Windows 11 : le portail de téléchargement usurpé par des hackers

Le spécialiste des solutions de cybersécurité dans le Cloud Zscaler a annoncé la découverte, dès le mois d'avril, d'un cas d'usurpation d'un portail officiel de téléchargement du système d'exploitation de Microsoft, Windows 11.

Les hackers profiteraient du stratagème pour diffuser le logiciel malveillant voleur d'informations, Vidar.

Un faux portail Windows 11

En surveillant le trafic suspect, le laboratoire de détection des menaces de Zscaler a découvert que plusieurs domaines tout récemment enregistrés ont été créés par un acteur cybermalveillant, dans le but de tromper les utilisateurs avec un faux portail de téléchargement de l'OS Windows 11.

Ces fameux sites usurpés ont été mis au point pour distribuer auprès des cibles des fichiers ISO malveillants qui aboutissent à une infection de la machine par un malware de type Vidar infostealer.

Dans le détail, les variantes de Vidar parviennent à récupérer la configuration C2 depuis des canaux de médias sociaux alors contrôlés par les cybercriminels et hébergés sur la messagerie instantanée Telegram et le réseau qui veut concurrencer Twitter, Mastodon.

Selon Zscaler, le même acteur de la menace ferait appel à l'ingénierie sociale pour piéger ses victimes et se faire passer pour des applications logicielles populaires légitimes, toujours pour distribuer le malware Vidar.

Un dépôt GitHub, qui héberge différentes versions de backdoors du logiciel Adobe Photoshop, a ainsi été identifié, et il est évidemment contrôlé par les hackers. Ces derniers distribuent Vidar, qui utilise des tactiques similaires d'abus des canaux de médias sociaux pour la communication C2.

Objectif : diffuser le malware Vidar

Là où les hackers ont été malins, c'est sur la taille du fichier ISO téléchargé au moment où vous pensez récupérer le dernier OS de bureau de Microsoft, car celui-ci pèse plus de 300 Mo. Cela lui permet d'échapper à la détection des produits de sécurité réseau. D'ailleurs, le binaire à l'intérieur de l'ISO est signé numériquement avec un certificat Avast (certes expiré et invalide).

Concernant le vecteur de distribution Adobe Photoshop plus particulièrement, le référentiel GitHub identifié et contrôlé par l'attaquant hébergeait aussi des versions dérobées de la suite applicative

Adobe Creative Cloud, également attribué au même acteur.

Ce qu'il faut retenir de tout cela, c'est la capacité des cyberattaquants à inciter leurs victimes à installer Vidar en utilisant des applications « à la mode » (de type Mastodon et Telegram) ou particulièrement populaires (de type Adobe Photoshop), en profitant bien évidemment de la période transitoire qui pousse les utilisateurs de Windows 10 à basculer sur Windows 11.

Notre recommandation première reste de ne télécharger des logiciels que depuis les sites web officiels, en ayant vous-même tapé la requête dans votre moteur de recherche.

Alexandre Boero