Comunicat de presa G Data 2009

Retelele de transmisii de fisiere Google: bandele de gangsteri cibernetici infecteaza rezultatele cautarilor

Autorii de malware folosesc Google pentru a face contrabanda

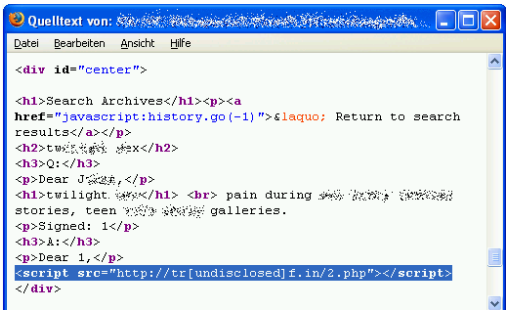
Bucuresti, 22 iunie 2009 - In ultimele zile G Data a observat atacuri la scara mare asupra utilizatorilor motorului de cautare Google. Procedura folosita de infractori este extrem de vicleana: inscrierea anumitor cereri de cautare conduce la rezultate cu link-uri manipulate. Daca navigatorul le acceseaza, la urmatorul pas un cod malitios este injectat din acel website care initiaza manevre de camuflaj foarte variate. Astfel, unii navigatori primesc un video codec, altii primesc oferte pentru program de antivirus falsificat. Conform studiilor efectuate de catre G DATA Security Labs, site-ul server-ului malware este in prezent in India. Prezentul val de atacuri este concentrat asupra utilizatorilor care cauta site-uri cu continut pornografic. Cu toate acestea, G DATA estimeaza ca in curand se va schimba directia atacurilor. Urmatorii care s-ar putea afla in „bataia pustii” pot fi fanii sporturilor, pasionatii de autoturisme sau chiar cei care cauta slujbe.

Ralf Benzmüller, manager G Data Security Labs: „In ultimile zile am observat o crestere semnificativa in rezultate periculoase ale cautarii Google. Aproximativ 10% din alarmele periculoase care sosesc au legatura directa sau indirecta cu rezultate manipulate ale cautarii Google. Prin acest val de atacuri este suficient un click fals din partea unui navigator pentru a cadea in plasa. PC-ul este protejat numai daca datele HTTP sunt verificate inainte de a fi afisate”.

Procedura utilizata de catre infractori: Atacatorii incearca sa introduca un cod malitios inlocuind text cu numere hexadecimale. Ca rezultat browser-ul poate procesa codul fara nici un fel de problema. Cu toate acestea, pentru oameni si motoare de cautare acest lucru este ilizibil. Prin aceasta procedura atacatorii se pot strecura printre filtrele Google. Codul hexadecimal contine cod HTML ascuns care este incorporat in rezultatul paginii web. Acesta este denumit „cross-site scripting”. Daca utilizatorul Google acceseaza rezultatul din cautare, atunci site-ul web dorit se va deschide, dar suplimentat de catre un script provenit de la un domeniu indian. Aparent Google foloseste continutul injectat in evaluarea termenilor cautarii. Link-urile manipulate sunt plasate de catre atacatori in blog-uri, forum-uri sau site-uri „hacked”, iar astfel se atinge un rating foarte bun pentru termenii cautati. Pentru

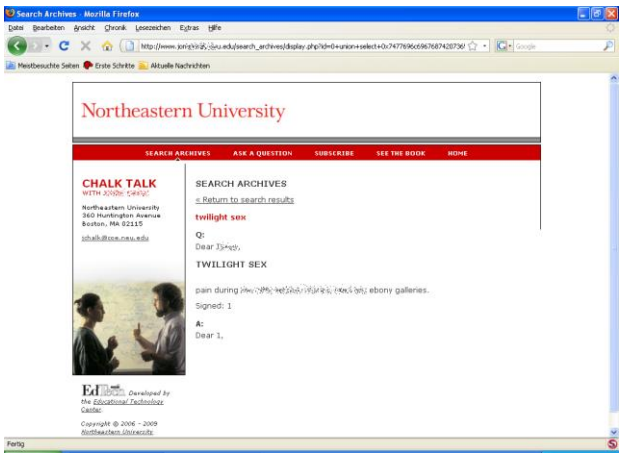
exemplificare, se pare ca un site putin accesat al unei universitati din Statele Unite a fost manipulat astfel incat anumiti termeni de cautare sa apara in topul rezultatelor cautarii.

Malware injectat:



Codul Script descarcat de pe site-ul indian este asemenea bine deghizat. Pagina web rezultata nu este produsa static de catre aceasta procedura, ci sunt o varietate de tipuri de infectii. In teste, expertii de la G DATA Security Labs au venit impotriva fisierelor flash infectate, codecurilor video aparente si a software-ului de antivirus falsificat. Cu toate acestea, intreaga varietate de inselatorii a avut acelasi rezultat – in final se descarca acelasi fisier malware.

Exemplu de website manipulat:



Masuri de protectie:
Clientii G Data erau protejati inca de la inceput impotriva acestei amenintari. Expertii de securitate din Bochum recomanda utilizatorilor Internet-ului, pentru protectia impotriva atacurilor similare:

1. **Intotdeauna sa mentineti sistemul de operare si soft-ul de antivirus actualizat**
2. **Asigurati-va ca protectia antivirus verifica continutul web, inainte de a ajunge la browser**
3. **Dezactivati Java Script din browser (exemplu: cu NoScript in Firefox)**
4. **Fara navigare cu drepturi de Administrator**