G Data press release 2012

Infractorii online vizeaza Android

G Data arata de ce sistemele de operare sunt atat de ademenitoare pentru infractorii cibernetici

Bucuresti (Romania), 11 iunie 2012 – Eddy Willems, Security Evangelist pentru G Data, semneaza un red paper intitulat „Targeting Android – a casual analysis“, in care investigheaza motivele pentru care sistemul Android are parte de cele mai multe atacuri.

Smartphone-urile si tabletele PC cu sistem de operare Android sunt foarte populare, nu doar printre utilizatori, ci si printre infractori cibernetici. Ei exploateaza dispozitivele mobile ce utilizeaza sistemul de operare dezvoltat de Google, pentru a prejudicia utilizatorii. De ce oare atacatorii isi concentreaza atacurile asupra sistemelor de operare Android si nu asupra Symbian sau iOS? G Data Security Evangelist, Eddy Willems, incearca sa raspunda la aceste intrebari in red paper-ul intitulat "Targeting Android - a causal analysis". Acesta a tras concluzia ca sistemul mobil de operare este aproape ideal, o tinta profitabila pentru infractori datorita celor 3 factori critici pentru tranzactiile infractionale: motiv, mijloace materiale si oportunitati. Popularitatea dispozitivelor cu Android este un motiv puternic pentru infractori de a folosi aplicatii malware pentru a fura date si bani. Intrucat aplicatiile nu sunt verificate inainte de a fi publicate in Google Play, acestea reprezinta o ideala oportunitate de atac pentru infractori.

"Pentru cyberinfractori, Android este o tinta aproape perfecta - pentru ca este relativ usor sa atace smartphone-urile si tabletele PC - sa fure datele personale ale utilizatorilor si sa obtina fraudulos sume de bani," explica Willems. "In general, Android nu este un sistem de operare nesigur, dar, pentru atacatori, efortul cerut pentru gasirea vulnerabilitatilor si dezvoltarea malware-ului ce poate fi distribuit prin intermediul aplicatiilor manipulate merita osteneala. In continuare, utilizatorii trebuie sa confirme autorizarile solicitate inainte de instalarea aplicatiilor, dar viitorul ar putea aduce aplicatii daunatoare care sa faca posibila ocolirea acestor piedici. Aceasta ar face ca numarul atacurilor reusite sa fie in crestere."

Trei factori care fac dispozitivele mobile cu Android populare printre infractori

Motivul

Android este in prezent larg raspandit ca sistem de operare mobil. Conform analizei IDC, in cel de-al treilea trimestru din 2011, aproape 53% dintre toate smartphone-urile vandute, au fost cele cu versiuni ale sistemului de operare dezvoltat de Google. Symbian a fost pe locul doi, urmat pe locul trei de Apple. Acesta este un motiv important pentru infractori de a dezvolta malware pentru dispozitive cu Android, care permite accesul la o larga audienta, de a initia atacuri asupra utilizatorilor si de a sustrage bani sau date personale.

Aceasta situatie este similara cu sistemele de operare Windows. Cea mai mare parte a programelor malware este programata pentru Windows datorita popularitatii uriase a sistemelor de operare Microsoft, care permit atacatorilor sa atinga cea mai mare productivitate.

Aplicatii ca mijloace materiale pentru atacatori
Android ofera infractorilor un mijloc foarte simplu de raspandire a malware-ului mobil: apps (aplicatiile mobile). Strategiile folosite pentru reusita includ distributii noi de versiuni manipulate ale apps-urilor de succes si oferte aparent inofensive si folositoare pe pietele Android, inclusiv pe Google Play. In aceasta categorie intra si DoridDream Trojan, care a fost descarcat de peste 250.000 de ori, in toata lumea, in doar cateva zile.

"Ingineriile sociale fac posibila prezentarea acestor programe intr-un mod atractiv, asftel incat utilizatorii se ofera sa le descarce benevol si sa le instaleze," noteaza Eddy Willems.

In contrast cu Android, candidatul promitator anterior, Symbian, nu a mai oferit suficiente mijloace care sa fie exploatate de infractori. Atacurile via Bluetooth au fost posibile, doar ca necesita o prea mare apropiere fizica de dispozitivul tinta pentru a activa interfata. Aceasta a limitat numarul persoanelor care ar fi putut deveni victime, astfel incat extinderea acestor metode au devenit neatractive.

Oportunitate
La fel ca si Android, Apple ofera utilizatorilor sai diferite apps-uri. Ca si Symbian, platforma iOS nu a fost o tinta predilecta pentru infractori deoarece Apple efectua o verificare amanuntita a tuturor aplicatiilor inainte de a fi publicate in app store. In plus, spre deosebire de Android, iOS nu este un sistem de operare semi-open source. O mare parte a codului sursa al sistemului de operare al Google este accesibil publicului, ceea ce face sa fie semnificativ mai simplu pentru atacatori sa descopere si sa exploateze vulnerabilitatile.

Un alt motiv pentru care este atat de simplu pentru infractori sa foloseasca apps-uri malware se datoreaza faptului ca pot da un numar nelimitat de autorizari. De exemplu, o aplicatie aparent inofensiva, gen lanterna, poate initia apeluri si citi datele de localizare GPS. Daca utilizatorii vor sa-si instaleze aceasta aplicatie pe un smartphone sau pe o tableta PC trebuie sa confirme autorizatiile la fel ca pe orice alta autorizare solicitata. Android nu furnizeaza nicio optiune pentru a acorda autorizari specifice individuale. Odata ce aplicatia a fost instalata, lucrurile devin foarte simple pentru infractori, deoarece malware-ul poate descarca orice alt malware care sa fie implementat in dispozitivul deja vizat.

-###-