Comunicat de presa

Website-uri care “pulverizeaza” virusi: riscul de infectare pandeste peste tot

Operatorii de website-uri reactioneaza lent atunci cand se confrunta cu infectari de malware

Bucuresti (Romania), 16 Octombrie 2009 – Atentie la riscul de a fi virusati: programele malware nu stau ascunse doar in “colturile intunecate” ale Internetului! Producatorul german al software-ului de securitate G Data acorda o deosebita atentie tendintei malware-ului de a se instala automat prin 'drive-by download' fara ca utilizatorul sa isi dea seama. Ingrijorator este ca acest fenomen se intampla din ce in ce mai des pe site-uri respectabile. Cum reactioneaza operatorii site-urilor in cauza? G Data a testat si contactat furnizorii de servere care au distribuit involuntar cantitati mari de malware. Concluzia controversata: 45% din webmasteri au avut nevoie de cateva saptamani pentru a indeparta distributia de malware, in cel mai bun caz.

Ca parte a Malware Information Initiative, G Data a acordat o deosebita atentie raspandirii soft-urilor malware pe Internet, in ultimele luni. Cresterea popularitatii acestei metode de distribuire a maleware-ului este evidenta datorita faptului ca e-mail-ul este principala sursa de raspandire. Deci, cum reusesc hackerii sa profite de site-uri renumite in scopuri personale? Ralf Benzmüller, director al G Data Security Labs, explica principalele trei metode folosite de infractori:

“Infractorii cibernetici, care distribuie malware prin intermediul site-urilor web deturnate, se folosesc de cele trei mari slabiciuni: accesul la servere este adesea securizat folosind parole slabe ca “admin123”. Acestea pot fi sparte in cateva secunde folosind asa-zisul “dictionar-de-atacuri” care ruleaza automat”, spune Ralf Benzmüller.

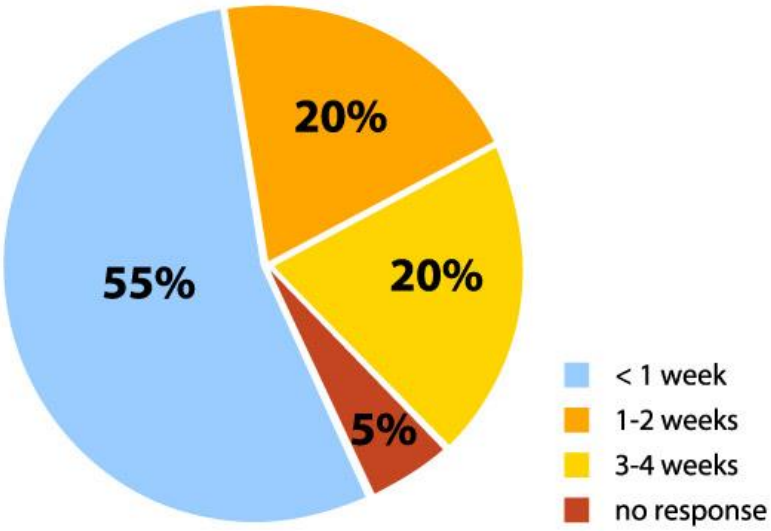
Dar nu doar parolele slabe faciliteaza deturnarea site-urilor de catre infractori. Adesea sunt exploatate punctele slabe care contin programe server de web, care sunt utilizate pentru a rula de exemplu, magazine online, sisteme de management sau bloguri si forum-uri. "Acestea ruleaza frecvent în configuratii standard sau prezinta numeroase brese de securitate cauzate de actualizarile insuficiente. Interogari speciale de pe motoarele de cautare pot fi utilizate pentru a localiza computere vulnerabile foarte repede, apoi în mod automat le atacă şi le preia. Acest lucru face deosebit de important pentru operatorii de servere Web sa efectueze actualizari de software regulate. Intrarile nefiltrate de utilizator, de exemplu, sub forma unor site-uri, sa prevada un alt gateway care poate fi folosit pentru atacuri cross site scripting sau SQL injections. Din pacate, o serie de module de filtrare ofera protectie insuficienta iar atacatorii au tot mai mult succes in utilizarea acestei metode pentru injectarea malware-ului in site-urile web".

Parolele slabe, bresele de securitate din software-ul serverului si filtrele inadecvate ale intrarilor folosite de utilizator sunt doar cateva dintre modurile in care operatorii activeaza sau face mai usoara calea infractorilor in a ataca site-urile web.

In ciuda avertismentului, nici un raspuns dupa trei saptamani!

Multi utilizatori de PC-uri au devenit in mod clar constienti de pericolele care "pandesc" pe Internet. Cu toate acestea ei presupun ca atacurile nu vor veni din partea site-urilor companiilor de renume precum: hoteluri, grupuri de actiuni sau comunitati web. Facand parte din G Data Malware Information Initiative, expertii inca lucreaza la serverele de web din aceste sectoare de distribuire a malware-ului. Pentru ca aceste centre de infectie sa ramana inofensive, G Data contacteaza regulat operatorii responsabili. Experienta specialistului german in securitate variaza foarte mult. Cea mai mare ingrijorare este reactia lenta a celor responsabili: din 100 de operatori de site-uri web pe care G Data i-a contactat cu privire la aceste cercetari, doar 55 au reactionat in mai putin de o saptamana.

Timpul de reactie a operatorilor de site-uri:



"De indata ce descoperim malware-ul pe un site, le spunem celor responsabili despre opţiunile pe care le oferim, pentru a opri raspandirea malware-ului in cel mai scurt timp posibil. Dar, in multe cazuri putem raporta ca raspunsurile acestora au fost extrem de lente sau inexistente", continua Benzmuller. "Ne dorim ca tot mai multi operatori de site-uri sa aiba responsabilitate fata de utilizatorii site-ului pe care il administreaza. Toti cei care nu vor sa aiba de-a face cu manevrele infractorilor ar trebui sa verifice serverul in mod regulat si, daca este necesar, sa raspunda rapid si eficient."

Sfaturi de securitate de la G Data

Posibilitatile de manipulare sunt infinite si nu este intotdeauna usor pentru webmasteri sa depisteze sursa de infectare. Site-urile sunt adesea construite folosind componente diferite. Este indeajuns ca doar un element al site-ului sa fie infectat sau pentru construirea site-ului care urmeaza sa fie modificat sa fie adaugata o linie de cod malware la fiecare pagina.

Din cauza numarului tot mai mare de atacuri ale hackerilor, G Data recomanda operatorilor sa verifice, de urgenta serverul, in mod regulat si sa raspunda cat mai repede posibil, atunci cand au gasit un virus.

Opţiunile autorilor atacurilor pot fi reduse semnificativ prin respectarea urmatoarele sfaturi:

1. Actualizarile de securitate pentru aplicatiile software ar trebui sa fie instalate cu promptitudine. Aceasta este singura modalitate de a inchide bresele de securitate inainte ca atacatorii sa le utilizeze la capacitate maxima. Din pacate, perioada de timp dintre anuntarea unui patch şi unele incercari de atac pot fi foarte mici.
2. Anumite programe antivirus, menite sa protejeze diferite tipuri de computere, pot sa esueze daca sunt instalate pe servere. De asemenea, trebuie avut grija ca ele sa aiba acces la cele mai noi semnaturi de virusi.
3. Operatorii de site-uri ar trebui sa verifice in mod regulat versiunile offline ale site-urilor lor cu ajutorul unui scanner de viruşi. In acest fel, chiar si malware-ul bine ascuns poate fi gasit rapid.
4. Administratorii ar trebui sa schimbe imediat toate parolele de acces atunci cand apare o infectie. In acest fel, se va opri posibilitatea infractorilor de a ataca serverul in ziua urmatoare.
5. Utilizatorii ar trebui sa fie atenti ca browser-ul lor si plug-in-urile sa fie intotdeauna actualizate. Programe vechi, asa-numitele "software dinosaurs" contin brese de securitate care sunt utilizate de infractori pentru contrabanda de cod malware.
6. Utilizatorii de PC-uri ar trebui sa foloseasca protectie antivirus care verifica in permanenta continutul site-urilor in cautare de malware. Aceasta face ca malware-ul sa fie gasit repede si sa fie oprit inainte de a ajunge in browser.

- ###-