Comunicat de presa G Data 2010

G Data riposteaza impotriva bresei de securitate din Windows

Un nou hotfix este disponibil in mod gratuit

Bucuresti (Romania), 3 august 2010 – O importanta bresa de securitate legata de shortcut-urile produselor Microsoft Windows este in prezent exploatata de diverse tipuri de malware, acestea conducand la aparitia de noi variante, mai nocive, care exploateaza această vulnerabilitate. Asa cum comunicatele media au relatat, primelor abordari ale acestei vulnerabilitati nu au fost considerate a avea un interes sporit. Ca raspuns, specialistii G Data au dezvoltat un utilitar de securitate (hotfix), numit "G Data LNK Checker", ce blocheaza executarea automata a acestui tip de fisier malware si afiseaza icon-urile folosite regulat, care sunt considerate sigure. Utilizatorul este astfel protejat impotriva fisierelor periculoase de tip ".lnk file". Programul este disponibil in mod gratuit, putandu-se descarca de pe site-ul G Data.

"Aceasta recenta bresa de securitate ofera cyber-criminalilor o gama larga de noi posibilitati de a infecta un PC. Ei trebuie doar sa se asigure ca un fisier .lnk este afisat pe calculator. Fisierul malware, la care trimite link-ul, nu este neaparat amplasat pe calculator - acesta poate fi chiar si pe Internet", explica Ralf Benzmueller, sef al G Data Security Labs. "Nu numai utilizatorii de memory stick-uri sunt afectati. In reteaua IT a unei companii, de exemplu, este suficient sa se salveze un fisier infectat pe unitatile de stocare din retea. Chiar si software-ul de baza, cum ar fi programele de editare text si clientii de e-mail, pot oferi posibilitatea de a afisa comenzile rapide (shortcuts). De aceea, potentialul de a exploata acest tip de vulnerabilitate este enorm. Ne asteptam ca aceasta bresa de securitate sa fie exploatata masiv in scurt timp."

Mai multe despre "G Data LNK Checker":
Specialistii G Data au dezvoltat hotfix-ul "G Data LNK Checker" dupa o analiza detaliata a scenariului dispus de acesta bresa de securitate. "G Data LNK Checker" functioneaza independent fata de suita de securitate antivirus deja instalata pe calculator si o completeaza cu o protectie generica impotriva executarii automate a malware-ului prin intermediul fisierelor de tip .lnk (shortcut). Dupa instalare, "G Data LNK Checker" monitorizeaza crearea shortcut-urilor si impiedica executarea automata a codului daunator la aparitia acestora. Mecanismul de malware este folosit doar in anumite cazuri, de exemplu, icon-urile folosite pentru a vizualiza elemente de control ale sistemului.

Daca printre icon-urile aflate in mod curent pe desktop apar si shortcut-uri ce contin mecanismul de malware, acest lucru este detectat si o pictograma rosie ce reprezinta un semnal de avertizare este afisat (imaginea alaturata).
Atentie: Exista posibilitatea ca aplicatii considerate sigure, sa fie exploatate de acest recent mecanism maltios. Daca utilizatorul decide totusi sa dea "dublu-click" pe un fisier .lnk (shortcut) care este marcat ca fiind periculos de

catre aplicatie, este nevoie de un antivirus de calitate.

Dupa ce Microsoft va remedia aceasta bresa de securitate printr-un patch disponibil in actualizarile sistemului de operare, iar utilizatorul va descarca si instala respectiva actualizare, programul "G Data LNK Checker" poate fi dezinstalat ca oricare alt software. "G Data LNK Checker" este destinat pentru toate sistemele de operare Windows, chiar si pentru Windows XP, in ambele versiuni 32-bit si 64-bit. Utilizatorii de Windows XP cu service pack 2 se pot considera protejati cu "G Data LNK Checker", chiar daca pentru acest sistem de operare suportul oficial Microsoft s-a incheiat recent.

Alte informatii:
Fiecare PC pe care ruleaza un sistem de operare de tip Windows are comenzi rapide (shortcuts) pe desktop-ul sau. Acest lucru ofera acces de tip "one-click" pentru cele mai importante programe si fisiere. Aceasta functie utila este utilizata repetat, in mod abuziv, de acest tip de malware, la fel ca in acest caz recent in care Microsoft a recunoscut "0-day-exploit" cu privire la toate versiunile noi ale Windows. In acest caz, mecanismul pentru afisarea pictogramelor este exploatat executand secventa de malware si castigand, in cele din urma, controlul asupra PC-ul. Ajunge ca utilizatorul sa afiseze shortcut-ul, de exemplu, in Internet Explorer, pe desktop sau in cadrul unei aplicatii.

Microsoft a reactionat imediat si a lansat o propunere de solutie (hotfix), care rezolva problema in sine, dar aceasta duce la faptul ca toate comenzile rapide (shortcuts) isi pierd icon-ul. Acest lucru este imposibil in practica si nu reprezinta o solutie satisfacatoare pentru remedierea problemei. "G Data LNK Checker" rezolva aceasta problema.

-###-