Zeichen: 3.561 inkl. Leerzeichen (Soll: 3.500 Zeichen)

Autor: Marco Preuss (Director Europe Global Research & Analysis Team bei Kaspersky Lab)

# Gefahr beim Zocken

# Werden Gamer von Cyberkriminellen an die Wand gespielt?

**Auch in diesem Jahr werden auf der gamescom in Köln wieder knapp 300.000 Gamer und Fachbesucher ihre Liebe zu Spielen und Konsolen zelebrieren. Doch bei allem Spielspaß sollten Zocker die eigene Sicherheit nicht aus den Augen verlieren.**

Gaming-Schädlinge sind weiter auf dem Vormarsch. Das zeigen die aktuellen Kaspersky-Zahlen [1]. Demnach konnte Kaspersky Lab im ersten Halbjahr dieses Jahres täglich 11.500 Angriffe auf Spieler in aller Welt verzeichnen. Insgesamt konnten der IT-Sicherheitsexperte zwischen Januar und Juni zwei Millionen Attacken gegen Gamer feststellen. Deutsche Spieler sind mit über 18.000 Angriffen das fünftbeliebteste Ziel von Cyberkriminellen in Europa. Spanien ist am stärksten von den Attacken betroffen, gefolgt von Polen, Italien und Frankreich.

Besorgniserregend ist auch der steile Anstieg an Schadprogrammen, die es explizit auf Gamer abgesehen haben. Deren Zahl kletterte von 3,3 Millionen im Vorjahr auf inzwischen 4,4 Millionen.

## Warum sind Gamer für Cyberkriminelle so attraktiv?

Gamer sind aus vielerlei Gründen ein lukratives Ziel für Cyberkriminelle. Eine Ursache liegt in der Art der Spiele selbst. Mittlerweile hat sich eine eigene Schattenwirtschaft rund um die virtuellen Güter und Schätze beliebter Online-Spiele entwickelt. Sie werden gegen harte Währungen gehandelt. So lässt sich mit gestohlenen Spiele-Account-Daten von professionellen Gamern auch reales Geld erwirtschaften.

Zudem sind Gamer generell Computer-affin, kaufen also regelmäßig online ein und erledigen auch ihre Bankgeschäfte im Netz. Und Gamer verfügen über sehr leistungsfähige Rechner und Netzzugänge, bieten also die idealen Plattformen für Bot-Netze [2].

## Attacken durch Malware und Phishing

Wie stark die Spiele-Industrie ins Visier von Cyberkriminellen geraten ist, zeigt der im April von uns aufgedeckte Fall „Winnti“ [3]. Diese weltweit operierende Organisation manipuliert die Systeme von Online-Spieleherstellern und stiehlt geistiges Eigentum sowie digitale Zertifikate. Der Betrug flog auf, weil ein Trojaner plötzlich auf den Rechnern ausgerechnet jener Gamer zu finden war, die sich alle am gleichen Online-Spiel beteiligten.

Viel öfter aber fangen sich Gamer Schädlinge, also Malware, auf illegalen Tauschbörsen, Piratenservern oder anderen dubiosen Quellen ein, wenn sie von dort ihre Online-Spiele oder Patches beziehen. Auch beim Gaming-spezifischen Phishing beobachtet Kaspersky Lab seit Jahren äußerst überzeugend formulierte Versuche, an die Spiele-Account-Daten von Gamern zu gelangen.

## Wie können sich Gamer schützen?

Viele Spiele bringen die Leistungsfähigkeit der Rechner an ihre Grenzen. Das mag manchen Gamer davon abhalten, sich mit Sicherheitssoftware einzudecken. Doch die genannten Beispiele zeigen: Aktuelle Antiviren-Software ist für Online-Gamer absolute Pflicht! Damit weder PC-Leistung noch Spielfreude beeinträchtigt werden, haben Lösungen wie Kaspersky Internet Security [4] einen Gaming-Modus, mit dem der Spieler sicher und ungebremst in virtuelle Welten eintauchen kann.

Gamer sollten außerdem für ihren Spiele-Account starke Passwörter mit mindestens 14 bis 16 Stellen sowie Buchstaben, Zahlen und Sonderzeichen [5] verwenden, die zusätzlichen Sicherheitsdienste der Spiele-Anbieter nutzen und keine zu hohen Guthaben auf ihren Kundenkonten vorhalten.

Um sich vor Phishing-Attacken zu schützen, hilft auch Gamern oft der schlichte gesunde Menschenverstand. Und der besagt: An Mitspieler gibt man keine Account- oder Bezahldaten weiter! Und E-Mails, die persönliche Daten abfragen, kommen garantiert nicht von seriösen Spiele-Anbietern.

[1] http://www.kaspersky.com/de/news?id=207566701
[2] http://www.kaspersky.com/de/news?id=207566700
[3] http://www.kaspersky.com/de/news?id=207566678
[4] http://www.kaspersky.com/de/internet-security
[5] http://www.kaspersky.com/de/news?id=207566607