



G Data press release 2012

Aplicatia G Data protejeaza impotriva vulnerabilitatii USSD

Furnizorul german de securitate ofera utilizatorilor afectati o aplicatie gratuita



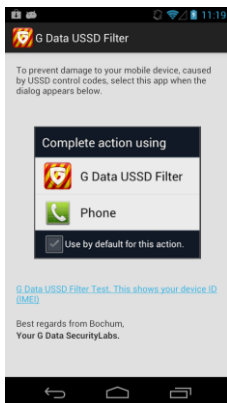
Bucuresti (Romania) 01.10.2012 – G Data furnizeaza utilizatorilor de smartphone-uri cu sistem de operare Android o aplicatie gratuita de protectie impotriva posibilelor consecinte ale vulnerabilitatii USSD. Filtrul USSD G Data intercepteaza toate URL-urile "tel:" si le verifica de codurile USSD corespunzatoare, ce pot fi manipulate pentru a sterge datele de pe dispozitive de la distanta. Aplicatia este disponibila gratuit in magazinul Google Play.

Unde gasiti URL-urile "tel:"?

Multe pagini web, ca de exemplu, directoare web de tipul agende online, contin aceste URL-uri practice. Daca utilizatorii dau click pe link-ul corespunzator, telefonul initiaza automat o convorbire telefonica. Vulnerabilitatea USSD existenta permite infractorilor cibernetici sa exploateze URL-urile "tel:" manipulate, cu scopul de a avaria si de a afecta dispozitivele. De exemplu, este posibil sa stearga intreaga memorie interna a telefonului.

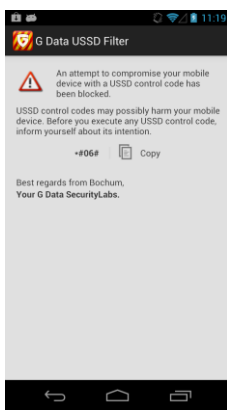
Cum functioneaza filtrul USSD G Data

Acesta poate inregistra anumite tipuri de URL-uri pe dispozitive cu Android. De exemplu, tipul de URL "tel:" permite apeluri din browser sau din aplicatie. Filtrul USSD G Data consemneaza aceste URL-uri specifice si le controleaza continutul.



Cand aplicatia este folosita pentru prima data, utilizatorul trebuie sa selecteze manual filtrul. Activarea se desfasoara in modul urmatoar: utilizatorul da click pur si simplu pe un URL "tel:" in browserul smartphone-ului sau, alternativ, initiaza apelul din URL-ul de test integrat.

Procedand astfel, utilizatorii ar trebui sa seteze checkmark-ul pentru "Use as default for this operation" in caseta de selectie aparuta si apoi selecteaza filtrul USSD G Data.



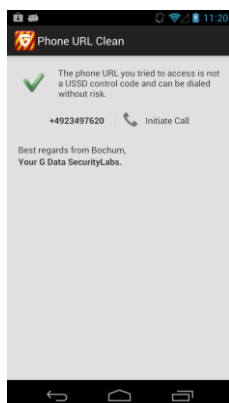
Filtrul USSD va intercepta apoi toate URL-urile telefonice de pe smartphone-urile cu Android si verifica daca acestea contin coduri USSD.

Daca "service number-ul" accesat contine un cod USSD, o pagina blocata apare, si astfel, selectarea codului de control este prevenita.

Poate totusi utilizatorul sa apeleze un numar blocat?



Da, daca utilizatorul vrea totusi sa sune pe un numar blocat, poate folosi butonul "Copy" pentru a copia numarul pe clipboard si apoi il lanseaza in aplicatia telefonului sau. Oricum, aplicatia avertizeaza impotriva executarii codului USSD.



Daca URL-ul contine un numar de telefon obisnuit, utilizatorul poate da click pe icoana aparuta si astfel, poate initia apelul.

Poate aplicatia sterge sau afecta alte aplicatii?

Nu, aplicatia actioneaza ca un filtru. Nicio data stocata in dispozitiv nu este modificata sau stearsa. Dispozitivul de blocare USSD G Data asigura ca aceste numere de servicii (cu coduri USSD) sa nu poata fi executate direct si astfel sa previna orice fel de exploatare a vulnerabilitatii.

Link-ul de pe care se poate descarca filtrul USSD G Data:

<https://play.google.com/store/apps/details?id=de.gdata.labs.telurlblocker>

-###-