



G Data

Whitepaper 08/2010

Gefahren für Gamer

Sabrina Berkenkopf, Ralf Benzmüller & Marc A. Ester
G Data SecurityLabs



Inhalt

| | |
|---|-----------|
| Inhalt..... | 1 |
| Einleitung..... | 2 |
| Angriffsarten | 3 |
| Phishing per E-Mail..... | 3 |
| Phishing auf Webseiten | 3 |
| Phishing in Foren und Chats | 4 |
| Weitere Arten von Datendiebstahl | 4 |
| Schädlingsfamilien - ihr Verhalten, ihre Aktivitäten | 5 |
| G Data Webseiten-Analyse | 7 |
| Der Untergrundmarkt..... | 9 |
| Verkaufsplattformen | 10 |
| Schutz vor Angriffen und Betrug | 11 |

Einleitung

Der Siegeszug der Entertainment-Industrie ist ungebrochen und Computerspiele halten noch immer einen großen Anteil an den Absatzzahlen der Branche. Der Bundesverband für Interaktive Unterhaltungssoftware e.V. weist für die ersten drei Monate des Jahres 2010 Umsätze von 344 Millionen Euro aus, 4 Millionen mehr als im Vorjahr.

Laut des Branchenverbands Bitkom spielen rund 25 % der deutschen Bundesbürger (21 Mio.) digitale Spiele¹. Die Vielfalt der Plattformen für Spiele nimmt zu - jedoch bleibt der PC das meistgenutzte Medium: Unter den Bitkom-Befragten nannte jeder vierte Spieler den Computer als beliebtestes Spielgerät und in den USA gaben ganze 85% der Online-Spieler in einer Studie an, dass sie den PC für ihre Spieleaktivitäten nutzen². Auch die aktuell gemeldeten Zahlen für Neuveröffentlichungen von Spielen nach Plattformen belegt, dass die Computerspiele noch immer die Nase vorn haben³. Aber, auch die immer größer werdende Landschaft an Spielen für mobile Geräte, wie Smartphones, binden zusätzlich immer mehr Spieler an digitale Geräte⁴. Auch die Konsolen erfreuen sich mit ihren vielfältigen Funktionen wachsender Beliebtheit.

Die immense Zahl an frei erhältlichen Spielen in Sozialen Netzwerken gewinnt ebenfalls immer mehr an Bedeutung – gerade auch der kürzlich auf fünf Jahre besiegelte strategische Zusammenschluss von Spieleentwickler Zynga und Social Network Branchenprimus Facebook wird sicherlich zu einer deutlichen Steigerung der Spielerzahl führen. Mit einer wachsenden Zahl von Spielern wird diese Gruppierung leider auch für Cyberkriminelle interessanter. Mit einer Steigerung der kriminellen Aktivität ist daher auch in diesem Online-Gaming-Segment zu rechnen und die Täter werden auch hier versuchen Spielern ihre Zugangsdaten, ihre Spielwährung und auch echtes Geld abzuknöpfen. Experten schätzen, dass Browser-Games auch in Zukunft stärker in den Spielemarkt rücken werden und ihre kommerzielle Bedeutung durchaus zunehmen wird.

Nach wie vor konzentriert sich jedoch das Kerngeschäft der Online-Kriminellen auf etablierte Spiele für PCs. Als repräsentatives Beispiel dient hier z.B. World of Warcraft und andere so genannte Massive Multiplayer Online Role Play Games (MMORPGs). Accounts und In-Game Waren erzielen auf einschlägigen Verkaufsplattformen mitunter Preise von mehreren Tausend Euro. Diese Summen sind natürlich ein Anreiz für Cyberdiebe, verstärkt Jagd auf Zugangsdaten von Online-Spielen zu machen.

¹ Umfrage im Auftrag des BITKOM - http://www.bitkom.org/de/presse/8477_64453.aspx

² Analyse von The NPD Group, Inc. - http://www.npd.com/press/releases/press_100302.html

³ Diagramm „Neuveröffentlichungen 2010“ in GamesMarkt 14/10, Seite 27

⁴ Analyse von The NPD Group, Inc. - http://www.npd.com/press/releases/press_100721.html

Angriffsarten

Cyberkriminelle versuchen in unterschiedlichster Form an die Zugangsdaten von Gamern zu gelangen. Sie benutzen dazu z. B. gefälschte E-Mails, die vorgeben, von offiziellen Absendern (Spielehersteller, Support, etc.) zu kommen, täuschend echt aussehende nachgebaute Login Webseiten oder aber auch spionierende Schadprogramme, die sie auf den Rechner der Opfer schleusen.

Phishing per E-Mail

Dem Einfallsreichtum der Betrüger sind hier fast keine Grenzen gesetzt. Eine beliebte Masche der Täter: Sie versenden millionenfach Spam-Mails an potentielle Online-Spieler. Hierbei fälschen die Versender häufig die Absenderadresse und ahmen so die Spielehersteller nach. Nachfolgende einige Beispiele von Betreffzeilen gefälschter E-Mails, die im Zusammenhang mit dem sehr beliebtem Online-Rollenspiel World of Warcraft stehen:

- 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

Mit den durchaus wichtig klingenden Überschriften bezwecken die Kriminellen, dass die E-Mail-Empfänger entweder eine Mail mit ihren kompletten Zugangsdaten an sie zurückschicken, oder eine gefälschte Login Webseite besuchen und dort durch den Anmeldevorgang ihre Zugangsdaten an die Betrüger senden. Oder aber: die Gamer sollen eine an die Mail angehängte Datei herunterladen (.exe-Datei, .pdf-Datei, etc.) und diese mit Schadcode infizierte Datei ausführen/öffnen. Hinter der schädlichen Datei soll sich zum Beispiel ein Patch, ein Upgrade, eine Rechnung oder ein Anmeldeformular befinden.

Phishing auf Webseiten

Hier sind einerseits die schon beschriebenen Webseiten zu nennen, die hinter den Links aus Spam Mails stecken. Phisher kopieren einfach den Quellcode der Originalwebseite, stellen die Seite auf ihrem eigenen Server online und leiten die eingegebenen Daten aus den Anmeldefeldern an sich selbst weiter.

Zusätzlich dazu gibt es noch Webseiten, die häufig optisch und technisch sehr



Screenshot 1: Eine optisch ansprechende Poker-Phishingseite, die angebliche Boni verspricht

einfach gestaltet sind und den Besuchern Extra-Goldmünzen, Bonus-Guthaben oder spezielle Spielgegenstände versprechen, wenn sie ihre Zugangsdaten auf dieser Seite eingeben. Klar ist: Wer seine Zugangsdaten eingibt, in der Hoffnung, Boni zu bekommen, der verliert mit höchster Wahrscheinlichkeit seinen kompletten Account an die Betrüger. Mehr Informationen dazu im Kapitel „G Data Webseiten-Analyse“.

Phishing in Foren und Chats

Eine scheinbar effektive Masche der Täter besteht darin, sich in Foren oder Chats als Support-Mitarbeiter der Spielehersteller auszugeben. In Foren oder Chats werden potentielle Opfer von diesen vermeintlichen Support-Mitarbeitern gezielt angesprochen indem sie ihre Hilfestellung bei spieletypischen Problemen anbieten. Vor allem Neueinsteiger, sog. Newbies, sind hierfür sehr anfällig. Um den Spielern zu helfen, bräuchten die Support-Mitarbeiter lediglich die Zugangsdaten zum Spiel. Diese Daten sollten aber natürlich unter keinen Umständen preisgegeben werden.

Weitere Arten von Datendiebstahl

Es gibt viele Arten, wie Gamer wichtige Daten verlieren können. Phishing-Attacken wurden bereits beschrieben. Aber auch Schadprogramme haben es auf die Daten von Spielern abgesehen. Häufig tarnen sie sich als (illegale) Kopien bekannter Spiele oder versprechen Spezialfunktionen für bestimmte Spiele (sog. Cheats). Schädlinge lauern aber nicht nur in Tauschbörsen, wo der Dateiname Crackz oder Key-Generatoren zu Gaming-Blockbustern verspricht, sondern auch als verlockende Angebote auf einschlägigen Webseiten. Viele Schadprogramme, die es auf Daten von Spielern abgesehen haben, verbreiten sich über die Funktionen, die automatisch von Windows ausgeführt werden, wenn man einen USB-Stick einsteckt. Viele Spieler nutzen die mobilen Speichermedien, um z.B. auf Gaming-Partys Software zu tauschen. Die Schadprogramme haben es auf unterschiedliche Daten abgesehen und können diese auf folgende Arten erlangen:

Software-Lizenzschlüssel

Die Lizenzschlüssel für Software werden an unterschiedlichen Stellen im Rechner abgelegt. Häufig sind es bestimmte Schlüssel in der Registry, aber mehr oder weniger versteckte Dateien enthalten an bestimmten Stellen die gewünschte Information. Computerschädlinge aus der Gruppe der Password-Stealer kennen diese Stellen und suchen sie gezielt nach Lizenzschlüsseln für Spiele und andere Software ab. Die erbeuteten Daten werden dann an Server übermittelt, die von den Datendieben kontrolliert werden.

Passwörter im Browser

Alle gängigen Browser bieten Funktionen, um Passwörter und Formulardaten zu speichern. Diese überaus nützliche und bequeme Funktion erleichtert die Nutzung von Passwörtern ungemein. Leider hat sie auch ihre Schattenseiten, denn: Die Daten müssen auf dem Rechner abgelegt werden. Leider sind die Passwörter dabei nur unzureichend gesichert und die oben schon erwähnten Password-Stealer können sie von dort abgreifen und erbeuten. Einige Browser bzw. Browser-Plugins bieten Verschlüsselungsfunktionen, die auf diese Art erbeutete Daten nutzlos machen, sofern die Verschlüsselung mit einem hinreichend langen

Passwort erfolgt. Einige Schadprogramme greifen die Daten daher dort ab, wo sie wieder entschlüsselt vorliegen: In den Formularfeldern der entsprechenden Webseiten. Solche „Form grabber“ können auch die Inhalte von Passwortfeldern auslesen und an die Server der Datendiebe weiterleiten.

Keylogger

Schadprogramme können auch Tastaturaktivitäten mitschneiden. Solche Programme nennt man Keylogger. Diese Bezeichnung greift aber in vielen Fällen zu kurz, weil Keylogger deutlich mehr aufzeichnen können. Die meisten überwachen zusätzlich die Zwischenablage und speichern alles, was in diese kopiert wird. Viele Keylogger machen in regelmäßigen Abständen Screenshots des gesamten Bildschirms oder speichern bei einem Mausclick Ausschnitte um den Mauszeiger. In vielen Fällen sind die Aufzeichnungen an Bedingungen geknüpft, wie etwa der Besuch einer bestimmten Webseite, die Anwesenheit von Webformularen, die Ausführung bestimmter Spiele oder anderer Software. Oft arbeiten die eingesetzten Keylogger aber ungerichtet, womit gemeint ist, dass sie weitaus mehr als die Passwörter von Spielen stehlen. In vielen Fällen verlieren Opfer von Keyloggern den Zugang zum E-Mail-Account, zu Foren, Online-Shops und Sozialen Netzwerken - kurz gesagt: ihre gesamte Online-Identität.

Wörterbuch- und Brute-Force-Angriffe

Die Zugangsdaten zu Accounts von Spielen, Foren etc. können auch über Ausprobieren erlangt werden. Dazu nutzen Angreifer lange Listen von häufigen Passwörtern (Wörterbuchattacke) oder kombinieren wahllos Buchstaben und Zahlenfolgen bis zu einer gewissen Länge (Brute-Force-Attacke). Wer zu kurze oder gängige Passwörter wie „123456“, „Admin“, oder „Master“ verwendet, kann schnell zum Opfer werden und seinen Spiele-Account leer geräumt vorfinden.

Schädlingsfamilien - ihr Verhalten, ihre Aktivitäten

Schadprogramme können aufgrund bestimmter Eigenschaften in ihrem Code erkannt werden. Anhand von Ähnlichkeiten im Programmcode von verschiedenen Schädlingen können die einzelnen Schädlingsvarianten zu Familien zusammengefasst werden. Die häufigsten Familien im Bereich Gaming und ihre typischen Aktivitäten werden hier kurz beschrieben.

OnlineGames

OnlineGames ist die häufigste Familie. Ihre Varianten machen 1,9 % aller Schädlinge im ersten Halbjahr 2010 aus und sie belegt damit Platz 7 der produktivsten Familien. OnlineGames zählt zur Gruppe der Passwort-Stehler. In dieser Familie werden Schädlinge zusammengefasst, die sich nicht auf einzelne Spiele beschränken. Die Liste der attackierten Spiele ist lang und enthält u.a. folgende Spiele:

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

Um sich zu tarnen, integrieren Schädlinge dieser Familie ihre Schadfunktionen in den Explorer. Einige verstecken ihre Dateien und Registry-Einträge auch per Rootkit-Treiber. Damit sie ungestört agieren können, werden auch Antihack-Tools von Spieleanbietern wie z.B. HShield oder GameGuard umgangen. Die meisten OnlineGames-Varianten kopieren sich auf alle Freigaben und tragen sich dort in eine Datei namens autorun.inf ein. Dadurch werden sie z.B. automatisch aktiv, wenn ein USB-Stick oder ein anderer Wechseldatenträger angeschlossen wird.

Magania

Diese Schädlingsfamilie ist vorwiegend in Ostasien aktiv. Mit 1,6 % Anteil am Gesamtvolumen der Schädlinge des ersten Halbjahrs 2010 bringt sie es auf Platz 11 der produktivsten Schädlingsfamilien. Magania gehört zur Gruppe der Keylogger und – das Wortspiel legt es nahe - zielt auf Spiele der taiwanesischen Spieleschmiede Gamania wie z.B. Lineage oder MapleStory. In den meisten Fällen treffen die Schädlinge per E-Mail ein. Wenn der Dateianhang ausgeführt wird, erscheint zur Ablenkung ein Bild. Im Hintergrund wird der Schädling aktiv. Zur Tarnung injizieren sich die Schädlinge der Magania-Familie in die Prozesse des Explorers und des Internet Explorers und sind so für den Anwender unsichtbar. Die gestohlenen Zugangsdaten werden auf mehrere Server im Internet übertragen. Häufig werden noch weitere Schadprogramme unterschiedlichster Art nachgeladen.

WOW

Die Schädlinge der Familie „WOW“ haben es auf Zugangsdaten von World of Warcraft abgesehen. Mit 0,3 % Anteil im ersten Halbjahr 2010 schaffen sie es auf Rang 49. Sie sind damit die größte Familie, die es auf ein einzelnes Spiel abgesehen hat. Die Daten werden per Keylogging gestohlen und an Server im Internet übermittelt. Die gestohlenen Zugangsdaten werden dazu genutzt, um die Accounts der Opfer zu plündern und die virtuellen Charaktere und Güter in einschlägigen Foren zu verkaufen.

Weitere Familien

Auf Platz 75 der produktivsten Schädlingsfamilien des ersten Halbjahrs 2010 steht „Lmir“. Seine Vertreter haben es auf die Zugangsdaten für das Spiel „Legend of Mir“ abgesehen, das insbesondere in China und Südkorea sehr populär ist. Auf Platz 103 folgt Tibia, eine Familie von Keyloggern, die es auf die Zugangsdaten des deutschen Spiels Tibia abgesehen haben.

G Data Webseiten-Analyse

Auf der Grundlage von 66.534 Webseiten aus dem Zeitraum Januar 2010 bis einschließlich Juni 2010 wurden Untersuchungen durchgeführt. Bei den untersuchten Webseiten handelt es sich um detektierte Phishingseiten und Seiten, die Schadcode enthalten.

Die Analysetools der G Data SecurityLabs entdecken und verarbeiten die Webseiten und die dazugehörigen Seiteninformationen automatisch und schreiben die Ergebnisse in eine Datenbank, die dann zur weiterführenden, manuellen Analyse bereitsteht. 6,5 % dieser Seiten sind dem Themenbereich Spiele zuzuordnen. Innerhalb der 6,5 % verteilen sich folgende Themen:

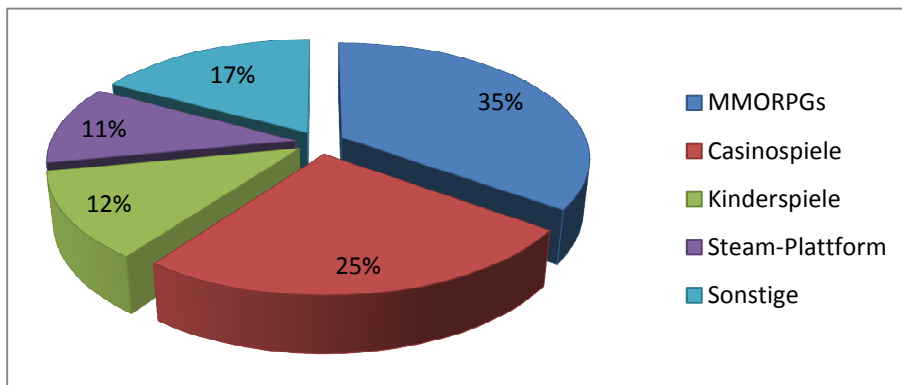
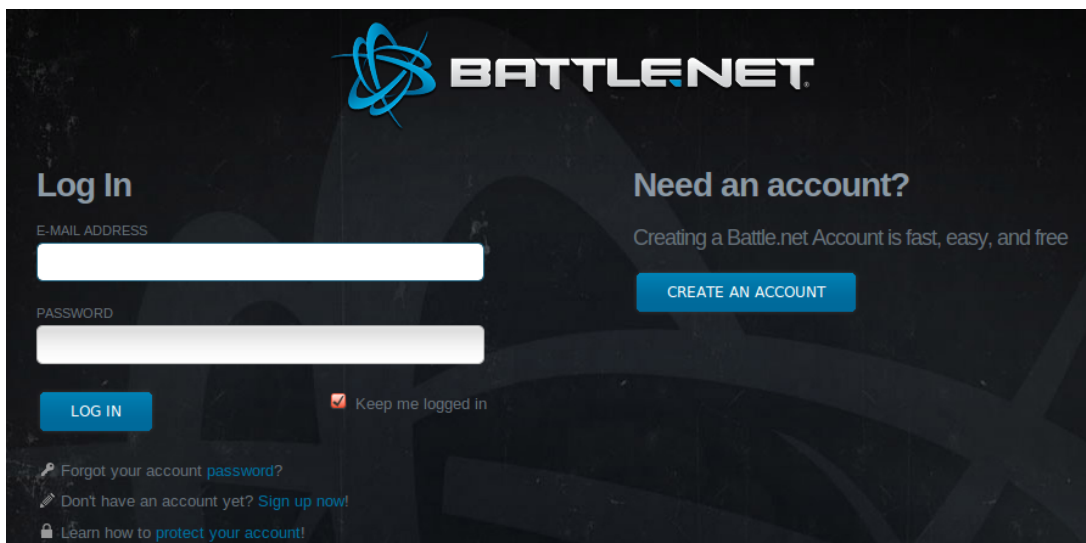


Diagramm 1: Prozentualer Anteil der einzelnen Themen bei untersuchten spielbezogenen Seiten

Die Massen-Online-Rollenspiele belegen mit einem Anteil von 35% eindeutig den ersten Platz: Dazu zählen Spiele wie World of Warcraft, Metin 2, Runescape, Tibia und mehr. Das am häufigste von G Data registrierte Angriffsszenario ist Phishing. Betrüger bauen sich die Original Login-Webseite der jeweiligen Spiele nach, stellen sie auf ihrem eigenen Server online, der typographisch oft kaum von Originalen zu unterscheiden ist, und greifen dann die Login Daten ab, sobald ein Gamer sie auf dieser gefälschten Seite eingibt.



Screenshot 2: Ein Ausschnitt aus einer falschen Login-Seite, die optisch nicht vom Original zu unterscheiden ist

| | |
|---------------------------|--|
| Original (USA) | https://us.battle.net/login/en/ |
| Beispiele für Fälschungen | 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 |

Tabelle 1: Typographische Ähnlichkeit der Webadressen von Battle.net-Phishingseiten zum Original

Gerade im Bereich der Casinospiele (vornehmlich Poker) und der Kinderspiele (oft virtuelle Communities), versuchen Betrüger die Accounts mit angeblichen Bonus-Seiten abzugreifen.

Accounts zur Steam-Plattform sind besonders deshalb gefragt, weil Spieler dort mehrere Spiele innerhalb eines Accounts benutzen können und die Gauner durch Phishing somit unter Umständen nicht nur den Zugang zu einem Spiel bekommen, sondern gleich zu mehreren. Diese Steam-Zugangsdaten werden dann unter anderem im Untergrundmarkt verkauft (siehe Tabelle 2).

In der Kategorie „Sonstiges“ wurden Webseiten eingeordnet, die nicht eindeutig einer der anderen Themenbereiche zugeordnet werden konnten. Unter anderem handelt es sich hier um vereinzelt aufgetretene Spiele, um Webseiten mit sog. Warez (unter anderem Cracks und Keygeneratoren für Spiele), andere Webseiten mit den Wörtern „Game“ oder „Gaming“ in der URL, etc.

Der Untergrundmarkt

Auf den Online-Schwarzmärkten der Untergrundszene wird so gut wie jede Ware verkauft – von Accounts diverser Bezahl Dienstleister und Online-Auktionshäuser über Ausweisdokumente, Kreditkartendaten bis hin zu Zugangsdaten und Keys für Programme und Spiele.

| Steam & Battle.net Accounts | Preis |
|--|---------|
| 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 und 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 |

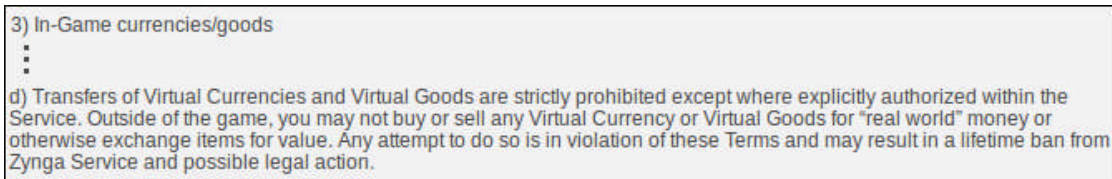
| Gamekeys | Preis |
|--|---------|
| Battlefield: Bad Company 2 – Limited Edition | 15 Euro |
| Assassin's Creed – Special Edition | 12 Euro |
| Command & Conquer 4: Tiberian Twilight | 12 Euro |
| World of Warcraft Wrath of the Lich King – Collector's Edition | 12 Euro |
| World of Warcraft Wrath of 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 |

| Gametime und Points | Preis |
|---------------------------------------|---------|
| Playstation Network Card (50,00 Euro) | 18 Euro |
| Xbox Live 12 Monate Gold | 12 Euro |
| World of Warcraft 60 Tage Gametime | 10 Euro |
| NCSOFT 60 Tage Gametime | 10 Euro |
| 1.000 Sim Points | 8 Euro |
| 1.000 Wii Points | 5 Euro |

Tabelle 2: Auswahl an Preisen für Game-Waren aus einigen Untergrundshops




Verkaufsplattformen

Virtuelle Güter und Accounts werden auch auf anderen, mal mehr und mal weniger legalen, Plattformen verkauft. Sehr beliebt ist ein weltweit bekanntes Online-Auktionshaus. Es haben sich jedoch auch spezielle Spiele-Auktionshäuser gegründet, auf denen nur In-Game Waren und Zugangsdaten verkauft werden. Als Beispiel seien playerauctions.com, mmobay.net oder auch wowbay.net genannt. Der Verkauf und Kauf von Gameartikeln und Accounts außerhalb der Spielumgebung widerspricht jedoch den meisten Nutzungsbedingungen der Spielehersteller, z.B. Blizzard, Zynga, etc.



Screenshot 3: Ausschnitt aus den Nutzungsbedingungen von Zynga, exemplarisch für das Verbot

Als Beispiel: Im Auktionshaus playerauctions.com werden hochwertige Accounts zu ganz anderen Preisen gehandelt, als die schon gezeigten „normalen“ Spiele-Accounts im Untergrund. Der Preis richtet sich nach Level des Charakters, Fähigkeiten, verfügbaren virtuellen Items und dem Server, auf dem dieser Charakter spielt. Das von 29 Accounts aktuell niedrigste Angebot wird für 40 US-Dollar angeboten. Die Angebote in Screenshot 3 zeigen aber, dass deutlich höhere Preise erzielt werden können:

| 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 achivement. | \$670.00 | 24 Hours | Jul-26 | View Details |

Screenshot 4: Die aktuell teuersten Accounts bei playerauctions.com

Durch diese Zahlen wird noch eindrucksvoller deutlich, warum Gamer in der Schusslinie der Cyberkriminellen stehen – Es geht schon lange nicht mehr nur um Spaß, Pixel und virtuelle Goldmünzen, sondern um nicht zu unterschätzende reale Geldwerte!

Schutz vor Angriffen und Betrug

Gamer sollten sich keine Sorgen um ihre Zugangsdaten und die Sicherheit ihres PCs machen müssen. Um den Spielspaß in vollem Umfang zu genießen, sollten folgende Tipps und Hinweise beachtet werden:

- Eine leistungsstarke, aber ressourcenschonende Sicherheits-Software mit http-Filter, Firewall und Wächterfunktion sollte installiert und aktiv sein, um sich vor Spyware und anderen Bedrohungen zu schützen. Eine gute Security Suite ist auf die Anforderungen von Spielern ausgerichtet und bremst den Rechner nicht aus.
- Ein aktueller Spamfilter hilft dabei, unerwünschte E-Mails auszusortieren, bevor sie im Posteingang landen.
- Die Absicherung des eigenen Spiel-Accounts durch ein starkes Passwort ist sehr wichtig. Am besten eignet sich dazu eine mindestens 8 Zeichen lange Kombination aus Ziffern mit groß- und kleingeschriebenen Buchstaben und Sonderzeichen.
- Für jeden Account sollte ein eigenes Passwort erstellt werden und die Passwörter sollten nicht im Browser gespeichert werden. Um sich die vielen Passwörter zu merken, kann man sie aus einem festen Teil und einem variablen Teil zusammensetzen.
- Die Phishing-Angriffe auf Online-Spieler sind oft raffiniert gemacht. Aber ein genauer Blick in die Adresszeile des Browsers offenbart in den meisten Fällen, ob man seine Daten gerade in eine gefälschte Seite einträgt. Ähnlich wie beim Online-Banking gilt auch hier, zur Anmeldung die Seite von Hand oder per Favorit aufrufen und keinesfalls dazu einen Link in einer E-Mail oder einer Webseite folgen.