

Tri julijske grožnje v ospredju – INF/Autorun, Win32/Conficker in Win32/Sality

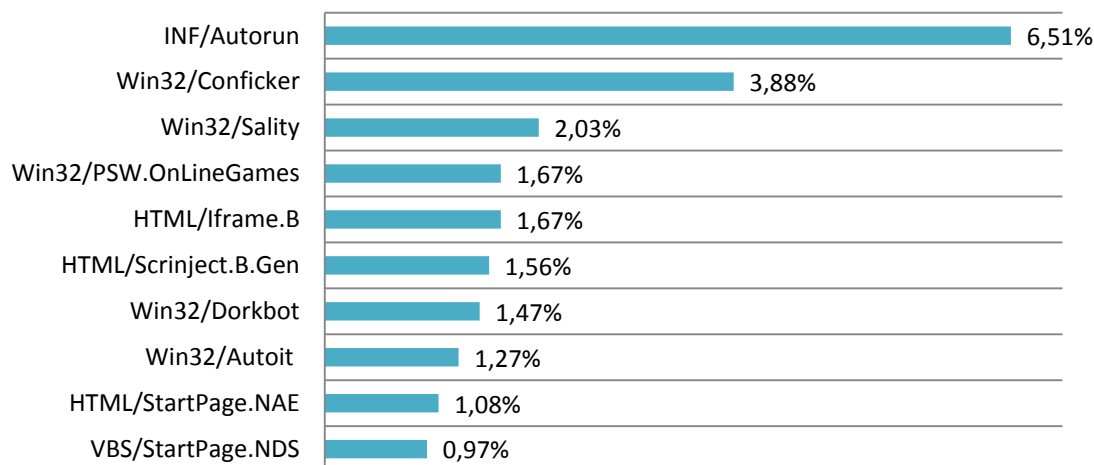
V mesecu juliju so bile v Evropi (5,27%) in globalno (6,51%) najpogostejše tiste iz družine INF/Autorun. Tudi drugo mesto je zasedel *oldtimer* – črv Win32/Conficker, ki je globalno predstavljal 3,88% vseh groženj (v Evropi 3,12%). Tretje mesto so iz prejšnjega meseca zadržale grožnje Win32/Sality (2,03% globalno), v Evropi pa so se na tretje mesto uvrstile grožnje HTML/IFrame.B.Gen (3,05%).

V družino INF/Autorun spadajo grožnje, ki za širjenje izkoriščajo datoteko autorun.inf. Ta vsebuje informacije o programih, ki se zaženejo, ko uporabnik v računalnik vključi izmenljivo napravo (najpogosteje so to USB ključki, zunanji trdi diski itn.). Protivirusni programi ESET takšne grožnje, ki ustvarjajo ali spreminjajo datoteko autorun.inf, prepoznajo s pomočjo hevrstike.

Win32/Conficker je omrežni črv, ki za širjenje izrablja varnostno luknjo v operacijskih sistemih Windows. Nekatere različice črva se lahko širijo tudi s pomočjo nezaščitenih skupnih map ali z izmenljivimi mediji, s pomočjo samodejnega zagona (Autorun), ki je v nekaterih starejših operacijskih sistemih Windows omogočens privzetimi nastavitvami (v Windows 7 temu ni tako). Win32/Sality je polimorfična grožnja, ki na okuženem računalniku ustvari in zažene novo zlonamerno storitev ter ustvarja in briše vnose v registru, ki so povezani z varnostjo. Poskrbi tudi, da se zlonamerni proces na računalniku zažene ob vsakem zagonu operacijskega sistema.

Win32/Dorkbot je z 1,47% med prvo deseterico groženj novinec, najpogostejši pa je v Južni Ameriki in Karibih. Gre za črva, ki se širi s pomočjo izmenljivih medijev. Črv vključuje tudi stranska vrata, ki avtorjem omogoča oddaljen dostop do okuženega računalnika. Črv zbira prijavnne podatke (uporabniška imena in gesla) za določene spletne strani, ki jih nato pošlje na oddaljen računalnik. Novinec med deseterico je tudi VBS/StartPage.NDS (0,97%), trojanski konj, ki v nekaterih spletnih brskalnikih spreminja nastavitve za domačo stran.

Globalne grožnje v mesecu juliju 2011, ESET ThreatSense.Net®

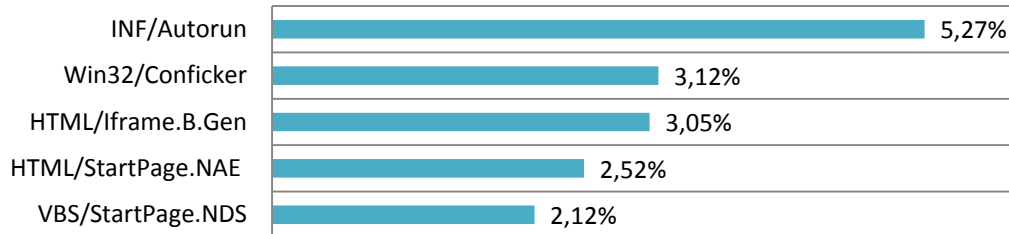


Grožnje v območju EMEA (Evropa, Bližnji vzhod in Afrika)

INF/Autorun je med najpogostejšimi grožnjami v Evropi stalnica. Gre za najbolj razširjeno grožnjo v Španiji (4,09%), Ukrajini (5,67%), Izraelu (5,95%) in Južni Afriki (10,12%). Statistika kaže, da je drugo mesto v Evropi zasedel črv Win32/Conficker (3,12%), ki je bil najdejavnejši v Bolgariji (8,12%) in Španiji (3,11%).

Tretje mesto v Evropi so predstavljale grožnje iz družine HTML/Iframe.B, ki so prevladovali v Rusiji (6,88%), na Norveškem (4,83%), Danskem (6,46%), Švedskem (7,44%) in Finskem (7,57%).

Najpogostejše grožnje v Evropi, ESET ThreatSense.Net® (julij 2011)



ThreatSense.Net®

Tehnologija ThreatSense.Net® zbira anonimne statistične informacije o grožnjah na računalnikih svojih uporabnikov. Zahvaljujoč tem informacijam lahko ESET-ovi razvijalci in analitiki spremljajo natančne in pomembne informacije o najpogostejših grožnjah in smernicah razvoja novih groženj. Grožnje, ki so prepoznane s heuristično tehnologijo, lahko razvijalci tako preučijo v realnem času in zanje pripravijo posodobitve takoj, še preden se lahko škodljiva koda razširi tudi globalno ali pa mutira v več različic.

ESET

Podjetje je bilo ustanovljeno leta 1992 in je že od samega nastanka usmerjeno v razvoj varnostnih rešitev. ESETovi produkti so že od vsega začetka ocenjeni kot eni od najboljših protivirusnih rešitev na trgu. Zaradi svoje tehnološke dovršenosti so bili že večkrat nagrajeni kot najučinkovitejši, najnatančnejši in najhitrejši protivirusni programi. Podjetje ima sedež v Bratislavi, svoje pisarne pa imajo še v Bristolu, Buenos Airesu, Pragi, San Diegu, s svojimi partnerji pa so prisotni v več kot 180 državah po celem svetu.

SI SPLET

SI SPLET d.o.o. je podjetje, ki se ukvarja s trženjem varnostnih in drugih rešitev na področju informacijskih tehnologij. V letu 2002 si je podjetje pridobilo ekskluzivno partnerstvo s podjetjem ESET za distribucijo varnostnih rešitev ESET v Sloveniji.

www.sisplet.com