G Data press release 2013

Gamerii online vizati de eCrime

G Data a alcatuit un top al riscurilor la care se expun jucatorii online si ofera sfaturi pentru jocuri in siguranta acestora pe Internet

Bucuresti (Romania), 14.08.2013

Jocurile online sunt mai populare decat au fost vreodata. Doar anul acesta, PriceWaterHouseCoopers estimeaza o cifra de afaceri de 639 milioane de euro numai in Germania pentru jocuri pe Internet. Asta ii face pe gameri sa devina tinte profitabile pentru atacatorii ce folosesc metode speciale pentru a-i urmari pe fanii jocurilor. Infractorii folosesc o gama variata de atacuri pentru a-i surprinde pe jucatori si, cu ajutorul programelor malware sau a site-urilor de phishing, sa sustraga conturi intregi de online gaming. Alta metoda utilizeaza oferte false pentru piese rare si bani virtuali pentru caractere digitale. In perioada premergatoare evenimentului Gamescom ce va avea loc in Koln, G Data a alcatuit Top 3 riscuri pentru gameri si prezinta cum se pot proteja impotriva acestora – pentru jocuri esfasurate in siguranta pe Internet.

"Furtul si comertul cu conturile de utilizator ale jocurilor online este foarte profitabil pentru infractori. Pentru a actiona in aceasta directie, atacatorii dezvolta programe malware speciale care tintesc conturile de utilizator sau incearca prin metode phishing," explica Ralf Benzmuller, seful G Data Security Labs. "Gamerii ar trebui sa utilizeze solutii de securitate eficiente care raman active pe toata perioada jocului, sa instaleze toate actualizarile de programe disponibile si sa aiba incredere doar in patch-urile oficiale ale jocurilor, provenite de la producator."

Top 3 riscuri pentru jucatorii online

Malware – programe keyloggers si altele
Infractorii ii ataca pe jucatori cu programe malware dedicate, inclusiv programe asa-numite keyloggers ce spioneaza activitatile de pe computer, face capturi de ecran sau inregistreaza activitatea de pe tastatura. Calul troian Tro-jan.PWS.OnLineGames.NVI fura datele introduse de utilizatori in browserul instalat.

Alt program malware este dezvoltat pentru a fura cheile licentelor. Acesti „hoti" cauta in special in registrii, dar si in alte zone ale computerului si transfera datele pe serverele infractorilor.
Conturile de jocuri compromise si alte date furate sunt vandute pe piata subterana; caracterele high-level ce echivaleaza cu sume mari ale echipamentelor speciale din jocuri sunt in mod special foarte profitabile.

Exemple de anunturi cu oferte ale conturilor de gaming furate:

Furt de date prin phishing
Phishing-ul este o metoda infractionala incercata si testata de infractori pentru a obtine date profitabile. Aceste actiuni implica frecvent email-uri in care fraudatorii pretind, de exemplu, ca sunt probleme cu contul de utilizator. Destinatarul este indemnat sa introduca datele de acces pe un anumit website.
Aceste site-uri sunt, de cele mai multe ori, create in asa fel incat create sa arate aproape identic cu cele originale. Daca destinatarul se lasa pacalit de mesaj, infractorii au acces direct la date de valoare.

Exemplu de site de phishing:

Oferte online false pentru caractere de jocuri, echipamente sau monede virtuale
Pe langa date, fraudatorii sunt interesati si de bani. Ei plaseaza, pe platforme automate, anunturi cu oferte pentru echipamente rare, bani virtuali si, uneori, caractere intregi high-level. Daca un utilizator cumpara bunurile din oferta, pierde banii pe care i-a platit fara sa primeasca articolele cumparate.

Sase sfaturi pentru gamerii online

- Instalarea unei solutii de securitate: Este recomandata utilizarea unei solutii complete de securitate, care sa includa firewall si actualizari regulate ale bazei de virusi. Protectia antivirus trebuie sa ramana activata pe toata durata jocului.
- Actualizarea permanenta a aplicatiilor: Gamerii ar trebui sa foloseasca actualizarile disponibile pentru sistemul de operare si celelalte programe instalate.
- Folosirea de parole puternice: Acest tip de parole ar trebui sa fie alese pentru toate conturile de utilizator. Acestea ar trebui sa fie compuse dintr-o secventa aleatoare de numere, caractere speciale, litere mari si mici. Astfel, infractorii nu au nicio sansa de spargere a parolei prin asa-numitele atacuri dictionar. Cu atat mai mult, parolele nu ar trebui salvate in browser.
- Atentie la patch-uri neoficiale si la add-on-uri: Sunt recomandate doar actualizarile si upgrade-urile oficiale de la producator, celelalte se pot transforma rapid in malware. Se recomanda ca si add-on-urile neoficiale sa fie evitate, deoarece malware-ul folosit in furtul de date se ascunde adesea in spatele imbunatatiri a programului.
- Nu dezvaluiti prea multe despre propria persoana: Gamerii folosesc cu regularitate un pseudonim mai degraba decat numele real. Acestia ar trebui sa nu dezvaluie prea multe informatii personale.
- Plata cu cardul de credit: Se recomanda ca banii virtuali sau alte accesorii ale jocului sa fie cumparate de pe piata oficiala a jocurilor online, deoarece oferte de pe alte piete se dovedesc a fi, adesea, false. Un card de credit ar trebui folosit pentru procesarea platilor.

-###-