

**ESET**

# Previdnost z USB ključki ne bo odveč

..OPERACIJSKI SISTEM WINDOWS VSAKIČ, KO V RAČUNALNIK VSTAVITE USB KLJUČEK, ZUNANJI DISK, CD IPD. IŠČE DATOTEKO AUTORUN.INF, V KATERI PIŠE, KATERI PROGRAM NAJ SE ZAŽENE. TO MOŽNOST PA S PRIDOM IZKORIŠČAJO PISCI ŠKODLJIVE KODE..



ESETovi raziskovalci pri svojem delu uporabljajo tehnologijo ThreatSense.Net. Gre za sistem sporočanja statističnih podatkov iz več milijonov računalnikov po celem svetu. Tako je lahko vsak računalnik, ki uporablja ESETov program za zaščito, posredno aktiven pri razvoju protivirusnih definicij. Vsak uporabnik se sam odloči, ali bo pri ThreatSense.Net tehnologiji sodeloval, informacije, ki se pošiljajo iz njegovega računalnika, so anonimne, vsebujejo pa okuženo datoteko, način kako je do okužbe prišlo, čas zaznave in informacije o operacijskem sistemu. Datoteke, ki bi lahko vsebovale osebne informacije (doc, xml ...), niso nikoli poslane. Takšen sistem ESETovim razvijalcem omogoča hitro reakcijo v primeru izbruha novih groženj, poleg tega pa jim zagotavlja natančno statistiko.

## AUTORUN ALI AUTOINFECT?

Operacijski sistem Windows vsakič, ko v računalnik

vstavite USB ključek, zunanji disk, CD ipd., išče datoteko autorun.inf, v kateri piše, kateri program naj se zažene. To možnost s pridom izkoriščajo pisca škodljive kode, ki se zavedajo, da so USB ključki in ostale izmenljive naprave nadvse popularne.

Možnost samodejnega zagona takšnih naprav je po privzetih nastavitvah sistema omogočena, večina strokovnjakov s področja računalniške varnosti pa se strinja, da je to napaka. Svoje zmete se zaveda tudi Microsoft, saj so na svoji uradni strani že opisali postopek, kako takšno funkcijo izklopimo (KB KB967715). Na začetku so to funkcijo izkoriščali le programi, ki so kradli gesla za spletne igre, danes pa se s pomočjo te funkcije širijo tudi ostale grožnje, tudi zloglasni črv Conficker, ki je v zadnjem času zelo razširjen.

ESETovi programi grožnje, ki poskušajo datoteko autorun.inf spremeniti, uvrščajo v družino INF/Autorun. Tehnologija ThreatSense.Net je prejšnji mesec takšnih groženj zabeležila nekaj več kot šest odstotkov, kar je tudi povprečje v lanskem letu. Čeprav vas pred njimi ščiti ESETova hevrstika, vam vseeno priporočamo, da samodejni zagon izmenljivih naprav izklopite.

## PREIZKUS Z VABAMI

Neka neimenovana finančna institucija je pred kratkim naredila zanimivo raziskavo. Na parkirišče pred svojim poslopijem so nastavili

eSet Top 10		www.eset.si
Deset najbolj razširjenih groženj v zadnjem tednu		
število okuženih e-sporočil		
Win32/Netsky.Q worm	40689	
Win32/Zafi.B worm	16574	
različica Win32/Injector.BZ trojan	10891	
Win32/Netsky.AB worm	2194	
Win32/Netsky.D worm	1647	
Win32/Bagle.HE worm	1497	
Win32/Mydoom.R worm	886	
Win32/Netsky.Z worm	579	
Win32/Scano.NBH trojan	373	
Win32/Netsky.C trojan	332	

dvajset USB ključkov s svojo programsko opremo. V roku treh dni je bilo kar petnajst takšnih ključkov priključenih v službene računalnike podjetja. Prav zaradi strahu pred takšnimi zlorabami se vse več podjetij odloča za omejevanje uporabe izmenljivih diskov.

## CONFICKER

Črv Conficker je bil med bolj razširjenimi že konec lanskega leta, nove različice tega črva pa so vse bolj agresivne, med drugim onemogočijo dostop do določenih strežnikov, zato protivirusni program na okuženem računalniku ne more posodobiti svojih definicij. Za informacije, ki bi privedle do aretacije avtorja črva, pa je Microsoft razpisal celo denarno nagrado. Če imate na svojem računalniku nameščen ESETov protivi-

## Odločite se za kvalitetne rešitve, tako doma kot na poslovnem mestu

Varnostne rešitve:

- Antivirus: ESET NOD32 in Smart Security
- Antispam: Cloudmark Desktop
- Antispyware: Webroot Spy Sweeper

Sistemske rešitve:

- Spletno gostovanje
- Servisne storitve
- Informacijska varnost



Uporabljate zaščito?