



G Data press release 2014

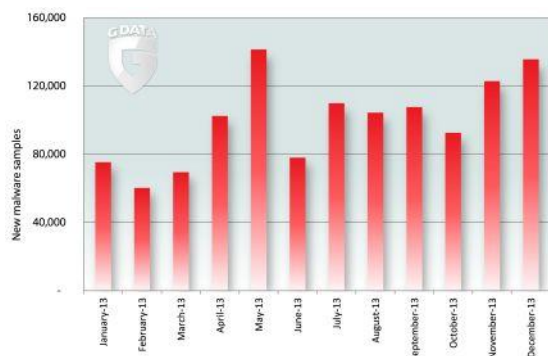
Indicator malware de Android: G Data a inregistrat aproape 1.2 milioane de noi programe malware in 2013 Furnizorul german de securitate IT a publicat Mobile MalwareReport

Bucuresti (Romania) 24.02.2014

Conform unei cercetari de piata realizate de Gartner, peste 877 de milioane de smartphone-uri si tablete cu Android au fost vandute anul trecut. Numarul programelor noi de malware a crescut exponential, in cea de-a doua jumatate a anului trecut, la aproape 673.000. Totalul noilor programe malware pe intreg anul a atins un nou record de 1.2 milioane. Atacatorii s-au axat pe troieni pentru a fura si vinde datele profitabile. O alta tendinta a criminalitatii informatice s-a bazat pe programele potential nedorite. Acestea nu sunt aplicatii malware conventionale, dar pot afisa reclame nedorite si pot spiona utilizatorii. G Data crede ca utilizarea acestor multiplatforme va creste in viitor, iar monedele digitale, precum Bitcoin, vor fi vizate de atacatori. Pe langa toate acestea, fraudarea cu mesaje SMS cu suprataxa este in declin datorita mecanismelor de securitate incluse in cele mai noi versiuni de Android. Raportul G Data Mobile Malware este disponibil online.

"G Data a inregistrat un nou record negativ in 2013, 1.2 milioane de programe malware de Android. Industria infractiunii informatice se bazeaza foarte mult pe sustragerea de date personale ce pot fi valorificate profitabil pe pietele dedicate," explica Eddy Willems, G Data Security Evangelist. Nu exista nicio sansa pentru expert de a da un verdict clar pentru acest an. "Din perspectiva atacatorilor, 2014 este anul furturilor de date, de vreme ce fraudarea ce implica mesaje SMS cu costuri ridicate nu mai este profitabila ca urmare a mecanismelor de securitate instalate in sistemele de operare Android, incepand cu 4.2. Asta inseamna ca atacurile cross-platform si monedele digitale vor avea un interes crescut pentru infractorii din sectorul mobil."

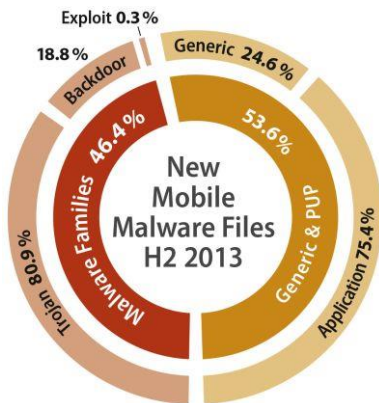
672.940 tulpini noi de malware de Android in cea de-a doua jumatate a anului 2013





Numarul programelor noi a crescut cu 30% in comparatie cu prima jumatate a anului 2013, inregistrand un nou record. Infractorii au atins un alt record negativ, cu un total de 1.199.758 de aplicatii malware noi – o crestere de 460 de procente comparativ cu intreg anul 2012.

Troienii continua sa domine



Opt din zece aplicatii malware clasificate in familiile malware sunt troieni. Acestea sunt folosite de infractori cu scopul de a sustrage date personale si de a le transforma in bani pe pietele dedicate.

O alta problema majora o reprezinta programele potential nedorite (PUP), care reprezinta mai mult de jumatate din programele malware contorizate in a doua jumatate a anului 2013. "PUP" includ aplicatii care nu sunt neaparat rau intentionate, dar includ in mod evident functii de spionaj si de afisare de publicitate nedorita. De regula, sunt foarte greu

de indepartat.

Trei previziuni pentru prima jumatate a anului in curs

- Programele malware bazate pe trimiteri de SMS continua sa fie in scadere: Frauda ce implica mesajele SMS trimise catre numere premium va continua sa scada, deoarece sistemele de operare Android contin, incepand cu versiunea 4.2, un mecanism de securitate special. Infractorii se vor reprofila, in special, pe furtul de date personale.

- Bitcoin si celelalte monede virtuale vor fi vizate: Acest tip de monede au devenit tot mai populare printre clientii si vanzatorii de pe Internet. Monedele sunt exclusiv digitale, ceea ce le face extrem de vulnerabile. G Data estimeaza ca infractorii vor folosi programele malware pentru a fura sumele de Bitcoin si alte monede digitale, direct de pe telefoane inteligente si tablete.

- Frecventa ridicata a atacurilor multiplatforma: Dispozitivele mobile sunt folosite tot mai des pentru operatiuni de online banking, efectuat printr-un proces mTAN, ce securizeaza tranzactiile de plata, spre exemplu. Infractorii vor continua sa se concentreze pe interceptarea acestor operatiuni, prin atacuri si programe malware multiplatforma.

-###-