Document d'information, Boîte à outils de cybersécurité de la GCA : Prévenir l'hameçonnage et les logiciels malveillants

Plus de 90 % des cyberattaques commencent par un e-mail d'hameçonnage. L'hameçonnage a pour but de faire croire aux gens qu'ils ont affaire à une entité digne de confiance afin que le criminel puisse leur demander des informations sensibles ou de l'argent.

Le terme « hameçonnage » est généralement associé à la communication par e-mail, le smishing par SMS et le vishing par téléphone. Voici quelques exemples de types d'hameçonnage parmi les nombreux types qui existent :

- **Hameçonnage** : attaque qui n'est généralement pas ciblée. Des e-mails sont envoyés en masse en se faisant passer pour des organisations fiables. Dans l'espoir que certains destinataires répondent à ces e-mails, leur contenu peut porter sur les dernières actualités, l'année fiscale, ou sembler provenir d'organismes connus d'un grand nombre de personnes.
- **Spear-Phishing** : attaque par hameçonnage plus ciblée. Le style de l'e-mail indique qu'il pourrait provenir d'une personne ou d'un organisme connu(e) de la victime. La cible visée a fait l'objet de recherches nécessaires, souvent avec un objectif précis.
- **Whaling** : attaque par hameçonnage très ciblée. Elle vise souvent les hauts responsables d'une organisation. Les criminels auront probablement effectué une reconnaissance en suivant les déplacements de la victime et en collectant des données sur elle pendant des mois avant de passer à l'action. Leur objectif est très précis.

Une fois l'e-mail dans votre boîte de réception, l'attaquant espère que vous allez cliquer sur un lien ou ouvrir la pièce jointe afin de faciliter l'activité prévue :

- **Programme malveillant** : terme général utilisé pour différents types de logiciels malveillants :
    - **Virus** : s'auto-propage et se répand par l'intermédiaire d'un hôte. Il peut s'attacher à un programme ou un fichier légitime et s'activer lors de la prochaine exécution du programme.
    - **Ver** : s'auto-propage et se répand de lui-même par l'intermédiaire de connexions réseau. Il peut par exemple se cacher dans une pièce jointe et s'envoyer par e-mail à tous les contacts de votre carnet d'adresses.
    - **Cheval de Troie** : ne se propage pas. Il se déguise en programme légitime utile (un économiseur d'écran par exemple) en provoquant des dégâts en arrière-plan.

Une **porte dérobée** peut être créée (un accès secret à l'ordinateur destiné à un usage ultérieur), les données peuvent être corrompues et un **logiciel espion** (permettant de suivre vos activités et d'accéder à vos informations personnelles) ou un **ransomware** peuvent être installés (afin de verrouiller vos données et demander une rançon pour pouvoir les récupérer).

Les e-mails d'hameçonnage ne sont PAS faciles à identifier.

- Ils semblent provenir d'une personne que vous connaissez.
- L'adresse e-mail de l'expéditeur peut être strictement identique à celle d'une personne que vous connaissez.
- Ils peuvent imiter les logos et le style des e-mails d'organisations bien connues.
- Ils peuvent faire référence à des « gros titres » ou à un travail que vous venez d'accomplir.
- L'attaquant peut avoir appelé votre entreprise ou effectué des recherches sur Internet pour personnaliser l'e-mail et le rendre plus légitime.

L'attaquant utilisera toutes les méthodes possibles pour que son e-mail paraisse authentique et attirant : ses compétences en la matière sont excellentes.

Les conséquences pour les particuliers et les entreprises sont graves. De nombreuses études montrent que les risques sont élevés pour les petites entreprises. À un moment donné, plus de 60 % des petites entreprises ont de grandes chances d'avoir subi une cyberattaque au cours de l'année précédente, l'e-mail étant le principal initiateur (ou vecteur d'attaque) utilisé.

Logiciel antivirus (AV) :

Ce logiciel aide à se protéger contre l'infection. Il vérifie les caractéristiques associées aux virus connus (également appelées « signatures »), puis bloque le virus une fois identifié et nettoie le fichier. De nouvelles souches de virus sont continuellement développées par les attaquants pour essayer de contourner les logiciels AV. Lorsque de nouveaux virus sont libérés, la procédure d'identification des caractéristiques et de blocage des virus prend un certain temps. Les attaques qui utilisent de nouveaux virus pour lesquels aucune solution n'a encore été trouvée sont connues sous le nom d'attaques « zero-day ».

Les logiciels antivirus peuvent également surveiller les comportements inhabituels des opérateurs (également appelés « heuristiques »). L'AV apprend vos schémas comportementaux et devient suspicieux si quelque chose d'inhabituel se produit (une connexion à un système à une heure inhabituelle par exemple).

Il est important de maintenir les logiciels antivirus à jour. De nouveaux virus sont constamment en cours de développement.

- *Veillez à installer des logiciels antivirus en temps réel sur tous vos ordinateurs et appareils mobiles.*
- *Réalisez une analyse périodique et régulière de tous vos systèmes.*

Filtrage des noms de domaine (filtrage DNS)

Des conditions s'appliquent lors de la configuration de nouveaux sites web afin de garantir qu'ils sont utilisés à des fins légitimes. Les criminels n'en tiennent pas compte et il est difficile d'identifier leur véritable intention tant qu'un site web n'est pas opérationnel.

- On estime que sur les 200 000 nouveaux domaines enregistrés quotidiennement dans le monde, jusqu'à 70 % peuvent être destinés à des activités malveillantes.
    - https://unit42.paloaltonetworks.com/newly-registered-domains-malicious-abuse-by-bad-actors/

De nombreuses sociétés spécialisées en cybersécurité surveillent l'utilisation des sites web parallèlement à d'autres informations afin d'identifier ceux dont le fonctionnement est suspect. Des renseignements sur les menaces sont ainsi générés. Une fois analysés, ils sont utilisés pour confirmer l'intention malveillante. Le filtrage des noms de domaine utilise ces renseignements (issus de plusieurs sources) pour bloquer l'accès à des sites web malveillants, permettant ainsi de prévenir le préjudice.

- **Quad9** est un service de filtrage DNS développé par la Global Cyber Alliance en partenariat avec IBM et Packet Clearing House. Il dispose de 19 flux de renseignements sur les menaces différents et bloque l'accès aux sites web malveillants connus en quasi temps réel. Pour ce faire, il refuse de convertir et d'acheminer le trafic vers l'adresse IP associée au nom de domaine du site web saisi dans le navigateur. Il peut également bloquer les adresses IP auxquelles vos appareils IdO ou vos ordinateurs se connectent automatiquement (à votre insu).

Le filtrage des noms de domaine ne peut bloquer un site web qu'après avoir identifié un seuil d'activité malveillante.

DNS : système de noms de domaine

- Le système de noms de domaine (DNS) est l'équivalent d'un annuaire téléphonique sur Internet.
- Un nom ou un domaine de site web unique, dans un format texte compréhensible (c.-à-d., globalcyberalliance.org), est converti par les serveurs de noms de domaine en un ensemble unique de nombres (l'adresse IP, 192.124.249.5) compréhensible par les ordinateurs.
- De nouveaux sites web et domaines sont constamment créés et enregistrés par les registraires de noms de domaine qui attribuent et consignent l'adresse IP correspondante (GoDaddy est un exemple de registraire de noms de domaine).

Les registraires doivent vérifier que chaque nom de domaine et chaque adresse IP d'un site web sont uniques. Un grand nombre de fraudeurs tentent d'utiliser des noms de domaine de site web ressemblants pour faire croire aux victimes qu'elles se connectent à un site légitime. Bien que ces sites peuvent ressembler au vrai nom d'un site web, une analyse plus approfondie peut révéler des différences (par exemple, « rn » peut être utilisé à la place de « m » dans l'adresse du site web).

Bloqueurs de publicités

Bien que certaines publicités ou messages qui apparaissent lorsque vous naviguez sur Internet sont utiles, la plupart ne le sont pas et contiennent du code malveillant. Un bloqueur de publicités peut être utilisé pour empêcher les publicités d'apparaître sur les pages web que vous consultez. Ils offrent une ligne de défense supplémentaire contre les attaques.

Utilisez les outils de la boîte à outils « Prévenir l'hameçonnage et les logiciels malveillants » pour vous protéger contre ces risques.

https://gcatoolkit.org/fr/petites-entreprises/prevenir-lhameconnage-et-les-logiciels-malveillants/