Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...



# Šta je anti-virus?

## Uvod

Anti-virus je bezbednosni program koji se instalira na računar ili mobilni uređaj u cilju zaštite od infekcija izazvanih „malware-om“ (štetnim softverom). Izraz „malware“ je zajednička fraza za sve tipove štetnog softvera kao što su „virusi“, „crvi“, „trojanci“ ili „spyware-i“. Ako se vaš računar zarazi „maleware-om“, sajber kriminalci mogu da saznaju tipke koje ste kucali, ukradu vaše dokumente ili koriste vaš računar za neke druge napadne. Suprotno uverenjima nekih ljudi, svaki operativni sistem može biti inficiran, uključujući Mac OS X i Linux.

### Gost urednik

Jake Williams je osnivač Rendition Infosec (**www.renditioninfosec.com**) i sertifikovani SANS instruktor i autor kurseva. Aktivan je na Twitter-u **@MalwareJake** i svom blogu **malwarejake.blogspot.com**.

Anti-virus se može kupiti kao zasebno rešenje, ili često kao deo uključen u neki sigurnosni paket. Problem je u činjenici da anit-virus ne može da drži korak sa sajber kriminalcima, obzirom da oni konstantno razvijaju i objavljuju nove tipove „malware-a“. Svakoga dana se objavljuju ogromne količine novog „malware-a“ tako da nijedan anti-virus program ne može sve da detektuje. Zato je važno da se razume da iako anti-virus pomaže u zaštiti računara, ne može se računati da će zaustaviti sve tipove „malware-a“. Da bi bolje razumeli zašto je to tako, potrebno je da se upoznamo kako većina ovih programa radi.

## Kako funkcioniše anti-virus

U principu postoje dva načina kako anti-virus softver identifikuje „malware“, detekcija potpisa ili detekcija ponašanja. Detekcija potpisa funkcioniše kao ljudski imunološki sistem. Skenira se računar na osnovu karakteristika ili potpisa poznatih štetnih programa, na osnovu baze podataka poznatog „malware-a“. Ako nešto na računaru odgovara uzorku iz baze, anti-virus program pokuša da ga neutralizuje. Kao i ljudski imunološki sistem, da bi se zaštitili od novog „malware-a“ baza podataka zahteva ažuriranje, slično vakcini za grip, tako da anti-virus može da zaštiti samo od onoga što je poznato. Problem je u tome što sajber kriminalci razvijaju novi „malware“ tako brzo da proizvođači anti-virus softvera ne mogu da drže korak sa njima. Kao rezultat, bez obzira koliko je skoro vaš anti-virus ažuriran, uvek postoje nove varijante „malware-a“ koje potencijalno mogu da „zaobiđu“ vaš anti-virus softver.

# Šta je anti-virus?

Kod detekcije ponašanja, anti-virus ne pokušava da identifikuje poznati „malware“, već prati ponašanje softvera instaliranog na računaru. Ako se neki program ponaša sumnjivo, na primer pokušava da pristupi zaštićenim fajlovima, ili da modifikuje drugi program, anti-virus koji detektuje ponašanje će to primetiti i signalizirati. Ovakav pristup obezbeđuje zaštitu od novih tipova „malware-a“ koji još uvek nisu registrovani u bazama podataka. Problem kod ovog pristupa je što može da generiše lažna upozorenja. Korisnik može da bude zbunjen svim upozorenjima, šta da dozvoli, a šta ne, i vremenom postane „neosetljiv“ na sva ta upozorenja. i može biti u iskušenju da klikne „Accept“ (Prihvati) prilikom svakog upozorenja, i tako računar izloži napadima i infekcijama. Takođe, dok „ponašanje“ ne bude detektovano, velika je verovatnoća da je „malware“ već aktivan na računaru i da se ne zna kakva je šteta pričinjena pre nego što ga je anti-virus softver identifikovao.

*Anti-virus je važan deo vaše bezbednosti, ali ne može da detektuje i zaustavi sve napade. Konačno, vi ste najbolja odbrane, ne samo tehnologija.*

Anti-virus je važna komponenta bezbednosti vašeg računara i mobilnih uređaja, i preporučljivo je da ga, kad god je to moguće, instalirate i aktivno koristite. Međutim, ključna stvar koju treba imati na umu je da bezobzira kako vaš anti-virus funkcioniše, nekada ne može da vas zaštiti od svih tipova „malware-a“. Na kraju krajeva, najbolja zaštita od današnjih sajber pretnji ste vi u kombinaciji sa raspoloživim tehnologijama

## Anti-virus saveti

1. Koristite anti-virus softver iz poznatih, pouzdanih izvora i proizvođača. Jedan od uobičajenih trikova sajber kriminalaca je da distribuiraju lažne anti-virus programe, koji su ustvari „malware“.
2. Budite sigurni da imate najnoviju verziju anti-virus softvera koji koristite, da je godišnja pretplata plaćena i aktivna, i da je anti-virus konfigurisan da se ažurira automatski. Ako je vaš računar bio van mreže ili ugašen neko vreme, anti-virus softver će trebati neko vreme da se ažurira kada bude ponovo uključen ili ponovo povezan na Internet. Ne odlažite ovo ažuriranje.
3. Budite sigurni da anti-virus automatski skenira prenosive medije, kao što su USB stikovi, i da je zaštita u realnom vremenu uključena.
4. Obratite pažnju na upozorenja i obaveštenja generisana od strane anti-virusa. Većina upozorenja uključuje

## Šta je anti-virus?

mogućnost dobijanja dodatnih informacija ili saveta što dalje činiti. Ako dobijete upozorenje na poslovnom računaru, odmah kontaktirajte IT podršku ili vašeg nadređenog.

5. Nemojte deaktivirati ili deinstalirati anti-virus softver zato što mislite da usporava rad vašeg računara, blokira određene Internet stranice ili onemogućava instalaciju određene aplikacije ili programa. Deaktiviranje će vas izložiti nepotrebnom riziku i može da prouzrokuje ozbiljne bezbednosne incidente. Ako se problem ponavlja na poslovnom računaru, kontaktirajte vašu IT podršku. Ako se ponavlja na privatnom računaru, pokušajte da kontaktirate proizvođača anti-virus softvera, posetite Internet stranicu za više informacija ili promenite anti-virus softver.
6. Ne instalirajte više anti-virus programa na jednom računaru u isto vreme. To bi verovatno uzrokovalo konfrontaciju među programima i umanjilo bezbednost računara.
7. Naučite da prepoznajete upozorenja koja vaš anti-virus softver prikazuje. Sajber kriminalci mogu da postave maliciozne Internet strane koje objavljuju veoma realistična lažna anti-virus upozorenja i ponude za pružanje pomoći u „popravljanju“ računara. Klikom na linkove ili tastere ovih Internet strana može da ozbiljno naudi vašem računaru.

## Saznaj Više

Prijavi se na OUCH! mesečni bilten bezbednosnih saveta za korisnike računara, pristupi prethodnim OUCH! izdanjima i saznaj više o SANS rešenjima u vezi svesnosti bezbednosti informacija na našoj internet prezentaciji http://www.securingthehuman.org/

## Dodatne informacije

| | |
|---|---|
| Poređenje anti-virus proizvoda: | http://www.av-test.org/en/ |
| Društveni inženjering: | http://www.securingthehuman.org/ouch/2014#november2014 |
| Napadi “pecanjem”: | http://www.securingthehuman.org/ouch/2013#february2013 |
| Hakovan si, šta onda?: | http://www.securingthehuman.org/ouch/2014#may2014 |



Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Preveo: Nenad Varinac