



## Presseinformation

### Xbox-Gamer im Visier von Hackern

*Hacker kapern derzeit verstärkt Xbox-Accounts – Spieler geben Zugangsdaten zu leichtfertig aus der Hand – Trojaner durch vermeintlich kostenlose Microsoft Points eingeschleust – Hacker-Software auf YouTube beworben*

**Wien, 06. Februar 2009** – Gamer der Spielkonsole Xbox stehen derzeit im Visier von kriminellen Hackern. Das haben Spezialisten des auf Sicherheitssoftware spezialisierten Unternehmens ESET herausgefunden. Die Cyber-Kriminellen versuchen vermehrt, mit falschen Versprechungen an die Zugangsdaten der Accounts zu kommen oder mittels kostenloser Software gefährliche Trojaner auf die Computer der User zu schleusen.

#### Der Worst Case: Xbox-Account ist verloren

Die Cyber-Kriminellen haben es dabei auf die virtuellen Identitäten der Spieler – die „Gametags“ – abgesehen. Mit Hilfe von Gametags werden Spieler bei Online-Games identifiziert. Punktestand, Fähigkeiten und Ausrüstungsgegenstände der virtuellen Figuren werden damit verwaltet. Wenn Hacker einen Xbox-Account übernommen haben, kann der Spieler im schlimmsten Fall wieder bei Null anfangen. Ein Fremder hat die Online-Identität übernommen, die Gamerscores, die Microsoft Points, die Friends List und käuflich erworbenen Spiele können vollständig verloren sein. „Der Handel mit virtuellen Spielcharakteren, Waffen, Punkten, etc. floriert. Hacker sind

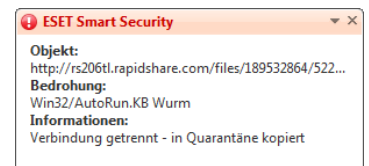
#### Pressekontakt:

Hr. Mag. Klaus Kraigher

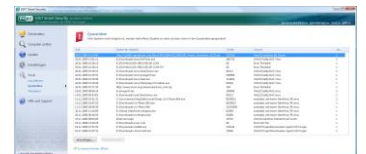
Hohegger|COM  
Schwarzenbergplatz 5|4  
1030 Wien  
Tel.: +43-1-242 02 - 222  
Email:  
[k.kraigher@hohegger.com](mailto:k.kraigher@hohegger.com)

#### Bildmaterial ESET:

Bildmaterial ist in Druckauflösung unter <http://www.eset.at/firmeninfo/presse/xbox> erhältlich:



ESET Alarmfenster



Screenshot Quarantäne-Log



Screenshot



Screenshot



demnach oft finanziell motiviert. Sie können aber genauso einfach nur auf den Kick als bössartiger Outlaw aus sein“, sagt Martin Penzes, technischer Direktor des österreichischen ESET-Vertriebspartners Sicontact.

### **User geben Zugangsdaten zu leichtfertig aus der Hand**

„Von Social Engineering-Techniken bis zu heimtückischer Software unternehmen die Kriminellen alles, um sich Zugang zu den Daten der Gamer zu verschaffen“, erklärt Penzes weiter. Im Rahmen von Social Engineering-Attacken versuchen Hacker mit falschen Versprechungen Zugangsdaten von leichtgläubigen Usern zu stehlen. So werden etwa zusätzliche Features, Punkte oder Game-Levels in Aussicht gestellt. Geben Gamer dafür ihre Nutzerdaten aus der Hand, haben die Hacker leichtes Spiel und übernehmen die entsprechenden Accounts.

### **Trojaner verstecken sich hinter kostenlosen Microsoft Points**

Eine weitere Hacker-Methode ist eine eigens programmierte Software, die Viren und Trojaner enthält. Das Programm „MS Point Generator“ verspricht Gamern kostenlose Microsoft Points. Mit dieser virtuellen Währung können auf der Online-Plattform Xbox live Demos, Videos, Hintergrundbilder und mehr für die Videokonsole Xbox gekauft werden. „Wer die Software installiert, lädt sich selbst einen Trojaner auf den Computer. Denn wie im echten Leben lässt sich auch in der virtuellen Welt Geld nicht per Knopfdruck vermehren“, betont Penzes. „Besonders hinterhältig ist, dass diese gefährliche Software sogar in Videos auf YouTube beworben wird.“

[http://www.youtube.com/watch?v=9CaRqQQHR\\_Y](http://www.youtube.com/watch?v=9CaRqQQHR_Y)

#### **Bildmaterial ESET:**



#### **SICONTACT**



Martin Penzes, Sicontact

#### **Bildmaterial Xbox:**

Bildmaterial rund um die Xbox ist abrufbar unter:  
<http://www.edelman-newsroom.de/cgi-bin/WebObjects/app.woa/wa/Nav/showAssetCompany?type=Image&cid=10&oid=285>



In dem Programm versteckt sich der Trojaner Win32/AutoRun.KB, der allerdings von ESET Smart Security und ESET NOD32 Antivirus erkannt wird. Schädlinge der AutoRun-Kategorie führen seit Monaten die Virus-Charts von ESET an und stellen somit derzeit eine der größten Gefahren für PC-User dar.

### **Sicherheitstipps für Xbox-Gamer**

Mit einigen einfachen Sicherheitsvorkehrungen sind Xbox-Spieler vor Hacker-Attacken sicher:

- Verraten Sie niemals Ihre Zugangsdaten im Tausch gegen virtuelles Geld, Punkte, Levels oder ähnliches. Hacker haben es auf Ihr Gametag abgesehen!
- Installieren Sie keine Software aus unseriösen Quellen!
- Offizielle Xbox live-Vertreter fragen online niemals nach Ihren Log In-Daten. Geben Sie Ihre Zugangsdaten fremden Personen keinesfalls bekannt!
- Schützen Sie Ihren PC mit aktueller Antivirussoftware!

Diesen Presstext finden Sie auch unter:

<http://www.eset.at/firmeninfo/presse/presseaussendungen>

Fotomaterial in druckfähiger Auflösung ist zum honorarfreien Download abrufbar unter:

<http://www.eset.at/firmeninfo/presse/xbox>.

### **Über ESET und NOD32**

ESET, gegründet 1992 in Bratislava (Slowakei), ist ein globaler Entwickler und Hersteller von sicherheitstechnischen Softwarelösungen, ESET NOD32



Antivirus das weltweit in vielen unabhängigen Tests ausgezeichnete Antivirenprogramm von ESET. Es bietet maximalen Schutz vor elektronischen Schädlingen mit minimalem Einsatz von Computerressourcen. ESET NOD32 Antivirus ist für die Betriebssysteme Microsoft Windows 2000 bis Windows Vista und unterschiedliche Linux-Distributionen sowie auch für Novell erhältlich, die Sicherheitssuite mit integrierter Firewall und Spamschutz ESET Smart Security läuft unter Microsoft Windows 2000 bis Windows Vista. ESET Mobile Antivirus schützt Windows Mobile Endgeräte vor Spam und Malware. Vertrieben wird die Software über Partner in mehr als 100 Ländern. Seit April 2007 ist die Sicontact Software Vertriebs GmbH mit Sitz in Wien der exklusive Vertriebspartner von ESET in Österreich. Für Institutionen im Bildungs-, Gesundheits-, Behördenbereich sowie für Schüler und Studenten bietet ESET bis zu 50 Prozent Rabatt. Weitere Informationen zu ESET, ESET NOD32 Antivirus, ESET Smart Security und ESET Mobile Antivirus finden Sie im Internet unter [www.eset.at](http://www.eset.at) und <http://www.eset.at/firmeninfo/presse>.