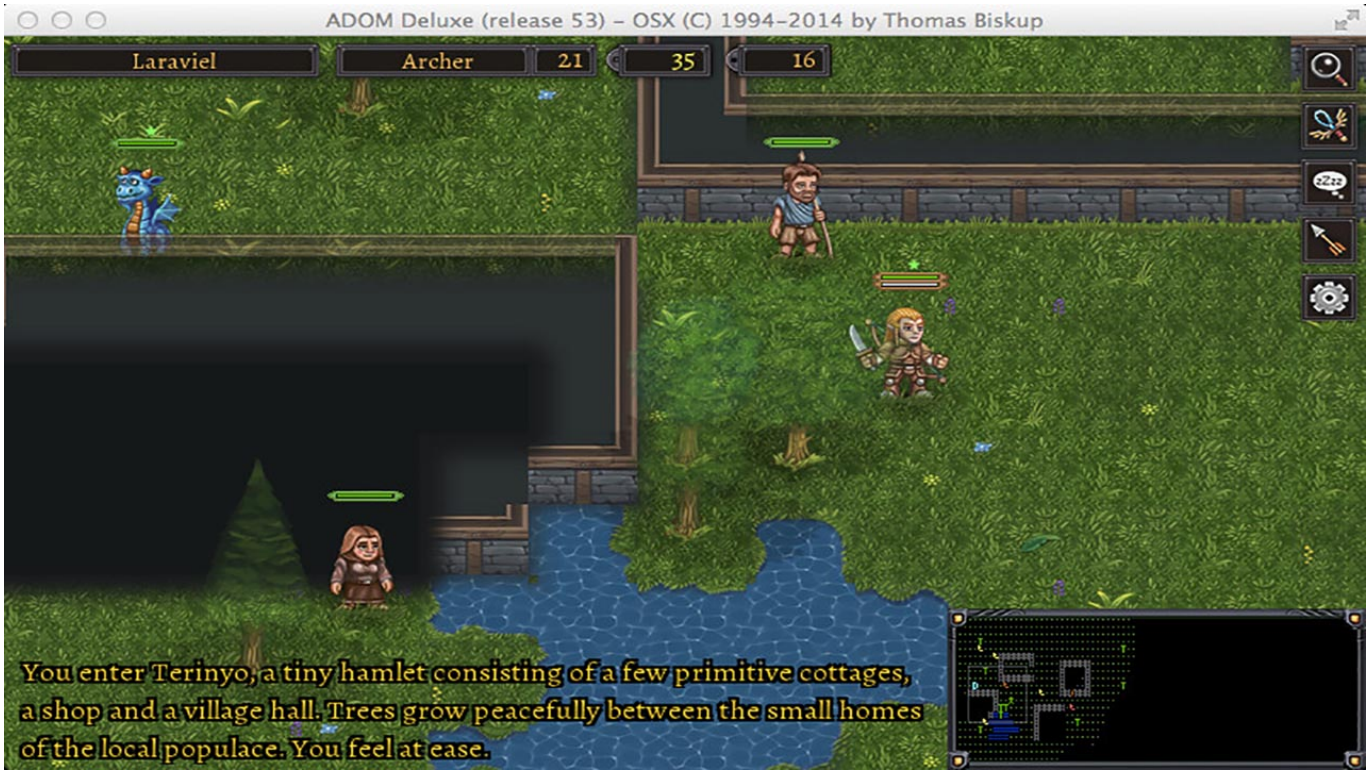
ADOM (Ancient Domains of Mystery)

ADOM (Ancient Domains of Mystery) è un RPG roguelike a turni pubblicato originariamente nel 1994 da **Thomas Biskup** su **Linux**. Inizialmente, la versione "originale" del titolo era stata sviluppata basandosi sul linguaggio di programmazione **C** ed è stata aggiornata costantemente fino al novembre del 2002, venendo trasportata, negli anni, anche sugli altri sistemi operativi conosciuti. Il gioco di cui sto parlando quest'oggi è "nato" invece grazie a un crowfunding ideato nel 2012 sulla famosa piattaforma **Indiegogo** (nella quale il creatore aveva proposto, per la modica cifra di 50.000 dollari, la possibilità di ricevere il codice per intero del suo gioco recapitato da lui in persona), che ha portato al rilascio di una versione "deluxe" su **Steam**, compatibile con **Windows**, **Linux** e **macOS**. All'interno del gioco vestiremo i panni di un'eroe incaricato di salvare la terra di **Ancardia** dalla forza maligna del caos.



Il titolo è stato dotato di una semplificazione a favore dei neofiti, con un'utile **modalità tutorial** e **difficoltà di gioco** scalabili a seconda delle capacità di ogni giocatore, nonché svariate modalità: una **modalità custom**, che permette di modificare a piacimento la difficoltà, mentre la **story mode** consente, a differenza delle difficoltà base, di salvare e ricaricare i salvataggi anche dopo la morte, e infine la **Crowd mode** che permette di giocare con degli amici. Come ogni RPG, che si rispetti anche *ADOM* ha una personalizzazione del personaggio ampia, molto ampia. Il nostro eroe, può essere generato casualmente o creato con le nostre mani. Il sistema di personalizzazione offre la bellezza di **12 razze** e altrettante, se non di più, classi (combattente, ladro, mago, cavaliere del caos ecc ecc). Ovviamente, ogni razza offre un bonus nelle statistiche mentre le classi, invece, hanno dei punti di forza e dei svantaggi unici. L'essere strutturato in turni permette al giocatore di strutturare il suo gameplay in maniera strategica, cambiare armi, scegliere la miglior mossa e quale nemico attaccare prima, tutto questo rende l'ambiente di gioco più piacevole e, soprattutto, interessante.

All’interno del titolo sono presenti molte **armi**, che variano da semplici spade a bacchette magiche. Un altro elemento importante che in *ADOM* è fondamentale è la **fame**. Se il nostro personaggio non si nutrirà a dovere, dopo un determinato numero di turni comincerà a **morire di fame**. Tuttavia, non è questa l’unica limitazione: infatti, dovrete cibarlo solamente con ottime razioni di cibo perché l’alimentazione a base di carne di mostro marcia potrebbe avvelenarlo o farlo ammalare. Inoltre, durante i movimenti del nostro personaggio sul territorio della mappa, si ha la possibilità di imbattersi in nemici di vario tipo: branchi di iene, goblin e tanto altro.

Sul piano grafico, il titolo è stato svecchiato grazie all’aggiunta di una grafica in stile cartoon senza molte pretese. Gli **effetti sonori** sono ben congegnati e la colonna sonora rimane orecchiabile anche dopo un periodo di gioco prolungato.

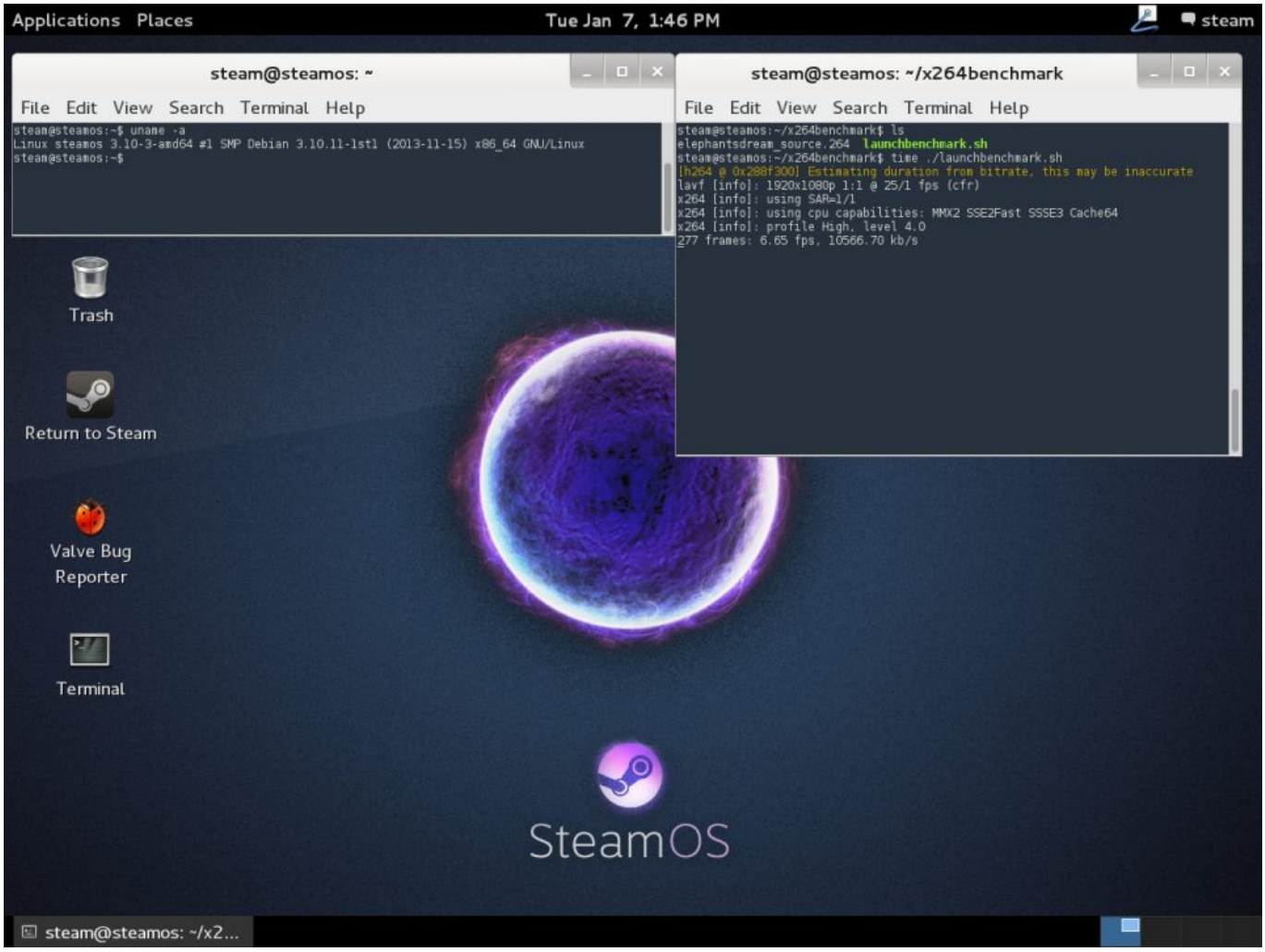
In conclusione, si può dire che *ADOM*, anche dopo tutti questi anni, rimane comunque una validissima scelta nel campo dei **roguelike**, grazie alle sue meccaniche, forse un po' datate, ma comunque ben strutturate. Il titolo del buon vecchio **Biskup**, anche dopo tutto questo tempo, riesce a far passare le varie ore di gioco con un pizzico di ansia e di piacevole gameplay che, ancora oggi, viene aggiornato costantemente con il rilascio di nuove patch. Titolo consigliato, soprattutto a tutti gli amanti dei videogiochi old-style.

Steam Machine e il gaming su Linux, occasione sprecata?

Facciamo un salto nel 2012: viene presentato **Windows 8**, nuova versione del sistema operativo **Microsoft**, successore di **Windows 7**. Anche qui non sono mancate le critiche, in primis rivolte a due delle novità appena presentate: l'introduzione del **Windows Store**, uno store proprietario e chiuso, simile a quello presente sui device **Apple**, dove non tutte le applicazioni disponibili per PC sono incluse nel negozio. Le critiche vengono principalmente dal mondo videoludico, capitanate da **Notch**, creatore di ***Minecraft*** che decise di non certificare la propria opera per il nuovo sistema operativo di casa Redmond. Successivamente tuonarono anche **Rob Pardo** di **Blizzard** e soprattutto **Gabe Newell**, capo di **Valve** che, con l'introduzione di **Steam** ha letteralmente resuscitato il gaming su **PC** diventando ben presto la bandiera videoludica della piattaforma, con circa il 75% dei giochi rilasciati sugli home computer di tutto il mondo.
Newell arrivò a definire il **Windows Store** e l'avvio protetto di **Windows 8** (che praticamente impediva l'installazione di qualsiasi altro sistema operativo) una «catastrofe per il mondo PC» ed espresse pieno supporto per l'ecosistema **Linux**, che, a suo avviso, rappresenta appieno la filosofia open source dell'home computing. Da lì a poco tempo, arrivò prima un client ufficiale di **Steam** per

Linux, seguito dalla modalità **Big Picture** e poi l'annuncio tanto atteso: il concetto di **Steam Machine**, un PC fortemente "consolizzato" e prodotto da terze parti come **Alienware** o **Gigabyte**, e supportato da **SteamOS**, sistema operativo basato su **Debian** (in questo caso si parla di *fork*, essendo una versione derivata dal sistema operativo di base) di **Linux** più usate ed apprezzate dagli utenti del pinguino.

Sulla carta sarebbe dovuto essere un successo: nessuna fatica per l'utente medio che vuole giocare su PC ma che, magari, è spaventato dall'assemblaggio dei vari componenti. E l'uso di una distro **Linux** avrebbe alleggerito molto il carico della macchina, rispetto alla pesantezza di **Windows**. Eppure, lo scorso Aprile, la sezione dedicata alle **Steam Machine** è sparita dallo store di **Steam**, venendo relegata a un piccolo link raggiungibile dall'esterno. Dei quattordici produttori iniziali sono rimasti solamente in tre, **Alienware**, **Maingear** e **Scan Computers.** Vi sarebbe anche un quarto produttore, **Materiel.net**, ma andando sul sito della compagnia non vi è nessuna traccia della **Steam Machine**.
Per tutta risposta, **Valve**, nonostante le esigue vendite delle macchine (si vocifera meno di 500.000 unità!) ha deciso di continuare a supportare la propria visione di un ecosistema per il gaming **open source** e, quindi, di sviluppare ancora **Steam OS.** Peccato che ci sia ancora tanto lavoro da fare, come dimostrano alcuni dati raccolti sul web.



Prendiamo ad esempio **Steam OS**: come detto prima, è una *fork* basata su **Debian**, una delle distribuzioni o distro più apprezzate dell'intera comunità **Linux**. Ma se andiamo a controllare su

distrowatch.com, aggregatore di news e recensioni sulle varie distribuzioni **Linux**, scopriamo che **Steam OS** è solamente al **novantunesimo posto** nella top 100 delle distro più votate nel 2018. Se consideriamo che le distro **Linux** più apprezzate e famose, come **Ubuntu**, **Linux Mint**, **Arch** o lo stesso **Debian** sono conosciute per un costante aggiornamento e supporto, il sistema operativo di **Valve**, invece, ha ricevuto l'ultimo update nel gennaio 2018, uscendo dallo stato di beta solamente con la versione 2.0! Uno sviluppo abbastanza lento, considerando sia la data d'uscita del novembre 2013, che, soprattutto, il costante sviluppo che hanno altre distro Linux più o meno grandi, che sia sotto forma di ***rolling release*** (ovvero, sistemi operativi costantemente aggiornati) o delle cosiddette **LTS** (acronimo di **Long Term Support**, versioni che ricevono solamente aggiornamenti testati e sicuri e che hanno un supporto che va dai tre ai cinque anni). Il quadro della situazione non è favorito dal fatto che **Steam OS** possiede sì un ambiente desktop (**GNOME**), ma abbastanza nascosto. Il che porta l'utente **Linux** navigato, ma anche il neofita, a chiedersi «per quale motivo dovrei usare questa distro, quando ne esistono altre più supportate dove alla fine basta installare il client di Steam per poter usufruire della sua libreria?».
Infatti non sorprende vedere distro più quotate, come **Ubuntu** o **Fedora**, che non solo sono più in alto di **Steam OS** nella classifica di Distrowatch (rispettivamente al terzo e ottavo posto), ma che presentano *fork* specifiche per il gaming, come **Ubuntu GamePack** o **Fedora Game Spin**. Se poi aggiungiamo anche il vantaggio di supportare app come **Wine** (celebre emulatore delle applicazioni **Windows**, principalmente usato su **Linux** e **Mac**), **PlayOnLinux** e **DOSBox**, programmi che **Steam OS** non supporta, il dubbio diventa più che legittimo.

Il problema giochi è un'altra questione da affrontare: dal 2012 a oggi, sono solamente 5.072 su 25.563 i giochi disponibili per **Linux**. Quasi il 20%. Un po' pochi per considerare non solo il passaggio totale da **Windows** a **Linux**, ma soprattutto per giustificare l'acquisto di una **Steam Machine** che parte da **599€**, un costo molto più alto rispetto a una console attuale e molti PC preassemblati. Aggiungiamo al lotto anche la scarsa ottimizzazione di molti giochi per **Linux**, rispetto alle controparti **Windows**: cosa che si presenta soprattutto nei titoli che sfruttano le librerie **DirectX**. Sebbene esista qualche eccezione, in primis per alcuni giochi che sfruttano per bene le **OpenGL**, libreria open-source e gratis, rispetto alle **DirectX**, native **Microsoft.** Come per esempio ***Left 4 Dead 2***, che, come provato da Valve, ha dimostrato di girare più velocemente su **Linux** che su **Windows**, questo grazie anche alla migliore ottimizzazione del motore grafico **Source** sulle librerie **OpenGL**.

Visti i risultati, non bisogna rimanere sorpresi dalla decisione di **Valve** di rimuovere le **Steam Machine** e **Steam OS** dalla homepage dello store di videogiochi per PC più usato al mondo. Al momento la mossa da parte di **Gabe Newell** e soci resta solo un curioso esperimento, e non aiuta il fatto che solamente lo 0,52% degli utenti **Steam** utilizzino una distro **Linux**. E nel sondaggio campeggiano due delle distro **Linux** più usate, come **Ubuntu** e **Linux Mint**, mentre di **Steam OS** non abbiamo nessuna traccia. Una grande occasione mancata, visto che l'ecosistema **Linux** è conosciuto ai più per essere particolarmente leggero e capace di resuscitare hardware dato per morto, com'è successo col mio HP 655 acquistato ben sei anni fa. All'annuncio delle **Steam Machine** e soprattutto di **Steam OS** ero particolarmente entusiasta all'idea di poter avere una sorta di PC "consolizzato" da mettere in salotto, coadiuvato, magari, da una distro **Linux** capace di essere usata sia come console che come media center, grazie ad applicazioni come **Kodi**. Alla fine il risultato ottenuto è molto lontano da ciò che pensavo: probabilmente il cambio di rotta da parte di **Windows** dopo le critiche per la sua ottava versione, e il ritorno in carreggiata dopo **Windows 8.1** e **Windows 10** (dove abbiamo avuto lo storico approdo di **Linux** sotto forma di subsistema) hanno fatto la loro, e la "ribellione" da parte di **Gaben** è solo un lontano ricordo. Tuttavia, bisogna tenere le orecchie aperte, visto che nell'ecosistema **Linux**, manca poco per passare dalle critiche alle lodi, com'è successo qualche anno fa con **Ubuntu**. Magari la distro del futuro sarà proprio **Steam OS**...

Shroud of the Avatar potrebbe arrivare su altre piattaforme

Shroud of the Avatar: Forsaken Virtues, nuovo MMORPG del leggendario **Richard "Lord British" Garriott** è in uscita su **PC**, **Mac** e **Linux** per il **27 marzo**. Ma pare che lo sviluppatore

inglese e il team **Portalarium** vogliano portare il proprio gioco anche su altre piattaforme.

Secondo lo stesso **Garriott**, il titolo è stato progettato su **Unity** proprio per la sua versatilità, così da rendere semplice l'espansione verso altre piattaforme. Originariamente il team aveva pensato al mobile, principalmente a un tablet come l'**iPad**, ma con l'uscita di **Nintendo Switch** i piani sono cambiati, tanto da considerare quest'ultima un'ipotesi migliore.
Lord British ha dichiarato che, dopo il lancio di ***Shroud of the Avatar***, deciderà insieme al team la prossima piattaforma.

Intel: grave falla sulle CPU, fix pronto e distribuito

Dopo la notizia di **MINIX**, l'OS installato su CPU **Intel** di ultima generazione, che ha accesso a informazioni importanti a nostra insaputa, nelle ultime 48 ore **The Register**, ne ha scoperto un nuovo bug sulle. Così riferisce **AMD**:

«L'esecuzione speculativa del bug sul kernel a livello hardware è da incolpare a Intel; non può essere fixato utilizzando un aggiornamento del microcode e richiederà una patch a livello KPTI per tutti gli OS colpiti.»

Prima di entrare in altri dettagli, una spiegazione sul problema: il bug è stato scoperto a livello hardware e riguarda un ***exploit*** che è in grado di garantire l'accesso a livello del kernel da malintenzionati. Dal momento che questo esiste a livello hardware, una patch tramite ***microcode*** non è apparentemente possibile. L'unica soluzione nota è intervenire tramite il sistema operativo, che richiederebbe una riprogettazione del l'OS stesso, su cui **Windows**, **Linux** e **Apple** hanno già lavorato.
Microsoft ha già rilasciato una patch per i propri sistemi Windows 10, con il codice **KB4056892**. Comunque, il problema è che qualsiasi patch potrebbe introdurre una **penalità temporale cruciale per il sistema**, il ché significa che in alcuni casi le CPU potrebbero **rallentare drasticamente**. Abbiamo visto numeri quotati fino al **30%**, ma le stime approssimative indicano un rallentamento di circa il **17%**. Quindi, qual è esattamente il problema?
Prima di entrare nei dettagli, ecco la dichiarazione di **AMD**, che fondamentalmente ha dato più dettagli su quale sia il problema:

> **«I processori AMD non sono soggetti ai tipi di attacchi a livello kernel. La microarchitettura AMD non consente riferimenti di memoria, inclusi riferimenti speculativi, che accedono a dati con privilegi più elevati quando vengono eseguiti in una modalità con privilegi minori quando tale accesso comporterebbe un errore di pagina.»**

Dato che Intel ha parlato a lungo di questo problema, possiamo dedurre abbastanza facilmente da questa affermazione che il problema ha a che fare con riferimenti speculativi nei processori Intel. L'esecuzione speculativa è fondamentalmente una forma di ***preemption*** che cerca di prevedere quale codice verrà eseguito, quindi lo preleva e lo esegue prima che l'ordine effettivo arrivi. Quindi si dovrebbe avere un kernel assolutamente pronto per ogni comando, invece di lasciarlo aspettare.
Il problema, come risulta dai commenti di AMD, è che è possibile sfruttare questa funzione per

eseguire in modo speculativo un codice che normalmente verrebbe bloccato, finché si interrompe l'esecuzione effettiva del codice prima che sia possibile eseguire un controllo. Questo significa che un utente di **livello 3** può leggere i dati del kernel di **livello 0** utilizzando l'esecuzione speculativa, poiché il controllo dei privilegi non verrà effettivamente attuato finché il codice non viene eseguito sul main.
Il ***layer* Kernel** è attualmente presente nello spazio di indirizzamento della memoria virtuale di tutti i processi per garantire una consegna rapida durante l'esecuzione del codice, ma è completamente invisibile a tutti i programmi. Il kernel proverà fondamentalmente a prevedere quale codice verrà eseguito successivamente e quando un programma effettua una chiamata di sistema a esso, sarà già pronto per la consegna. Ciò può aumentare significativamente i tempi di esecuzione ma, rappresenta anche un fastidioso errore di sicurezza poiché nessun controllo dei privilegi è presente allo stadio del kernel. L'unico modo per aggirare questa caratteristica di livello hardware è usare quella che viene chiamata una tecnica ***Kernal Page Table Isolation*** (***KPTI***) che renderà il kernel completamente cieco al sistema e lo rimuoverà dallo spazio di memoria virtuale, fino a quando non si verificherà una chiamata di sistema. Inutile dire che questo potrebbe introdurre severe penalità nel tempo in situazioni di commutazione di contesto in cui sono richieste molte chiamate di sistema. Il team di Linux ha anche rimuginato su ***FUCKWIT*** (**Forcefully Unmap Complete Kernel with Interrupt Trampolines**) che dovrebbe dare un'idea di quanto sia frustrante il bug per gli sviluppatori.
Secondo alcune fonti, questo numero può variare dal **5%** al **30%** a seconda del tipo di processore in uso, poiché le moderne CPU hanno una funzionalità denominata **PCID** che può ridurre l'impatto sulle prestazioni. Secondo una soluzione KPTI esistente pubblicata su ***Postgresql***, ci si dovrebbe aspettare un rallentamento del caso migliore del **17%** e un rallentamento del **23%** nel caso peggiore. In ogni caso, tutte le fonti concordano sul fatto che un rallentamento si verificherà quasi sicuramente e questo non è qualcosa che Intel può semplicemente applicare a un microcodice. I processori AMD in questo momento non sono interessati dal momento che non utilizzano l'esecuzione speculativa. Quindi la domanda è: chi avrà questo impatto e come questo inciderà sugli utenti finali? La buona notizia per tutti i gamer o utenti "normali" è che non si noterà quasi nessuna differenza una volta applicata la patch poiché i videogiochi e il rendering di base non sono carichi abbastanza pesanti per avere quei rallentamenti. I *client* aziendali come **Google EC2** e **Amazon Compute Engine**, tuttavia, subiranno un drastico impatto dal momento che utilizzano macchine virtuali che possono seriamente compromettere le prestazioni. In secondo luogo, come utente generico, le password e altre informazioni sensibili sono memorizzate nel kernel e questo bug potrebbe potenzialmente garantirne un accesso aperto.
Nelle ultime ore il team di **Phoronix** ha eseguito dei test con KPTI attivo su due CPU, un **Intel Core i7 6800K** e un **Intel Core i7 8700K**; i grafici mostrano un sostanziale degrado di performance che parte dall' **1%** al **53%** nei casi peggiori, ma comunque ciò non comprometterebbe l'utilizzo dei videogiochi.

Il comunicato stampa ufficiale da parte di Intel

Come detto si parla che la patch possa risolvere il problema almeno parzialmente ma a discapito delle prestazioni in modo variabile. Intel però si è subito fatta sentire ed ecco cosa dice nel suo comunicato stampa:

> **«Intel e altre aziende tecnologiche sono state messe a conoscenza di una nuova ricerca di sicurezza che descrive metodi di analisi software che, se usati per scopi dannosi, hanno il potenziale per raccogliere impropriamente dati sensibili da dispositivi informatici che funzionano come progettato. Intel ritiene che questi *exploit* non abbiano il potenziale per**

> **corrompere, modificare o eliminare dati. Le recenti notizie secondo cui questi *exploit* sono causati da un "bug" o una "falla", unicamente legati ai prodotti Intel sono scorrette. In base all'analisi fino a questo momento, molti tipi di dispositivi – con processori di aziende differenti e sistemi operativi – sono suscettibili a questi *exploit*. Intel è impegnata nel garantire la sicurezza dei prodotti e dei clienti e sta lavorando a stretto contatto con molte altre aziende tecnologiche tra cui AMD, ARM Holdings e diversi fornitori di sistemi operativi, per sviluppare un approccio a livello industriale per risolvere questo problema in modo rapido e costruttivo. Intel ha iniziato a fornire aggiornamenti software e *firmware* per mitigare questi exploit. Contrariamente ad alcune notizie, qualsiasi impatto sulle prestazioni è legato al carico di lavoro e, per l'utente medio di un PC, non dovrebbe essere importante e sarà mitigato nel tempo. Intel si impegna a seguire le *best practice* industriali nella divulgazione responsabile di potenziali problemi di sicurezza, e per questo motivo Intel e altre aziende avevano intenzione di parlare di questo problema la prossima settimana quando gli aggiornamenti di *software* e *firmware* saranno disponibili. Intel si trova tuttavia costretta a pubblicare questo comunicato in seguito ai report inaccurati dei media. Rivolgetevi al fornitore del sistema operativo o al produttore del sistema e applicate tutti gli aggiornamenti non appena disponibili. In generale seguire le buone pratiche di sicurezza che proteggono dai malware aiuterà anche a proteggervi dal possibile sfruttamento della falla fino a quando gli aggiornamenti non saranno applicati. Intel ritiene che i suoi prodotti siano i più sicuri al mondo e che, con il supporto dei suoi partner, le attuali soluzioni a questo problema offrano la migliore sicurezza possibile per i propri clienti.»**

Anche se la questione non è per niente conclusa, in attesa di nuovi aggiornamenti, ecco il riassunto di cosa Intel ha detto in modo specifico per capire meglio la situazione:

- Intel ritiene che questi exploit non possono corrompere, modificare o eliminare i dati.
- Intel afferma che non sono solo i suoi prodotti a essere coinvolti. Si parla di prodotti con CPU diverse e sistemi operativi differenti, quindi anche smartphone.
- Intel fa i nomi di **AMD** e **ARM**. Un saggia mossa che sposta l'attenzione, fino ad ora focalizzata sul proprio brand.
- Intel afferma che l'impatto prestazionale per chi usa il PC in modo tradizionale – come la stragrande maggioranza di noi, e quindi per giocare, navigare ecc… sarà di poco conto e sarà mitigato ulteriormente in futuro.
- Intel ritiene che i suoi prodotti siano i più sicuri al mondo.

Test svolti dalla redazione

Abbiamo fatto due semplici ***benchmark*** su lato CPU ovviamente con Windows 10, prima della patch e dopo la patch (KB4056892) per vedere se ci sono dei cambiamenti. Abbiamo usato una CPU Intel Core i5 6600K portato a 4,60 GHz stabili, e come programmi: **Geekbench 4** e **Aida 64**:

Da come si può vedere dai *benchmark* la situazione è cambiata poco e, se i valori su **Geekbench 4** nel prima sono più alto è da attribuirsi a tanti fattori tra cui servizi aperti, cosa stava facendo il PC in quel momento ecc… Su Aida 64 invece alcuni valori sono aumentati, per il motivo descritto prima. Quindi in conclusione, dai primi test nei *benchmark*, si spera in gaming le cose non dovrebbero cambiare. A breve faremo delle verifiche su lato gaming se ci sono cambiamento e aggiorneremo questo articolo, quindi rimanete aggiornati con noi !

Two Worlds II, dopo 6 anni, torna a far parlare di sé.

Proprio cosi, dopo più di 6 anni la **TopWare** rispolvera la versione PC di ***Two Worlds II***, infatti i possessori del gioco, potranno godere presto di una espansione principale nuova di zecca, che avrà il nome di "***Call of the Tenebrae***". In effetti questa era stata annunciata già a Marzo dello scorso anno, quando venne annunciato anche ***Two Worlds III***, ma è stata definita solamente adesso la sua data di rilascio ufficiale.

La nuova espansione ***Call of the Tenebrae***, vedrà la luce giorno **25 Maggio**. Prevede più di 10 ore di gameplay e inoltre, come ci si aspettava, l'espansione avrà una nuova grafica HD, con nuove mappe, obiettivi, armi e nemici inediti.

Call of the Tenebrae verrà distribuita come semplice **DLC** al costo di **10$** per chi già possiede ***Two Worlds II***, mentre ne costerà **15$** come avventura **standalone**, in modo che tutti possano giocarla liberamente.

La **TopWare**, cavalcando l'onda, ha inoltre programmato il rilascio di un **Pass Stagionale**, per poter avere tutti i contenuti di **TW2**, e di un ulteriore espansione chiamata "***Shattered Embrace***"

(tra Ottobre e Dicembre), che includerà mappe per multiplayer e altri contenuti esclusivi.