Déjà des backdoors et keyloggers pour Windows 10 chez Hacking Team | Le Net Expert Informatique

Déjà des backdoors et keyloggers pour Windows 10 chez Hacking Team

Anticipant sur les besoins de ses clients, Hacking Team s'est assuré d'être prêt au lancement de Windows 10. La société italienne a adapté ses outils pour être capable d'installer un backdoor sous Windows 10, et ainsi de pouvoir collecter à distance toutes les frappes de touches au clavier.

Windows 10 n'est pas encore officiellement sorti, mais les firmes qui fournissent aux autorités les outils permettant d'accéder à distance aux données sont déjà à pied d'oeuvre pour s'adapter au niveau système d'exploitation de Microsoft. Ainsi l'entreprise italienne Hacking Team, dont les e-mails ont fuité ce mois-ci, s'est assurée dès l'an dernier de pouvoir fournir à ses clients de quoi espionner des utilisateurs de Windows 10.

« Nous avons testé Windows 10 Preview et ça fonctionne », a ainsi expliqué Marco Valleri, le directeur de Hacking Team, dans un e-mail du 4 novembre 2014. Il répondait à l'ancien responsable des opérations à Singapour, Serge Woon, qui se demandait si « RCS 9.4 supporte Windows 8.2 » (en fait Windows 10). RCS est l'acronyme de « Remote Control System », le malware qui permet à Hacking Team de prendre à distance le contrôle d'un ordinateur pour accéder à ses données.

Un autre e-mail du 29 juin 2015 montre que deux employés de Hacking Team, Marco Fontana et Andrea Di Pasquale, ont testé avec succès l'installation hors ligne de plusieurs outils sur Windows 10 Enterprise Insider Preview. Ils disent avoir vérifié notamment « l'installation d'un backdoor », « l'exportation de preuves depuis le backdoor », et la « désinstallation du backdoor ».

« Super ! », s'enthousiasme le directeur technique Marco Valleri, qui propose aussitôt une réunion pour déployer la mise à jour dans un git, probablement celui de RCS.

La société Hacking Team dispose également d'un outil invisible pour Windows 10 permettant de collecter toutes les frappes de touches au clavier (un « keylogger »), comme le montre un courriel du 5 juin. Marco Fontana, qui semble être une petite star dans l'entreprise, y rend compte d'une réunion du mercredi 3 juin 2015, où « l'un des thèmes de la réunion était le test du mécanisme d'injection dans l'application Metro ».

Il explique que « le POC du keylogger pour Windows 10 est prêt et peut être testé pour vérifier sa « compatibilité » avec les antivirus ». Le POC (Proof-of-concept) est une démonstration de faisabilité.

Dans un e-mail du 15 juin, Marco Fontana précise à son équipe qu'il a testé une « technique d'injection dans l'application Metro de Windows 10 », et que « l'exécutable 'ExeLoader' injecte la DLL ApiHookDll dans un processeur notepad.exe et capture les touches ». Il s'agit d'un POC visant à collecter les touches tapées sous sur l'application « Bloc Notes » de Windows 10.

« Si tout fonctionne correctement, dans le dossier temporaire de Windows (%temp%) vous verrez un fichier texte créé qui contient les touches enfoncées dans notepad. Le fichier a un préfixe KBD_ et une valeur aléatoire (ex: KBD_000407E600C553CE.txt) ».

Tout l'objet du logiciel RCS de Hacking Team est justement d'installer à distance les backdoors qui permettent d'installer des outils tels que ce keylogger, lequel permet ensuite de récupérer, par exemple, les mots de passe saisis pour accéder à des comptes e-mail, ou des mots de passe de clés de chiffrement.

« On ne peut pas croire à la sécurité d'un OS pour le grand public », s'était amusé en novembre dernier David Vincenzetti, le président de Hacking Team, en lisant une actualité selon laquelle Windows 10 pourrait signer la fin des malwares.

Source : http://www.numerama.com/magazine/33727-deja-des-backdoors-et-keyloggers-pour-windows-10-chez-hacking-team.html
par Guillaume Champeau