Messagerie : le ver Exim s'attaque à Microsoft Azure

Microsoft a averti ses clients Azure, ce 14 juin, qu'un ver Linux avait attaqué son infrastructure Cloud.

Il s'agit du même ver qui a pris pour cible la semaine dernière les serveurs email qui exécutent le logiciel Exim. Ce n'est pas une petite attaque puisque plus de la moitié des serveurs de messagerie sont concernés.

Les serveurs de messagerie Exim menacés par un ver

Le malware, qui se propage automatiquement, infecte les serveurs de messagerie Exim en exploitant la vulnérabilité CVE-2019-10149, qui permet aux pirates d'exécuter des commandes à distance et de prendre le contrôle des serveurs sans correctifs.

En l'occurrence, le ver utilise cette faille de sécurité pour prendre le contrôle d'un serveur, puis il cible d'autres serveurs et tente de les infecter également en y transférant un mineur de crypto-monnaie.

Selon Microsoft, Azure « dispose de contrôles permettant de limiter la propagation de ce ver » mais les serveurs risquent d'être ralentis par le mineur, très exigeant en ressources système.

Seule solution : mettre à jour Exim exécuté sur des machines Azure vers Exim 4.92, seule version corrigée.

Et si le mal est fait, Microsoft prévient que seule une réinstallation complète d'Azure ou la restauration d'une sauvegarde effectuée avant l'infection permettra de se débarrasser du ver.