G Data press release 2012

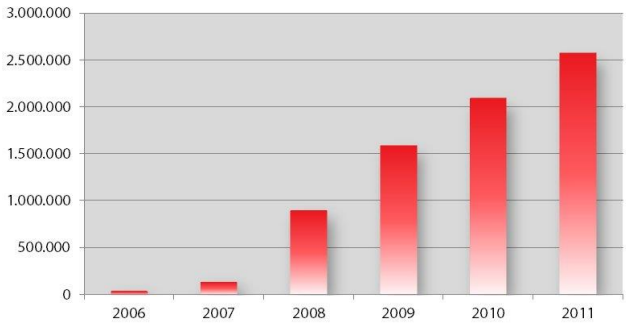
Infractorii cibernetici vizeaza smartphone-urile si online banking-ul

G Data publica raportul despre amenintarile curente de pe Internet

Bucuresti (Romania), 5 martie 2012 – Infractorii cibernetici si-au relocat activitatea pe utilizatorii de Internet mobil – aceasta este avertizarea rezultata din cel mai recent raport malware G Data. Analiza G Data Security Labs a aratat ca numarul de tulpini noi de malware a crescut de 2,5 ori, doar in a doua jumatate a anului 2011. Accentul a fost pus in special pe sistemul de operare Android, unde atacurile au crescut de 8 ori in aceeasi perioada. Analiza arata, de asemenea, ca intervalele de distributie de malware concepute pentru a ataca clientii de online banking sunt foarte scurte. Cu fiecare varianta mai noua şi cu cicluri de viaţă medii de 27 ore, autorii de malware încerca să eludeze mecanismele de apărare reactive din software-ul antivirus. Anul trecut, G Data a inregistrat un numar record de mai mult de 2,5 milioane de tulpini noi de programe malware – si nu exista semne ca fluxul de malware sa scada nici in 2012.

"Infractorii online ataca intotdeauna acolo unde este mai profitabil. De aceea nu este o surpriza ca autorii de malware se concentreaza tot mai mult pe telefoane inteligente si tablete PC, de vreme ce doar un numar mic de utilizatori isi protejeaza propriile dispozitive. Asta face ca atacurile infractorilor sa aiba succes, fara un efort prea mare, in a fura date personale sau informatii confidentiale ale companiilor," explica Ralf Benzmüller, Director al G Data Security Labs. "Noi am vazut deja un trend periculos al troienilor bancari. Ciclul de viata al acestui tip de malware a fost scurtat drastic ajungand in prezent la o medie de 27 de ore. Majoritatea producatorilor de antivirus sunt in imposibilitatea de a furniza o semnatura corespunzatoare intr-un interval de timp atat de scurt. Datorita tehnologiei BankGuard, noi suntem singurii provideri capabili sa dezvoltam o semnatura independenta in timp real impotriva acestui tip de malware si care poate, asadar, sa protejeze eficient clientii de online banking de aceste riscuri."

Fluxul de malware in cifre



Pe parcursul anului trecut, G Data Security Labs a contabilizat un total de 2.575 de milioane de tulpini malware noi. Doar in a doua jumatate a anului au fost detectate 1.330.146 de noi programe daunatoare. Comparat cu anul anterior, malware-ul a crescut cu 23%. Troienii sunt in

continuare categoria predominanta. Expertii G Data au vazut o crestere acuta a numarului de programe adware si spyware.

Mobile malware inca in crestere

Infractorii isi indreapta in continuare atentia asupra smartphone-urilor si a tabletelor PC cu sistem de operare Android. Numarul programelor malware din 2011, comparativ cu 2010, a crescut de mai bine de 10 ori. Atacatorii folosesc variante de apps-uri malware care au fost deja raspandite la fel de mult ca si copiile manipulate ale unor aplicatii inofensive. Acestia trimit mesaje text catre numere de telefon cu supratAxa, vizeaza datele personale ale utilizatorilor si creeaza conturi pe numele acestora pentru servicii premium.

In plus, hackerii activisti au descoperit aceste dispozitive mobile ca pe instrumente prin care sa raspandeasca mesaje motivate politic si alte informatii. De exemplu, troianul Android.Trojan.Arspam.A trimite postari de pe forumuri cu topicul Orientul Mijlociu catre toate contactele din agenda.

In trecut, apps-urile periculoase puteau deveni active doar in anumite tari. In prezent, infractorii trebuie sa opereze doar cateva schimbari minore pentru a activa programele malware mobile in numeroase tari.

Infractorii cibernetici targeteaza online banking

Online banking este un serviciu popular pe care tot mai multe persoane il adopta. Asemenea multor alte servicii, odata cu cresterea popularitatii, acesta a devenit mai atragator pentru infractori. Acestia folosesc troieni bancari pentru a manipula tranzactiile obisnuite, ca de exemplu, transferul unei sume de bani dintr-un cont in altul.

In concordanta cu analiza facuta de G Data Security Labs, sunt doar cateva familii de troieni bancari, dar acestea sunt de obicei baza pentru crearea constanta de noi variante de tulpini cu durata de viata cat mai scurta. Cel mai des folosit troian este Sinowal, care este caracterizat prin schimbarea frecventa a mecanismelor de infectare, printre altele.

Familii de troieni bancari in a doua jumatate a anului 2011