

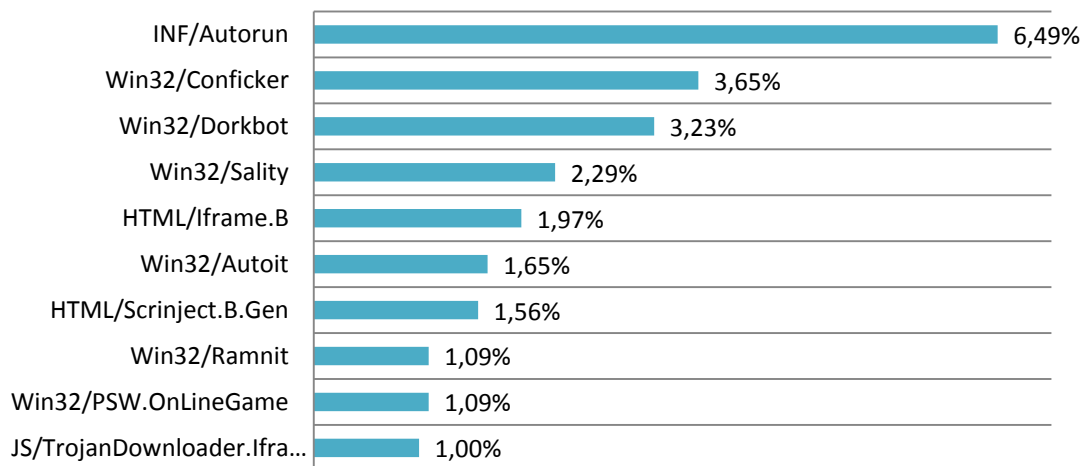
Septembrske grožnje: PDF trojanski konji na Mac OS X; Glavna grožnja so izmenljivi mediji

Septembra se je škodljiva koda iz družine INF/Autorun zopet izkazala kot vodilna grožnja v svetu, saj je predstavljal kar 6,49 odstotka vseh groženj, medtem ko je v Evropi predstavljal 5,42 odstotka vseh groženj. Na drugo mesto se je uvrstil črv Win32/Conficker z 3,65 odstotka groženj na globalni ravni, v Evropi pa je dosegel 3,40 odstotka vseh groženj. Statistika nastaja na podlagi ESET Live Grid® tehnologije v oblaku, ki zbira podatke o škodljivih kodah in grožnjah. Podatke o teh grožnjah ESET Live Grid® pridobiva od uporabnikov ESET zaščitne tehnologije iz celega sveta.

INF/Autorun je ime ki označuje vrsto škodljivih programov, ki izkoriščajo datoteko autorun.inf, kot način okužbe računalnika. Ta datoteka vsebuje informacije o programih, ki se samodejno zaženejo, ko se v računalnik vstavi izmenljiv medij (običajno USB naprava) in ko uporabnik dostopa do tega medija. Win32/Conficker je omrežni črv, ki prvenstveno izkorišča varnostne luknje v operacijskih sistemih Windows. V svojih različicah se ta črv lahko širi preko nezavarovanih map v skupni rabi ali izmenljivih medijev. Pri starejših operacijskih sistemih Windows (razen Windows 7) za širjenje uporabi funkcijo samodejnega zagona (autorun), ki je običajno omogočena kot privzeta nastavitvev.

Win32/Dorkbot je relativno nova grožnja, ki se pojavlja v zadnjih mesecih, vendar pa vztrajno narašča število okuženih računalnikov s to škodljivo kodo, ki se tako pomika navzgor po lestvici najbolj pogostih groženj. Trenutno je na globalni ravni dosegel 3,23 odstotka vseh groženj in je trenutno na tretjem mestu. Ta računalniški črv je posebno razširjen v Latinski Ameriki in na območju Karibov, kjer dosega kar 10,14 odstotka vseh groženj. Tudi Win32/Dorkbot se večinoma širi preko izmenljivih medijev in vsebuje kodo, ki omogoča nadzor okuženega računalnika na daljavo. Zbira tudi uporabniška imena in gesla za dostop do določenih spletni strani, ki jih nato posreduje na oddaljene računalnike kiberkriminalcev. Seveda se uporabnik ob tem ne zaveda, da se njegovi podatki na okuženem računalniku posredujejo tretjim osebam.

Globalne grožnje, ki jih je zaznala ESET Live Grid® tehnologija (september 2011)



Septembra 2011 se je pojavila tudi nova grožnja, ki napada uporabnike Mac OS X, v obliki trojanskega konja, ki cilja predvsem na uporabnike Macintosh v kitajskem jeziku. Ta grožnja v obliki trojanskega konja se uporabniku predstavi kot PDF dokument, kateri vsebuje članek o dolgoletnem mednarodnem sporu glede otočja Diaoyu v kitajskem jeziku. Ko uporabnik odpre okuženo »PDF« datoteko, se prične nameščanje škodljive kode, hkrati pa se dejansko odpre PDF z omenjeno zgodbo. Ko je namestitev škodljive kode končana, le ta omogoča napadalcem oddaljeni dostop do okuženega računalnika. Napadi te vrste so pogosti na Windows platformah, sedaj pa se pojavljajo tudi na Mac platformah.

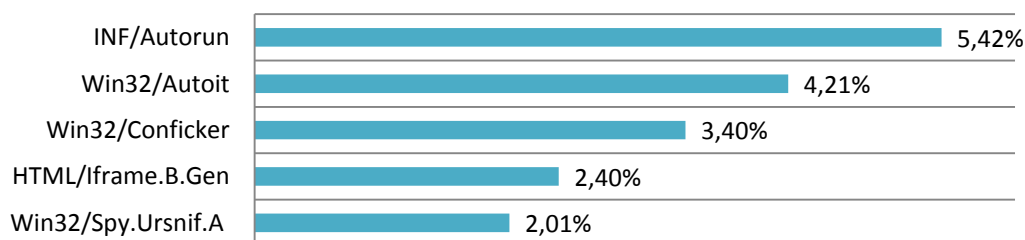
Primeri dobre prakse za zmanjšanje možnosti okužbe:

- Nikoli ne odpirajte datotek pripetih v elektronskih sporočilih, ki jih niste pričakovali in ne prihajajo od zaupanja vrednega pošiljatelja.
- Datoteke s spleta prenašajte le iz zaupanja vrednih in uglednih spletnih strani.
- Uporabljajte protivirusno zaščito na vseh vaših napravah.

Evropa, Bljižnji vzhod, Afrika

INF/Autorun še vedno ostaja najbolj razširjena grožnja v Evropi. Zaseda prvo mesto med grožnjami tako v Evropi, bližnjevzhodnih, ter afriških državah, kot so Južna Afrika z 10,15 odstotka vseh groženj, Ukrajina 5,47, Izrael 3,70 in Španija 3,70 odstotka vseh groženj. V Turčiji je prevladovala grožnja Win32/Autoit z 13,30 odstotki. Win32/Conficker je bil ponovno najhitreje rastoča grožnja v Bolgariji s 6,53 odstotki, medtem, ko se Win32/Dorkbot pojavlja med prvimi petimi grožnjami v številnih evropskih državah, vključno z Ukrajino, kjer je predstavljal 2,50 odstotka vseh groženj.

Grožnje v Evropi, ki jih je zaznala ESET Live Grid® tehnologija (september 2011)



O Live Grid®

ESET Live Grid® tehnologija v oblaku, je nova metoda pregledovanja in zgodnje zaznave globalnih groženj na podlagi podatkov ESET-ovih uporabnikov po celem svetu. Vedno sveže informacije, ki prihajajo od uporabnikov, omogočajo strokovnjakom v laboratorijih ESET odziv v realnem času. Natančna analiza groženj, smeri napada in uporabljeni vzorci napada, služijo ESET-u, da lahko z uporabo hevrstike in posodobitev poskrbijo za zaščito uporabnikov pred grožnjami jutrišnjega dne.

O 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. Za več informacij obiščite www.eset.com ali pokličite +1 (619) 876-5400.

O SI S P L E T

Podjetje 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. Več na www.sisplet.com.