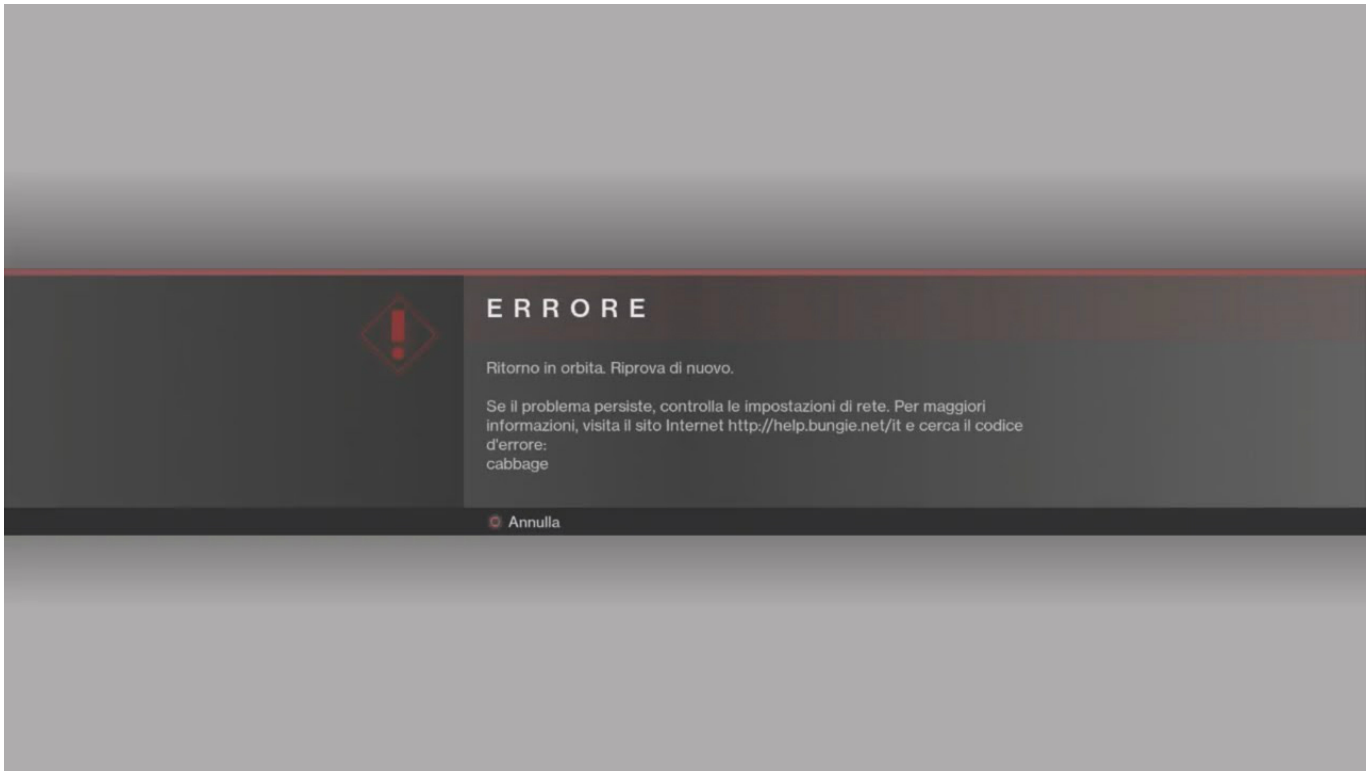
La dura vita di un recensore e di Destiny 2

Moltissimi giochi hanno subìto lanci disastrosi per poi essere scartati pochissimo tempo dopo, sono stati abbandonati per lunghi mesi fino ad avere improvvisamente un **boom di vendite**, diventando quasi virali. Ma ne esistono altrettanti che hanno visto avverarsi un meccanismo inverso, vendendo parecchie copie al lancio, per essere abbandonati dopo aver deluso la maggioranza dei giocatori. Ottimi esempi sono sicuramente ***Tom Clancy's Rainbow Six Siege***, ***The Division***, ***Destiny***, ***Watch Dogs*** e moltissimi altri titoli, tutti accomunati da un lancio accompagnato da un fortissimo hype da parte degli utenti ma che poi si sono rivelati disastrosi o deludenti.
Il feedback negativo dei giocatori, nel caso di *Rainbow Six* per esempio, ha acceso una lampadina in casa **Ubisoft**, che ha subito contattato dei player professionisti e competenti che, lavorando in team, hanno evidenziato tutte quelle problematiche che, secondo loro, affliggevano il gioco. Una simile mossa ha dato nuova vita a ***R6S,*** che è riuscito, durante l'inizio del 2017, a vendere moltissime copie e vive tuttora con la pubblicazione di diversi **bundle** e aggiornamenti gratuiti.
Il caso non si è ripetuto con un titolo che mi sta particolarmente a cuore, e che dopo l'iniziale boom, ha visto decrescere l'interesse nei suoi confronti, lasciando poche speranze su una sua eventuale risalita: ***Destiny 2***.

In molti, dai più noti redattori delle grandi testate videoludiche ai più piccoli e meno noti, hanno dibattuto riguardo la scelta di **recensire un gioco pochi giorni dopo la pubblicazione** o se attendere qualche settimana in più per non incorrere nel rischio di non approfondire alcuni aspetti fondamentali, e compiere dunque una buona analisi. Le grandi testate tendono sempre più a pubblicare le recensioni di titoli più importanti e famosi al day one, o comunque pochi giorni dopo, ma c'è chi sostiene – e fra questi ci includiamo noi di GameCompass, che sposiamo dall'inizio del nostro percorso la filosofia dello Slow Journalism – la necessità di **prendersi il tempo adeguato per riuscire a fare una disamina più articolata e approfondita di un gioco**.
Un simile dibattito riguarda molto da vicino titoli come ***Destiny 2***, recensito su queste pagine poco dopo l'uscita – seppur dopo altre testate di settore – non facendo completamente caso a problemi, anche abbastanza gravi, che sono presenti tuttora all'interno del gioco.
Questo articolo può essere considerato in parte una rettifica postuma della recensione, andando in parallelo a una community intenta tutt'oggi a segnalare **le problematiche che affliggono l'ultimo titolo di casa Bungie**, ma difficilissime da notare durante la concitata fase di recensione.
Questo non significa "non fidatevi di ciò che scriviamo", ma serve a segnalare come, a volte, l'analisi di videogiochi complessi non venga adeguatamente approfondita per mancanza di tempo, in un mondo estremamente competitivo come quello dell'editoria.

Destiny 2 è un gioco che a primo acchito sembra davvero ben strutturato e degno erede del primo *Destiny*, ma che dopo pochi mesi dall'uscita si è rivelato abbastanza noioso e poco convincente per i fan.
Il primo capitolo della saga non ha avuto inizialmente un grande successo, ma pian piano, con i vari aggiornamenti ed espansioni, ha ricevuto una spinta tale da arrivare a essere considerato uno dei migliori FPS degli ultimi anni. Il titolo di Bungie è **riuscito a raggruppare una vastissima community in tutto il mondo**, accogliendo nuovi player e facendo ritornare chi l'aveva mestamente abbandonato. Per sfortuna, ***Destiny 2***, ha avuto un "destino" molto simile a quello del suo predecessore, ma per vari versi ben peggiore: la maggior parte della community, formatasi già durante il ciclo di vita del primo capitolo, è rimasta molto delusa e – come il sottoscritto – amareggiata dopo aver giocato praticamente per due mesi intensivi.
Destiny 2 presenta parecchi problemi che, all'occhio di un neofita, possono sembrare semplici scelte tecniche, ma per chi ha già molta familiarità con il mondo di gioco e con le scelte di Bungie, risultano in maniera più lampante il frutto di una **cattiva gestione delle meccaniche del gameplay**.

Si potrebbe partire parlando del ***drop rate***, una **feature** parecchio equilibrata nel precedente capitolo, che è riuscita ad aumentare di parecchio le ore di gioco, con la possibilità di trovare l'arma con i ***perk*** giusti e con le giuste caratteristiche, versatile sia in **PvE** che in **PvP**, oppure un materiale/arma di grande rarità. Una simile meccanica in *Destiny 2* è stata completamente cancellata: le armi sono facilmente ottenibili dopo qualsiasi attività e hanno un set di abilità programmato, quindi non si possono trovare più armi differenti. A detta di **Bungie** questo doveva servire per equilibrare il lato PvP, creando un **gunplay** meno sbilanciato, ma così non è stato. **Il drop rate è aumentato esponenzialmente** a ogni partita, come in "**Crogiolo**" o in ogni attività PvE, in cui si riceve sempre un cospicuo bottino, rendendo le partite PvP sì più bilanciate, ma troppo monotone e soprattutto poco competitive, vista la presenza delle stesse identiche armi, con lo stesso identico *roll*.
Altra modalità bistrattata è stata "**Cala la Notte**", una delle attività più difficili e riuscite di *Destiny*, ma resa inutile da questo ultimo capitolo (anche se, a essere onesti, la sua decadenza era iniziata durante l'ultimo periodo di vita di *Destiny*). I *drop* ottenuti nei "**Cala la Notte**" sono praticamente sempre gli stessi e la possibilità di trovare un'arma esotica è quasi pari a zero; scelta davvero infelice perché, dopo svariati minuti o addirittura ore passate a provare a completare questa modalità, resa più difficile da *buffer* e *malus* per aumentare la sfida, il *drop* ottenuto non riesce a ricompensare le nostre fatiche e, in molti casi, frustra il giocatore fino a disinteressarlo alla modalità per farmare. Molti scelgono di virare verso il "Crogiolo" o altre attività, meno difficili e sicuramente più redditizie.



Dulcis in fundo, il problema che ha fatto impazzire letteralmente l'intera nazione italiana: **l'infrastruttura online, il network**. Proprio così, un gioco che basa tutto il proprio gameplay sul comparto online ha avuto problemi di questo, più precisamente ha sofferto di una mancanza di compatibilità. Dopo che Bungie ha aperto le porte della **closed beta**, sia su PC che su console, molti utenti, soprattutto italiani, hanno riscontrato un problema specifico, un **codice d'errore** che ha terrorizzato mezza utenza: **il codice Cabbage**.
Un'incompatibilità tra i **modem Technicolor** e i server di Bungie, ha creato non pochi problemi al D1 (non ancora risolto), che ha costretto tutta l'utenza a impostare il tipo **NAT 1** o, addirittura, cambiare modem, una decisione abbastanza drastica per un videogioco.
Fortunatamente però, questi problemi, principalmente l'ultimo elencato, sono stati presi in considerazione dalla stessa Bungie che sta cercando, con i vari aggiornamenti futuri, di sistemare o quantomeno arginare le problematiche. Infatti **è già stato annunciato un nuovo grande update che porrà fine alla maggior parte degli errori e complicazioni vari**. Sperando che con il nuovo DLC, in uscita per il prossimo Maggio, *Destiny 2* possa risollevarsi e riesca a riottenere la gloria e l'utenza che non ha ancora avuto, rimane ancora un problema: quanto tempo occorre davvero per recensire un titolo in un'epoca come quella che stiamo vivendo? Ed è il caso di pensare, in certi casi, a dei "richiami" alla recensione, degli update che fotografino lo stato dell'arte in parallelo all'andamento dei videogame nel medio periodo e ai loro cambiamenti in presenza di update sostanziosi?
Interrogativi da tener presenti se si vuole un giornalismo videoludico sempre migliore.

Errori di programmazione per Civilization 6

Pochi giorni fa, **Straight White Shark**, un noto modder dei forum **Something Awful**, sembra aver

scoperto un **errore tipografico** nel file di gioco che regola i comportamenti di default dei vari leader del gioco. I programmatori, infatti, hanno erroneamente castrato i parametri dell'Intelligenza artificiale per la produzione della statistica **Fede** come la più bassa a differenza delle restanti presenti nel gioco.
Come qualcosa del genere possa essere sopravvissuto alle migliaia di ore di test e valutazione è un mistero, specialmente per un titolo come ***Civilization VI***. Non è chiaro, tuttavia, se questi errori fossero presenti già nella versione originale del gioco o se siano il risultato di un recente aggiornamento.
A difesa di ciò, alcuni giocatori hanno notato come, per esempio, Pedro II del Brasile producesse **100 punti Fede** in meno rispetto a una partita giocata con il codice corretto nelle stesse condizioni della partita giocata con il codice non corretto.
Per la gioia di tutti i player di questo titolo è già presente una mod che corregge questo bug presente nel **WorkShop** di **Steam**

Patch in arrivo per Smite

In vista del **Campionato Mondiale dei Videogames**, gli sviluppatori di ***Smite***, titolo action-online rilasciato su **Xbox One**, **PC** e **PS4**, hanno deciso di dare finalmente voce alle numerose lamentele da parte degli utenti, sui vari bug all'interno del gioco, in particolare su Xbox One e PS4. **HiRezsaih** ha pubblicato proprio su **Reddit** una panoramica dei problemi che il team di sviluppo dovrà affrontare**,** come numerosi errori di *turnaround* e un sistema di segnalazione dei bug, che verranno esaminati e corretti dal team di ***Smite***, cresciuto recentemente proprio per offrire ai suoi utenti più qualità del supporto e del marketing. *Smite* sta aggiornando anche la mappa per la modalità conquista ed elementi di gioco in preparazione del lancio della Stagione 5.

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.

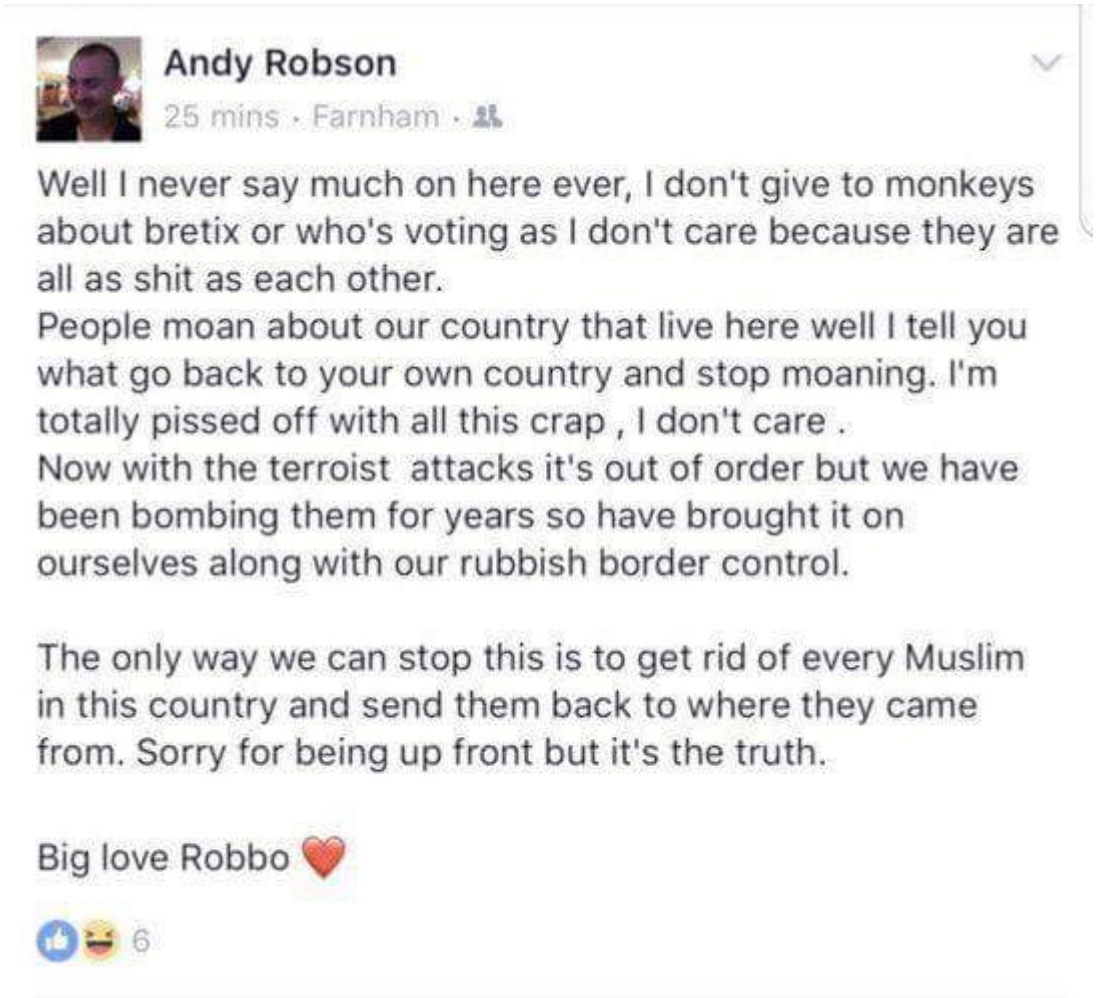
Test svolti dalla redazione

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 !

Razzismo: bufera sul managing director di Testology

In queste ultime ore **Testology**, la famosa compagnia di Quality Assurance, con clienti del calibro di **Warner Bros.**, **Team17**, e **Rebellion**, è stata indirettamente coinvolta in una polemica a sfondo razzista riguardo l'ultimo attacco terroristico avvenuto a Londra. In particolare, il managing director **Andy Robson**, ha pubblicato un post sul proprio profilo Facebook affermando «il solo modo per fermare gli attacchi terroristici è sbarazzarsi di ogni musulmano presente nel paese e rimandarlo indietro da dove è venuto.



Questa frase ha suscitato non poco scalpore, scatenando aggressive polemiche nei riguardi della società.
Successivamente Andy Robson ha cercato di calmare gli animi scusandosi, precisando di aver scritto sull'onda dell'emotività e di non voler offendere la comunità musulmana ma soltanto gli estremisti «who use their religion as an excuse for terrorism», sottolineando successivamente quanto **Testology** stessa tenga in gran conto il tema delle pari opportunità all'interno dell'azienda.