Cybersécurité 101

Les pirates informatiques sont créatifs et rusés. Ils cherchent constamment de nouvelles façons d'accéder à vos renseignements. Il est donc difficile d'en assurer la protection, sans compter tout le jargon à retenir. C'est pourquoi nous avons créé cet aide-mémoire pratique qui vous explique certaines des attaques les plus courantes qu'il vous faut connaître.

ÉCOUTE ÉLECTRONIQUE PAR RÉSEAU WI-FI

Un cybercriminel installe un réseau Wi-Fi en apparence légitime dans un lieu public. Une fois branchés à ce « point d'accès sans fil malicieux ou indésirable », les utilisateurs deviennent vulnérables à une ATTAQUE DE L'INTERCEPTEUR.

ATTAQUE DE L'INTERCEPTEUR

Un cybercriminel s'insère entre la victime et un serveur réseau légitime (p. ex., un site Web) afin d'espionner l'activité et d'accéder à des renseignements privés ou sensibles.

HAMEÇONNAGE

Un cybercriminel tente de faire passer un courriel malicieux comme légitime afin d'influencer l'action désirée de la victime (p. ex., pour qu'elle clique sur un lien ou ouvre une pièce jointe).

Un cas classique est le téléchargement, au moyen d'un lien ou d'une pièce jointe, d'un LOGICIEL MALVEILLANT qui affiche un formulaire ou une fenêtre d'ouverture de session servant à subtiliser des mots de passe et des renseignements personnels.

DÉVOIEMENT

Un cybercriminel redirige le navigateur Internet de la victime vers un site Web malicieux en exploitant les vulnérabilités de son logiciel de système de noms de domaine.

Ces sites Web factices sont d'ordinaire une imitation crédible de la destination souhaitée et visent à collecter des renseignements personnels ou sensibles.

TYPOSQUATTAGE

Un cybercriminel utilise les fautes d'orthographe les plus courantes dans les adresses URL pour rediriger les victimes à leur insu vers des sites Web malicieux qui sont souvent une imitation crédible de la destination voulue. Ces faux sites Web servent à recueillir les renseignements personnels ou sensibles de la victime.

DÉNI DE SERVICE (DdS)

Un cybercriminel provoque une surcharge de données sur un serveur ou un appareil afin d'en perturber le fonctionnement. L'afflux massif de demandes empêche les utilisateurs légitimes d'accéder au site Web, au réseau ou à l'appareil connecté à Internet.

Voici les trois principales astuces pour éviter d'être victime d'une attaque :

1. **Mettez à jour votre logiciel fréquemment — Les nouvelles versions comprennent des correctifs de sécurité qui remédient aux vulnérabilités les plus récentes.**
2. **Assurez-vous que le site Web consulté est sécurisé — Ne fournissez jamais de renseignements sensibles sur un site dont la barre d'adresse ne contient pas le code « HTTPS:// » ou un symbole de cadenas.**
3. **Soyez très vigilant lorsque vous recevez une communication suspecte — Prêtez une attention particulière à l'objet du message et à l'adresse URL, et méfiez-vous des liens, des offres ou des demandes qui exigent d'entrer un mot de passe, de remplir un formulaire ou de divulguer des renseignements sensibles.**

LOGICIEL MALVEILLANT

Tout logiciel malveillant installé sur un réseau ou un appareil sans le consentement de la victime — p. ex., virus, cheval de Troie, logiciel publicitaire, espion ou rançonneur. Les fonctions comprennent le plantage informatique, la collecte de renseignements et la prolifération de publicités ou de logiciels malveillants sur d'autres appareils.

LOGICIEL ESPION

Logiciel permettant aux cybercriminels de surveiller l'activité d'un utilisateur à son insu.

Les capacités comprennent l'enregistrement de frappe, l'utilisation non autorisée de la caméra vidéo ou du micro, la vidéocapture d'écran et la collecte de données.

LOGICIEL RANÇONNEUR

Logiciel malveillant qui permet aux cybercriminels d'accéder aux renseignements privés ou sensibles d'un utilisateur autorisé (c.-à-d. la victime) pour ensuite lui restreindre la capacité à se servir de l'ordinateur ou du réseau infecté.

D'habitude, les cybercriminels exigeront un paiement (souvent en cryptomonnaie), en échange duquel l'utilisateur pourra récupérer l'accès ou éviter la divulgation publique des renseignements sensibles.

TÉLÉCHARGEMENT FURTIF

Les cybercriminels dissimulent, sur un site Web ou un serveur non sécurisé, un programme capable de déclencher le téléchargement automatique d'un logiciel malveillant lorsque la victime visite la destination compromise.

Ce type d'attaque n'exige aucune action de la part de la victime (comme cliquer sur un lien).

LOGICIEL EFFACEUR

Logiciel malveillant qui efface complètement le disque dur et tout support de stockage connecté à l'ordinateur ou au réseau.

Êtes-vous prêt en cas de cyberattaque? Communiquez avec MNP dès aujourd'hui pour apprendre comment prévenir une attaque et protéger vos actifs informationnels les plus précieux.

Tom Beaupré, BaSc, QSA, CISSP, CISA Chef - Cybersécurité Québec
Tél. : 514.228.7844
tom.beaupre@mnp.ca