Jeux VidÃ©o : Les diffÃ©rentes menaces affÃ©rentes aux jeux en ligne
Jeux VidÃ©o
PostÃ© par : JerryG
PubliÃ©e le : 30/5/2012 12:00:00

Alors que la popularitÃ© des jeux vidÃ©o en ligne ne cesse de progresser, la fraude sur Internet est devenue une menace bien rÃ©elle. **Le jeu vidÃ©o en ligne pÃ¨se plusieurs milliards de dollars** et est la cible dâ□□attaques variÃ©es lancÃ©es par des fraudeurs piratant les comptes des diffÃ©rents utilisateurs

Les jeux vidÃ©o en ligne massivement multijoueurs (Massively Multiplayer Online Games, MMOG), dont la popularitÃ© ne se dÃ©ment pas, sont particuliÃ¨rement touchÃ©s. Les MMOG sont des jeux vidÃ©o capables de supporter des centaines de milliers de joueurs simultanÃ©s. Des millions de joueurs interagissent dans un univers virtuel, endossant le rÃ´le de hÃ©ros, amassant objets et sommes dâ□□argent virtuels pour permettre Ã leurs personnages de se battre contre des dÃ©mons tout aussi virtuels.

Ces millions dâ□□utilisateurs du monde entier contribuent significativement au chiffre dâ□□affaires de lâ□□industrie du jeu. Ce marchÃ© lucratif est devenu la cible des cybercriminels. DÃ¨s lors, ceux-ci menacent rÃ©ellement la pÃ©rennitÃ© des MMOG. Puisque le vol de compte nâ□□est pas un mal inhÃ©rent Ã la conception des jeux, les dÃ©veloppeurs exercent un contrÃ´le limitÃ©. Mais cela ne rÃ©duit en rien lâ□□importance de la menace et les dÃ©veloppeurs de jeux devraient sÃ©rieusement envisager ces risques de sÃ©curitÃ©. Le piratage de comptes reprÃ©sente une menace rÃ©elle susceptible de nuire Ã la clientÃ¨le des jeux en ligne.

Les Ã©conomies virtuelles sont une source importante de motivation pÃ©cuniaire pour les pirates

Les MMOG ont introduit un nouveau phÃ©nomÃ¨ne : les Ã©conomies virtuelles. Les joueurs peuvent accumuler des liquiditÃ©s virtuelles, des piÃ¨ces dâ□□armure, des armes, de lâ□□Ã©nergie et de lâ□□Ã©quipement pour modifier leur apparence virtuelle. Les joueurs consacrent des heures entiÃ¨res Ã faire Ã©voluer leurs personnages, leurs compÃ©tences, et Ã acquÃ©rir des Ã©quipements virtuels pour augmenter leurs capacitÃ©s Ã combattre des dÃ©mons virtuels. Certains comptes de joueurs peuvent Ãªtre estimÃ©s Ã plusieurs milliers de dollars.

Les fraudeurs ont rapidement saisi lâ□□importante opportunitÃ© de pirater les comptes de joueurs et subtiliser les crÃ©dits et lâ□□Ã©quipement ayant Ã©tÃ© virtuellement acquis pour les revendre au plus offrant. Le lien entre Ã©conomies virtuelles et liquiditÃ©s rÃ©elles est facilement Ã©tabli. Les cybercriminels ont une source importante de motivation pÃ©cuniaire avec les comptes de jeux en ligne : le retour est important alors que le risque est relativement limitÃ©.

Les Ã©diteurs de jeux continuent de proposer de nouveaux contenus pour amÃ©liorer ou influencer le jeu. Ces Ã©lÃ©ments peuvent Ãªtre tÃ©lÃ©chargÃ©s pour des sommes modiques. Davantage, lâ□□industrie du jeu fournit encore des contenus supplÃ©mentaires, sous la forme de mises Ã jour ou de packs dâ□□extension. SÃ©curiser les comptes des joueurs devient alors essentiel pour prÃ©server le succÃ¨s des jeux vidÃ©o : aprÃ¨s tout, câ□□est sur les joueurs que se construit ce succÃ¨s.

Des menaces classiques

Lâ□□un des premiers moyens utilisÃ©s pour obtenir les mots de passe de comptes est lâ□□hameÃ§onnage (phishing) : les fraudeurs peuvent par exemple se faire passer pour lâ□□Ã©diteur du jeu et envoyer de faux courriers Ã©lectroniques pour conduire les joueurs vers des sites Web malicieux oÃ¹ ils devront indiquer leurs nom dâ□□utilisateur et mot de passe.

De nombreux cybercriminels utilisent en outre des outils servant Ã lâ□□enregistrement des frappes au clavier (keyloggers). Ces logiciels malveillants enregistrent donc nom dâ□□utilisateur et mot de passe tapÃ©s au clavier, avant de les transmettre au pirate via le rÃ©seau. Câ□□est un moyen courant dâ□□obtention de mot de passe Ã lâ□□insu du joueur. Ce type de logiciel malveillant peut Ãªtre dissimulÃ© au sein dâ□□un fichier exÃ©cutableâ□¦ parfois maquillÃ© pour prendre lâ□□apparence dâ□□un outil de triche.

Etant donnÃ© que la plupart des gens ont plusieurs comptes pour des services en ligne â□□ quâ□□il sâ□□agisse de jeu en ligne, de site de commerce Ã©lectronique, etc. -, ils utilisent frÃ©quemment le mÃªme couple nom dâ□□utilisateur / mot de passe. La menace est dâ□□autant plus grande quâ□□ils ont tendance Ã crÃ©er des mots de passe faciles Ã mÃ©moriser ; le mot Â« password Â» est toujours le plus utilisÃ© Ã ce jour. GrÃ¢ce Ã des attaques par dictionnaire (dictionary attacks), les fraudeurs peuvent aisÃ©ment retrouver ces mots de passe trop simples et utiliser des comptes en ligne Ã des fins malicieuses.

Le partage de comptes utilisateur est un danger supplÃ©mentaire. Bien que cela soit interdit par le rÃ¨glement de la plupart des applications de jeu en ligne, les utilisateurs partagent souvent leurs comptes, entre membres dâ□□une mÃªme famille ou entre amis. Lâ□□exposition au risque nâ□□en est Ã©videmment que plus grande.

Des mots de passe dynamiques pour mieux protÃ©ger

Les dÃ©veloppeurs de jeux en ligne ne peuvent pas grand-chose pour protÃ©ger les informations des comptes de leurs utilisateurs ainsi que leurs actifs virtuels puisque cela ne correspond pas Ã leur conception du jeu. Quoique. Bien quâ□□ils pourraient arguer du fait que la sÃ©curitÃ© des mots de passe relÃ¨ve de la responsabilitÃ© des utilisateurs, les dÃ©veloppeurs rÃ©alisent quâ□□ils devraient proposer Ã leurs clients des moyens sÃ©curisÃ©s de protÃ©ger leurs personnages de jeu.

Lâ□□une des faÃ§ons de se protÃ©ger contre les menaces prÃ©cÃ©demment Ã©voquÃ©es est de mettre en place un systÃ¨me dâ□□authentification forte. VASCO, lâ□□un des fournisseurs leaders de solutions dâ□□authentification et de sÃ©curitÃ© sur Internet, sâ□□est construit une solide rÃ©putation dans la sÃ©curisation des applications de jeu en ligne. En utilisant sa technologie renommÃ©e DIGIPASS, les mots de passe statiques et fragiles peuvent Ãªtre remplacÃ©s par une authentification forte Ã deux facteurs. Pour quelques dollars, les joueurs peuvent sâ□□offrir sÃ©rÃ©nitÃ© et protection de leurs actifs virtuels.

Lâ□□entreprise fournit une plateforme dâ□□authentification ouverte pouvant Ãªtre intÃ©grÃ©e Ã des serveurs de jeu afin de prendre en charge automatiquement le processus dâ□□authentification. Les fournisseurs de jeux en ligne peuvent choisir de distribuer des authentificateurs matÃ©riels ou des logiciels dâ□□authentification Ã leurs utilisateurs finaux. Ces Ã©quipements assurent la gÃ©nÃ©ration dâ□□un mot de passe dynamique Ã chaque ouverture de session. Les mots de passe dynamiques permettent de contourner les faiblesses gÃ©nÃ©ralement associÃ©es aux mots de passe statiques. Tout dâ□□abord, ils ne peuvent Ãªtre utilisÃ©s quâ□□une seule fois. Ainsi, les fraudeurs ne peuvent pas les stocker en vue de traitements par lots. Qui plus est, la validitÃ© des mots de passe est fortement limitÃ©e dans le temps : les criminels doivent opÃ©rer en temps rÃ©el et lâ□□impact lucratif du piratage de compte en est considÃ©rablement rÃ©duit. Et puisque chaque joueur reÃ§oit un Ã©lÃ©ment dâ□□authentification unique et personnalisÃ©, lâ□□exposition des mots de passe liÃ©e au partage de compte est Ã©liminÃ©e. Accessoirement, cela permet aux fournisseurs de jeux en ligne de rÃ©duire les pertes de chiffre dâ□□affaires. Enfin, puisque le mot de passe est gÃ©nÃ©rÃ© par un outil matÃ©riel ou sur une plateforme logicielle locale, il nâ□□est pas exposÃ© sur Internet.

FlexibilitÃ© et adoption assurÃ©e Ã un prix modique

La mise en Å□uvre dâ□□un systÃ¨me de sÃ©curitÃ© nâ□□est pas sans crÃ©er dâ□□importants dÃ©fis pour les dÃ©veloppeurs de jeux. Tout dâ□□abord, cela reprÃ©sente un investissement. Ensuite, la solution doit pouvoir supporter des dÃ©ploiements massifs, Ã lâ□□Ã©chelle de plusieurs millions dâ□□utilisateurs. En outre, les fournisseurs de jeux vidÃ©o en ligne doivent Ãªtre sÃ»rs que la solution sera pÃ©renne. Enfin, les freins Ã lâ□□adoption de la solution par les utilisateurs doivent Ãªtre minimes â□□ sans que la sÃ©curitÃ© soit pour autant sacrifiÃ©e.

Les solutions dâ□□authentification de VASCO sont conÃ§ues Ã partir dâ□□une unique plateforme ouverte. Cela Ã©vite de devoir reconstruire toute une infrastructure et permet de rÃ©aliser dâ□□importantes Ã©conomies tout en gagnant en flexibilitÃ©. Lâ□□authentification DIGIPASS offre une grande Ã©lasticitÃ©. Et celle-ci a Ã©tÃ© dÃ©montrÃ©e Ã de nombreuses reprises. VASCO supporte actuellement des millions de joueurs en ligne qui font confiance Ã ses Ã©quipements et logiciels dâ□□authentification. Le logiciel de VASCO est capable de supporter plus de 9 000 demandes dâ□□authentification par seconde. La plateforme est taillÃ©e pour supporter de nombreux jeux et utilisateurs supplÃ©mentaires ; câ□□est une solution assurÃ©ment pÃ©renne, nous confie **Jan Valcke** PrÃ©sident et COO de VASCO Data Security depuis 2002

Lâ□□adoption par les utilisateurs est un point clÃ© pour lâ□□authentification de masse. La technologie DIGIPASS de VASCO, quâ□□elle soit matÃ©rielle ou logicielle, est si simple Ã utiliser que les fournisseurs de jeux en ligne seront rapidement persuadÃ©s quâ□□il sâ□□agit dâ□□un parfait outil dâ□□authentification pour leurs joueurs. Ceux-ci nâ□□ont pas besoin dâ□□installer de logiciels supplÃ©mentaires sur leurs ordinateurs pour en profiter â□□ aucun mode dâ□□emploi ou service de support spÃ©cifique nâ□□est nÃ©cessaire. Lâ□□expÃ©rience de jeu reste la mÃªme, si ce nâ□□est quâ□□elle est sÃ©curisÃ©e.