TrickBot : la nouvelle vie d'un botnet qu'on croyait démantelé

Faut-il plus que jamais se méfier de TrickBot ? Peu avant les présidentielles américaines, il avait fait l'objet d'une tentative de démantèlement sous la houlette de Microsoft. Depuis lors, le *trojan* bancaire, devenu « *malware* à tout faire », semble remonter en puissance.

L'opération destinée à le mettre hors d'état de nuire avait démarré vers le 20 septembre. Elle avait impliqué la saisie de serveurs de commande. Et la distribution d'un fichier qui isolait les machines infectées en les faisant pointer vers l'adresse 0.0.0.1:1.

Microsoft avait officialisé la démarche le 12 octobre. À ce moment-là, l'activité de TrickBot semblait déjà avoir repris. On trouvait notamment trace d'échantillons distribués via Emotet*. Ils assignaient aux victimes des étiquettes spécifiques suggérant une volonté de suivre la reconstitution de la base infectée.

Depuis lors, on a repéré diverses campagnes reposant supposément sur TrickBot. L'une des dernières en date a visé, en Amérique du Nord, des sociétés des secteurs juridique et de l'assurance. Son vecteur : un lien envoyé par mail. Il aboutit à une page qui invite l'utilisateur à télécharger un fichier. Il s'agit d'une archive. Elle héberge un fichier JavaScript qui, une fois exécuté, télécharge une autre charge malveillante.

De TrickBot à TrickBoot

Après la tentative de démantèlement, on a observé de nouvelles versions de TrickBot. L'une d'entre elles introduisait un mécanisme de certification des mises à jour du *malware*. Une autre présentait, d'une part, une infrastructure de commande mise à jour, exclusivement à base de routeurs Mikrotik. Et de l'autre, des changements dans la liste des modules complémentaires téléchargeables.

Parmi ces modules, il y a celui qu'on a appelé TrickBoot. Il entre dans la catégorie des *bootkits*. En d'autres termes, il est capable de s'immiscer dans des BIOS/UEFI. Pour y parvenir depuis l'espace utilisateur, il exploite un pilote système tiré du logiciel RWEverything. Ses cibles : de nombreux *chipsets* Intel, des générations Skylake à Comet Lake, y compris sur des serveurs. Les conséquences : un contrôle potentiellement total sur les appareils contaminés.

Le *bootkit* vient compléter une méthode déjà effective avant la tentative de démantèlement : la mise en place d'une tâche planifiée pour résister aux redémarrages. Elle a toutefois évolué, avec l'introduction d'une étape intermédiaire susceptible de mieux passer sous les radars des solutions de sécurité. On appelle toujours un exécutable, mais au travers d'un fichier batch. Le nom de la tâche n'est pas ailleurs plus fixe, de par la présence d'un mécanisme de randomisation.

** On surveillera dans quelle mesure le come-back de TrickBot pourrait être perturbé par une autre opération de démantèlement. En l'occurrence, celle qui a visé son principal vecteur de diffusion : Emotet.*

Photo d'illustration © lolloj – Fotolia