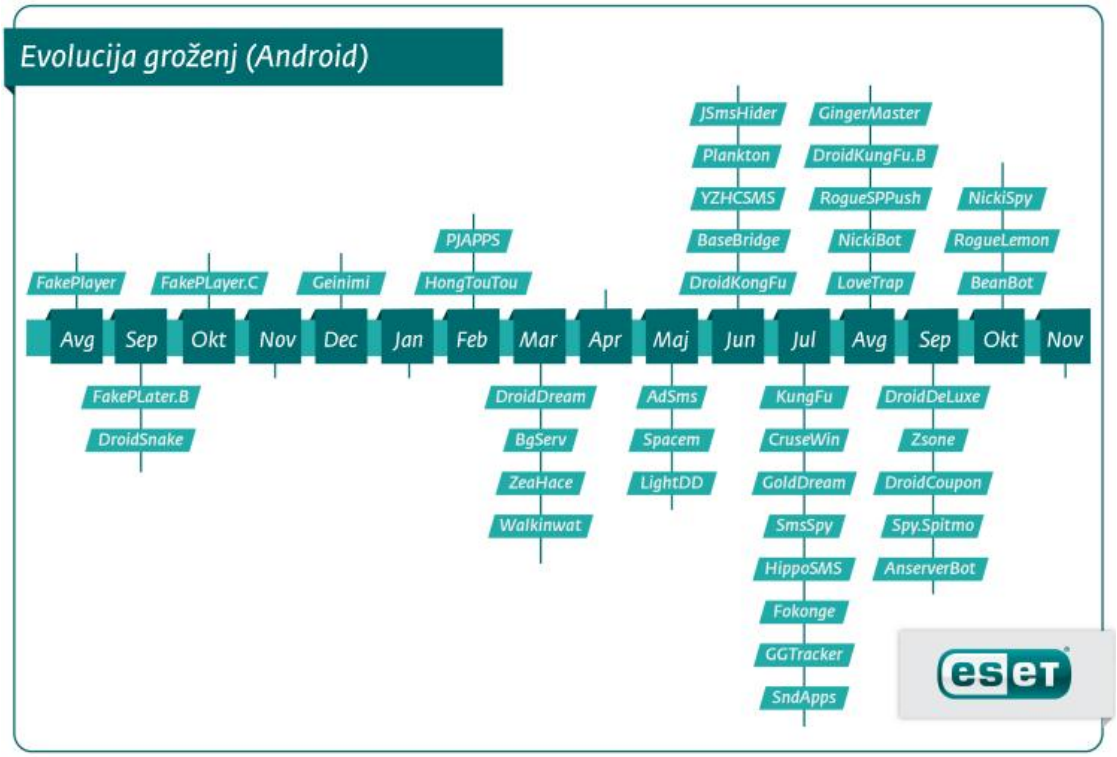
Predvidevanja za 2012: več groženj za pametne telefone in več lokaliziranih napadov

Navade uporabnikov in način uporabe tehnologij narekujejo trende razvoja novih škodljivih programov. V prihodnjem letu lahko zato pričakujemo prevlado groženj za pametne telefone. To so tiste mobilne naprave, s katerimi se lahko povezujemo na splet, dostopamo do elektronske pošte, družimo v socialnih omrežjih in s katerimi lahko opravljamo tudi elektronsko bančništvo. Teh naprav je po svetu že več kot pet milijard.

Med operacijskimi sistemi, ki jih pametni telefoni poganjajo, prevladuje Android s 43 odstotnim tržnim deležem. V letu 2012 lahko za omenjeni operacijski sistem pričakujemo povsem nove grožnje in nove različice že znanih groženj. Spodnja slika prikazuje evolucijo 41-ih škodljivih programov za platformo Android:



Zgornja časovnica se začne v avgustu 2010, ko je bil odkrit FakePlayer, prvi trojanski konj za platforme Android. Med avgustom 2010 in novembrom 2011 je bilo za omenjeno platformo odkritih 41 resnih groženj. Na sliki lahko opazimo tudi, da je bilo kar 65 odstotkov groženj odkritih v zadnjih petih mesecih, kar nakazuje trend za leto 2012. Poleg tega analiza groženj odkriva tudi:

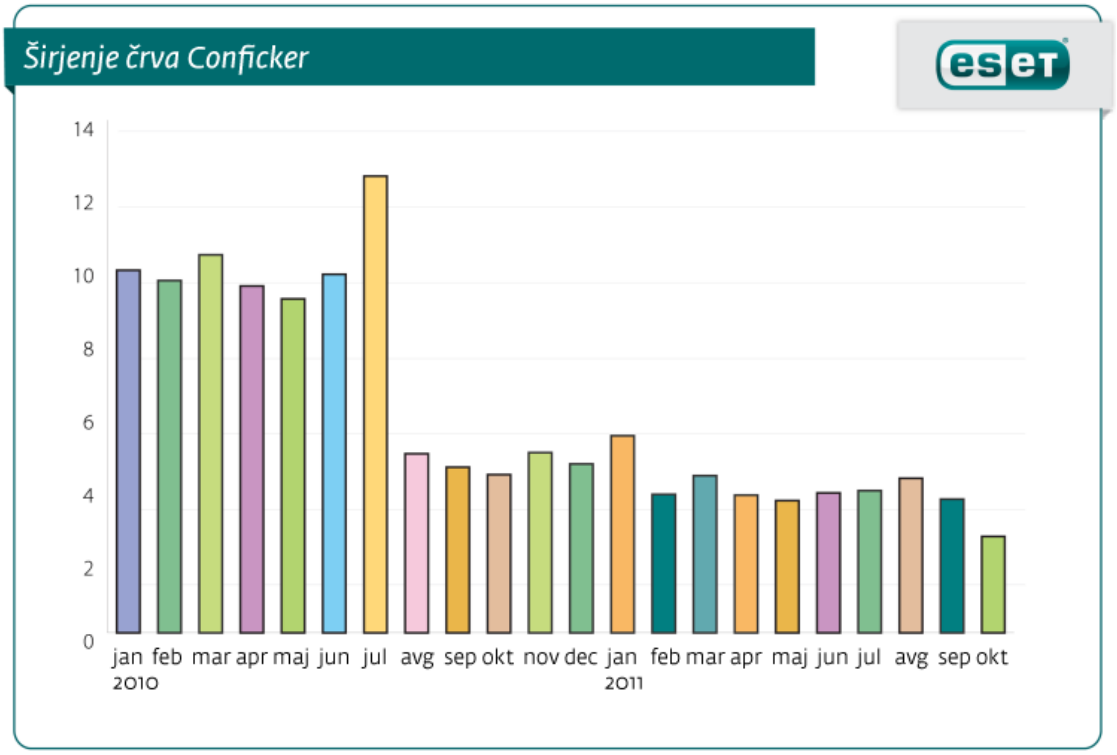
- 30 odstotkov groženj je bilo možno prenesti z Android Marketa,
- 37 odstotkov predstavljajo SMS trojanski konji,
- 60 odstotkov škodljive kode ima karakteristike botnetov, ki napadalcem omogoča oddaljen nadzor nad okuženo napravo.

Poleg groženj za pametne telefone lahko v letu 2012 pričakujemo še:

1. Do konca prihodnjega leta bo Windows 7 z 42 odstotki tržnega deleža postal najbolj razširjen operacijski sistem na svetu (statistika analitske hiše Gartner). S prvega mesta bo končno padel Windows XP, kar bo zagotovo prineslo določene spremembe pri načinu pisanja in širjenja novih groženj. Novejši operacijski sistem ima naprednejše varnostne mehanizme, kar pomeni, da so tudi grožnje za ta operacijski sistem tehnološko bolj napredne, da se lahko izognejo varnostnim mehanizmom. Predvidimo lahko razvoj bolj kompleksnih škodljivih programov, ki bodo usmerjeni v operacijske sisteme, kot sta Windows 7 in Windows 8. To velja tudi za 64-bitne operacijske sisteme.

2. Pričakujemo lahko več lokaliziranih napadov. Kiberkriminalci znajo izrabiti lokalne incidente v svojo korist, največkrat s pomočjo socialnega inženiringa. Pri nas lahko pričakujemo še več ribarskih napadov (phishinga), s katerimi želijo napadalci pridobiti uporabniške podatke za prijavo v spletne banke.

3. Ena od posledic migracije uporabnikov z Windows XP na Windows 7 bo verjetno tudi zaton računalniškega črva Conficker. Ta je izbruhnil novembra 2009 in hitro postal najbolj znan črv v zadnjih letih, saj se med najbolj pogoste grožnje po celem svetu uvršča že kar tri leta. Tehnologija ESET Live Grid že kaže, da se delež Confickerja opazno zmanjšuje:



4. Pričakujemo lahko tudi več hektivizma - spletnih napadov, ki imajo namesto finančnih namenov bolj ideološko noto. Podjetja in organizacije bodo morale poleg zaščite pred klasičnimi kiber grožnjami razmišljati tudi o zaščiti pred skupinami, kot so Anonymous in ideološko motiviranimi napadi. Podjetja in vladne ustanove bodo morala razmisliti tudi o zmanjšanju možnosti za izgubo in odtekanje podatkov.

Svet škodljivih programov je bil v zadnjih letih relativno stabilen. Spremljali smo lahko predvsem črve in trojanske konje, ki so se širili s pomočjo elektronske pošte in socialnih omrežij. Njihov glavni cilj je bil kraja podatkov. Danes lahko v mobilnem svetu in na novih platformah spremljamo občutno večji nabor škodljive kode. Nove naprave prinašajo nove navade uporabnikov in nove tarče za kiberkriminalce. Pametni telefoni vključujejo vrsto zaupnih podatkov, uporabljajo pa se za opravila, ki smo jih lahko do nedavnega opravljali le z osebnimi računalniki. Kraja podatkov na pametnih telefonih ne predstavlja le seznama telefonskih številk iz adresarja, ampak tudi zaupnih datotek, zasebnih slik ali celo gesla za različne storitve.

To odpira vrata za nove načine širjenja škodljivih programov, kjer imajo pametni telefoni velik pomen. Uporabniki se moramo zavedati vrednosti informacij, ki jih vsak dan prenašamo na svojih mobilnih napravah, hkrati pa ne smemo zanemariti groženj za osebne računalnike. Vse to ne napoveduje vsesplošne migracije groženj na pametne telefone, prikazuje pa pomembne spremembe v svetu kiberkriminala in škodljivih programov.