Raport HP: Noua din zece fisiere malware detectate la nivel global au fost livrate în e-mail

O pondere de 89% dintre tipurile de fisiere malware detectate la nivel global, în trimestrul III al acestui an, au fost livrate prin e-mail, în timp ce descarcarea fisierelor de pe web a fost responsabila pentru 11% dintre cazuri, reiese din raportul HP Threat Insights, publicat vineri.

Echipa de cercetare HP Wolf Security a raportat ca atacatorii cibernetici folosesc furnizori legitimi de Cloud pentru a stoca malware si schimba tipurile de fisiere pentru a ocoli instrumentele de detectare.

De asemenea, expertii au descoperit ca atacatorii cibernetici se mobilizeaza rapid pentru a profita de noile vulnerabilitati de tip zero-day, iar exploatarea vulnerabilitatii CVE-2021-40444 - o vulnerabilitate prin care poate fi exploatat motorul de browser MSHTML utilizând documente Microsoft Office - a fost descoperita pe data de 8 septembrie, cu o saptamâna înainte de lansarea unui update (patch) în data de 14 septembrie.

Conform raportului de specialitate, 12% din malware-ul primit în e-mail, care a fost izolat, a trecut de cel putin un scaner gateway. În acelasi timp, cele mai uzuale atasamente folosite pentru a livra malware au fost fisierele de arhiva (38% fata de 17,26%, în trimestrul trecut), documentele Word (23%), documentele Excel (17%) si fisierele executabile (16%).

Totodata, cele mai utilizate amenintari de tip phishing au utilizat cuvinte despre tranzactii business, precum "comanda", "plata", "nou", "cotatie" si "cerere". O constatare importanta este aceea ca o pondere de 12% din totalul de malware detectat nu era cunoscut pâna acum.

Raportul întocmit de HP Wolf Security releva faptul ca numarul de hackeri care folosesc furnizori legitimi de Cloud si Internet pentru a încarca malware a crescut. "O campanie recenta GuLoader încarca troianul Remcos Remote Access (RAT) pe platforme importante, precum OneDrive, pentru a evita sisteme de protectie si pentru a trece de testele de verificare. De asemenea, HP Wolf Security a descoperit mai multe familii de malware pe platforme social media precum Discord", precizeaza sursa citata.

În plus, a fost detectat un malware tip JavaScript care eludeaza instrumentele de detectare, precum si utilizarea fisierelor de tip HTA pentru a raspândi malware printr-un singur click un exemplu în acest sens fiind troianul Trickbot, livrat în prezent prin aplicatia HTML.

Datele incluse în raportul HP au fost obtinute în cadrul cercetarii HP Wolf Security, în perioada iulie - septembrie 2021.

Lansat de catre producatorul celor mai sigure computere si imprimante din lume, HP Wolf Security este un nivel de securitate pentru punctele terminale. Portofoliul HP de functii de securitate aplicate hardware-ului si de servicii de securitate pentru punctele terminale sunt concepute pentru a ajuta organizatiile sa-si protejeze computerele, imprimantele si angajatii împotriva atacatorilor cibernetici.