

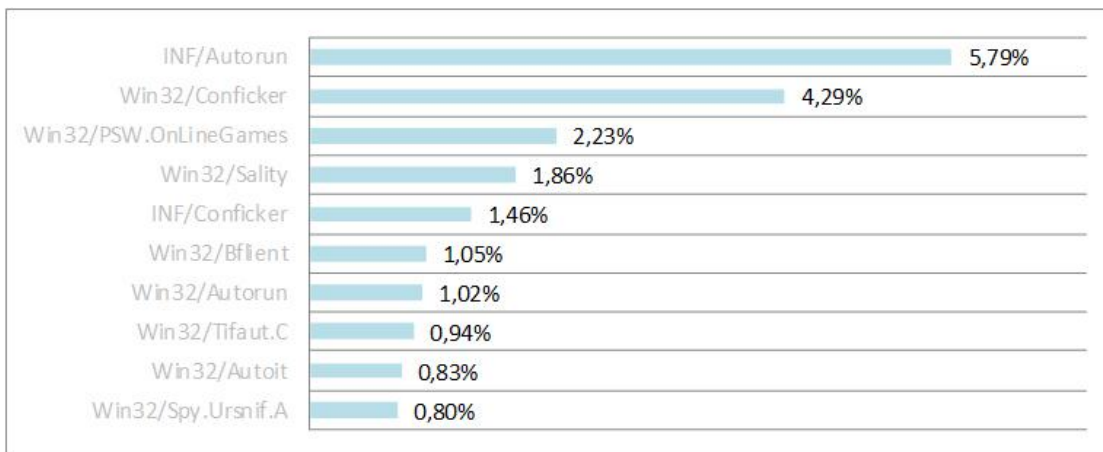
## Grožnje v marcu: kiberkriminalci izrabljali katastrofo na Japonskem; med škodljivo kodo prevladovala INF/Autorun in Win32/Conficker

INF/Autorun je po statističnih podatkih, ki jih zbira tehnologija ThreatSense.Net, marca znova zasedel prvo mesto med najpogostejšimi grožnjami. Predstavljal je kar 5,79 odstotka vse zabeležene škodljive kode. Drugi najpogostejši je bil črv Win32/Conficker, tretji pa trojanski konji iz družine Win32/PSW.OnLineGames.

ESET-ovi strokovnjaki so analizirali tudi izrabljanje katastrofe na Japonskem, ki so jo z željo po zaslužku izvajali kiberkriminalci. S tehnikami optimizacije za spletne iskalnike (Black Hat Search Engine Optimization) in s pomočjo socialnega inženiringa so računalnike nepredvidnih in (pre)radovednih uporabnikov ob iskanju novic o potresu in tsunamiju okužili z lažno protivirusno programsko opremo. Spodaj je nekaj osnovnih priporočil iz ESET-a:

- Uporabniki naj se v socialnih omrežjih in e-pošti izogibajo klikanju na povezave s senzacionalnimi naslovi "shocking news", "shocking video" ipd.
- Novicam sledite na uradnih spletnih straneh medijskih hiš, ki jim zaupate.
- Nikoli ne pošiljajte denarja dobrotelnim ustanovam, ki jih ne poznate.
- Če se vam ob kliku na naslov spletne strani odpre pojavno okno, ki vas opozarja na to, da je vaš računalnik okužen, bodite previdni.

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



Po podatkih ThreatSense.Net je v marcu prevladovala škodljiva koda iz družine INF/Autorun. Gre za celo vrsto groženj, ki za širjenje in okužbo računalnikov izrabljajo datoteko autorun.inf. Ta datoteka vsebuje informacije o programih, ki se zaženejo, ko uporabnik v računalnik vključi izmenljivo napravo (najpogosteje so to USB ključki). Na drugem mestu se je znašel omrežni črv Win32/Conficker, ki za širjenje izrablja varnostne luknje v operacijskih sistemih Windows, na tretjem mestu pa so bile grožnje iz družine Win32/PSW.OnLineGames. Sem spadajo trojanski konji, ki za širjenje uporabljajo ribarjenje (phishing), namenjeni pa so predvsem igralcem računalniških iger. Ti trojanski konji pogosto vključujejo korenski komplet (rootkit) in sposobnost beleženja pritisnjenih tipk na okuženem računalniku.

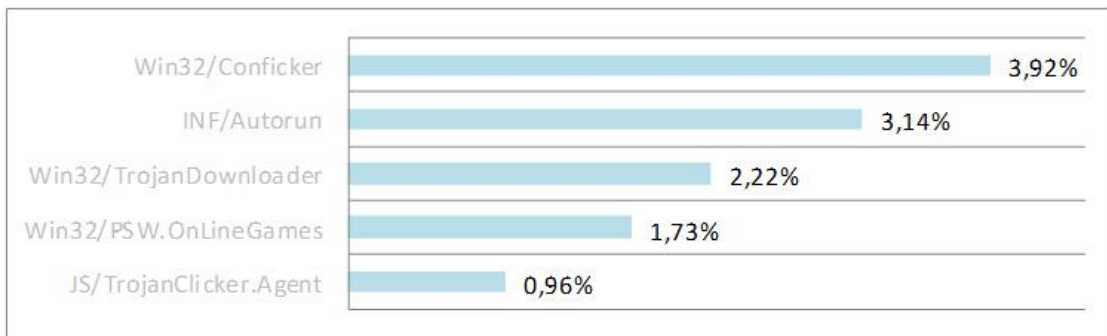
#### Grožnje v območju EMEA (Evropa, Bližnji vzhod in Afrika)

Črv Win32/Conficker je marca znova povzročal preglavice v večini držav iz območja EMEA. Iz drugega mesta v februarju se je tokrat povzpel na prvo, predstavljal je 3,92 odstotka vseh groženj. Najpogostejši je bil v Bolgariji (9,18%), Ukrajini (5,15%), na Madžarskem (4,30%) in v Španiji (3,64%). V Sloveniji je med grožnjami z 2,79 odstotka zasedel tretje mesto.

Druga najpogostejša grožnja v regiji je bila škodljiva koda iz družine INF/Autorun. V Izraelu je INF/Autorun predstavljal kar 7,73 odstotka vseh groženj, pogost pa je bil tudi v Romuniji (5,97%). V Sloveniji so te grožnje zasedle prvo mesto, predstavljale so 3,19 odstotka vseh groženj pri nas.

JS/TrojanClicker.Agent je zasedel peto mesto, najpogostejši pa je bil na Švedskem (2,33%), v Franciji (3,86%) in Nemčiji (1,83%). Trojanski konj JS/TrojanClicker.Agent na okuženih računalnikih simulira klike na reklamne oglase in tako svojim avtorjem prinaša dobiček.

#### Najpogostejše grožnje v Evropi, ESET ThreatSense.Net® (marec 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.

[www.sisplet.com](http://www.sisplet.com)