Crestere cu 11% a numarului de fisiere de arhiva ce contin malware, în T2 (raport)

Numarul de fisiere de arhiva care contin malware, prin care infractorii cibernetici plaseaza deseori pe e-mail documente în atasamente ZIP, a crescut cu 11% în trimestrul II, comparativ cu intervalul anterior, conform raportului trimestrial "Threats Insights", publicat joi.

"Comenzile rapide înlocuiesc macrocomenzile Office - care încep sa fie blocate implicit în Office - ca modalitate prin care hackerii acceseaza retele, pacalindu-i pe utilizatori sa îsi infecteze PC-urile cu programe malware. Odata dobândit, accesul poate fi folosit pentru a fura date importante ale companiei sau poate fi vândut unor grupuri de ransomware, ceea ce ar provoca brese la scara larga care ar putea bloca operatiunile si pentru care ar fi nevoie de costuri semnificative de remediere", arata raportul HP Wolf Security Threat Insights.

Cel mai recent raport global al companiei, care ofera o analiza a atacurilor cibernetice din lumea reala, arata o crestere de 11% a numarului de fisiere de arhiva care contin malware, inclusiv fisiere LNK (shortcut). Astfel, infractorii cibernetici plaseaza deseori fisiere shortcut în atasamente ZIP, evitând în acest mod, filtrele de securitate care scaneaza e-mailul.

Pe lânga cresterea numarului de fisiere LNK, echipa de cercetare HP a mai descoperit numeroase campanii de phishing care au folosit e-mailuri ce pretindeau a fi initiate de servicii postale regionale sau de evenimente majore, precum Doha Expo 2023 (care va atrage peste 3 milioane de participanti la nivel mondial), pentru a livra programe malware.

O alta constatare a specialistilor arata ca hackerii exploateaza fereastra de vulnerabilitate creata de Follina (CVE-2022-30190 - vulnerabilitate Zero Day din Microsoft Support Diagnostic Tool (MSDT) pentru a distribui QakBot, Agent Tesla si Remcos RAT (Remote Access Trojan) înainte ca o solutie de tip patch sa fie disponibila.

Totodata, s-a descoperit o campanie care distribuie o noua familie de malware, numita SVCReady, conceput în special pentru a descarca fisiere rau intentionate secundare în computerele infectate.

Pâna în prezent, clientii HP au accesat peste 18 miliarde de atasamente de e-mail, pagini web si fisiere descarcate, fara sa fie raportate brese.

Raportul de specialitate evidentiaza ca 14% dintre programele malware înregistrate de HP Wolf Security au ocolit cel putin un instrument de securitate, precum si faptul ca hackerii au folosit 593 de familii malware diferite, fata de 545 în trimestrul precedent.

În plus, 69% dintre programele malware detectate au fost livrate prin e-mail, în timp ce descarcarile de pe internet au fost responsabile pentru 17%. Cele mai frecvente momeli phishing au fost tranzactiile de afaceri, cum ar fi "Order", "Payment", "Purchase", "Request" si "Invoice".

Datele incluse în studiul HP au fost colectate în mod anonim de la clientii HP Wolf Security în perioada aprilie - iunie 2022.

HP Inc. este o companie de tehnologie ce are în portofoliul de produse si servicii sisteme de calcul, imprimante si solutii de imprimare 3D.