



Sicherheitslücken, Falschaussagen

Das Half-Life-Debakel

Valve ist das Opfer des spektakulärsten Kriminalfalls der PC-Spielegeschichte.

Gestohlener Quelltext und Alphaversion erlauben peinliche Blicke hinter die Kulissen.

Bis vor wenigen Wochen sah es für Valves **Half-Life 2** nach einem Sieg in allen Disziplinen aus. Engine, Charaktere und Spielwelt sollten das Shooter-Genre in die nächste Generation katapultieren. Die gesamte Presse – auch GameStar – war voll des Vorablobes. Seit dem 19. September 2003 ist alles anders: An diesem Tag stehen Cracker aus Valves Firmen-Netzwerk, woran das vierzigköpfige Entwickler-Team in den letzten Jahren unter höchster Geheimhaltung gearbeitet hat: Der **Half-Life 2-**

Quelltext steht ebenso illegal wie frei zugänglich im Netz. Kurz darauf folgt gar eine spielbare Version. Wir haben recherchiert, was bei den Angriffen geschehen ist und was die Konsequenzen sind.

Uns geht es nicht um die Demontage von **Half-Life 2**, das wir nach wie vor für einen der zwei spannendsten kommenden Action-Titel halten (zusammen mit **Doom 3**). Aber wir wollen der Frage nachgehen, ob Valve der Spielewelt wissentlich ein nicht haltbares Release-Datum genannt hat.

19. September 2003: Der Sourcecode-Diebstahl

Als Valves Geschäftsführer Gabe Newell am 2. Oktober in einem Fan-Forum um Hilfe bittet, kann man sein Entsetzen förmlich spüren: Jemand hat den kompletten **Half-Life 2**-Sourcecode (von Version 0.0 an) aus dem Firmen-Netzwerk gestohlen und veröffentlicht. Für diese Software zahlen Lizenznehmer wie Troika (**Vampire 2**) üblicherweise Millionenbeträge. Ein uns be-

kannter Spezialist hat das Datenpaket analysiert, einen Microsoft **Visual Studio 6**-Code in der Programmiersprache C++. Mit überraschendem Ergebnis: Valve hat offensichtlich viel mehr verloren, als zunächst gedacht. Die gestohlene Software enthält das komplette »Master Development Directory« mit allen Routinen und Tools (für Grafik, Sound, Levels), die zur Entwicklung verwendet werden. Die insgesamt 2.198.000 Zeilen lassen sich ohne einen Fehler kompilieren; ein Athlon 2500 braucht dafür rund eine Stunde. Das widerlegt die Aussagen von Christophe Ramboz, Präsident der Spielesparte von Vivendi Universal. Der hatte kurz nach dem Diebstahl behauptet, nur ein Drittel des Codes sei gestohlen worden.

So ging der Cracker vor

Was ist passiert? Schritt 1: Über eine ungepatchte Sicherheitslücke in Microsoft Outlook erlangt der Angreifer vollen Zugriff auf Newells Arbeitsrechner samt Administrator-Rechten. Schritt 2: Via Hacker Defender



So unfertig sieht eine Vielzahl der Levels in der **Half-Life-2-Alpha** aus.

(schützt Hacker-Dateien vor Entdeckung) kopiert der Angreifer Software zum Packen und Transferieren von Dateien auf das System. Darunter ist auch das Fernwartungswerkzeug RemotelyAnywhere. Dessen Installations-Routine war eigens für diesen Angriff angepasst. Schritt 3: Ein sogenannter Key-Logger zeichnet sämtliche Tastatureingaben auf, darunter Server- und E-Mail-Passwörter. Der Cracker wertet diese aus – und kann fortan als zweiter Gabe Newell im Firmennetz frei schalten und walten.

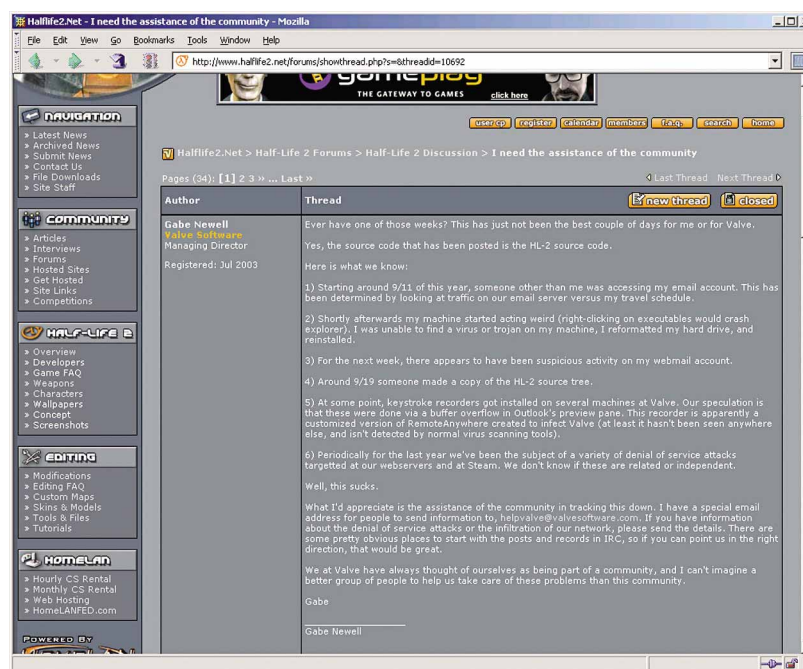
Auch als Gabe Newells Rechner sich seltsam verhält und nach Rechtsklicks abstürzt, schöpft Gabe keinen Verdacht – laut Anti-Viren-Software ist alles OK. In der folgenden Woche gibt es rätselhafte Aktivitäten auf dem Webmail-Account des Geschäftsführers. Bis der Unbekannte am 19. September schließlich eine Kopie des Sourcecode-Trees erstellt. Erst zwei Wochen später, nachdem es längst zu spät ist, kappt Valve die Internet-Verbindung: Mittlerweile sind weitere Firmen-PCs infiziert.

Das alles ist zumindest Valves Darstellung nach passiert. Es gibt aber Anzeichen, dass der Einbruch anders – noch einfacher – vonstatten ging. Doch auch der geschilderte Ablauf erfordert kein extremes Fachwissen, sondern ist typisch für einen Angriff auf schlecht gesicherte Systeme. Jeder einigermaßen versierte Internet-User könnte das wiederholen. Man würde von einer Top-Firma wie Valve erwarten, dass sie ihre einzige Geschäftsgrundlage, eben den Quellcode, besser schützt. Etwa durch nicht vernetzte Server, Authentifizierung per Dongle oder per Digital Rights Management. Gerade Newell als ehemals leitender Microsoft-Angestellter hätte mehr auf die Sicherheit seines Netzwerks achten können.

Fatale Folgen

Da Texturen, Modelle und generelle **Half-Life 2**-Inhalte fehlen, ist der reine Quelltext für Spieler zunächst unbrauchbar – wie ein Automotor ohne Lenkrad, Karosserie und Reifen. Auch Valves Konkurrenz kann wenig Nutzen aus der C++-Textwüste ziehen. Zudem würde jeder, der Programmteile 1:1 kopiert, immense Schadensersatzklagen riskieren. Doch Klagen drohen nun eher Valve: Offenbar sind im geklauten Quelltext Teile der lizenzierten **Havok**-Physik-Engine enthalten. Ob die Firma Havok Incorporated es still erduldet, dass womöglich Fahrlässigkeit zur freien Verbreitung ihres geistigen Eigentums geführt hat?

Freude kommt nur bei Cheat-Entwicklern und Crackern auf. Anhand der penibel dokumentierten Codezeilen können sie Funktionen studieren, um in Zukunft Multiplayer-Partien zu ruinieren. Schlimmer



Helpvalve@valvesoftware.com: Gabe Newell fordert die Half-Life-Community in diesem Forumsbeitrag auf, Valve bei der Suche nach dem Sourcecode-Dieb zu unterstützen.

noch, der Sourcecode verrät fast alles über Valves Vertriebsplattform **Steam**. Wenn der Hersteller diese Passagen nicht komplett neu schreibt, sind persönliche Daten der **Steam**-Nutzer wie Name, Adresse und Kreditkartennummer problemlos auslesbar. Auch die Routinen zur CD-Key-Verifizierung liegen offen. Sicher, das kann Valve beheben. Aber ob sich der Vertrauensverlust von Nutzern und potenziellen Lizenznehmern ohne weiteres patchen lässt?

7. Oktober: Alpha-Version geklaut

Am 7. Oktober 2003 setzt ein zweiter Cracker noch einen drauf: »Viel Spass mit Half-Life 2. Nach der Quelltext-Veröffentlichung gab es keinen Grund, die Version länger für mich zu behalten«. Der »Anonymous Leaker« stellt eine Version ins Netz, die er vermutlich am 26. September gestohlen hat – zumindest wird dieses Datum nach dem Start eingeblendet. »Ich betone, dass diese Version alles ist, was in Valves Netzwerk zu finden ist.« Und weiter: »An Valve: Ich schlage vor, dass ihr aufhört, eure Kunden darüber zu belügen, was und wieviel gestohlen wurde. Ihr wisst genau so gut wie ich, was ihr habt.«

Wir wissen nicht, ob der Räuber die Wahrheit sagt – er könnte die Datumsanzeige auch selbst eingebaut haben. Mehrere Fakten sprechen aber dafür, dass es sich bei der Alpha-Version wirklich um das Neueste handelt, das Valve zu bieten hat. Wenn dem so wäre, müsste man alle Aussagen der Firma aus den letzten Monaten, die vom 30. September 2003 oder auch nur von der diesjährigen »Holiday Season« (Weihnachtszeit) als Releasetermin gesprochen haben, als bewusste Falschaussage einstufen.

Testspiel der Alpha-Version

GameStar hat LAN-Teilnehmern lange beim Spielen der Alpha-Version über die Schulter geschaut. Und dabei folgendes festgestellt: Das entpackt 3,2 GByte große Datenpaket enthält alle von **Half-Life 2** bislang offiziell vorgestellten Levels, Charaktere und Inhalte – aber sonst nichts. Zu sehen sind die Fahrt mit dem Buggy, Dr. Kleiners Labor inklusive Gefährtin Alyx, der spinnenartige Strider sowie das auf der E3 gezeigte Material.

Nun könnte man meinen, dabei handele es sich um eine abgespeckte Version zu Demonstrationszwecken – in diesem Fall hätten die Cracker es versäumt, die aktuelle Version zu finden. Doch erstens scheinen die Einbrecher über einen längeren Zeitraum freien Zugriff auf das Valve-Netzwerk gehabt zu haben, wodurch ihnen die angenommene »echte« Version kaum entgangen wäre. Zweitens hängen in der Alpha-Version nur ein einziges Mal zwei Level-Abschnitte zusammen – dem Rest der Karten fehlen Ein- und Ausganges



Ein LAN-Teilnehmer spielt die illegale Alpha-Version.

Von weitem nicht zu sehen: Die Gebäude im Hintergrund hängen teilweise in der Luft oder besitzen keine Rückwand.



punkte. Bei einer abgespeckten Version würden zwar Teile des Spiels fehlen, aber die vorhandenen wären sicherlich miteinander verbunden. Indiz Nummer drei: Auch die erst kürzlich veröffentlichte DirectX-9-Technik-Demo (GameStar 11/2003) ist enthalten.

Längst nicht fertig

Noch auf der Spielmesse ECTS (28. bis 30. August 2003) beteuerte Valve-Mitarbeiter Greg Coomber, dass »es zwar eng wird, Half-Life 2 aber pünktlich am 30. September erscheint.« Eine Woche vor dem ominösen Termin verschiebt Valve das Vorhaben plötzlich: »Das bisherige Datum hat sich verschoben, wir peilen jetzt die Weihnachtsferien an, aber ohne einen konkreten Erstverkaufstag.« Was wir anhand der illegalen Version gesehen haben, lässt diese Erkenntnis als reichlich verspätet erscheinen: Die Version ist noch meilenweit von der Veröffentlichung entfernt.

Ein Beispiel: Die bereits aus Videos bekannte City-17-Straßenschlacht, in der Sie sich an der Seite von KI-Mitstreitern Meter um Meter gegen die Combine-Soldaten vor-

kämpfen, ist nicht wirklich spielbar. Wie Hollywood-Kulissen hängen einzelne Häuser und Objekte in der Luft oder haben keine Rückseite. Wie in fast allen Levels gibt es keine Kartengrenze, Gordon fällt irgendwann ins Clipping-Nichts.

Scripts statt KI

Auch die künstliche Intelligenz der Mitstreiter reagiert keinesfalls eigenständig auf komplexe Situationen, sondern beruht auf vorberechneten Ereignissen (Scripts): Eine Tür wird wie von Geisterhand eingetreten, keine Figur ist weit und breit zu sehen. Auf der E3 stellte Gabe Newell genau die gleiche Szene vor, allerdings mit Gegnern. Dabei machte er dem versammelten Fachpublikum weis, die Schurken würden selbständig die Tür eintreten. Mittlerweile hat Valve die KI-Lücken zugegeben. In einem Forumsbeitrag schreibt Valve-Mann Chris Borkitch: »Die gezeigten KI-Szenen sollten nur ein Ausblick auf das sein, wie es im fertigen Spiel mal funktionieren wird.«

Das finden wir an sich nicht verwerflich – die meisten Designer arbeiten während der Spiele-Entwicklung mit Platzhaltern. Aber in Kombination mit Valves fortlaufenden Termin-Beteuerungen entstand ein völlig falsches Bild bei Spielefans und Presse. Gabe Newell rechtfertigt sich so: »Wir haben am 30. September nur festgehalten, um uns selbst ein klares Bild vom Release-termin bilden zu können.«

Benchmarks ohne Aussagekraft

Ähnlich irreführend sind die von Valve verlautbarten Benchmark-Ergebnisse, bei denen Nvidias Geforce-Chips erheblich schlechter abschneiden als die Radeons von Ati. Der Hintergrund: Ati-Karten berechnen Texturen in 24 Bit, getreu der DirectX9-Spezifikation. Nvidias Chips fahren zweigleisig: Weniger detaillierte Pixel-Shader werden derzeit nur mit 16 Bit, hochdetaillierte hingegen mit 32 Bit gerendert. Bei den von Valve verwendeten Treibern führte das zu weniger Leistung.

Doch mit den aktuellen Treibern – so zeigten Versuche mit der Alphaversion, denen wir beiwohnten – liegen die Nvidia-Chips bereits gleichauf, in manchen Szenen sogar vorn.

Wie uns Branchen-Insider verriet, sitzen längst Experten beider großen Grafikfirmen direkt bei Valve, um dort die Source-Engine an ihre jeweiligen Chips anzupassen. Wieso trotzdem immer wieder eine der beiden Firmen öffentlich von Valve bevorzugt wird? Weil dabei viel Geld fließt. Erstmals vorgestellt wurde **Half-Life 2** im März 2003 – auf Nvidias Geforce Ti 4600. Zwei Monate später aber war das Spiel auf der E3 plötzlich exklusiv am Ati-Stand zu finden. Ati hatte sich nämlich mittlerweile für 6 Millionen US-Dollar die offizielle Valve-Partnerschaft gesichert. Die führt auch dazu, dass neuerdings allen Radeon-Karten **Half-Life 2** beiliegt. Freilich nur als Gutscheine. Wann der einzulösen sein wird und wie das mit dem deutschen Jugendschutzgesetz klappen soll, weiß vorerst niemand.

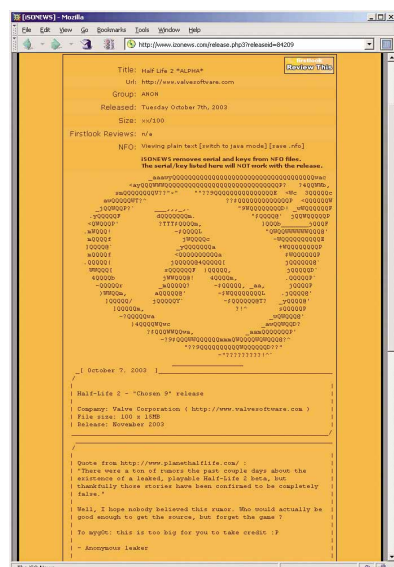


Statt Half-Life 2 liegt Radeons dieser **Gutschein** bei.

Wann kommt's denn nun?

Wir wagen eine Prognose: **Half-Life 2** wird nicht bis Weihnachten 2003 erscheinen! Uns erscheinen die Indizien schlüssig, dass die geklaute Alphaversion ungefähr den tatsächlichen Stand der Entwicklung aufzeigt. In diesem Fall ist noch viel zu programmieren, bis aus den vorliegenden Fragmenten das packende Spiel wird, das wir uns alle wünschen. Zudem muss Valve viele sensible Passagen neu schreiben, die mit dem Sourcecode aufgedeckt wurden, darunter den Netzwerk-Code, die CD-Key-Abfrage und die sensiblen **Steam**-Funktionen.

Offiziell spricht Publisher Vivendi bereits von einer Verschiebung bis April 2004. Inoffiziell hörten wir aus dem selben Hause »erst in einem Jahr«. Wer einen Release um den Oktober 2004 herum für völlig unglaublich, weil viel zu spät, hält: Schon bei der Vorstellung des Vorgängers auf der E3 1997 präsentierte Valve fantastische Technik-Tricks und wollte drei Monate später fertig sein. Doch **Half-Life** ließ noch anderthalb Jahre auf sich warten. Manchmal wiederholt sich Geschichte – auch wenn wir es in diesem Fall nicht hoffen wollen.



Als 100 jeweils 15 MByte große Dateien veröffentlicht »Anonymous Leaker« die **spielbaren Inhalte** im Netz.