Vulnérabilité des serveurs BlackBerry: la réponse de RIM

RIM, le fabricant du célèbre BlackBerry, doit à nouveau faire face à des questions sensibles de sécurité. Ce mercredi, nous évoquions ici le programme BBProxy qui semble être l'un des premiers codes malveillants à cibler le célèbre PDA.

Son créateur, Jesse D'Aguano, a fait part de sa découverte lors du Defcon. BBProxy, un logiciel cheval de Troie téléchargé délibérément, exploiterait une faille entre le terminal et le serveur email, et pourrait être utilisé pour placer différents codes plus ou moins dangereux sur un réseau interne. Un véritable risque pour les milliers d'entreprises utilisatrices du terminal.

Lors de cette annonce, le directeur de la sécurité de BlackBerry déclarait simplement: *« cela pourrait être le premier code malveillant à cibler le Blackberry »,* toutefois, la société ne considère pas la menace comme très sérieuse.

Aujourd'hui, face à l'ampleur médiatique que prend cette information, RIM a décidé de réagir de façon plus explicite.

Dans un communiqué, le groupe canadien explique que *« la solution BlackBerry intègre des règles de sécurité qui empêchent l'exploitation de tels logiciels malveillants »*.

Et d'ajouter: *« Des mesures supplémentaires peuvent également être prises en installant les serveurs BlackBerry sur un réseau segmenté. Les administrateurs peuvent se référer aux deux documents publiés sur le site de BlackBerry : « Protecting the BlackBerry Device Platform Against Malware » et « Placing the BlackBerry Enterprise Solution in a Segmented Network ». Ces documents sont disponibles à l'adresse : https://www.blackberry.com/security »*.

Concernant le mode de propagation, un fichier joint à un mail (comme par exemple un jeu), RIM rapelle que *« le BlackBerry Enterprise Server n'autorisant pas l'utilisateur à télécharger les pièces jointes sur le terminal, le logiciel cheval de Troie ne peut en aucun cas être transmis en tant que pièce jointe d'un e-mail à un utilisateur BlackBerry »*.

Research In Motion explique enfin que l'exploitation de cette attaque doit se faire dans un contexte particulier. *« Le scénario décrit repose sur plusieurs suppositions concernant le déploiement du BlackBerry Enterprise Server. La capacité de charger et d'exécuter toute application tierce sur un terminal BlackBerry est contrôlée par le paramétrage des règles de sécurités du BlackBerry Enterprise Server, et doit être autorisée par l'administrateur. De plus, la capacité pour une application tierce d'établir une connexion externe à partir d'un appareil BlackBerry est également contrôlée par le paramétrage de l'une des règles de sécurité du BlackBerry Enterprise Server, et doit être autorisée par l'administrateur. Par ailleurs, l'autorisation de la connexion au réseau de l'entreprise grâce a la solution BlackBerry Mobile Data System est également contrôlée par l'un des paramètres des règles de sécurité informatique du BlackBerry Enterprise Server, qui aurait également du être autorisé par l'administrateur »*.

Le groupe estime que Jesse D'Aguano veut se faire de la publicité avec cette annonce infondée. Pour autant, dangeureuse ou pas, cette vulnérabilité viendra apporter de l'eau au moulin des

détracteurs du célèbre terminal.