G Data press release 2015

Superfish: cazul Lenovo este doar varful aisbergului

G DATA SecurityLabs analizeaza un certificat de securitate dubios.

Bucuresti (Romania) 27.02.2015

Expertii in securitate de la G Data SecurityLabs au analizat adware-ul Superfish. In acest proces, analistii au intalnit o componenta de tehnologie in program, numita SSL Digestor. Acesta foloseste un certificat root care este slab securizat și are drepturi extinse pe calculator. SSL Digestor intercepteaza conexiuni HTTPS sigure si le poate descifra. In acest fel, conexiunile care sunt de fapt securizate ar putea fi interceptate si atacate. Acest lucru inseamna ca infractorii cibernetici ar putea folosi un atac man-in-the-middle pentru a spiona sau manipula fluxul de date dintre doi parteneri de comunicare, de exemplu o banca si clientul sau, prin utilizarea unui site bancar fals. Potrivit expertilor G DATA, aceasta parte din program este continuta si in alte produse software. Solutiile de securitate G Data detecteaza software-ul ca Gen: Variant.Adware.Superfish.1 (motor A) si Win32.Riskware.Fishbone.A (Engine B). Pentru a elimina certificatul periculos, utilizatorii trebuie sa ia masuri.

"Superfish este program adware discutabil. Cu toate acestea, din cauza certificatului slab securizat SSL Digestor, este periculos pentru utilizatori," explica Ralf Benzmuller, seful G DATA SecurityLabs. " Utilizatorii afectati ar trebui sa elimine imediat certificatul."

Ce este Superfish?
Programul Superfish Visual Discovery este livrat pre-instalat pe mai multe modele de notebook-uri Lenovo. Adware-ul a fost un oaspete nedorit de majoritatea utilizatorilor pentru o lunga perioada de timp, chiar daca, de multe ori aceasta nu este neaparat periculos. Superfish este, cu toate acestea, neobisnuit, deoarece contine o componenta de tehnologie numita SSL Digestor, distribuita de Komodia. Aceasta componenta contine un element care declanseaza problema de securitate actuala - un certificat root foarte slab securizat.

Superfish este utilizat chiar si pe dispozitive Android
Expertii G Data Security au descoperit doua aplicatii de cautare pentru dispozitive Android care se bazeaza pe Discovery Visual Superfish. Similar cu componenta PC, utilizatorilor le sunt

prezentate prin reclame anumite interogari de cautare. Cu toate acestea, aplicatiile nu se bazeaza pe SSL Digestor si nu pun in pericol securitatea protocolului HTTPS.

Tehnologia submineaza securitatea HTTPS
SSL Digestor instaleaza un certificat care permite programului sa analizeze si sa manipuleze fluxul de date in conexiunile HTTPS. Aceasta componenta este gasita in programe adware pe care utilizatorii le instaleaza involuntar si in programe clasificate a fi troieni de catre furnizorii de securitate IT. Chiar si programe aparent legitime se bazeaza pe aceasta componenta.

O verificare rapida prin care puteti afla dacă certificatul root este prezent pe computer se poate face aici:
https://www.gdatasoftware.com/securitylabs/quickcheck/fishbone?no_cache=1

Informatii detaliate, plus instructiuni cu privire la modul in care poate fi indepartat certificatul Superfish gasiti pe G DATA SecurityBlog: https://blog.gdatasoftware.com/blog/article/the-power-of-trust-superfish-case-turns-into-a-worst-case-scenario.html

-###-