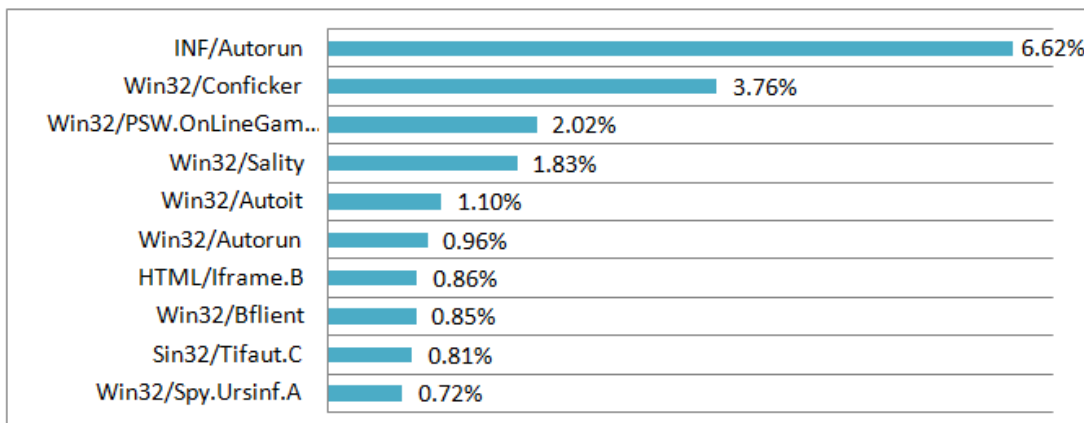


Izrabljanje novic o Libiji in Osami bin Ladnu; med škodljivo kodo prevladoval INF/Autorun

Smrt Osame bin Ladna je še vedno aktualna tema na številnih blogih in v socialnih medijih, spletni iskalniki pa neprestano obdelujejo terabajte podatkov z govoricami, namigovanji in teorijami zarot, ki se širijo s svetlobno hitrostjo. V nekaj zadnjih tednih se je povečalo tudi število prevarantskih, takoimenovanih nigerijskih sporočil, ki izrabljajo trenutno stanje v Libiji. Po statističnih podatkih, ki jih zbira tehnologija ThreatSense.Net, so aprila prevladovale grožnje INF/Autorun (6,62 %), na drugem mestu je bil črv Win32/Conficker (3,76 %), tretje pa so zasedle grožnje iz družine Win32/PSW.OnLineGames (2,02 %).

Deset globalno najpogostejših groženj, ESET ThreatSense.Net® (april 2011)



Množično iskanje fotografij in video posnetkov po objavi novice o smrti Osame bin Ladna so s pridom izkoriščali tudi kiberkriminalci. S tehnikami optimizacije svojih nevarnih spletnih strani (Black Hat SEO) so povzročili, da je veliko število radovednih uporabnikov spletnih iskalnikov pristalo prav na njihovih straneh. "Takšne zlonamerne tehnike optimizacije so postale nekaj povsem običajnega. So zelo avtomatizirane, ogromno število iskanj pa je tokrat sprožilo pravi val širjenja prevar in škodljivih programov," poroča Aryeh Goretsky, ESETov raziskovalec.

"Globalne grožnje se širijo na račun zatona globalnega terorizma, pri ESETu pa opažamo podobne trende tudi na Facebooku. Razlaga za to je povsem preprosta. S petsto milijoni aktivnih uporabnikov bi Facebook, če bi bil država, med največjimi zasedel visoko tretje mesto, takoj za Kitajsko in Indijo," dodaja Goretsky. Kiberkriminalci izrabljajo socialni inženiring, s katerim pretentajo varnostne mehanizme Facebooka za zaščito pred škodljivo kodo JavaScript, saj uporabniki kopirajo in prilepijo spletne naslove kar neposredno v naslovne vrstice svojih brskalnikov.

Veliko navdiha so kiberkriminalci v zadnjih tednih našli tudi pri vojni v Libiji. ESETovi raziskovalci poročajo o porastu števila nigerijskih sporočil z različnimi prevarami, ki vsako leto naivne uporabnike po celem svetu stanejo milijarde dolarjev. Po poročilu spletne strani 419hell.com, kjer obdelujejo in raziskujejo takšna pisma, nigerijskim prevaram uporabniki nasedejo vsakih 44 sekund.

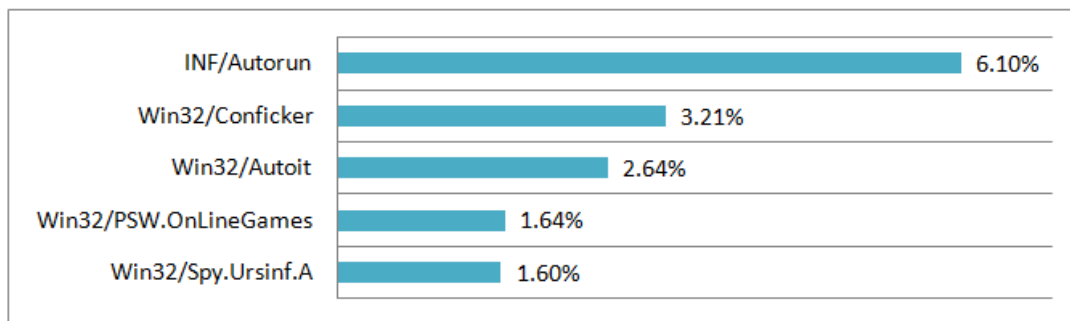
Grožnje v območju EMEA (Evropa, Bližnji vzhod in Afrika)

Med evropsko statistiko najpogostejših groženj se je pojavil novinec, Win/Autoit. Gre za računalniškega črva, ki za širjenje izrablja predvsem izmenljive medije, nekatere različice pa se širijo tudi s programi za neposredno sporočanje. Prenese se lahko tudi iz okuženih spletnih strani ali pa ga namesti druga škodljiva koda, s katero je računalnik že okužen. Črv na okužene računalnike prenese še svoje druge različice ali pa računalnik okuži še z drugo škodljivo kodo. Z 8,13 % vseh groženj je bil najpogostejši v Turčiji.

Najpogostejšo grožnjo v Evropi so aprila predstavljale grožnje INF/Autorun. Sem spada široka paleta nevarnih programov, ki za širjenje izrabljajo datoteko autorun.inf. Najpogostejše so v Južni Afriki (11,13 %), Ukrajini (6,25 %), Izraelu (6,25 %), na Hrvaškem (5,68 %), v Avstriji (4,68 %), na Madžarskem (4,38 %), v Italiji (4,11 %) in Belgiji (4,0 %). V Sloveniji so te grožnje predstavljale 2,75 % vse škodljive kode.

Črv Win32/Conficker je aprila zasedel drugo mesto, najdejavnejši pa je bil v Bolgariji, kjer je predstavljal 7,72 % vseh groženj. Grožnje iz družine Win32/PSW.OnLineGames so zasedle tretje mesto. Sem spadajo trojanski konji, ki za širjenje uporabljajo ribarjenje (phishing), namenjeni pa so predvsem igralcem računalniških iger. Najpogostejši so bili na Poljskem, kjer so predstavljali 5,7 % vseh groženj.

Najpogostejše grožnje v Evropi, ESET ThreatSense.Net® (april 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 hevristično 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.