

Punkbuster: Böse Lücke im Streaming-System

2008-09-20 18:32

Am 12. September 2008 hat ein streamender Server manipulierte Logfiles verarbeitet und falsche Daten via Stream an einen großen Streaming-Anbieter verschickt. Diese Daten sorgten dafür, dass Spieler auf deren Bannliste landeten, die sich aber tatsächlich nichts hatten zuschulden kommen lassen.

Laut bashandslash.com hat eine Hacker-Seite kurz nach dem Bekanntwerden der Lücke im Punkbuster-Datentransfer einen Versuch gefahren. Dazu hätten sie einen Game-Server in der Schweiz gemietet und sich bei <http://www.pbbans.com>, einer sehr bekannten und viel genutzten Streaming Community, angemeldet. Über den Datenstrom zu diesem Anbieter haben sie es dann durch manipulierte Logfiles geschafft, 80 spanische BF2-Spieler auf die Bannliste von pbbans.com zu setzen.

Doch was bedeutet das für Admins und Spieler? Ist Punkbuster selbst nun nutzlos oder gar gefährlich geworden?

Nein. Das Programm Punkbuster basiert auf Kicks, die einen Spieler immer wieder vom Game-Server schmeißen, bis er die Ursache für diese Kicks entfernt hat.

Will ein Server-Admin Aimbot-Nutzer, Wallhacker etc. jedoch dauerhaft von seinem Server fernhalten, muss er die entsprechenden Logfiles dieser Kicks sichten und die Schuldigen einzeln manuell von seinem Server bannen.

Da diese Arbeit mühsam und nur auf den einen Game-Server beschränkt ist, Cheater jedoch nicht nur auf einem Server aktiv sein dürften, entstanden die freiwilligen, vom Punkbuster-Hersteller Evenbalance unabhängigen Streaming Communities.

Diese sammeln die übermittelten Daten von angemeldeten Servern in Echtzeit, stellen aus diesen Logfiles Bannlisten zusammen und bieten sie wiederum zum Download für jeden an. Jede Streaming-Community im Netz hat ihre eigenen Bannlisten, die sie an die angemeldeten Server-Admins verteilen und es dadurch Wiederholungstätern sehr viel schwerer machen, ihre Cheats auf Servern zu nutzen.

Und genau in diesen Datenstrom im pbbans.com-Netzwerk haben die Hacker manipulierte Dateien eingeschleust und die Informationen auf den Bannlisten dadurch verfälscht.

Wer ist von der jetzt entdeckten Lücke überhaupt betroffen?

Betroffen sind aktuell jene Admins, welche die Bannlisten von pbbans.com nutzen, da diese fehlerhafte Informationen enthalten können. Außerdem wird davon jedes Punkbuster-unterstützte Spiel berührt, welches die Streaming-Gesellschaften betreuen.

BITTE BEACHTEN!

Die offizielle **MASTER BAN LIST** (MBL) vom Punkbuster-Hersteller <http://www.evenbalance.com> hat mit dem ganzen **nichts** zu tun!

Darauf landen nur Spieler, die mittels PB-HACK das Programm Punkbuster selbst umgehen wollen. Jeder Streaming-Anbieter im Netz hat seine eigenen Bann-Listen, die **nichts** mit der offiziellen MBL von

Punkbuster selbst zu tun haben!

Einen globalen Bann oder gar Hardware-Bann wird man über das Streamen und diese entdeckte Lücke nicht erhalten! Punkbuster selbst funktioniert weiterhin problemlos! Deshalb bitte keine Panikaktionen starten und diesen deaktivieren!

Dieser erste aufgedeckte Angriff betraf pbbans.com, jedoch ist nicht auszuschließen, dass auch andere Streaming-Gesellschaften irgendwann Zielscheibe einer solchen massiven Manipulation werden könnten oder bereits geworden sind. Momentan ist nur bekannt, dass für einen derartigen Eingriff in den Datenstrom ein entsprechend eingerichteter und bei dem Streaming-Anbieter angemeldeter Game-Server verantwortlich ist.

Das heißt im Klartext, dass das System des Streamens, welches ursprünglich als ein wertvoller zusätzlicher Schutz und Arbeitserleichterung für alle Server-Admins gedacht war, nun unsicher und damit nicht mehr nutzbar ist, solange diese Lücke nicht gefunden und gefixt wurde.

pbbans.com geht davon aus, dass dieses Problem nur durch Evenbalance selbst gelöst werden kann und hat eine Petition gestartet: [pbbans-Petition](#)

Ob und inwiefern Evenbalance reagieren kann und muss, wird sich noch herausstellen. Momentan liegen leider noch nicht genug Informationen vor um festzustellen, wer tatsächlich diese Lücke schließen kann.

2008-09-20 18:32 von [OL]YODA