

Noms de domaine : en rachetant corp.com, Microsoft éloigne les hackers

Microsoft a racheté le nom de domaine corp.com pour un montant resté confidentiel. Le [chercheur en sécurité Brian Krebs](#) a révélé l'information.

En février dernier, le domaine en question était proposé à la vente aux enchères à un prix de départ de 1,7 million de dollars par un particulier qui le détenait depuis 26 ans. Basé dans le Wisconsin, l'homme espérait que Microsoft l'achète car des « *centaines de milliers de PC sous Windows tentent constamment de partager des données sensibles avec corp.com* », a-t-il indiqué.

Le problème est lié à la collision de noms (namespace collision).

Quand la collision menace

Selon l'ICANN (Internet Corporation for Assigned Names and Numbers), le phénomène de collision de noms « *se produit lorsqu'une tentative de résolution d'un nom utilisé dans un espace de noms privé donne lieu à la résolution d'une requête envoyée au système des noms de domaine (DNS) public. Lorsque les frontières administratives entre l'espace de noms privé et public se chevauchent, la résolution de noms peut entraîner des résultats inattendus ou nuisibles.* »

Dans des versions antérieures de Windows – Windows 2000 Server, par exemple -, la suggestion de nom par défaut pour les administrateurs configurant le service d'annuaire [Active Directory](#) (AD) de Microsoft était « corp ». Le problème est double. L'éditeur de Redmond a lié la suggestion par défaut à une adresse réelle, d'une part. De nombreuses entreprises ont adopté ce paramètre sans le modifier, d'autre part.

De quoi aiguïser l'appétit de hackers ou pirates informatiques.

« *Concrètement, cela signifie que quiconque contrôle corp.com peut intercepter passivement les communications privées de centaines de milliers d'ordinateurs qui finissent par être retirés d'un environnement d'entreprise qui utilise cette désignation « corp » pour son domaine Active Directory* », a précisé le chercheur en sécurité sur son blog KrebsOnSecurity.

Sécuriser noms et réseaux internes

Microsoft a confirmé avoir acquis le nom de domaine corp.com.

« *Pour aider à protéger les systèmes, nous encourageons les clients à adopter des pratiques de sécurité sûres lors de la planification des noms de domaine et de réseaux internes* », a déclaré l'éditeur dans un communiqué. « *Nous avons publié un avis de sécurité en juin 2009 et une mise à jour de sécurité qui contribue à la protection des utilisateurs. Dans le cadre de notre engagement continu envers la sécurité des clients, nous avons également acquis le domaine corp.com.* »

L'initiative peut protéger des entreprises qui ont basé leurs infrastructures utilisant le service Active Directory sur « corp » ou « corp.com ». Malgré tout, Brian Krebs prévient : « *toute entreprise qui a lié son réseau Active Directory interne à un domaine qu'elle ne contrôle pas s'expose à un cauchemar potentiel en matière de sécurité.* »

(crédit photo : [morrisonbrett](#) via [VisualHunt.com](#) / [CC BY](#))