Achtung Potter-Fans: Finger weg von kostenlosen Preview-Angeboten

Millionen Harry Potter-Fans in Deutschland und weltweit können es kaum erwarten den neuen Harry-Potter-Film „Harry Potter und der Halbblutprinz“ zu sehen. Aber Vorsicht: Einige kriminelle Muggel (so heißen die Nicht-Zauberer in den Romanen von Joanne K. Rowling) versuchen im Internet den Hype um den jungen Zauberer auszunutzen, wie das australische Sicherheitsunternehmen PC Tools herausfand. Die Sicherheitsexperten warnen vor Quellen, die den Film angeblich kostenlos zum Anschauen im Internet anbieten.

Die Internet-Kriminellen bedienen sich dabei populärer Internettauschbörsen, Blogs und sozialer Netzwerke wie etwa digg.com, blogspot.com, um die Potter-Fans zu erreichen. Freunde des jungen Zauberers finden dort verlockenden Angebote wie *„‘Harry Potter und der Halblutprinz‘ kostenlos online anschauen“*. Zusätzlich kommen Kommentare zum Einsatz, die mit Schlüsselwörtern gespickt sind, um die Lock-Angebote in den Trefferlisten der Internet-Suchmaschinen auf vordere Plätze zu bringen. Auf dem ThreatFire Research Blog von PC Tools ist ein Beispiel für ein solches Lockangebot im Bild zu sehen: http://blog.threatfire.com/2009/06/wanna-see-harry-potter-and-half-blood.html

So oder so ähnlich sehen die Lockangebote aus, mit denen gutgläubige Potter-Fans geködert werden

Computer-Schädling statt Filmgenuss

Wer auf den Link im Lock-Angebot klickt, kommt auf einen Blogspot-Beitrag, der weitere Bilder aus dem Film enthält und den Eindruck vermittelt, man sei nur noch einen Klick vom Filmgenuss entfernt. Tatsächlich wird man jedoch aufgefordert, einen „Streamviewer“ herunterzuladen und zu installieren, den man angeblich benötigt, um den Film ansehen zu können. Hinter diesem “Streamviewer” verbergen sich jedoch täglich wechselnde Schadprogramme (sogenannte “Malware”), die im Computer des Benutzers auf unterschiedlichste Art und Weise Schaden anrichten können.

Um sich vor dieser und ähnlichen Bedrohungen zu schützen sollten Anwender bei Download-Angeboten sehr vorsichtig sein. Ist ein Angebot eigentlich „zu schön um wahr zu sein“, steckt in der Regel eine böse Absicht dahinter. Als technische Maßnahme, um das Computersystem und die eigenen Daten vor Online-Bedrohungen zu schützen, empfiehlt sich eine Kombination aus herkömmlicher Antiviren-Software und verhaltensbasiertem Schutz, beispielsweise durch ThreatFire von PC Tools. Threatfire ist für Privatanwender kostenlos.

„Hacker sind heute nicht mehr auf eine möglichst weite Verbreitung einer bestimmten Malware aus. Sie wechseln regelmäßig zwischen verschiedensten Arten und Varianten von Schadsoftware und passen auch die Lockangebote ständig an das aktuelle Geschehen an, um weniger berechenbar zu sein und ‚unter dem Radar‘ der Antivirenwächter zu bleiben,“ warnt Michael Greene, Vice President für Produktstrategie bei PC Tools. *„Wir haben ähnliche Bedrohungen rund um die Geschehnisse im Iran, die Schweinegrippe, den Absturz der Air-France-Maschine und andere aktuelle Ereignisse gesehen.“*