G Data press release 2014

G DATA USB KEYBOARD GUARD – protectie fiabila impotriva dispozitivelor USB manipulate

Instrumentul gratuit pus la dispozitia utilizatorilor de expertii germani previne atacurile ce folosesc tastaturi USB.

Bucuresti (Romania) 10.09.2014

Programele malware ce infecteaza computerele atunci cand un stick USB manipulat este conectat, sunt des intalnite de mai multi ani. Cercetatorii de la Berlin Security Research Labs (SRLabs) au descoperit o metoda noua de infectare, nedescoperita pana acum. Noul scenariu de atac a fost demonstrat la conferinta Black Hat USA 2014 din Las Vegas de la inceputul lunii august: firmware-ul unui dispozitiv USB poate fi schimbat astfel incat, la conectare, sa poata pretinde a fi orice alt tip de dispozitiv. Un stick USB aparent inofensiv se poate conecta la sistem drept tastatura si poate introduce in secret linii de comanda periculoase in interfata PowerShell. Astfel, atacatorul poate sa preia controlul asupra sistemului infectat. Aceasta metoda de atac este posibila deoarece dispozitivele USB, precum imprimantele, camerele foto sau stick-urile USB sunt considerate, in general, a fi sigure si astfel au acces complet la sistem. Expertii in securitate de la G DATA au dezvoltat un tool gratuit numit G DATA USB KEYBOARD GUARD, destinat protectiei impotriva dispozitivelor USB manipulate.

Consecintele potentiale ale acestei noi forme de atac pot fi extrem de grave, desi nu exista date concrete despre un atac efectiv, pana in acest moment. Totusi, sunt concepute atacuri mai putin evidente bazate pe conexiunile USB. "In cazul in care firmware-ul este suprascris, orice dispozitiv USB se poate transforma intr-o potentiala sursa de pericol. In cel mai rau caz, pot fi creati virusi care se raspandesc prin USB," avertizeaza despre gravitatea situatiei Ralf Benzmuller, sef al G DATA SecurityLabs. Cel mai eficient mod de executie al acestor atacuri este folosirea tastaturilor USB. Daca cineva are posibilitatea de a utiliza comenzile unei tastaturi pentru a deschide o linie de comanda intr-o interfata precum PowerShell, poate detine controlul complet al computerului si poate scrie comenzi. Acestea sunt imposibil de distins de actiunile legitime ale unei tastaturi reale si nu sunt inregistrate de catre mecanismele de securitate incluse in solutiile antivirus.

Prevenirea accesului la o noua tastatura
G DATA a raspuns imediat la aceasta si a dezvoltat tool-ul G DATA USB KEYBOARD GUARD. Acesta ofera protectie impotriva celor mai probabile forme de abuz ce pot fi folosite intr-un atac – dispozitive USB ce pretind a fi tastaturi. Cand un sistem detecteaza o noua tastatura, prima data este impiedicat accesul si este afisata o fereastra pop-up. Utilizatorul are astfel ragaz sa verifice este dispozitivul este intr-adevar o tastatura si poate permite sau bloca permanent accesul. Daca dispozitivul respectiv a fost manipulat (un stick USB sau o camera

web care a fost infectata cu un virus USB, de exemplu), accesul la dispozitiv poate fi blocat, prevenind astfel, in mod eficient, atacurile.

Sistemul de operare este in imposibilitatea de a distinge intre o intrare falsa sau una reala
Atacurile USB ce tintesc companiile sunt deosebit de grave, dar si utilizatorii casnici sunt expusi la risc. Luand in considerare ca aproape 100 milioane de stick-uri USB sunt in circulatie in Germania (sursa: Statista), acest risc trebuie tratat in mod serios. "Situatia in care un dispozitiv USB infectat este conectat la un computer este asemanatoare cu situatia in care un hacker se afla in fata acelui computer," evalueaza consecintele Ralf Benzmuller. "Sistemul de operare este incapabil sa distinga intre o intrare pretinsa a fi legitima si una reala. Cu G DATA USB KEYBOARD GUARD, noi va oferim cea mai eficienta protectie impotriva acestui gen de atacuri."

Instrumentul gratuit este independent de solutia antivirus instalata si este compatibil cu orice solutie antivirus de pe piata: www.gdatasoftware.com/usb-keyboard-guard

Cum se poate instala G DATA USB KEYBOARD GUARD:
Dupa ce sunt urmati pasii de instalare si dupa restartul solicitat, G DATA USB KEYBOARD GUARD ruleaza in background, iar sistemul este protejat. Cand sistemul detecteaza o tastatura noua, G DATA USB KEYBOARD GUARD o blocheaza si afiseaza un mesaj de avertizare. Utilizatorul poate decide ce e de facut cu noul dispozitiv detectat si poate alege dintre opțiunile "Allow keyboard" si "Block keyboard". G DATA USB KEYBOARD GUARD memoreaza decizia luata pentru un dispozitiv acceptat, astfel incat acesta nu va fi interogat de fiecare data cand este conectat.

Cerinte de sistem
Windows (32 bit / 64 bit): Windows 8.x / 8 / 7 / Vista, cel putin 1 GB RAM; (32 bit): Windows XP (minim SP2), cel putin 512 MB RAM