On peut voler des identifiants Active Directory depuis Internet via SMB | Le Net Expert Informatique

On peut voler des identifiants Active Directory depuis Internet via SMB

Deux chercheurs ont montré sur la conférence Black Hat 2015 qu'une attaque via le protocole de partage de fichiers SMB connue pour s'effectuer au sein d'un réseau local peut en fait servir à attaquer des serveurs Windows hébergés dans le cloud.

Lors de la conférence Black Hat 2015 (Las Vegas, du 1er au 6 août), deux chercheurs ont montré qu'une technique d'attaque via le protocole de partage de fichiers SMB que l'on croyait ne fonctionner que sur les réseaux locaux peut en fait être exécutée sur Internet. Avec cette attaque, dite de relais SMB, un ordinateur Windows appartenant à un domaine Active Directory laisse apparaître les informations d'identification de l'utilisateur quand celui-ci consulte une page web, un courriel dans Outlook ou regarde une vidéo dans Windows Media Player. L'attaquant peut ensuite détourner ces identifiants pour s'authentifier au nom de l'utilisateur sur des serveurs Windows où il dispose d'un compte, y compris ceux hébergés dans le cloud.
Dans un réseau Active Directory, les ordinateurs Windows retournent automatiquement leurs informations d'identification pour accéder aux différents services de partage de fichiers à distance, aux serveurs de messagerie Microsoft Exchange ou aux outils de collaboration SharePoint. Ces informations d'authentification – en l'occurrence le nom de l'ordinateur, le nom de l'utilisateur, tous deux en texte clair, et un hash cryptographique dérivé du mot de passe de l'utilisateur – sont envoyées à l'aide du protocole d'authentification NTLMv2. En 2001, des chercheurs en sécurité avaient déjà mis au point une attaque dite par relais SMB : en se positionnant entre un ordinateur Windows et un serveur, les attaquants pouvaient intercepter les informations d'identification, puis les relayer vers le serveur et s'authentifier à la place de l'utilisateur légitime. Mais à l'époque, tout le monde pensait que l'attaque ne fonctionnait qu'en local.

Authentification configurée par défaut dans IE
Sauf que, dans Internet Explorer, l'authentification de l'utilisateur est configurée par défaut avec l'option « ouverture de session automatique réservée à la zone intranet ». Or, les chercheurs en sécurité Jonathan Brossard et Hormazd Billimoria, ont constaté que cette option était ignorée et qu'il était possible de duper le navigateur pour que celui-ci laisse fuiter vers Internet les informations Active Directory de l'utilisateur – c'est à dire son nom et la séquence de code cryptographique basée sur son mot de passe – pour les transmettre à un serveur SMB distant contrôlé par les pirates. Les chercheurs ont pu suivre le trajet d'un fichier DLL propre à Windows, utilisé aussi bien par Internet Explorer que par de nombreuses applications pouvant accéder aux URL, comme Microsoft Outlook, Windows Media Player ou d'autres programmes tiers. « Quand l'application veut accéder à une URL, le fichier DLL vérifie les informations d'authentification dans le registre, mais tout en les ignorant », ont expliqué les chercheurs pendant leur présentation.

Toutes les versions actuelles de Windows et d'Internet Explorer (ou encore supportées) sont concernées par le problème. « C'est la première attaque à distance capable de compromettre potentiellement Windows 10 et le nouveau navigateur Microsoft Edge », a alerté Jonathan Brossard. « Nous sommes au courant de ce problème et nous enquêtons à ce sujet », a déclaré jeudi un représentant de Microsoft par courriel.

Plusieurs scénarios possibles
« Une fois que les attaquants ont mis la main sur les informations d'identification de l'utilisateur, ils peuvent les utiliser de différentes façons », a précisé Jonathan Brossard. Un premier scénario consisterait à monter une attaque par relais SMB pour s'authentifier à la place de la victime sur des serveurs hébergés hors du réseau local en utilisant une fonctionnalité appelée « NTLM over http », ajoutée pour étendre le périmètre des réseaux dans les environnements cloud. Les pirates pourraient notamment accéder à un shell distant sur le serveur qu'ils utiliseraient ensuite pour installer des logiciels malveillants ou exécuter des programmes exploitant des failles. Si le serveur distant est un serveur Exchange, les attaquants pourraient télécharger toute la boîte aux lettres de l'utilisateur.

Un autre scénario impliquerait de casser la séquence de code cryptographique et de l'utiliser pour accéder à un serveur Remote Desktop Protocol. Des pirates peuvent y arriver en utilisant des plates-formes spécialisées ou des services donnant accès à une grosse puissance de calcul. Un mot de passe de huit caractères ou moins peut être craqué en deux jours environ. « Et, déchiffrer toute une liste de hashs volés ne serait pas plus long, puisque le processus teste toutes les combinaisons à la fois », a ajouté le chercheur. Des identifiants Windows volés via Internet seraient également utiles à des attaquants qui ont déjà réussi à se faufiler dans un réseau local, mais ne disposent pas des privilèges d'administration. En envoyant un simple message électronique à l'administrateur légitime, ils pourraient récupérer ses identifiants dans Outlook et utiliser le hash volé pour mener une attaque par relais SMB contre les serveurs connectés au réseau local.

Source : http://www.lemondeinformatique.fr/actualites/lire-black-hat-2015-on-peut-voler-des-identifiants-active-directory-depuis-internet-via-smb-62000.html
Par Jean Elyan et IDG News Service