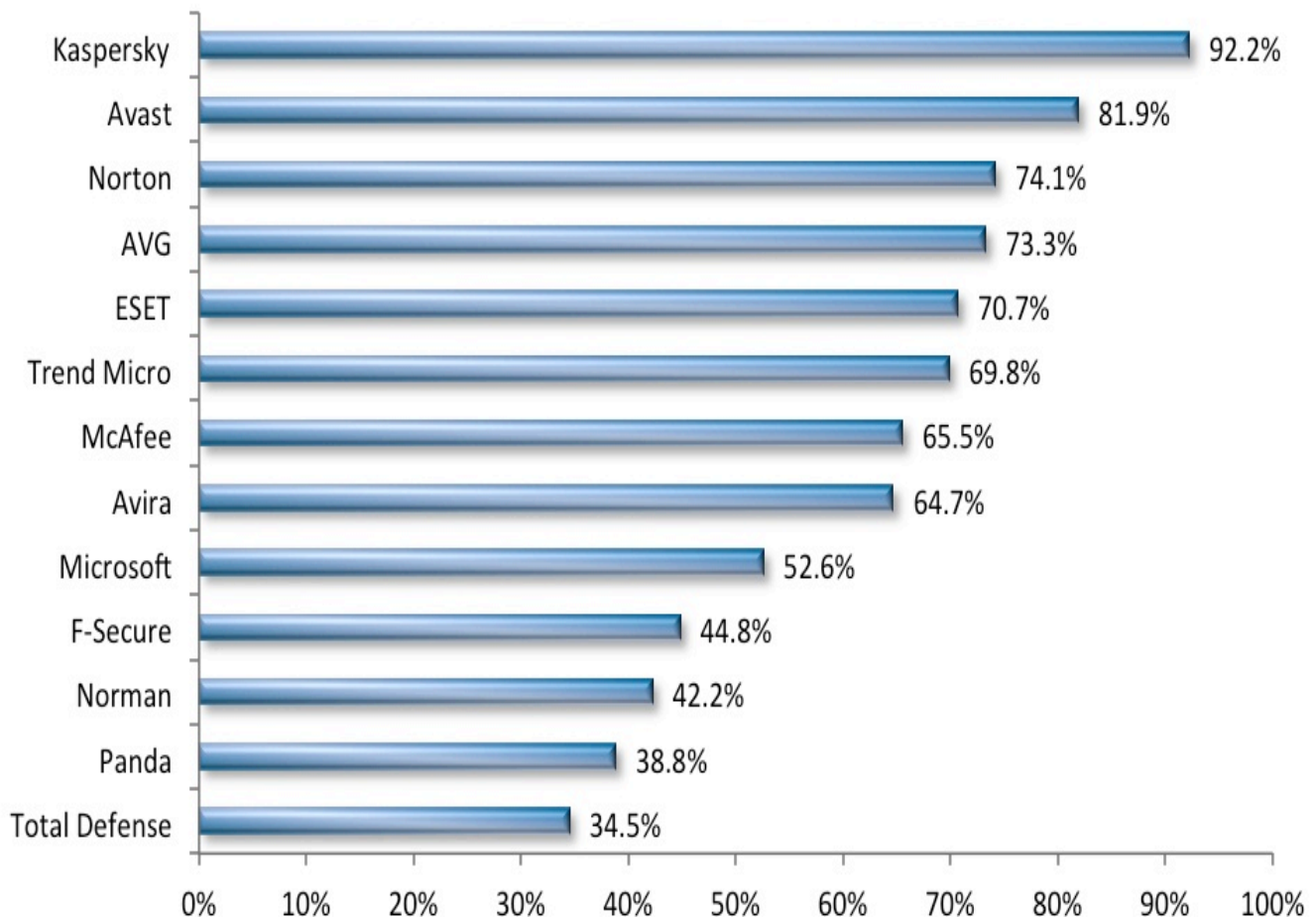


Vodeći antivirusni programi nedovoljni za obranu od exploita



Prema [istraživanju](#) [1] koje je provela tvrtka NSS Labs, od 13 vodećih antivirusnih programa samo su dva blokirala više od 80% poznatih *exploita*. Za potrebe testiranja NSS Labs koristio je web server za infekciju računala poznatim *exploitima* koji slobodno cirkuliraju Internetom već mjesecima, a neki od njih i godinama. Dakle "Zero-day" ranjivosti nisu korištene u ovom istraživanju. Pored toga, NSS Labs testirao je i reakciju web preglednika na različite *exploite*, i to svih verzija Internet Explorera, počevši od verzije 6, zatim različite verzije Firefoxa, kao i Safari i Google Chrome.

Kaspersky Internet Security 2012 blokirao je 92,2% prijetnji, a Avast Pro Antivirus 7 81,9%. Za njima slijede Symantec Norton Internet Security verzija 19 (74,1%), AVG Internet Security 2012 (73,3%), ESET Smart Security 5 (70,7%), Trend Micro Titanium Maximum Security verzija 6 (69,8%), McAfee Internet Security 11 (65,5%) i Avira Internet Security 2012 (64,7%). Ne tako sjajne rezultate pokazali su F-Secure Agent (verzja 1.57) koji je blokirao 44,8% napada, te Microsoft Security Essentials sa 52,6%.



Rezultati istraživanja pokazuju da u vrijeme cyber prijetnji kao što su ATP (*Advanced Persistent Threat*), *phishing* napadi, i dr., mnogi antivirusni programi ne pružaju adekvatnu zaštitu korisnika.

Iskorištavanje ranjivosti u softverskim programima omogućuje krađu identiteta, bankovne prijevare, preuzimanje e-mail računa i nekoliko drugih kriminalnih radnji.

Za većinu korisnika postoje preventivne mjere za borbu protiv opasnosti koje ih vrebaju na Internetu. Na primjer, redovita instalacija zakrpa (*patching*) jedna je od najvažnijih obrana. Međutim mnogi korisnici ne krpaju sve aplikacije na svojim osobnim računalima. Java je trenutno ranjiva, pa kako ne postoje ispravke, savjetuje se da se do daljnjega ukloni sa računala (o tome smo već pisali na [portalu](#) [2]).

Također, NSS Labs je upozorio korisnike ali i tvrtke da svatko tko još uvijek koristi Internet Explorer 6 mora biti dovoljno tehnički obrazovan da bi mogao koristiti i druge vidove obrane osim antivirusa ili će njegovo računalo skoro sigurno biti zaraženo. Na žalost, mnoge web aplikacije još uvijek zahtjevaju rad sa IE6.

Samo McAfee antivirus uspio je blokirati sve *Drive-by Download* napade na IE6 preko HTTP ili HTTPS protokola. Još su četiri antivirusna programa pokazala dobre rezultate u zaštiti IE6. Pradoksalno, Microsoftov antivirus nije među njima, štoviše, Microsoft Security Essentials je bio među onima koji su pokazali najlošije rezultate u obrani korisnika Internet Explorera verzije 6.

Internet Explorer 6 predstavljen je davne 2001. godine, te je standardno dolazio sa Windows XP, te Window Serverom 2003. Microsoft više ne pruža klasičnu podršku za navedeni preglednik, jedino se još može koristiti produženi oblik podrške do travnja 2014. za Win XP, te do srpnja 2015. za Win Server 2003. Ova verzija Internet Explorera trpi globalne kritike zbog svojih sigurnosnih problema i nedostatka podrške. Često se može naći u listama "najgorih tech proizvoda svih vremena", a koliko je nezadovoljstvo sa IE6 pokazuje i [web site](#) [3] namjenjen što skorijem prestanku njegova korištenja.

Za razliku od IE6, njegov nasljednik Internet Explorer 9 je po nedavnim testovima proglašen za najsigurniji web preglednik. O IE9 već je bilo govora u [članku](#) [4] o sigurnosti web preglednika.

Potpun i zaista zanimljiv izvještaj NSS Labsa možete preuzeti u PDF formatu sa ovog [linka](#) [5].

ned, 2012-10-28 20:31 - Ivan Sokač **Vijesti:** [Sigurnost](#) [6]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/1127>

Links

[1] <https://www.nsslabs.com/reports/consumer-avepp-comparative-analysis-exploit-protection>

[2] <https://sysportal.carnet.hr/node/1092>

[3] <http://www.ie6countdown.com/>

[4] <https://sysportal.carnet.hr/node/1114>

[5] https://www.nsslabs.com/system/files/content/report/files/2012_EPP_CAR_Consumer_Exploit_Protection.pdf

[6] <https://sysportal.carnet.hr/taxonomy/term/13>