L'OS nord-coréen Red Star 3.0 dévoile ses services secrets

À quoi ressemble le système d'exploitation d'une dictature ? **Red Star 3.0** est en fuite sur la Toile. C'est le système d'exploitation promu par la **Corée du Nord**.

Tous les outils nécessaires sont présents, comme une suite bureautique (Sogwang Office, sur base OpenOffice), un navigateur Internet (Naenara, s'appuyant sur Firefox) ou encore des applications multimédias et un outil de chiffrement des données.

Si Red Star 2.5 copiait ouvertement le look de Windows XP, Red Star 3.0 se veut visuellement très proche d'OS X. Il s'appuie toujours sur la distribution Linux Fedora (sur base KDE), mais avec plusieurs modifications de taille. La première réside dans **l'espionnage massif** opéré par cet OS. Là où les systèmes Linux sont des apporteurs de liberté, Red Star est – sans surprise – un privateur de ces mêmes libertés.

De premières études ont été faites sur cet OS, menant à des découvertes plutôt inquiétantes, quoique attendues de la part du gouvernement nord-coréen. *The Guardian* explique ainsi que l'antivirus intégré au système d'exploitation a un rôle plus pernicieux que celui auquel nous pouvons nous attendre de la part d'un tel outil.

Suivi des fichiers non autorisés

Florian Grunow et Niklaus Schiess, de la société de sécurité allemande ERNW, ont remarqué que l'antivirus se charge de marquer les fichiers copiés depuis un média externe. Cette marque unique permet de savoir sur quelles machines ont été présents les fichiers (films, photos, documents, etc.), et ainsi de retrouver aisément toutes les personnes ayant accédé à des données non autorisées. Au besoin, l'antivirus pourra effacer ces fichiers.

Les périphériques amovibles sont la voie privilégiée pour les opposants au régime souhaitant se partager des informations. Chose d'autant plus vraie que la Corée du Nord utilise **un intranet offrant un accès limité et filtré** aux informations habituellement présentes sur la Toile. Cet intranet est étroitement surveillé lui aussi, y compris par le navigateur web de Red Star (basé sur Firefox), qui opère des interceptions massives de données.

Protection anti-hackers

Les experts en sécurité ont également découvert qu'il est **presque impossible de désactiver cet antivirus**, chaque action allant dans ce sens menant au redémarrage de la machine dans son état précédent. Le pare-feu ne peut pas non plus être désactivé. La présence d'une porte dérobée dans l'outil de chiffrement n'a pas été démontrée, mais reste probable.

Ironiquement, Red Star n'est pas le seul OS de type Linux servant d'espion pour des gouvernements. **Des pays comme Cuba et la Chine** disposent eux aussi de leurs propres

systèmes d'exploitation, dont la sûreté des données est loin d'être démontrée.

Florian Grunow et Niklaus Schiess ont animé une présentation dans le cadre du **Chaos Communication Congress de Hambourg**, le 27 décembre dernier. Une présentation assurée avec une machine fonctionnant… sous Red Star.

À lire aussi :
L'Internet gratuit de Facebook retoqué en Inde
Le chiffrement de Windows 10 sous écoute de la NSA ?
Microsoft alertera ses clients lorsque leurs données seront piratées

Crédit photo : © Filip Bjorkman – Shutterstock