Quand Street Fighter V installe un malware... pour la sécurité

TOPICS: Hack Street Fighter

POSTED BY: DANDU 29 SEPTEMBRE 2016

Récemment, la dernière mise à jour de Street Fighter V a créé la polémique. Pas pour la coupe de cheveux improbable d'un personnage, mais à cause d'un malware.

Avant de commencer, notons que Capcom **a retiré** le malware en question du jeu, avec une nouvelle mise à jour.

La mise à jour installait un pilote en douce (il était caché) qui permettait d'exécuter du code arbitrairement. Le pilote `capcom.sys` commençait par désactiver le SMEP – Supervisor Mode Execution Protection -, une protection intégrée dans les processeurs x86 récents et utilisée depuis Windows 8. Cette protection permet en fait d'éviter qu'un logiciel « utilisateur » utilise des instructions réservées au noyau de l'OS (Windows dans le cas présent). Une fois le SMEP désactivé, le pilote permettait un accès à la mémoire avec les droits du noyau, à travers une mémoire tampon. Quand l'application – en théorie Street Fighter V – avait terminé, le SMEP était réactivé.

Une partie du code du pilote

La solution de Capcom visait essentiellement à détecter les logiciels de triche qui permettent de modifier le jeu en temps réel, mais elle posait des problèmes de sécurité énormes. Le principal, c'est que le pilote ne vérifiait absolument pas ce qui passait dans la mémoire tampon : n'importe quel logiciel pouvait écrire des données à la bonne adresse et exécuter du code arbitrairement, avec tous les droits. À côté de cette ouverture béante dans la sécurité des joueurs, la « protection » de Capcom avait tendance à créer des écrans bleus chez certains joueurs et – plus étonnant – elle **semble** avoir été conçue à partir d'un rootkit.

Cet exemple montre que plus de 10 ans après la débâcle du rootkit dans les CD Audio de Sony, les développeurs et les éditeurs n'hésitent toujours pas à utiliser des méthodes de hacker pour essayer de contrer la triche dans les jeux vidéo, spécialement quand elle est liée à des espèces sonnantes et trébuchantes. Parce que ne soyons pas naïfs : Capcom essaye d'éviter que les joueurs débloquent (en trichant) des personnages vendus en achats in-app, même s'il est parfaitement possible de gagner la monnaie (virtuelle) nécessaire en jouant beaucoup de parties.

En attendant, vous pouvez vérifier la présence du malware et le supprimer le cas échéant avec la méthode de nos confrères **de Bas Gros Poing**. À noter que le pilote semble être passé dans les mailles du filet de la validation de Microsoft : depuis juillet 2015, tous les pilotes qui utilisent le kernel mode doivent passer par une validation et une signature des créateurs de Windows. Le pilote lui-même utilise un certificat issu de chez Symantec, un éditeur d'antivirus qui – ironiquement – détecte maintenant `capcom.sys` comme un malware...

SHARE TWEET PIN SHARE

ABOUT THE AUTHOR

Dandu

Espion de Cupertino dans la rédac' de Canard PC Hardware. Aime beaucoup les formats totalement obsolètes ainsi que les technologies bizarres et oubliées. Possède un chien robot, des lapins Wi-Fi et un vrai perroquet.

CPC HARDWARE N°30

Au menu : le guide des GPU (fonctionnement, benchs, upgrade, SAV,...), les nouveautés côté refroidissement, Calyos LHP, la fin du disque optique, USB Killer, Oculus et Nosulus Rift, etc.

TROLL'N'TWEET

CPC Hardware @CPCHardware
Quand Street Fighter V installe un malware... pour votre sécurité - https://t.co/9SvK2WStu4
- 8 minutes ago

Follow @CPCHardware

ARTICLES RÉCENTS

Quand Street Fighter V installe un malware... pour la sécurité
Canard PC Hardware N°30 est disponible !
L'informatique au cinéma : vous avez le droit de rigoler
Des SSD à 3,5 Go/s chez Samsung
Comment démarrer le Raspberry Pi 3 sur une clé USB

CATÉGORIES

Débrief (11)
Hors sujet (4)
Langue de pute (3)
Magazine (2)
News (1)
Tests (6)
Tutorial (1)
x86-secret (2)