FAILLE DUPLICATION VIA MODE MARCHAND SUR SERVEURS DOFUS 1.29

Nous n'étions pas obligé de communiquer là-dessus, mais je pense que cela intéresse beaucoup d'entre-vous qui m'ont sollicité via mps pour avoir plus d'informations liées à la découverte de cette faille duplication sur les serveurs Dofus 1.29. Bonne lecture.

Il y a une semaine et demie, Xelino et moi (HeyImOliive) recevons des messages privés pour nous parler d'un mode marchand suspect au nom de « Mozane ». Le mode marchand est inspecté mais rien ne nous paraît louche à ce moment là : effectivement les Kralamansions alors en vente ont toutes +6 soins, ce qui peut inviter à suspecter du boting mais pas de la duplication à ce stade. Des screens du mode marchand ont été quand même pris, ce qui va être utile par la suite.

Barcka postant sur le discord de Fruiks sous le pseudonyme « Ah l'Ivraugne » poste alors un gyazo dimanche dernier qui prouve qu'il s'agit d'une faille duplication et non d'un botting forgemagie exotique : https://gyazo.com/7d1d6deea094d7a81aa6a10eac6bd2a7 : d'autres joueurs ont corroboré ces éléments, ce qui invite à se pencher sérieusement sur le cas.

Beaucoup pensent que les items sont dupliqués en dehors du mode marchand et remis en vente après duplication. Nous adoptons immédiatement une approche différente pour mener l'enquête, car les screens précédemment effectués par nos soins, ceux envoyés via messages privés une semaine auparavant et croisés avec les gyazos postés sur le discord de Fruiks montrent quelque chose de remarquable : les items vendus dans ce mode marchand sont toujours ordonnées de la même façon ! Cela nous apprend deux choses :

- soit la personne propriétaire du mode marchand enlève systématiquement tous ces exos et les remets en vente exactement dans le même ordre à chaque fois qu'il réapprovisionne l'item dupliqué (*car c'est la seule façon de faire pour ordonner ses items mis en mode marchand)*,
- soit la personne n'est pas au courant de la faille, et les items sont remis en vente automatiquement, à son insu.

Cette deuxième théorie nous semble la plus probable : dans ce cas, la personne nommée « Mozane » dupliquerait à son insu et la faille serait liée au mode marchand.
On choisit de creuser en ce sens : le mode marchand vendait pour plus de 2 milliards 200 millions d'items - ce qui est en soi notable - car relativement peu de joueurs dispose de cette fortune. On pouvait alors penser que la personne ait également des kamas en cash sur elle, et que l'achat de quelques exos lui fasse passer outre la limite de 2 147 483 647 ; limite au-delà de laquelle les kamas sont habituellement remis à zéro : la personne perd purement et simplement tous ses kamas.

D'autres informations circulent sur les discords selon lesquelles « les exos sont réapprovisionnés au bout de quelques heures » , nous pensons alors à un bug via la sauvegarde : à chaque sauvegarde, le mode marchand serait réapprovisionné. Mes connaissances en informatiques sont limitées mais je me demande si dépasser la limite de kamas lors de l'achat d'un objet/ressource en mode marchand ne crée pas un conflit, de sorte que le mode marchand soit refresh à chaque sauvegarde du serveur en se basant sur l'ancienne sauvegarde de ce mode marchand.

Par conséquent, seule une personne ayant 2 milliards 147 millions cash pourrait dupliquer des items

à chaque sauvegarde ? Si cette théorie se trouve infondée, c'est 2 milliards 147 millions qui s'évaporent … Souvenez-vous d'Aizy et Subarekk (RIP). Pour vérifier, fallait donc risquer 2 milliards de kamas.

Allons-voir ce qu'on a en stock sur Henual … et vers minuit le 31/07/2019, les kamas sont rassemblés et le test est lancé. Fallait avoir les burnes pour risquer 2 milliards, même sur Henual : mais il s'agit du bien-être du serveur, donc la décision est prise.

Le lendemain vers 9h30, nous allons vérifier le mode marchand et rien n'a repop ... On reconnecte le compte et cette fois, MIRACLE ! les ressources sont toujours dans le mode marchand alors qu'elles sont également présentes dans l'inventaire du personnage qui les avaient acheté. Ce qui est également remarquable, c'est que les kamas du personnage s'étant en mis en mode marchand n'ont pas bougé, alors qu'on pouvait s'attendre à ce qu'ils disparaissent.
Dans ce test nous avons volontairement laissé d'autres ressources non achetées dans le mode marchand, car nous sommes persuadés qu'en cas d'achat complet de toutes les ressources, le mode marchand est déconnecté, les kamas sont remis à zéro et que la duplication est impossible.

Il faut savoir que lorsque vous cherchez à report une faille duplication, Ankama vous demande de leur expliquer précisément la méthode employée pour dupliquer. S'ils ont été avertis dès la veille de la présence d'une faille sur Eratz, nous devions la réaliser pour la report efficacement. Ici, nous avons eu la chance de pouvoir le faire, ce qui est normalement quasiment impossible à trouver via des moyens de joueur.
Grâce à nos tests, nous étions alors en mesure de décrire précisément son fonctionnement et c'est ce qui a été immédiatement fait : vers 10h30 le 31/07/2019, le message au Support a été envoyé et une confirmation vocale via téléphone de la bonne réception du ticket support a été effectuée.

Nous souhaitions entériner nos reports en y apportant une preuve vidéo, ce qui a été fait courant après-midi : une duplication a été effectuée sur le serveur Eratz et les items dupliqués à l'occasion ont été reportés au Support. Nous avons également constaté que la sauvegarde serveur n'était pas en cause alors que nous le pensions précédemment, et que la duplication via mode marchand pouvait être reproduit à tout moment et à l'infini.

Questions/réponses

- Quel est l'ampleur de cette faille avant le 31/07/2019 ? Personne ne le sait. Mais il fallait 2 milliards de lamas et connaître la faille pour en abuser et peu de personnes sur le serveur disposent de cette somme. Ceux qui disposent de cette somme savent également que dépasser 2 milliards 147 millions et des brouettes te font normalement perdre tes kamas donc ne prennent pas le risque.

- Depuis quand cette faille existe ? Je ne saurais le dire. Quelque chose doit cependant vous rassurer : Aizy a perdu 2 milliards de kamas le 26 mars dernier, puisqu'il vendait pour plus de cette somme et que la limite de 2 147 483 647 kamas a été dépassé lors de l'achat de ses objets mis en vente. Si la faille était présente à cette date, il aurait dupliqué malgré lui à sa reconnexion comme l'a fait le propriétaire du mode marchand « Mozane ». Ce n'est pas arrivé, alors même que tous les items de son mode marchand n'avaient pas été achetés, donc les conditions d'une duplication auraient été remplies.

Je pense – et cela n'engage que moi – que cette faille est apparue il y a environ deux semaines lors d'un crash du serveur. Elle n'est pas ancienne car aurait été découverte bien plus rapidement : les conditions permettant sa réalisation se seraient produits par le fruit du hasard bien plus tôt.

- « Mozane » est-il coupable ? Je ne pense pas. Je pense qu'il dupliquait à son insu, et que lorsqu'il se reconnectait pour vérifier ses ventes, ses kamas n'avaient pas bougé et ses items en vente étaient toujours dans son mode marchand. Il se remettait donc naturellement en mode marchand.
  Avec ce bug, seul l'acheteur perd ses kamas et d'ailleurs, à lui seul profite le crime. Il peut acheter à chaque reconnexion/déconnexion du mode marchand plusieurs fois l'item dupliqué. Évidemment, il est possible de s'acheter à soi-même un item à bas coût pour le dupliquer, mais dans le cas de Mozane, je ne pense pas que c'était sa démarche. En effet, il aurait donc été obligé de dépenser des centaines de millions en achetant les objets présents dans son mode marchand : ce n'est pas logique.

- Qu'avez-vous dupliqué ? Nous avons délibérément choisi de dupliquer des boucliers hispaniques. En effet, cela permettait premièrement de confirmer aux yeux des joueurs crédules ce qu'on avait annoncé dès 14h sur notre discord communautaire : la duplication est réelle et un risque de rollback/perturbations des serveurs risquait d'intervenir. Les joueurs savent que ce type de bouclier est rarissime et de voir quelques boucliers apparaître en même temps saurait les convaincre.
  Également, dupliquer des boucliers hispaniques pouvait être l'occasion d'en prêter à des amis pour qu'ils fassent des « photos souvenirs », car une faille est un événement désagréable mais qu'on parle en rigolant avec le temps. Ça permettait de faire quelques screens funs avec ceux qui prenait ça du bon côté, dans l'attente d'un rollback salvateur.

En espérant que la situation revienne à la normale début de semaine prochaine !