

Oktobrske grožnje: Nove grožnje za Mac OS X; v vrhu še vedno grožnje preko izmenljivih medijev

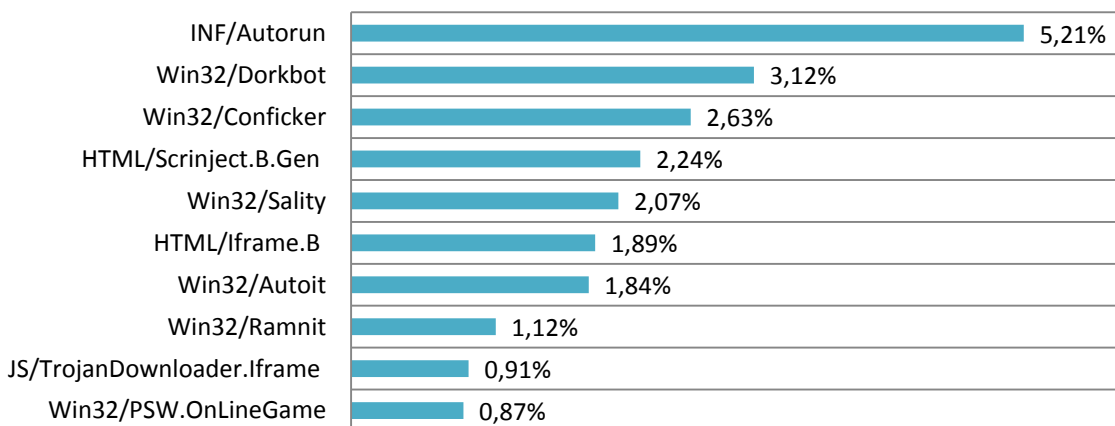
V mesecu oktobru je ESETova ekipa raziskovalcev odkrila novo grožnjo, ki je bila ustvarjena za Linux platforme, sedaj pa lahko okuži tudi Mac OS X platforme. Ta škodljiva koda je modifikacija kode Linux/Tsunami in je trenutno znana pod imenom OSX/Tsunami.A. Med ostalimi grožnjami sta tako v Evropi kot globalno v vrhu dve starejši škodljivi kodi, in sicer INF/Autorun in Win32/Conficker. Na svetovni lestvici groženj pa se je Win32/Dorkbot povzpел na drugo mesto s 3,12 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.

Trojanski konj, ki napada Mac OS X, poimenovan Tsunami, omogoča nadzor nad okuženimi računalniki preko IRC kanalov in strežnikov. Okuženi računalniki so nato uporabljeni v porazdeljenih napadih za zavrnitev storitev (Distributed Denial of Service). Avtorji lahko skozi stranska vrata, ki jih trojanski konj Tsunami odpre, namestijo tudi posodobitve za svojo škodljivo kodo ali druge zlonamerne programe. S tem pa lahko napadalci v celoti prevzamejo kontrolo nad okuženim računalnikom.

“Dva vzorca enake škodljive kode, ki se razlikujeta v malenkostih, sta bila zaznana na različnih koncih sveta. ESETovi telemetrični podatki kažejo, da je zaenkrat število okuženih računalnikov nizko, kar nakazuje na to, da je trojanski konj še v fazi preizkušanja. Ta grožnja zaenkrat ni kompleksna ali sofisticirana, zato je možnost okužbe za Mac uporabnike omejena”, opozarja Pierre-Marc Bureau, višji raziskovalec na ESET-u.

Že več mesecev zapored grožnje preko izmenljivih medijev predstavljajo najvišji odstotek vseh groženj in tudi mesec oktober ni bil nobena izjema. INF/Autorun še vedno vodi na globalni ravni s 5,21 odstotkov ter v Evropi s 4,30 odstotkov vseh groženj. INF/Autorun je ime, ki označuje vrsto škodljivih programov, ki izkoriščajo datoteko autorun.inf kot način okužbe računalnika. Win32/Conficker je bil globalno gledano na tretjem mestu z 2,63 odstotki in četrti v Evropi z 1,99 odstotki vseh groženj. Win32/Conficker je omrežni črv, ki prvenstveno izkorišča varnostne luknje v operacijskih sistemih Windows. Win32/Dorkbot se počasi vzpenja po lestvici škodljivih programov in je že globalna številka dve s 3,12 odstotka vseh groženj. Tudi Win32/Dorkbot se širi preko izmenljivih medijev, napadalcem pa omogoča nadzor nad okuženimi računalniki. Prav tako zbira uporabniška imena in gesla, ki jih uporabnik vpisuje na določene spletne strani, nato pa vse zbrane podatke pošlje na oddaljen računalnik.

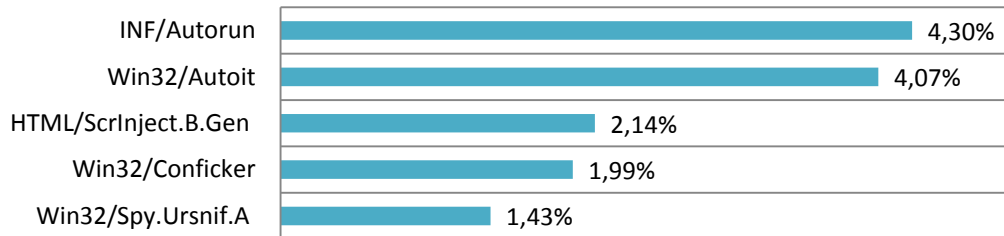
Globalne grožnje, ki jih je zaznala ESET Live Grid® tehnologija (oktober 2011)



Evropa, Bližnji vzhod, Afrika

INF/Autorun še vedno ostaja najbolj razširjena grožnja v Evropi. Zaseda prvo mesto med grožnjami v Evropi, Bližnjem vzhodu in Afriki, v državah kot so Južna Afrika (8,33%), Izrael (4,92%) in Ukrajina (3,76%). Win32/Conficker je bil ponovno najhitreje rastoča grožnja v Bolgariji s 5,15 odstotki. Evropska številka dve je tokrat Win32/Autoit, še posebno v zadnjih mesecih je bil njegov porast viden v Turčiji, saj trenutno tam zaseda prvo mesto z neverjetnimi 14,57 odstotki. Na tretje mesto pa se je v uvrstil HTML/ScrInject.B.Gen, ki se je pojavil v vrhu številnih zahodnoevropskih državah, vključno s Švedsko 6,93 odstotka, Norveško 5,85, Finsko 5,42, Veliko Britanijo 4,63, Francijo 2,96 in Španjijo z 1,82 odstotka vseh groženj.

Grožnje v Evropi, ki jih je zaznala ESET Live Grid® tehnologija (oktober 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.

ESET prejel rekordno sedemdeseto nagrado VB100

Neodvisna organizacija Virus Bulletin je ESET-u podelila prestižno nagrado VB100. To je za ESET že sedemdeseta tovrstna nagrada, kar je med razvijalci protivirusnih rešitev absolutni rekord.

Pri Virus Bulletin so zapisali: *“ESET naša testiranja še naprej opravlja brez težav. Grafični vmesnik programa je atraktiven in preprost za uporabo, napredne možnosti programa pa ponujajo natančno nastavljanje vseh funkcij. Delovanje programa je gladko in stabilno, brez neprijetnih presenečenj ali težav.”*

“Ponosni smo, da je protivirusna tehnologija ESET NOD32 osvojila več zaporednih Virus Bulletin nagrad VB100, kot katerakoli druga rešitev. Zahvaljujoč naši talentirani skupini razvijalcev in raziskovalcev, ESET ostaja pri neverjetnem rekordu, saj od začetka testiranj v maju 1998, še nikoli ni izpustil črva ali virusa »In-the-Wild“, je dodal ESET-ov varnostni analitik Jan Vrabec.

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 SPLET

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