



Comunicat de presa

Sarbatorile de Craciun 2009: hotii virtuali sunt gata de start

G Data avertizeaza impotriva phishing-ului si ofera sfaturi pentru siguranta cumparaturilor online



Bucuresti (Romania), 7 noiembrie 2009 – Multi cumparatori prefera indeosebi cumparaturile online datorita ocaziei de a face o comparatie rapida intre preturi si datorita posibilitatii de a cumpara produse la orice ora din zi stand confortabil pe propria canapea. Aceste avantaje sunt foarte pretuite in contextul agitatiei de Craciun, deoarece cumparatorii pot evita inghesuiala din centrele comerciale. Infractorii virtuali vor incerca sa profite de aceasta tendinta pe perioada sezonului de iarna prin consolidarea vanatorii de informatii ale utilizatorilor, informatii ale cartilor de credit sau ale conturilor PayPal. De aceea, G Data se asteapta la o crestere a phishing-ului si a campaniilor de inselaciune.

Cea mai des utilizata inselaciune pentru a obtine informatii despre utilizatori este trimiterea de email-uri de phishing, al caror format se potriveste de cele mai multe ori cu forma email-urilor din partea unor mari organizatii importante. In vreme ce in trecut email-urile de phishing erau de cele mai multe imediat recunoscute datorita izbitoarelor greseli de ortografie, in prezent, acestea sunt adesea perfecte atat din punct de vedere al formei, cat si al limbajului, ceea ce le face imposibil de recunoscut la o prima vedere. Banci renumite, servicii de expediere cu baze automate de livrare si colectare si producatori de jocuri pe calculator sunt sursa preferata a modelelor pentru aceste genuri de email.

„In cursa pentru cumparaturile de Craciun ne asteptam la o activitate crescuta din partea infractorilor online, care vor desfasura actiuni ce tintesc informatii despre cartile de credit

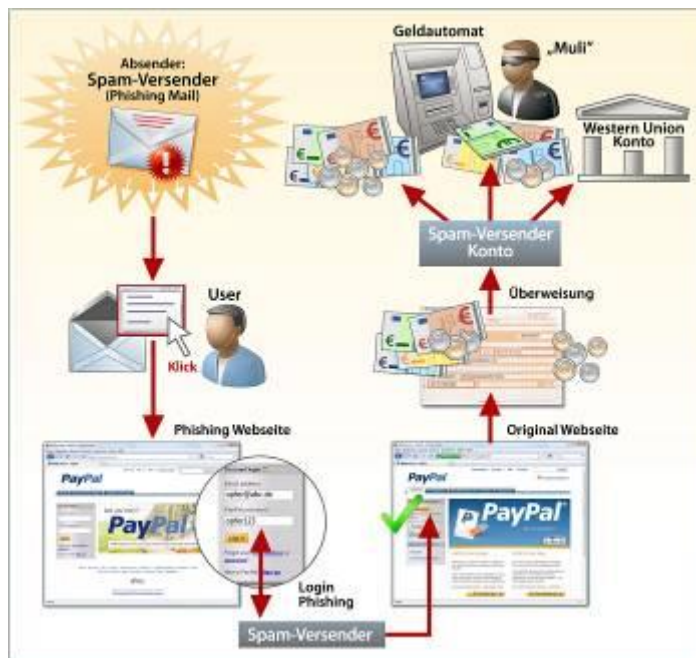
sau despre utilizatori. Printre cele mai preferate inselaciuni sunt facturile fictive sau cererile de plata, pe care infractorii le folosesc pentru a atrage posibilele victime catre website-uri false unde sunt incurajati sa-si introduca informatiile de acces”, avertizeaza Ralf Benzmueller, manager al Laboratoarelor G Data Security. „Un alt tip de inselaciune este folosirea fisierelor atasate infectate, care se pretind a fi necesare la procesarea platii. Putem doar sa recomandam tuturor destinatarilor sa nu raspunda la astfel de email-uri, deoarece acest lucru serveste la verificarea adresei lor de email pentru viitoare atacuri, si nici sa deschida atasamentele. In cel de-al doilea caz, PC-ul este infectat cu malware care transfera toate informatiile de acces ale utilizatorului catre raufacatori.”

Phishing : acces la informatiile cumparatorilor

Furtul si abuzul de informatii personale a crescut deosebit de mult in ultimii ani. Raufacatorii online gasesc in vanzarea datelor de pe carti de credit, online banking sau a conturilor serviciilor de plata (de ex. PayPal) informatii foarte avantajoase.

Principala tinta a infractorilor virtuali sunt deci parolele si informatiile de acces pentru contul de utilizator cum ar fi online banking si serviciile de plata, platformele de tranzactionare, retelele sociale si jocurile online.

Diagrama cu pasii urmati intr-un caz clasic de atac de phishing asupra utilizatorilor de PayPal



Sfaturi pentru imbunatatirea sigurantei pe perioada cumparaturilor de Craciun:

G Data Software recomanda urmatoarele masuri pentru a reduce la minimum posibilele riscuri in timpul cumparaturilor online de Craciun:

1. Folosiți un program antivirus actualizat, firewall si filtre HTTP.

2. Asigurati-va ca software-ul de securitate, sistemul de operare si alte software-uri sunt intotdeauna actualizate cu cea mai recenta versiune.
3. Daca nu aveti incredere in email-urile primite de la expeditori necunoscuti – nu dati click pe niciun link si nu incarcati sau deschideti fisierele atasate.
4. Introduceti adresele website-urilor si autentificarea utilizatorului manual sau folositi functiile de favorite sau bookmark ale browser-ului dumneavoastra.
5. Atentie la detaliile de securitate ale browser-ului dumneavoastra atunci cand cumparati online, urmatoarele aspecte sunt importante: lacatul browserului, abrevierea "https" in fata adresei introduse, bara pentru adresa evidentiata cu culoarea verde la multe browser-e moderne si afisarea corecta a domeniului top-level.
6. Verificati daca magazinul online ales are termenii si conditiile, recunoasterea meritelor, si declaratii despre costuri expuse in mod clar (ex. Costurile de expediere si posibilele costuri suplimentare.)

- ###-