ALERTE DE SECURITE

Objet :	**ALERTE EXTENSIONS NAVIGATEURS MALVEILLANTES**
Niveau de criticité :	**IMPORTANT**
Référence :	**CICERT-BAS-2021-002**

Résumé

Dans le cadre de ses activités de monitoring et de veille, le CI-CERT a noté que plusieurs extensions des navigateurs Web « **Google Chrome** » et « **Microsoft Edge** », ont servi à détourner les clics des utilisateurs dans les pages de résultats de recherche vers des URL arbitraires, comprenant des sites de phishing, de téléchargement de logiciel malveillants, d'annonces, etc.

Ces extensions malveillantes ont utilisé une astuce sournoise pour cacher leurs activités et dissimuler leur véritables finalités. En effet, lors de l'installation, les extensions malveillantes affichent une page usurpée ressemblant à un site ou page officielle connue (Google Analytics). Cependant, elles téléchargent et installent dans le même temps un logiciel malveillant JavaScript. Ce logiciel malveillant est en mesure de collecter toutes les informations sensibles de l'utilisateur, telles que la date de naissance, les adresses e-mail, la géolocalisation et l'activité de l'appareil, avec un accent particulier sur la collecte des données de Google.

Ensuite, le code malveillant infecte l'ensemble du navigateur et détourne de ce fait, les clics menant à des sites Web légitimes. Les utilisateurs sont alors redirigés vers des sites malveillants et frauduleux quand bien même ils effectuent une recherche dans le moteur de recherche.

Par ailleurs, ces extensions malveillantes qui étaient disponibles même dans les magasins officiels des navigateurs ont été configurées pour ne pas présenter de comportement suspect pendant les trois premiers jours suivant l'installation, afin d'échapper aux antivirus.

En l'état actuel des connaissances sur cette menace, les propriétaires des navigateurs les ont retirés de leurs espaces de téléchargement et invitent à prendre des mesures correctives, afin de prévenir une plus large infection des utilisateurs.

Recommandations

Si vous avez déjà installé une ou plusieurs des extensions citées ci-dessous, il est vous est recommandé de :

- Supprimer ou désactiver immédiatement l'extension infectée ;
- Effectuer un scan antiviral complet de votre ordinateur ;
- Modifier systématiquement vos identifiants de compte en ligne (réseaux sociaux, e-mail, etc.) ;
- Utiliser des applications fiables de nettoyage de navigateurs web.

Liste des extensions malveillantes

Pour les extensions Chrome infectées	Pour les extensions Edge infectées
Direct Message for Instagram	Direct Message for Instagram
DM for Instagram	Instagram Download Video & image
Invisible mode for Instagram Direct Message	App Phone for Instagram
Downloader for Instagram	Universal Video Downloader
App Phone for Instagram	Video Downloader for Facebook
Stories for Instagram	Vimeo Video Downloader
Universal Video Downloader	Volume Controller
Video Downloader for Facebook	Stories for Instagram
Vimeo Video Downloader	Upload photo to Instagram
Zoomer for Instagram and Facebook	Pretty Kitty, The Cat Pet
VK Unblock. Works fast.	Video Downloader for YouTube
odnoklassniki Unblock. Works quickly.	SoundCloud Music Downloader
Upload photo to Instagram	Instagram App with Direct Message DM
Spotify Music Downloader	Downloader for Instagram
The New York Times News	
FORBES	