budućih postupaka ispitivanja antivirusnih alata u svrhu njihovog usklađivanja sa standardima.

Slika 10. *Logo organizacije AMTSO*

Izvor: AMTSO.org

Organizacija AMTSO od svog nastanka izdala je niz dokumenata sa standardima i preporukama za kvalitetnije ispitivanje antivirusnih alata. Neki od tih principa i preporuka opisani su u ovom dokumentu, a potpuni dokumenti mogu se dohvatiti sa web adrese:

http://www.amtso.org/documents.html

Osim razvoja dokumenata sa standardima i savjetima, prema odluci sa sastanka članica u Budimpešti u svibnju 2009. godine, organizacija AMTSO također će provoditi revizije postojećih postupaka ispitivanja antivirusnih alata. Analiza ispitivanja provodit će se usporedbom metodologije testiranja sa smjernicama iz službenih dokumenata organizacije AMTSO. Glavni cilj revizije je informiranje krajnjih korisnika o pouzdanosti i točnosti pojedinih ispitivanja koje institucije provode, te poboljšanje ukupne kvalitete ispitivanja.

4.1. Osnovni principi ispitivanja antivirusnih proizvoda

Osnovni principi ispitivanja antivirusnih proizvoda prvi su službeni dokument [4] koji je izdala organizacija AMTSO u cilju savjetovanja organizacija koje provode ispitivanja antivirusnih alata. Prema njihovim riječima, ovi principi zasnovani su na njihovoj vjeri da svatko tko sudjeluje u ispitivanjima ove vrste mora poštovati neke osnovne etičke norme, zatim obavljati ispitivanja koja poštuju standarde u industriji te objavljivati metodologiju testiranja i rezultate na točan i nepromijenjen način. U daljnjem tekstu navedeni su i ukratko opisani principi iz ovog dokumenta.

Princip 1: Ispitivanja ne smiju ugrožavati javne korisnike.

Ovo je jedan od osnovnih i najvažnijih principa organizacije AMTSO i njenih članica. Korisnici antivirusnih proizvoda očekuju da se oni proizvode, te da se ispitivanja nad njima provode prvenstveno u svrhu njihove bolje zaštite. Zato proizvodi, kao i ispitivanja, moraju biti oblikovani tako da ne ugrožavaju sigurnost svojih korisnika. Dodatno, ispitivači moraju slijediti odgovarajuće procedure kako bi izbjegli slučajna curenja testnih uzoraka zlonamjernih programa u javnu mrežu te ne smiju stvarati nove zlonamjerne programe u svrhu testiranja.

Princip 2: Testovi moraju biti nezavisni.

Ovaj princip od ispitivača antivirusnih alata traži da svaki ispitivani proizvod bude tretiran na isti način. Bez obzira je li testiranje naručio netko od proizvođača u svrhu marketinga ili neki magazin, dužnost ispitivača je izvesti ispitivanje koje poštuje etičke principe te objaviti točne i neizmijenjene rezultate.

U mnogim okolnostima proizvođači daju financijske donacije u svrhu izvođenja i objavljivanja rezultata ispitivanja. Iako se ove donacije ne smatraju nužno neetičkim, AMTSO smatra da one (u svrhu transparentnosti) moraju biti javno obznanjene. Zato se savjetuje svim ispitivačkim institucijama da objave sve veze, pa tako i one financijske prirode, sa proizvođačima i drugim entitetima u antivirusnoj industriji.

Princip 3: Ispitivanja moraju biti otvorena i transparentna.

Iako je poznato da neke organizacije iz raznih razloga ne žele otkriti metodologiju svojih testiranja, organizacija AMTSO smatra da bi te informacije morale biti objašnjene i javno dostupne. To je važno kako bi se osigurala pouzdanost i konzistentnost metoda koje se koriste prilikom ispitivanja. Savjetuje se da prilikom objave rezultata svakog ispitivanja bude objašnjena i metodologija ili objavljena referenca na istu.

Informacije koje su vezane uz ispitivanje, a trebaju biti objavljene moraju odgovarati na sljedeća pitanja:

1. Koji proizvodi su ispitivani?
2. Otkud su navedeni proizvodi prikupljeni i jesu li bili osvježeni najnovijim potpisima?

3. Otkud su prikupljeni testni uzorci zlonamjernih programa i kako su provjereni?
4. Koje inačice ispitivanih alata su korištene?
5. Koje konfiguracije alata su korištene?
6. Kada i pod kojim uvjetima su ispitivanja izvršena?
7. U kakvo okruženju su ispitivanja izvršena? (npr. operacijski sustav, drugi programi koji su pokrenuti tijekom testa i sl.)

Što se tiče informacija o metodologiji, one moraju sadržavati odgovore na sljedeća pitanja:

1. Kako su odabrani testni primjerci zlonamjernih programa?
2. Koji su izvori testnih primjeraka?
3. Kako su testni primjerci korišteni?
4. Kako je mjerena reakcija antivirusnih alata?
5. Jesu li uspoređivani alati sličnih funkcionalnosti ili različiti alati?
6. Ukoliko su uspoređivani alati značajno različitih funkcionalnosti, koje je bilo mjerilo?
7. Kako su konačni rezultati izračunati i interpretirani?

Princip 4: Učinkovitost i performanse ispitivanih alata moraju biti mjerene na uravnotežen način.

Sumiranje rezultata ispitivanja učinkovitosti proizvoda pomoću samo jednog testa je teško i često dovodi do krivih zaključaka. Ispitivačima se zato savjetuje provođenje više mjerenja performansi na različitima područjima rada alata kako bi se krajnjim korisnicima pružila točna i potpuna informacija.

Primjerice, ispitivači moraju obratiti posebnu pažnju na balansiranje rezultata ispitivanja „lažno pozitivnih" i „lažno negativnih" prijava. Proizvod koji je uspješan u detekciji raznih vrsta zlonamjernih programa, no ima veliku razinu lažno pozitivnih prijava, ne mora nužno biti bolji od proizvoda koji detektira manji broj zlonamjernih programa, ali također ima manji broj lažno pozitivnih prijava.

Princip 5: Ispitivači moraju detaljno provjeriti da su njihovi testni uzorci zaista zlođudni.

Često se znalo dogoditi da naizgled pouzdani rezultati ispitivanja u biti nisu valjani, jer su testni primjerci korišteni tijekom ispitivanja bili krivo klasificirani. Na primjer, ako ispitivač tvrdi da neki proizvod ima visoku razinu lažno pozitivnih prijava, to ne mora biti točno ukoliko su neki korišteni uzorci pogreškom proglašeni dobroćudnima. Upravo kako bi se izbjegle takve situacije, ispitivačima se savjetuje obratiti posebnu pažnju prilikom kategoriziranja primjeraka, naročito prilikom ispitivanja lažno pozitivnih i negativnih prijava.

Također, testne primjerke treba posebno provjeriti na ispravnost, održivost te da li se njihova zlođudna aktivnost očituje u ispitnom okruženju.

Princip 6: Metodologija mora biti konzistentna s obzirom na cilj ispitivanja.

Svaka institucija koja obavlja ispitivanja antivirusnih alata mora jasno istaknuti ciljeve svojih testova. Također, metodologija koju u svojim ispitivanjima koriste mora biti konzistentna sa krajnjim ciljevima. Primjerice, objavljivanje rezultata u magazinu orijentiranom na kućne korisnike, bez isticanja da su ispitivani proizvodi namijenjeni poduzećima nije dobro, jer može zavarati čitatelje budući da taj tip proizvoda nije namijenjen njima.

Kao dodatna literatura u kojoj su detaljnije objašnjeni problemi nekonzistentnosti metodologije i ciljeva ispitivanja može poslužiti rad Davida Harleya dostupan na web adresi:

http://www.smallblue-greenworld.co.uk/AV_comparative_guide.pdf

Princip 7: Zaključci iz konačnog izvještaja moraju biti izvedeni iz rezultata testiranja

Ovo je važan princip koji naglašava veliki problem kod mnogih objavljenih izvještaja čiji zaključci nisu bili odraz rezultata postignutih testiranjem, pa time nisu bili valjani i informativni.

Princip 8: Rezultati ispitivanja moraju biti statistički valjani.

Ispitivači moraju koristiti dovoljan broj testnih uzoraka i scenarija kako bi se rezultati mogli statistički obraditi. Dodatno, važno je elaborirati i objaviti analizu mjernih pogrešaka. Organizacija AMTSO preporuča korištenje što više različitih testnih scenarija kako bi rezultati bili reprezentativni.

Više detalja o načinu testiranja i problemima prilikom prezentacije i interpretacije rezultata može se pronaći u radi Igora Muttika, dostupnom na web adresi:

http://www.mcafee.com/common/media/vil/pdf/imuttik_VB_conf_2001.pdf

Princip 9: Ispitivači, proizvođači i izdavači moraju održavati aktivni kontakt za razmjenu informacija vezanih uz testove.

Ovaj princip važan je zbog daljnjeg razvoja metodologije ispitivanja. Aktivni kontakt između svih strana koje su, na ovaj ili onaj način, dio procesa ispitivanja antivirusnih alata ključan je faktor u rješavanju svih nesporazuma i problema te temelj daljnjeg napretka na ovom osjetljivom području.

4.2. Smjernice za dinamičko ispitivanje

U drugom važnom dokumentu [5] koji je objavila organizacija AMTSO opisane su najbolje prakse i savjeti za kvalitetno dinamičko ispitivanje antivirusnih alata. Ovaj dokument je svojevrsni nastavak na osnovne principe kvalitetnog ispitivanja. Pod dinamičkim testiranjem smatra se proces kod kojeg se antivirusni alati izlažu realnim provjerama tako da se zlonamjerni programi pokreću na testnom računalu. Ovakvom vrstom ispitivanja realnije se može ocijeniti učinkovitost pojedinog alata u borbi protiv zloćudnih programa (za razliku od običnih statičkih testova, kao npr. „*on demand*" skeniranje). Dok je dinamičko testiranje jedini način za ispitivanje učinkovitosti pojedinih antivirusnih tehnologija, lako je primjenjivo na sve vrste antivirusnih proizvoda. U narednim poglavljima dani su neki savjeti za kvalitetnije izvođenje ove vrste ispitivanja, te su opisani problemi s kojima se ispitivači često susreću.

4.2.1. Ponavljanje ispitivanja

Za razliku od statičkih, dinamičke testove puno je teže reproducirati, u smislu da provođenje istog ispitivanja u različitim trenucima može proizvesti potpuno drugačije rezultate. Uzrok tome može biti izmjena alata od proizvođača (npr. osvježavanje baze potpisa) ili promjene u testnom okruženju. Primjerice, neki zloćudni programi obavljaju svoju aktivnost samo ukoliko su odgovarajući servisi pokrenuti na napadnutom računalu (npr. NTP servis). Iako je moguće simulirati neke od ovih uvjeta na testnom računalu, teško ih je sve obuhvatiti sa potpunom točnošću. To u konačnici dovodi do situacije u kojoj je teško izvoditi čvrste zaključke iz nekoliko ponovljenih krugova ispitivanja.

Postoje dva moguća rješenja za izbjegavanje ovog problema:

- Prvi je sakupljanje dovoljne količine informacija i dnevničkih zapisa sa testnih računala kako bi se nedvosmisleno mogle potvrditi akcije koje su se odvijali prilikom testiranja. Primjerice, tvrdnja da proizvod X nije detektirao zlonamjerni program Y u trenutku Z mora biti potkrijepljena odgovarajućim informacijama.
- Drugi način je korištenje dostatnog broja uzoraka zloćudnih programa i ponavljanje testova tijekom određenom vremenskog razdoblja (npr. mjesec dana). Time se izbjegavaju nekonzistentnosti u ponašanju zlonamjernih programa, a kao relevantna mjera se mogu promatrati razine detekcija po danima i trendovi u performansama alata.

4.2.2. Odabir antivirusnih alata

Ponekad su antivirusni zaštitni mehanizmi ugrađeni u veće sigurnosne proizvode (npr. u tzv. komplete za sigurnost na Internetu), dok se neki na tržištu pojavljuju kao zasebni proizvodi. Ispitivači moraju biti svjesni razlika između ovih tipova proizvoda i pažljivo odabirati proizvode kako bi proizveli kvalitetne komparativne rezultate. Dobar izvor informacija za testiranje pojedinih funkcionalnosti ovih proizvoda su upute proizvođača. Ukoliko proizvođač tvrdi da njegov proizvod koristi tehniku X, onda ima smisla usporediti taj proizvod sa nekim drugim koji koristi istu tehniku.

4.2.3. Odabir ispitnih uzoraka

Odabir uzoraka je važan kod svake vrste ispitivanja. Kod dinamičkog ispitivanja kvaliteta uzoraka bitnija je od kvantitete, jer se radi o testovima kod kojih je važno ponašanje antivirusa u slučaju zaraze, a ne količina detektiranih zloćudnih programa. Uzorci se moraju odabirati prema sljedećim kriterijima:

1. **Funkcionalnost**

   Za provođenje dobrog testa antivirusnih alata svi uzorci zlonamjernih programa moraju biti funkcionalni što znači da je prije ispitivanja važno provjeriti da svi uzorci rade i provode neku zloćudnu aktivnost.

2. **Raznolikost**

   Dinamički testovi često se provode na manjem skupu uzoraka nego je to uobičajeno. Zato je važno da su programi iz tog skupa funkcionalno različiti. Važno je izabirati zlonamjerne programe koji pripadaju različitim familijama i ne sadrže slične funkcionalnosti.

3. **Važnost**

   Savjetuje se prilikom ispitivanja koristiti samo one zlonamjerne programe koji se pojavljuju u svakodnevnom korištenju računala zbog čega je važno da ih svaki antivirus detektira. „Beznačajne" viruse, tj. one koji se gotovo nikada ne pojavljuju, nije preporučljivo uključiti u testiranja.

4. **Starost**

   Važno svojstvo svake antivirusne tehnologije je zaštita protiv tzv. „*zero day*" zlonamjernih programa. Upravo zato je prilikom ispitivanja važno koristiti najnovije i najaktualnije uzorke.

4.2.4. Ispitivanje na lažno pozitivne prijave

Kako bi dali realnu ocjenu korisničkog iskustva ispitivači moraju u svoja ispitivanja uključiti testove na lažno pozitivne prijave. Ovdje se radi o testiranjima koji se provode nad običnim programima koji sustavu korisnika ne predstavljaju nikakvu prijetnju. Programi koje bi trebalo uključiti u ovu vrstu testiranja su oni koje prosječan korisnik koristi svakodnevno, a testovi moraju uključivati i svakodnevne korisničke akcije – instaliranje i osvježavanje aplikacija i operacijskih sustava, korištenje web preglednika i njegovih dodataka i dr. Također, treba provjeriti da sve instalirane aplikacije ispravno rade.

4.2.5. Ispitno okruženje

Kod dinamičkog ispitivanja performanse alata strogo su određene ponašanjem zlonamjernih programa, dok je ponašanje zlonamjernih programa određeno okruženjem u kojem su oni pokrenuti. Zato je važno stvoriti realno ispitno okruženje kako bi se dobili relevantni i pouzdani rezultati. Karakteristike ispitnog okruženja u ovom slučaju predstavljaju instalirani operacijski sustav, zatim je li ispitni sustav fizičko ili virtualno računalo, mrežna veza, način na koji je zlonamjerni program pokrenut i dr. Ne postoji definicija idealnog ispitnog okruženja, pa ispitivači moraju biti spremni na ograničenja koja uvode odabirom određenog okruženja. Ipak, prilikom odabira važno je obratiti pažnju na sljedeće stavke:

- **Korištenje virtualnih računala**

Mnogi zlonamjerni programi ne obavljaju u potpunosti svoju aktivnost u virtualnim okruženjima (npr. VMware ili Virtual PC). Čak niti korištenje nekih antivirusnih proizvoda nije potpuno podržano na virtualnim računalima. Iako je korištenje fizičkih računala dobra alternativa, ispitivanja su u tom slučaju tehnički teže izvediva i složenija te ih je teže automatizirati. Usprkos ovim poteškoćama, korištenje virtualnih računala je preporučljivo kod dinamičkih ispitivanja antivirusnih alata. Kako bi se lakše prevladale poteškoće, organizacija AMTSO potiče svoje članice da učine korisne ispitivačke alate dostupnima drugim članovima. Također, ispitivači bi uvijek trebali naglasiti na kakvoj vrsti računala su ispitivanja izvršena.

- **Mrežni pristup**

Razni oblici zlonamjernih programa, kao i antivirusnih alata zahtijevaju mrežni pristup kako bi radili u punom opsegu svojih funkcionalnosti. Zato je važno ovim programima omogućiti pristup Internetu prilikom ispitivanja. Ipak, ovakav pristup je opasan, jer zlonamjerni programi mogu iskoristiti vezu i proširiti se na druga računala. Postoje dva osnovna pristupa za rješavanje ovog problema. Prvi pristup je omogućavanje mrežnog pristupa, no ograničavanje dozvoljenih protokola. Primjerice, uobičajeno je dozvoliti HTTP (eng. HyperText Transfer Protocol), a zabraniti sve druge. Ovo se obično postiže promjenom konfiguracije na mrežnom uređaju, najčešće usmjerniku. Alternativa ovom pristupu je stvaranje virtualnog Interneta (poznatog i kao Trumanova kutija). Kod ovog pristupa na sve mrežne zahtjeve se šalju lažni odgovori, pa tako ispitivani programi imaju privid potpunog mrežnog pristupa. Još jedna alternativa je korištenje spore internetske veze (npr. ISDN veze umjesto ADSL-a). Ni ovdje ne postoji idealan odabir, pa ispitivači moraju odluku donijeti na temelju specifičnih zahtjeva za pojedinu provjeru. Pritom je iznimno važno da se ta odluka i dokumentira.

- **Pokretanje zlonamjernih programa**

Antivirusni alati su često podešeni tako da posebnu pažnju obraćaju na neke uobičajene načine kompromitiranja računala. Tako, primjerice, posebno analiziraju programe koji se pokreću automatski prilikom njihovog dohvaćanja sa Interneta. Zato način pokretanja zlonamjernih programa prilikom ispitivanja često može značajno utjecati na konačne rezultate. Najbolja praksa je pokretati programe onako kako bi oni najčešće bili pokrenuti u svakodnevnom radnom okruženju. Na primjer, ako se određena vrsta zlonamjernog programa najčešće širi dohvaćanjem putem HTTP protokola, tada je preporučljivo pokrenuti program na isti način i prilikom ispitivanja. Ovo je obično teško implementirati u ispitivanjima, pa se kao lošija alternativa preporuča pokrenuti program ručno, te mijenjati načine na koje ga se pokreće.

4.2.6. Praćenje promjena

Budući da kod dinamičkog ispitivanja antivirusnih alata ponašanje zlonamjernog programa ima bitan utjecaj na performanse, važno je detaljno bilježiti sve promjene koje su se tijekom ispitivanja dogodile. Posebnu pažnju treba obratiti na sljedeće stvari:

1. Akcije koje poduzima zlonamjerni program na kompromitiranom računalu.
2. Promjene koje se događaju u datotekama, posebno u sistemskom području.
3. Tragove mrežnih aktivnosti programa.

4.2.7. Mjerenje uspješnosti

Upravo zbog toga što dinamička ispitivanja zahtijevaju pokretanje zlonamjernog programa, a pokrenuti zlonamjerni programi mogu imati razne učinke na rad sustava (instalacija programa, promjene u konfiguraciji, curenje informacija i dr.), iznimno je važno definirati što se smatra uspješnom detekcijom. Postoje razni načini za mjerenje uspjeha, od kojih su neki više ili manje primjenjivi na određene vrste ispitivanja. Neki od tih načina su:

- **Detekcija**

Ovdje se provjerava je li antivirusni alat prijavio neki zlonamjerni program ili zabilježio nešto u svojim zapisima.

- **Uklanjanje zlonamjernog programa**

Ovdje je važno provjeriti jesu li sve promjene na sustavu, koje je uzrokovao zlonamjerni program svojom aktivnošću, uklonjene. Neke provjere mogu uključivati uklanjanje svih promjena na sustavu, dok neke mogu zanemariti beznačajne datoteke koje su ostale nakon uklanjanja, a nemaju utjecaja na daljnji rad sustava. Također, neki alati ne uklanjaju u potpunosti zlonamjerni program, već ga samo onemogućavaju u daljnjem radu, pa i ovaj pristup treba uzeti u obzir prilikom određivanja načina ocjenjivanja alata.

- **Održivost zlonamjernih programa**

Da li se zlonamjerni program opet aktivirao nakon ponovnog pokretanja računala? Ovo bi značilo da ga antivirusni alat nije uklonio na odgovarajući način.

- **Šteta**

Dobro je provjeriti je li zlonamjerni program uspješno kompromitirao napadnuti sustav. Ovo je posebno važna stavka kod zlonamjernih programa koji kradu informacije jer označava kako postoji mogućnost da su informacije ukradene ili izmijenjene iako je antivirusni alat blokirao program u radu. Ovakve situacije je prilično teško detektirati prilikom ispitivanja.

4.2.8. Interakcija sa korisnikom

Mnogi antivirusni proizvodi koriste *„pop-up“* prozore za komunikaciju sa korisnikom tijekom svog rada. Ovo može izazvati popriličnu konfuziju u rezultatima ispitivanja. Na primjer, ukoliko alat kod detekcije pita korisnika za željenu akciju (blokiraj program ili zanemari upozorenje), a ispitivač prilikom testa svaki puta odabere opciju zanemarivanja upozorenja, rezultati ovog proizvoda biti će značajno lošiji nego da je ispitivač izabrao blokiranje. Važne smjernice kod baratanja *„pop-up“* prozorima su sljedeće:

- **Politika**

Ispitivači se moraju odlučiti za jedan način rukovanja interakcijom alata sa korisnikom. To može biti način koji „ide na ruku“ ispitivanom alatu ili onaj koji odmaže uspješnosti njegovih konačnih rezultata. Ova politika treba biti eksplicitno opisana u dokumentaciji metodologije.

- **Konzistentnost**

Jednom kada se odabere određena politika rukovanja *„pop-up“* prozorima treba ju primjenjivati na svim proizvodima i u svim ispitivanjima.

- **Izvještavanje**

Ispitivači bi trebali mjeriti količinu interakcije koju alat traži od korisnika. Ova informacija biti će korisna krajnjim korisnicima da bi ocijenili odgovara li im ispitivani alat u tom smislu (količina interakcije). Postoji nekoliko tipova interakcije koje treba razlikovati prilikom izvještavanja:

1. Alat izvodi akciju bez eksplicitnog dopuštenja korisnika, ali ga nakon izvođenja o tome obavještava.
2. Alat traži eksplicitno dopuštenje korisnika prije izvođenja bilo koje akcije.
3. Općenite obavijesti koje ne zahtijevaju interakciju korisnika i nisu nužno vezane uz akcije alata.

4.2.9. Stilovi dinamičkih ispitivanja

U ovom poglavlju opisana su dva različita stila izvođenja dinamičkih ispitivanja. Ovo nisu jedini mogući načini, ali mogu biti korisni ispitivačima kao izvori ideja.

Prvi stil ispitivanja naziva se i „jedan po jedan“ pristup. Kod ovog pristupa ispituje se jedan antivirusni alat u određenom trenutku i njemu se predaje jedan zlonamjerni program na analizu. Nakon toga se analiziraju promjene koje su se dogodile u sustavu i utvrđuje se je li alat uspješno detektirao zloćudni program. Nakon procesa utvrđivanja, ispitni sustav se vraća u početno stanje i test se ponavlja za sljedeći zlonamjerni program. Ovaj pristup je iznimno precizan no vremenski vrlo zahtjevan jer se između predaje svakog novog zlonamjernog programa sustav mora detaljno analizirati.

Kod drugog pristupa antivirusnom alatu se predaje više zlonamjernih programa odjednom. Iako je ovaj postupak manje precizan, on je vrlo učinkovit sa stajališta analize sustava nakon ispitivanja. Zanimljiva varijacija ovog pristupa je posjećivanje velikog broja zloćudnih web stranica sa ispitnog računala. To se lako može postići izradom jednostavne skripte za višestruko pokretanje web preglednika na ispitnom sustavu. Nakon što su posjećene sve zloćudne stranice, ispitni sustav se može analizirati kako bi se ocijenila uspješnost antivirusnog alata u zaštiti korisničkog računala. Ovaj test je dobra simulacija realne situacije u kojoj se korisnik može naći. Jedina zamjerka ovom pristupu je činjenica da zloćudni poslužitelji često ne mogu posluživati više zloćudnih programa u isto vrijeme. Također, prilikom ovakvog ispitivanja teško je garantirati da će svi ispitivani alati biti izloženi istim prijetnjama. Zato je važno koristiti veliki broj različitih zloćudnih stranica i ponavljati testove u više navrata kako bi se mogli uočiti trendovi u performansama ispitivanih alata.

4.3. Provjera uzoraka

Peti osnovni princip za ispitivanje antivirusnih alata organizacije AMTSO kaže da ispitivači moraju obratiti posebnu pažnju kod odabira ispitnih uzoraka te moraju detaljno ispitati jesu li oni valjani, funkcionalni i provode li neku zloćudnu aktivnost. Ovaj princip zahtjeva posebne metode za vrednovanje uzoraka iz ispitnog skupa. Provjera uzoraka može se provesti u dva koraka koji su detaljnije opisani u idućim poglavljima.

4.3.1. Ispitivanje funkcionalnosti uzoraka

Provjera funkcionalnosti ispitnih uzoraka obično se svodi na provjeru zloćudnih aktivnosti programa. Aktivnost zloćudnog programa može se provjeriti aktivnim bilježenjem promjena prilikom njegovog pokretanja ili pasivnom usporedbom. Kod aktivnog bilježenja preporuča se koristiti sljedeće programske alate:

1. HIPS (eng. host intrusion prevention system) alati
2. Sandbox alati
3. Sistemski alati
4. Alati za otkrivanje rootkit programa
5. Alati za aktivno praćenje mrežnog prometa

Ispitivači moraju biti oprezni kod korištenja alata za praćenje aktivnosti, jer neki primjerci zloćudnih programa se ponašaju drugačije ukoliko detektiraju prisutnost takvih alata. Ovo se može izbjeći izmjenom standardnih alata, kako bi se njihova prisutnost teže otkrila.

Koda pasivne usporedbe zlonamjerni program se izvršava na ispitnom računalu koje se zatim gasi i analiziraju se promjene koje su se prilikom izvršavanja dogodile. Ovaj proces uključuje sljedeće korake:

1. Pokretanje (eng. mount) datotečnog sustava.
2. Bilježenje promjena na sustavu.
3. Praćenje mrežne aktivnosti izvan ispitnog sustava.

4.3.2. Ispravnost izvršnog programa

Ponekad nije moguće provjeriti funkcionalnost svih ispitnih uzoraka. U tom slučaju ispitivač bi barem trebao provjeriti da se zlonamjerni program može pravilno učitati u ispitnom okruženju. Važno je primijetiti da se u slučaju zloćudnih skripti ispitno okruženje mora sastojati od odgovarajućeg operacijskog sustava i skriptnog interpretera, odnosno, u slučaju makro virusa, odgovarajuće aplikacije.

Ispravnost izvršne datoteke može se provjeriti statičkom analizom uzorka ili ako je moguće i dinamičkom analizom (odnosno pokretanjem iste na ciljnom operacijskom sustavu). U slučaju zlonamjernih programa za operacijski sustav Windows, statička analiza podrazumijeva provjeru ispravnosti PE (eng. Portable Executable) formata datoteke. Kod dinamičke analize program se pokreće unutar ispitnog operacijskog sustava nakon čega se provjerava stvaranje procesa i dretvi.

Na primjer, važno je provjeriti sljedeće minimalne kriterije za jedan izvršni program namijenjen operacijskim sustavima Windows (koji čine većinu ispitnih kolekcija danas):

- Provjera valjane tablice sekcija (eng. section table)
- Provjera valjane ulazne točke (eng entry point)
- Provjera veličine ulazne datoteke (ne smije biti kraća od zbroja veličina svih sekcija)
- Provjera formata svih sekcija
- Provjera valjanosti sekcije u kojoj se nalazi ulazna točka (mora biti izvršiva)

5. Budućnost

Osnivanje organizacije AMTSO i razvoj prvih dokumenata sa smjernicama za kvalitetnije ispitivanje antivirusnih alata velik je korak u rješavanju problema nastalih sa pojavom nekvalitetnih testova. Članstvo svih značajnih proizvođača, kao i institucija koje provode ispitivanja u ovoj organizaciji znak je dobre volje i želje da se stvari na ovom osjetljivom području pomaknu na bolje. Revizije postupaka ispitivanja koje će AMTSO provodi svakako bi trebale razlučiti kvalitetne od neodgovarajućih postupaka i pružiti korisnicima kvalitetne informacije na koje se mogu pouzdati prilikom odabira antivirusnog rješenja. Može se pretpostaviti da će ovo za posljedicu imati teži opstanak institucija koje ne provode svoja ispitivanja na odgovarajući način i u skladu sa pravilima struke.

Slika 11. *Panda Antivirus – jedan od predvodnika „antivirusa u oblaku“*

Izvor: cloudantivirus.com

Još jedna važna stvar na koju treba obratiti pažnju je pojava nove generacije antivirusnih alata – „antivirusa u oblaku“. Riječ je o novim alatima kod kojih se osnovni program (eng. core program) nalazi na računalu korisnika, a znanje i informacije o zlođudnim programima nalazi se na poslužiteljima proizvođača (odnosno „u oblaku“) kojima se može pristupiti Internetom. Ispitivanje ove nove generacije antivirusa je prilično složen i delikatan postupak, jer je teško napraviti odgovarajuće ispitno okruženje koje će sve alate tretirati jednako. Kako bi obuhvatilo i ovu vrstu ispitivanja, organizacija AMTSO je već objavila dokument sa osnovnim smjernicama i savjetima za ispitivanje ove vrste alata. Dokument se može dohvatiti na sljedećoj web adresi:

http://www.amtso.org/uploads/amtso-best-practices-for-testing-in-the-cloud-security-products.pdf

6. Zaključak

Zlonamjerni programi svakim danom postaju sve složeniji i sofisticiraniji, te ih je teže otkriti i spriječiti u izvršavanju zloćudnih aktivnosti. Antivirusne kompanije razvijaju nove, naprednije, tehnologije kako bi se uspjele nositi sa najnovijim oblicima zlonamjernih programa. Da bi se utvrdila uspješnost novih tehnologija važno je antivirusne alate redovito ispitivati i evaluirati njihovu kvalitetu. Da bi se izbjegli nekvalitetni testovi potrebno je postaviti standarde struke prema kojima će se svi ravnati i koje će poštivati. Upravo na ovom osjetljivom i važnom području ispitivanja antivirusnih alata takve smjernice dugo nisu postojale. To je bio jedan od glavnih razloga nastanka brojnih loše dizajniranih testova koji su korisnike često krivo informirali i tako im u biti odmagali prilikom odabira antivirusnog alata.

Baš iz tih razloga stručnjaci iz struke odlučili su osnovati organizaciju AMTSO, koja je zadužena za razvoj standarda i smjernica za ispitivanje antivirusnih alata te poticanje diskusija vezanih uz ovo područje. AMTSO organizacija također je zadužena za reviziju postojećih i budućih postupaka evaluacije antivirusnih alata. Ova inicijativa trebala bi u doglednoj budućnosti rezultirati kvalitetnijim testovima i realnijim pregledom mogućnosti brojnih antivirusnih alata na tržištu. Time bi u konačnici najviše trebali profitirati krajnji korisnici koji će dobivati točnije informacije o proizvodima koje odabiru, što je posebno važno za podizanje globalne svjetske računalne sigurnosti na višu razinu.

7. Reference

[1] Sarah Gordon, Fraser Howard: Antivirus Software Testing for the New Millenium, http://csrc.nist.gov/nissc/2000/proceedings/papers/038.pdf, 2000.

[2] Andreas Clementi: Anti-Virus Testing Websites, http://www.av-comparatives.org/seiten/ergebnisse/AVTW.pdf, travanj 2007.

[3] Sarah Gordon, Richard Ford: Real world anti-virus product reviews and evaluations – The current state of affairs, http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper019/final.PDF, 1996.

[4] AMTSO: The Fundamental Principles of Testing http://www.amtso.org/uploads/AMTSO_Principles_-_FINAL_31_Oct_2008-1.pdf, listopad 2008.

[5] AMTSO: Best Practices for Dynamic Testing http://www.amtso.org/uploads/AMTSO_Best_practices_for_Dynamic_Testing_-_FINAL_31__Oct_2008.pdf, listopad 2008.

[6] AMTSO Best Practices for validation of samples http://www.amtso.org/uploads/amtso-suggested-methods-for-the-validation-of-samples.pdf, svibanj 2009.

[7] Computer World: Consumer group slammed for creating 'test' viruses, http://www.computerworld.com/s/article/9002499/Consumer_group_slammed_for_creating_test_viruses?source=rss_topic17, kolovoz 2006.

[8] Computer World: Symantec false positive cripples thousands of Chinese PCs, http://www.computerworld.com/s/article/9019958/Symantec_false_positive_cripples_thousands_of_Chinese_PCs, svibanj 2007.