Outbreak: nuova modalità per Rainbow Six Siege

Dopo tre anni dal suo rilascio, ***Rainbow: Six Siege***, ha ricevuto un nuovo aggiornamento denominato ***Outbreak***, che porta cambiamenti sostanziali all'esperienza di gioco. Infatti non si agirà più come unità anti-terrorismo ma come **unità anti-zombie**. *Outbreak* è una modalità cooperativa per tre giocatori ma disponibile solo per quattro settimane. Gli operatori si troveranno a combattere una misteriosa infezione nella città di **Truth of Consequenses** che, nonostante lo strano nome, esiste realmente.
Tutti in città sono stati sottoposti in quarantena nelle loro case per colpa dell'epidemia; i giocatori, quindi, potrebbero rischiare di contrarre l'infezione, avvicinandosi a quanto visto in ***The Division***.
Con questa nuova modalità sono stati **aggiunti 50 nuovi oggetti** dal costo di 300 crediti l'uno; quattro di questi, però, verranno regalati al primo accesso. **Ubisoft** ha inoltre promesso che ogni pacchetto conterrà oggetti diversi e quindi non ci saranno doppioni.

L'Incredibile personalizzazione in Monster Hunter: World

Uno degli aspetti più affascinanti di ***Monster Hunter: World*** è senza dubbio il menù dedicato alla personalizzazione del proprio alter ego, realizzato davvero con grande cura per i dettagli.
Sia gli ***Hunter*** maschili che quelli femminili hanno a disposizione tantissime opzioni per rendere unici i visi dei propri protagonisti, talmente tante da dover impiegare anche delle ore per trovare la combinazione perfetta. Il titolo, però, pecca di una completa caratterizzazione del resto del corpo, ma comunque trascurabile vista l'enormità di combinazioni facciali possibili, nelle quali possiamo trovare anche una **donna barbuta**.
Anche i **Palico**, seppur in minor quantità, hanno una dose discreta di personalizzazioni, nelle quali possiamo modificare dal colore della pelliccia agli occhi, sino alle orecchie e alla coda.
Monster Hunter: World sarà disponibile da **domani, 26 gennaio,** per PS4 ed Xbox One. La versione PC, invece, sarà rilasciata nel **periodo autunnale**

Tutte le esclusive Xbox disponibili al lancio di Game Pass

La rivoluzione di **Xbox Game Pass** ha portato un interessante novità, confermata da **Aaron**

Greenberg (General Manager Xbox) sul suo profilo **Twitter**: **g**li abbonati **Xbox Game Pass** potranno giocare con i titoli **Play Anywhere** anche su PC. Sebbene il servizio non sia disponibile in modo ufficiale su Windows, coloro che possiedono un abbonamento attivo **Game Pass** potranno utilizzare anche l'edizione PC di qualsiasi titolo correlato a **Xbox Play Anywhere.** Inoltre, tutte le esclusive uscite fino a ora saranno disponibili al lancio del servizio. Le prime esclusive **Microsoft** disponibili saranno ***Sea of Thieves*** (dal 20 marzo), ***Crackdown 3*** e ***State of Decay 2***. **Phil Spencer** ha inoltre confermato che lo stesso trattamento sarà riservato anche per i nuovi giochi in esclusiva come ***Halo***, ***Gears of War*** e ***Forza***.

Accuse di manipolazione dei media per Electronic Arts?

Negli ultimi anni **Youtube** e **Twitch** si sono evolute da semplici piattaforme adibite al caricamento di gameplay a vere e proprie piattaforme pubblicitarie per tutte le software house e i loro titoli. Fra queste software house abbiamo senza dubbio **Electronic Arts**, società fra le più attive in tal senso, principalmente tramite accordi con alcuni youtuber come **LevelCapGamging,** il quale, con i suoi anni di esperienza e contenuti videoludici incentrati proprio su ***Battlefield***, sembrerebbe ben inserito fra le grazie di EA. Purtroppo per lui, non è proprio così: lo **youtuber** ha annunciato tramite **Twitter** che non sarà presente all'evento organizzato da EA per presentare il nuovo DLC di *Battlefield 1, **Apocalypse**.* Qui le parole di LevelCap:

> Fed up with @Battlefield manipulating the media's voice by dis-inviting select YouTubers from early access DLC capture events. Not liking the new era @EA controlled press. I guess 7 years of covering BF games isn't enough, I also need to be more favorable in my reviews...
>
> — LevelCap (@LevelCapGaming) January 18, 2018

Secondo queste parole, sembrerebbe infatti che all'evento, siano stati invitati solo gli youtuber che hanno dato una recensione positiva al titolo. Risulta, quindi, alquanto sospetto che uno youtuber del suo calibro non sia stato invitato nonostante i suoi anni di esperienza sulla nota saga.

Un nuovo gioco di Alien in arrivo?

Ebbene sì, il nuovo gioco dedicato al franchise ***Alien*** arriverà presto. Il nuovo titolo è in fase di sviluppo negli studi di **Cold Iron Studios,** sviluppatore abbastanza recente, acquistato poco tempo

fa da **FoxNext Games.** Il gioco promette bene visto la quantità di veterani del settore che hanno partecipato al progetto, i quali hanno contribuito alla realizzazione di titoli come *Neverwinter*, *BioShock Infinite*, *Borderlands*, e *Metroid Prime*.
Non sappiamo molto; le poche informazioni che abbiamo ci suggeriscono che questo sarà il primo titolo dello studio, e definito come «uno sparatutto per PC e console ambientato nello scenario cinematografico di *Alien».* Ovviamente mancano informazioni relative alla data di uscita o su quale piattaforma sarà presente, ma siamo sicuri che arriveranno novità a breve.
Sarà particolarmente interessante vedere l'approccio del nuovo team al franchise di ***Alien*** data la sua lunga storia cinematografica e videoludica. Possiamo solo sperare che non si discostino tanto dalle atmosfere originali, visto che, a livello videoludico, c'è ancora tanto potenziale inespresso.

Rumor: Microsoft lavora a nuovo controller Elite

Il controller **Xbox Elite** di **Microsoft** è costoso, ma probabilmente è la scelta ideale per i possessori di **Xbox One** che desiderano un gamepad adatto alle proprie esigenze. E a quanto pare, c'è abbastanza richiesta per meritare un seguito. **Molti *rumor*** sembrano indicare l'arrivo di un nuovo controller **Elite** che si basa sulle esperienze apprese dal primo modello. Se i suggerimenti sono accurati, include **Bluetooth** (per collegarsi senza problemi al PC), una connessione cablata **USB-C**, un connettore di ricarica **Apple MagSafe** sul retro e una **batteria incorporata**. E naturalmente, più modifiche per i giocatori che desiderano controlli più precisi e personalizzati.

Stando a queste informazioni, che – come riportato in basso – sono contornate di immagini del nuovo controller (dall'utente **Reddit EDDS86**), il nuovo dispositivo avrebbe nuovi *grip* in modo da assicurare che le proprie mani siano ben salde durante sessioni frenetiche, un interruttore a tre profili, tre livelli di blocco per il *trigger,* e la regolazione della tensione degli *stick*. Dato che Microsoft fece domanda per un brevetto su quest'ultimi a dicembre, pare che tali affermazioni siano veritiere. Tra l'altro, una fonte di **The Verge**, confermerebbe tutto.
Non si fa menzione alla data di rilascio del controller sul mercato ma Microsoft, abitualmente, tende a riservare i suoi grandi annunci per l'**E3** (quest'anno, a metà giugno), rilasciando tutte le informazioni del caso.

Annunciata la Remastered di Dark Souls

A un anno di distanza dall'uscita di Switch, Nintendo ha pubblicato sul proprio sito l'ultimo **Nintendo Direct Mini** dove, fra i vari titoli annunciati per il 2018, è stata annunciata la ***Dark Souls Remastered***.

Dark Souls arriverà anche per **PC, PS4, e Xbox** e uscirà il **25 maggio 2018**. Un cambiamento di cui siamo certi è che il multiplayer sarà espanso per supportare **sei giocatori simultanei**, il che ha senso se l'obiettivo è quello di far funzionare il sistema di alleanze dei *Dark Souls* un po' più agevolmente. Le principali migliorie saranno svariati SFX, basati su quelli di *Dark Souls 3,* e il comparto luci rinnovato.

Una fonte abbastanza attendibile, come riporta anche **Kotaku Uk**, conferma anche che **Bandai Namco** ha tutta l'intenzione di portare l'intera trilogia su Switch.

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 !

Un rumor rivelerebbe alcune straordinarie esclusive Xbox

Secondo alcune voci, il 2018 potrebbe essere un anno esaltante per Xbox. In un recente thread su ResetEra, l'utente **Klobrille** – che ha acquisito credibilità dopo aver anticipato notizia come quella del nuovo ***Age of Empires***, del secondo capitolo di ***State of Decay***, riguardo l'ambientazione australiana di ***Forza Horizon 3*** e riguardo la natura MMO-lite di ***Sea of Thieves*** – sostiene che sarebbe in fase di sviluppo un nuovo ***Fable***, sul quale dovrebbe essere al lavoro uno studio britannico, a seguito della chiusura di Lionhead dello scorso anno.

Ci sarebbe poi un nuovo ***Perfect Dark***, su cui sarebbe al lavoro **The Coalition**, sviluppatore di ***Gears of War***, che vedrebbe una Joanna Dark questa volta in terza persona.
Spazio anche per ***Forza Horizon 4***, che uscirà quasi sicuramente entro la fine di quest'anno e che potrebbe essere ambientato in Giappone.
Altre informazioni riguardano infine la co-op della campagna per quattro giocatori in ***Crackdown 3***, il prossimo ***Halo***, che coinvolgerebbe un numero di giocatori "molto alto" (con una probabile modalità **Battle Royale**) e il ritorno di ***Mech Assault***.
Stando a Klobrille, queste informazioni sarebbero state trovate nelle tabelle del database di Microsoft accessibili tramite l'SDK dell'API di Xbox Live e gli utenti della console di Redmond si augurano vivamente che siano vere

---

L'OMS aggiunge alla sua lista delle malattie il "Disturbo del Gioco"

L'Organizzazione mondiale della sanità (OMS) ha aggiunto il "**disturbo del gioco**" a una prima stesura della sua prossima **undicesima** revisione del Compendio internazionale delle malattie. Qui la stesura:

> "Il disturbo del gioco è caratterizzato da un comportamento ossessivo, persistente o ricorrente, ciò è manifestato da: 1) il contesto del gioco e da vari fattori legato ad esso (durata, frequenza, intensità); 2) crescente priorità data al gioco nella misura in cui il gioco ha la precedenza su altri interessi della vita e attività quotidiane; 3) Persistenza nel giocare al determinato gioco nonostante evidenti conseguenze negative. "

La *Electronic Software Association* (ESA), dal canto suo, ha replicato con una dichiarazione:

> "Proprio come gli appassionati di sport ed i consumatori di tutti i tipi di intrattenimento, anche i videogiocatori sono appassionati e dediti al loro tempo. Avendo affascinato i giocatori per più di quattro decenni e più di 2 miliardi di persone in tutto il mondo possiamo affermare con l'aiuto del buon senso e la ricerca obiettiva dimostrano che i videogiochi non provocano dipendenza e mettendo su di essi un'etichetta ufficiale, incautamente banalizza i veri problemi di salute mentale come la depressione e il

disturbo d’ansia sociale che meritano la piena attenzione e il pieno trattamento da parte della comunità medica.