



G Data

Whitepaper 08/2010

Pericoli per i giocatori

Sabrina Berkenkopf, Ralf Benz Müller e Marc A. Ester
G Data SecurityLabs

Go safe. Go safer. **G Data.**



Sommario

Sommario	1
Introduzione	2
Tipi di attacchi.....	3
Phishing tramite e-mail.....	3
Phishing sui siti Web	3
Phishing nei forum e nelle chat.....	4
Altri tipi di furti di dati	4
Famiglie di malware: comportamento e attività	5
G Data: analisi delle pagine Web	7
Il mercato underground.....	9
Piattaforme di vendita	10
Protezione da attacchi e truffe	11

Introduzione

La marcia trionfale dell'industria dell'entertainment è inarrestabile e i videogiochi continuano a occupare una grande percentuale delle cifre di vendita del settore. Nel 2009, solo nell'Europa occidentale nel commercio al dettaglio sono stati venduti 253 milioni di videogiochi per una cifra superiore a 8 miliardi di euro.¹

Secondo la Interactive Software Federation of Europe, i gamer rappresentano circa il 25 % degli europei adulti². La pluralità delle piattaforme per videogiochi cresce, tuttavia il Pc rimane il mezzo più utilizzato: tra gli intervistati dalla ISFE, uno su due ha indicato il computer come la periferica di gioco preferita e uno studio condotto negli Stati Uniti ha dimostrato che ben l'85% dei giocatori online utilizza il Pc per i videogiochi³. Anche le cifre recentemente annunciate dei prossimi giochi in uscita su varie piattaforme dimostrano che i videogiochi su computer continuano a detenere il primato⁴. Ma anche il panorama sempre più popolato di giochi per device portatili, come gli smartphone, attira sempre più i giocatori verso i dispositivi digitali⁵. Persino le console sono sempre più amate, grazie alle loro numerose funzionalità.

L'immenso numero di giochi gratuiti dei social network assume sempre più importanza: la recente unione strategica sigillata per cinque anni tra lo sviluppatore di giochi Zynga e il leader dei social network Facebook porterà certamente a un notevole incremento dei numeri dei giocatori. Ma l'aumento costante dei giocatori rende purtroppo questo gruppo più interessante anche per i cyber criminali. Pertanto, è necessario prevedere un incremento dell'attività criminale persino in questo segmento dell'online gaming: anche in questo settore i criminali cercheranno di estorcere ai giocatori i dati di accesso, la valuta di gioco e anche vero e proprio denaro. Gli esperti stimano che i giochi per browser torneranno sul mercato anche in futuro e che la loro importanza commerciale crescerà notevolmente.

Tuttavia, l'attività principale dei criminali online continua a incentrarsi sugli ormai affermati giochi per Pc. World of Warcraft e altri giochi appartenenti al genere dei Massive Multiplayer Online Role Play Games (MMORPG) ne sono l'esempio più rappresentativo. A volte, gli account e gli oggetti in-game sulle piattaforme di vendita del settore possono raggiungere prezzi di diverse migliaia di euro. Tali somme naturalmente invogliano i cyber criminali a incrementare la caccia ai dati di accesso dei giochi online.

¹ ISFE Consumer Survey 2010 – <http://www.isfe.eu>

² ISFE Consumer Survey 2010 – <http://www.isfe.eu>

³ Analisi di The NPD Group, Inc. - http://www.npd.com/press/releases/press_100302.html

⁴ Grafico "Nuove uscite 2010" di GamesMarkt 14/10, pagina 27

⁵ Analisi di The NPD Group, Inc. - http://www.npd.com/press/releases/press_100721.html

Tipi di attacchi

I cyber criminali utilizzano varie strategie per estorcere i dati di accesso dei giocatori. Ad esempio, inviano e-mail che fingono di provenire da mittenti ufficiali (produttori di giochi, assistenza, ecc.), creano pagine Web di accesso falsificate identiche a quelle originali o anche spyware che si nascondono nel Pc della vittima.

Phishing tramite e-mail

L'ingegnosità dei truffatori non conosce praticamente limiti. Uno dei trucchetti più amati: gli autori inviano milioni di volte le e-mail di spam ai potenziali giocatori online, falsificando l'indirizzo del mittente e imitando quello del produttore del gioco. Segue una serie di esempi di righe di oggetto di e-mail falsificate che fanno riferimento all'amato gioco di ruolo online World of Warcraft:

- Blizzard Notification About World of Warcraft Account
- FREE Games gold Warcraft
- WorldofWarcraft mounts Trial notice
- World of Warcraft Account Security Verification
- World of Warcraft Account – Subscription Change Notice
- World of Warcraft – Account Instructions
- World of Warcraft – Account warning

Utilizzando titoli così significativi, i criminali sperano che i destinatari rispondano con un'e-mail contenente i dati di accesso completi oppure che visitino una pagina di accesso falsificata e vi inseriscano i propri dati, consegnandoli in tal modo nelle mani dei truffatori. Un'altra possibile alternativa: i giocatori devono scaricare un file allegato al messaggio (file .exe, .pdf, ecc.) ed eseguire/aprire il file infettato da malware. Il file dannoso dovrebbe contenere, ad esempio, una patch, un aggiornamento, una fattura o un modulo di registrazione.

Phishing sui siti Web

Da un lato comprendono le pagine Web già citate, che si celano dietro ai link alle e-mail di spam. I phisher copiano il codice sorgente della pagina Web originaria, posizionano la pagina sul loro server online e si auto inoltrano i dati inseriti dall'utente nei campi di accesso.

Inoltre, esistono anche delle pagine Web che spesso hanno un aspetto visivo e tecnico assai semplice e che promettono all'utente monete d'oro extra, crediti bonus o oggetti di gioco speciali, a patto



Schermata 1: una pagina di phishing di poker dall'aspetto accattivante, che promette presunti bonus

di inserire i propri dati di accesso nella pagina. Una cosa è chiara: chi inserisce i propri dati di accesso sperando di ottenere così dei bonus, è altamente probabile che perderà l'intero account, il quale finirà così nelle mani del truffatore. Ulteriori informazioni al riguardo sono presenti nel capitolo "G Data: analisi delle pagine Web".

Phishing nei forum e nelle chat

Un trucco apparentemente efficace sembra essere quello di fingersi un collaboratore del supporto tecnico del produttore del gioco all'interno di forum e chat. Qui i presunti collaboratori del supporto si rivolgono in modo mirato alle vittime potenziali, offrendo loro assistenza nei problemi tipici di gioco. Soprattutto i nuovi arrivati, i cosiddetti "newbies", sono i più esposti agli attacchi. Per aiutare i giocatori, i collaboratori del supporto chiedono soltanto i dati di accesso al gioco. Naturalmente, questi dati non devono essere comunicati in nessun caso.

Altri tipi di furti di dati

Esistono numerosi modi per rubare dati importanti ai giocatori. Abbiamo già descritto gli attacchi di phishing. Ma anche i malware puntano ai dati dei giocatori. Spesso, si mascherano da copie (illegali) di giochi noti, oppure promettono funzioni speciali per determinati giochi (i cosiddetti cheat). I malware non sono in agguato solo nelle borse di scambio, dove il nome del file promette *crackz* o *key generator* per i titoli più famosi e venduti, ma si presentano anche sotto forma di offerte allettanti sui siti Web del settore. Molti malware interessati ai dati dei giocatori si diffondono con le funzioni di esecuzione automatica di Windows, ad esempio quelle attivate all'inserimento di una penna USB. Spesso i giocatori utilizzano le periferiche di memorizzazione mobili per scambiarsi software durante i gaming party. I malware mirano a dati diversi e possono ottenerli con le seguenti strategie:

Codice di licenza software

I codici di licenza per il software vengono memorizzate in diverse posizioni del computer. Spesso si trovano in alcune chiavi del registro di sistema, ma i file più o meno nascosti in alcuni percorsi contengono le informazioni desiderate. I malware del gruppo dei password stealer conoscono questi percorsi, puntando in modo mirato ai codici di licenza di giochi e altri software. I dati sottratti vengono quindi trasmessi al server controllati dai ladri di dati.

Password nel browser

Tutti i browser più comuni offrono delle funzioni per il salvataggio di password e dati di moduli. Questa funzione incredibilmente utile e pratica facilita moltissimo l'utilizzo delle password. Ma anch'essa possiede il suo lato oscuro, visto che i dati devono essere archiviati sul computer. Purtroppo queste password non sono sufficientemente sicure e i già citati ladri di password sono in grado di trovarle e rubarle. Alcuni browser o plugin del browser offrono funzioni di cifratura che rendono inutili questi tipi di dati rubati, purché tale cifratura sia eseguita con una password sufficientemente lunga. Pertanto, alcuni malware prelevano i dati proprio dove questi si trovano nuovamente decifrati: nei campi dei moduli dei siti Web

corrispondenti. I cosiddetti "form grabber" possono leggere anche il contenuto del campo password e inoltrarlo ai ladri di dati.

Keylogger

I malware possono anche registrare le attività sulla tastiera. Questi programmi vengono chiamati keylogger. La definizione però in molti casi è limitante, dato che i keylogger sono in grado di registrare molto di più. La maggioranza monitora anche gli Appunti di Windows e salva tutto ciò che qui viene copiato. Molti keylogger eseguono screenshot dell'intero schermo a intervalli regolari oppure salvano l'area intorno al puntatore del mouse ogni volta che viene premuto un pulsante del mouse. In molti casi, le registrazioni sono collegate a condizioni, come ad esempio la visita di una determinata pagina Web, la presenza di moduli Web, l'esecuzione di determinati giochi o software. Spesso i keylogger nascosti operano però senza una direzione precisa, nel senso che rubano molto più delle password dei giochi. In molti casi, le vittime dei keylogger perdono l'accesso all'account della posta, ai forum, ai negozi online e ai social network, in poche parole la loro intera identità online.

Attacchi a dizionario e brute force

I dati di accesso agli account di giochi, forum ecc. possono essere ottenuti per tentativi. Per ottenerli, gli aggressori utilizzano lunghi elenchi di password di uso comune (attacchi a dizionario) oppure combinano a caso lettere e sequenze di cifre fino al raggiungimento di una determinata lunghezza (attacchi brute force). Chi utilizza password troppo brevi o comuni come "123456", "Admin" o "Master", presto potrebbe essere vittima di questi attacchi e trovare il suo account di gioco completamente depredata.

Famiglie di malware: comportamento e attività

I programmi malware sono riconoscibili per determinate caratteristiche presenti nel loro codice. In base a tali somiglianze di codice tra malware diversi, le singole varianti possono essere raggruppate in famiglie. Verranno brevemente illustrate le famiglie più frequenti del settore gaming e le loro attività tipiche.

OnlineGames

OnlineGames rappresenta la famiglia più diffusa. Le sue varianti costituiscono l'1,9 % di tutti i malware del primo semestre 2010, occupando così la settima posizione tra le famiglie più produttive. OnlineGames rientra nel gruppo dei ladri di password. Questa famiglia raggruppa i malware che non si limitano ai singoli giochi. L'elenco dei giochi attaccati è lungo ed include ad esempio:

2moons	Fly for fun	Maple Story	Twelve Sky
Age of Conan	Gash	Metin 2	Valhalla
Aion Online	Goodluck	Perfect World	World of Warcraft
Cabal Online	Knight Online	Seal Online.	
Dekaron	Last Chaos	Silk Road Online	
Dungeon Fighter	Lineage	The Lord of the Rings Online	

Per nascondersi, i malware di questa famiglia integrano le loro funzioni dannose in Risorse del computer. Alcune annidano i loro file e voci di registro anche tramite driver rootkit. Per poter agire indisturbati, aggirano anche strumenti anti-hacking dei provider di giochi, come ad esempio HShield o GameGuard. La maggioranza delle varianti di OnlineGames si copia in tutte le condivisioni, inserendovi un file denominato autorun.inf. Quindi il malware si attiva in automatico, ad esempio quando si collega una penna USB o un altro supporto dati rimovibile.

Magania

Questa famiglia di malware è prevalentemente attiva nell'Asia dell'Est. Con una percentuale dell'1,6 % del volume complessivo di malware nel primo semestre del 2010, raggiunge la posizione 11 delle famiglie di malware più prolifiche. Magania appartiene al gruppo dei keylogger e, come suggerisce il gioco di parole, mira ai giochi della casa produttrice di giochi Gamania, come ad es. Lineage o MapleStory. Nella maggioranza dei casi, i malware arrivano per e-mail. Quando si esegue il file allegato, per distrarre l'utente viene visualizzata un'immagine. Intanto, il malware si attiva in background. Per nascondersi, i malware della famiglia Magania si inseriscono nei processi di Risorse del computer e di Internet Explorer, risultando così invisibili all'utente. I dati di accesso estorti vengono trasferiti su più server su Internet. Spesso vengono caricati altri malware del tipo più disparato.

WOW

I malware della famiglia "WOW" puntano ai dati di accesso di World of Warcraft. Con una percentuale dello 0,3 % nel primo semestre del 2010, si piazzano alla posizione 49. Rappresentano così la famiglia più grande creata per un singolo gioco. I dati vengono rubati tramite keylogging e trasmessi al server su Internet. I dati di accesso estorti vengono utilizzati per saccheggiare l'account delle vittime e rivendere sui forum del settore i caratteri virtuali e i beni in loro possesso.

Altre famiglie

Alla posizione 75 delle famiglie di malware più produttive del primo semestre 2010 troviamo "Lmir". I suoi sostenitori lo hanno realizzato per estorcere i dati di accesso del gioco "Legend of Mir", assai popolare in Cina e nella Corea del Sud. Alla posizione 103 segue Tibia, una famiglia di keylogger che punta ai dati di accesso del gioco tedesco Tibia.

G Data: analisi delle pagine Web

Le analisi sono state effettuate su una base di 66.534 pagine Web del periodo compreso tra gennaio e giugno 2010. Le pagine Web analizzate erano pagine di phishing rilevate e pagine contenenti codice dannoso.

Gli strumenti di analisi di G Data SecurityLabs hanno scoperto ed elaborato in automatico le pagine Web e le relative informazioni, registrando i risultati in un database che è rimasto disponibile per ulteriori analisi manuali. Il 6,5 % di queste pagine è classificabile nel settore tematico dei videogiochi. Nel 6,5 % sono presenti i seguenti temi:

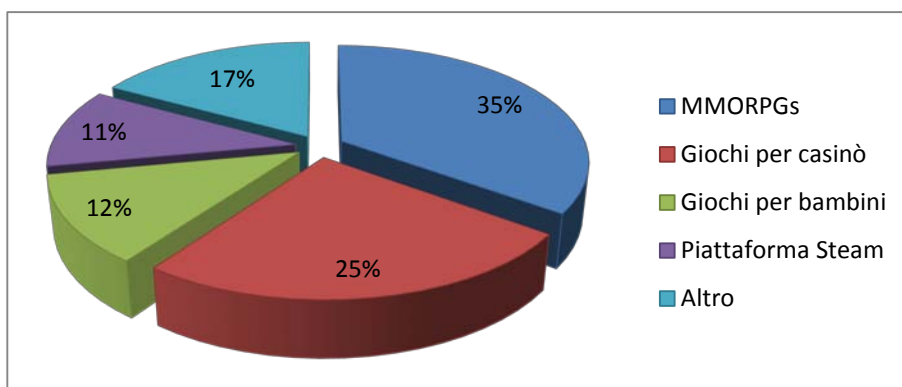
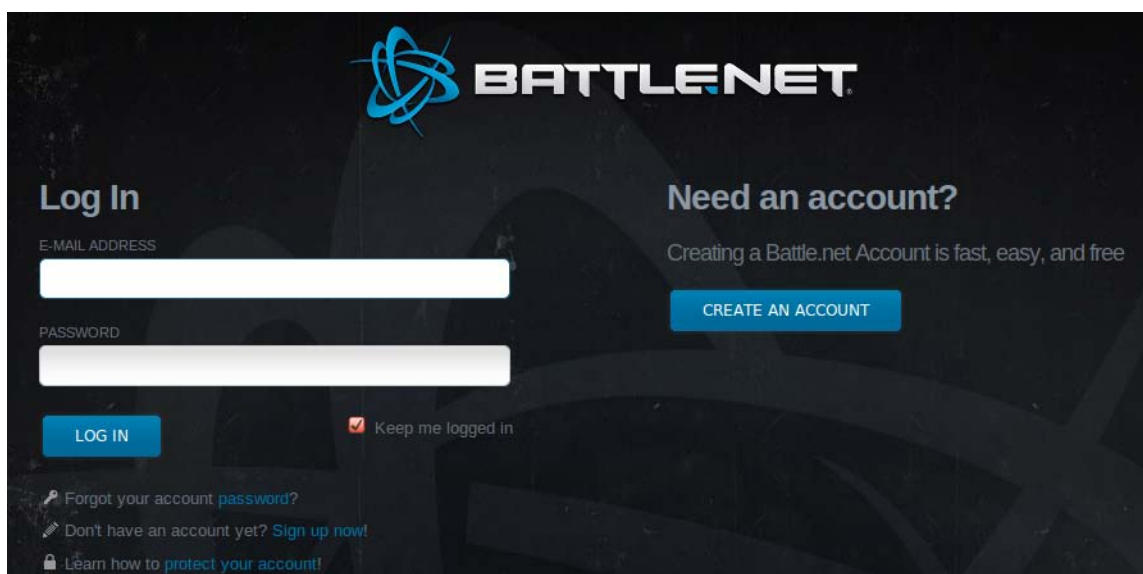


Grafico 1: quota percentuale dei singoli temi nelle pagine di videogiochi esaminate

Con una quota del 35 %, i giochi di ruolo online di massa occupano inequivocabilmente il primo posto: la categoria comprende World of Warcraft, Metin 2, Runescape, Tibia e altro ancora. Lo scenario di attacco più registrato da G Data è il phishing. I truffatori riproducono la pagina Web di accesso originale del gioco in questione e la collocano sul proprio server online. Questa pagina è difficilmente distinguibile dall'originale a livello tipografico e non appena un giocatore vi accede e inserisce i suoi dati questi gli vengono estorti.



Schermata 2: una schermata di una pagina di accesso falsa, che visivamente non si distingue dall'originale

Originale (USA)	https://us.battle.net/login/en/
Esempi di falsificazioni	http://us.bvttie.net/login/login.htm http://us.bottlo.net/login/login.xmlref.html http://us-battlefusbattlenet.net http://us-battletests.net http://us.bbattlie.net http://us.balittlie.com http://www.account-battle.net/wow http://www.wowsupport.net

Tabella 1: somiglianza tipografica degli indirizzi Web di pagine di phishing di Battle.net rispetto all'originale

Proprio nel settore dei giochi di casino (principalmente poker) e dei giochi per bambini (spesso nelle comunità virtuali), i truffatori cercano di impossessarsi degli account utilizzando le cosiddette pagine bonus.

Per questo gli account della piattaforma Steam sono molto richiesti. Qui i giocatori possono utilizzare più giochi con un unico account e così i truffatori tramite il phishing, non solo ottengono accesso a un gioco, ma anche a tutti gli altri. I dati di accesso di Steam vengono quindi venduti anche nei mercati underground (vedere tabella 2).

Nella categoria "Altro" vengono classificate le pagine Web che non possono essere assegnate in modo univoco all'uno o all'altro settore tematico. Tra l'altro, comprendono giochi apparsi sporadicamente, pagine Web dei cosiddetti warez (tra cui crack e keygenerator per giochi), altre pagine con le parole "game" o "gaming" nell'URL, ecc.

Il mercato underground

Nei mercati neri online della scena underground viene venduta praticamente qualsiasi merce, da account di vari servizi di pagamento e aste online a documenti d'identità, dati di carte di credito fino a dati di accesso e codici per programmi e giochi. I prezzi indicati sono esempi di quelli praticati sulle piattaforme di commercio illegali:

Account Steam e Battle.net	Prezzo
Counter-Strike 1.6, Counter-Strike: Source, Counter-Strike: Condition Zero, Day of Defeat, Day of Defeat: Source, Half-Life, Half-Life Deathmatch Classic, Half-Life Opposing Force, Half-Life Blue Shift, Half-Life 2, Half-Life 2 Deathmatch, Half-Life 2 Lost Coast, Red Orchestra: Ostfront 41-45, Ricochet, Saints Row 2, Speedball 2 Tournament, Team Fortress Classic	40 euro
Counter-Strike: Source, Dark Messiah of Might & Magic, Day of Defeat: Source, Left 4 Dead, Left 4 Dead 2, Metro 2033, Saints Row 2, Supreme Commander	35 euro
Call of Duty: Modern Warfare 2 Uncut	22 euro
Counter-Strike: Source, Counter-Strike 1.6, Half-Life 2 Episode 1 e 2, Team Fortress 2	20 euro
Call of Duty: Modern Warfare 2, Order of War, Order of War Challenge	20 euro
Counter-Strike: Source, Day of Defeat: Source, Half-Life 2 Lost Coast, Half-Life 2 Deathmatch	16 euro
Alien vs. Predator Uncut	12 euro
Starcraft II: Wings of Liberty, World of Warcraft	10 euro
Empire: Total War, Warhammer 40,000 Dawn of War II, Warhammer 40,000: Dawn of War II Chaos Rising	10 euro
GRID	5 euro
Trackmania United Forever, Tombr Raider: Underworld	5 euro
Counter-Strike 1.6	5 euro

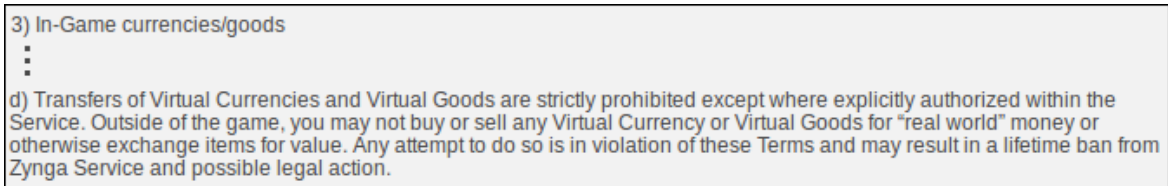
Game key	Prezzo
Battlefield: Bad Company 2 – Limited Edition	15 euro
Assassin's Creed – Special Edition	12 euro
Command & Conquer 4: Tiberian Twilight	12 euro
World of Warcraft Wrath of the Lich King – Collector's Edition	12 euro
World of Warcraft Wrath of the Lich King	10 euro
Aion	10 euro
Battlefield: Bad Company 2	10 euro
FIFA 10	9 euro
World of Warcraft Burning Crusade	6 euro
World of Warcraft Classic	5 euro

Game time e punti	Prezzo
Playstation Network Card (50 euro)	18 euro
Xbox Live 12 mesi Gold	12 euro
World of Warcraft 60 giorni di game time	10 euro
NCSOFT 60 giorni di game time	10 euro
1.000 Simpoints	8 euro
1.000 Wii Points	5 euro

Tabella 2: selezione dei prezzi dei warez dei giochi sui relativi negozi underground




Piattaforme di vendita

I beni e gli account virtuali vengono venduti anche su altre piattaforme, a volte più o meno legali. Molto amato è un sito di aste online dei più noti. Tuttavia, sono state fondate anche aste per giochi specifiche, dove si vendono solo oggetti in-game e dati di accesso. Tra gli esempi citiamo playerauctions.com, mmobay.net o anche wowbay.net. Tuttavia, la vendita e l'acquisto di articoli di gioco e account al di fuori del gioco stesso rappresenta una violazione delle condizioni di utilizzo dei produttori dei giochi, come ad esempio Blizzard, Zynga, ecc.



Schermata 3: estratto dalle condizioni di utilizzo di Zynga, esempio del divieto

Ad esempio, nell'asta clandestina playerauctions.com, gli account di valore elevato vengono trattati a prezzi totalmente diversi, rispetto a quelli "normali". Il prezzo dipende dal livello del personaggio, dalle abilità, dagli oggetti virtuali disponibili e dal server dove gioca il personaggio in questione. Attualmente, l'offerta più bassa per 29 account di livello inferiore è pari a 40 dollari. Le offerte nella schermata 3 illustrano tuttavia che è possibile ottenere prezzi notevolmente superiori:

Offer	Price	Seller's Delivery Guarantee	Date	Secure Payment
 Superior WoW account - Offering: Mage + Rogue + DK tank/DPS 6420 GS ++ all of em and include SC2	\$2,550.00	24 Hours	Aug-06	View Details
Ashes of Al'ar mount and full t10 Tank/Kitty/Tree and pvp gear sets!	\$2,212.00	24 Hours	Jul-28	View Details
 Level 80 lock gnome alliance 3900 SP 6190 GS pve and 6075 GS pvp 11/12 ICC25 heroic + 5 lvl 80 toons	\$1,100.00	24 Hours	Aug-08	View Details
 2xLVL 80 Kingslayer Account + Everything you would ever want	\$800.00	20 Minutes	Aug-08	View Details
80 Orc hunter 6k gs & 80 Troll shaman 6k gs. 12/12 in both 10/25man and 11/12 HM achievement.	\$670.00	24 Hours	Jul-26	View Details

Schermata 4: gli account attualmente più cari su playerauctions.com

Queste cifre rendono ancora più chiaro il motivo per cui i giocatori sono sotto il tiro dei cyber criminali: da tempo non è più una questione di divertimento, pixel e monete d'oro virtuali, ma di valore in denaro vero. Un aspetto da non sottovalutare.

Protezione da attacchi e truffe

I giocatori non devono preoccuparsi dei loro dati di accesso e della sicurezza dei loro Pc. Per poter godere appieno del divertimento del gioco, basta osservare i seguenti suggerimenti e avvisi:

- Per proteggersi dallo spyware e da altre minacce, deve essere installato e attivo un software di sicurezza performante, ma con un uso limitato delle risorse, dotato di filtro http, firewall e funzione di guardiano. Una buona suite di sicurezza risponde alle esigenze dei giocatori e non rallenta il Pc.
- Un filtro antispam aggiornato aiuta a eliminare le e-mail indesiderate prima che arrivino nella posta in arrivo.
- La protezione del proprio account di gioco con una password sicura è di assoluta importanza. Si consiglia una combinazione di almeno 8 caratteri, costituita da cifre e lettere maiuscole e minuscole, oltre a caratteri speciali.
- Per ogni account deve essere creata una password diversa, che non dovrà essere memorizzata nel browser. Per ricordarsi tutte le password, è possibile costruirle con una parte fissa e una variabile.
- Gli attacchi di phishing ai giocatori online vengono spesso realizzati in modo scaltro. Ma nella maggioranza dei casi è sufficiente un'attenta analisi della riga dell'oggetto del browser, per capire che si stanno inserendo i propri dati in una pagina falsificata. Come nel banking online, anche qui è bene accedere al sito digitando manualmente l'indirizzo o richiamandolo dai preferiti ed evitando di seguire il link di una e-mail o di una pagina Web.