Protéger votre organisation contre le piratage psychologique

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Octobre 2023 | ITSAP.00.166

Les attaques par piratage psychologique se produisent lorsque des auteures/auteurs de menace se servent d'un lien social et de manipulation pour pousser ou inciter des utilisatrices et utilisateurs à divulguer quelque chose qui va à l'encontre des intérêts d'une organisation (comme le fait de fournir des détails sensibles, des mots de passe ou de l'information financière). Les auteures et auteurs de menace peuvent se faire passer pour une personne, une organisation reconnue ou un fournisseur, ou même une employée ou employé du gouvernement. Ces personnes peuvent tenter d'influencer les utilisatrices et utilisateurs pour les contraindre de faire quelque chose qui leur permettra d'accéder à leur environnement, comme changer le mot de passe d'un compte. Munis de ces renseignements, les auteures et auteurs de menace sont en mesure de voler les renseignements commerciaux et financiers de votre organisation, d'accéder aux comptes d'utilisateur et éventuellement de déployer un maliciel. N'importe qui peut faire l'objet d'une attaque par piratage psychologique, d'une employée individuelle ou d'un employé individuel jusqu'au chef de direction de votre organisation. Il est primordial de savoir reconnaître les attaques par piratage psychologique et d'assurer la protection du personnel contre celles-ci. Vous serez ainsi en mesure de protéger le réseau, les systèmes et les données de votre organisation.

Comment fonctionne le piratage psychologique?

Les attaques par piratage psychologique sont aussi appelées « piratage humain » puisque les auteures et auteurs de menace mettent à profit les renseignements qu'ils trouvent sur Internet et les plateformes de médias sociaux pour cibler des individus et des organisations. Ils utilisent ces renseignements comme moyen pour tromper les utilisatrices et utilisateurs et les inciter à divulguer des renseignements concernant leurs comptes, les mots de passe et même l'accès aux systèmes de votre organisation. Ces auteures/auteurs de menace utilisent des techniques psychologiques pour susciter des réactions émotives et ainsi exercer suffisamment de pressions pour qu'une personne exécute une tâche, ou ils utilisent des titres accrocheurs pour inciter une personne à cliquer sur des liens malveillants.

Exemples d'attaques par piratage psychologique

- **L'hameçonnage** est une tactique qu'utilisent les auteures et auteurs de menace et qui consiste à envoyer à un grand nombre de destinataires un courriel semblant provenir d'une source de confiance. Le courriel peut inviter les destinataires à fournir de l'information sensible, à exécuter une action (comme changer un mot de passe personnel ou réseau) ou à cliquer sur un lien qui semble légitime, mais qui est en réalité malveillant. Pour en savoir plus, consultez Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)
- **Le harponnage** est une attaque par hameçonnage ciblant un groupe d'individus donné ou une seule personne. Les courriels envoyés lors d'une telle attaque sont personnalisés pour paraître encore plus vraisemblables et pour donner à la source une apparence légitime.
- **La chasse à la baleine** est un type de harponnage qui cible une cadre supérieure ou un cadre supérieur comme un PDG ou un DPF.
- **L'hameçonnage par message texte** est une attaque déclenchée par le biais de service d'envoi de messages courts (SMS) ou de textos.
- **L'hameçonnage par code QR** se produit lorsqu'une attaque par hameçonnage implique la lecture d'un code QR qui dirige une personne vers un site Web malveillant une fois ce code scanné. Pour en savoir plus, consultez Facteurs relatifs à la sécurité à considérer pour les codes QR (ITSAP.00.141)
- **L'hameçonnage vocal** est une attaque par hameçonnage exécutée par le biais d'un message vocal ou d'un appel vocal envoyé à un téléphone filaire, à un téléphone cellulaire ou à une voix sur IP. Les auteures et auteurs de menace peuvent utiliser un numéro de téléphone trafiqué ou modifier leur voix pour masquer leur identité. Ils peuvent également avoir recours à l'intelligence artificielle (IA) pour se déguiser ou imiter une personne que vous connaissez. Pour en savoir plus, consultez Qu'est-ce que l'hameçonnage vocal? (ITSAP.00.102)
- **L'appâtage** est une attaque par piratage psychologique à partir de laquelle une auteure ou un auteur de menace tente de convaincre une personne de faire quelque chose (comme cliquer sur un lien malveillant) en faisant miroiter à cette personne une offre attrayante comme un prix.
- **L'arnaque de contrepartie** est considérée comme une attaque par piratage psychologique au cours de laquelle une victime se fait convaincre de divulguer de l'information sensible à son sujet ou au sujet de son organisation, ou exécute une tâche (comme cliquer sur un lien) en échange d'une promesse de service.
- **Les pièges sentimentaux** se produisent dans le cadre des attaques par piratage psychologique lorsqu'une auteure ou un auteur de menace entraîne une personne dans une fausse relation amoureuse en ligne pour obtenir de l'argent de sa victime ou lui soutirer de l'information sensible.
- **Un alarmiciel** est une forme d'attaque par piratage psychologique qui survient lorsqu'une auteure ou un auteur de menace arrive à convaincre une personne que son ordinateur ou réseau est à risque et l'incite à poser certains gestes (comme cliquer sur un lien malveillant).

Attention aux communications non sollicitées qui comportent :

- des pièces jointes,
- des liens cachés;
- des sites Web mystifiés;
- des codes QR malveillants;
- des pages de connexion;
- des demandes urgentes;
- un langage menaçant ou démontrant un sentiment d'urgence;
- des demandes de renseignements personnels ou d'information sensible;
- des appelants qui prétendent être des représentantes/représentants du gouvernement ou d'une institution bancaire.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Cycle de vie du piratage psychologique

Les pirates suivent habituellement un modèle similaire lors du déploiement d'attaques par piratage psychologique. Connaître et comprendre les actions que pose l'auteure ou l'auteur de menace dans le cadre de ce modèle peut vous aider à éduquer votre personnel et à protéger votre organisation.

Le schéma ci-dessous montre les phases de l'attaque par piratage psychologique et les principaux gestes que peuvent poser les pirates à chaque phase.

1.L'appât

Les auteures et auteurs de menace font des recherches sur votre organisation et son personnel; ils les ciblent ensuite par le biais d'une attaque qui semble provenir d'une source fiable. Les auteures et auteurs de menace peuvent tirer profit de l'information affichée sur les sites des médias sociaux, comme Facebook ou TikTok, pour accroître leurs connaissances de la cible. Ces connaissances les font paraître plus crédibles et fiables.

2.L'hameçon

En faisant appel à un lien social, à la sympathie, à un sentiment d'urgence, à des menaces ou à un ton désarmant, une auteure ou un auteur de menace s'assure que sa victime morde à l'hameçon. La victime croit que le scénario ou la demande présentés sont réels et que l'auteure ou l'auteur de menace est authentique.

3.L'attaque

Les utilisatrices et utilisateurs sont amenés par la ruse à donner de l'information sensible à leur sujet ou au sujet de l'organisation en cliquant sur un lien malveillant, en changeant des mots de passe qui donnent accès à l'auteure/auteur de menace aux comptes et aux réseaux, ou en ouvrant une pièce jointe malveillante. Ceci donne ainsi au pirate la clé dont il a besoin pour déverrouiller et voler votre information.

4.La fuite

Dès que l'auteure ou l'auteur de menace réussit à convaincre sa victime d'exécuter la tâche demandée, ou lorsqu'il obtient l'information dont il a besoin, il disparaît. Il peut aussi avoir recours à des tactiques alarmistes pour réduire au silence sa victime.

Que pouvez-vous faire pour protéger votre organisation?

Les attaques par piratage psychologique peuvent nuire à votre organisation et perturber vos activités si votre environnement de TI est compromis. La liste suivante de mesures peut aider à protéger votre organisation :

- Utilisez l'authentification multifactorielle. Pour en savoir plus, consultez Étapes à suivre pour déployer efficacement l'authentification multifacteur (AMF) (ITSAP.00.105)
- Formez le personnel pour qu'il sache quoi faire s'il soupçonne une attaque par piratage psychologique. Pour en savoir plus, consultez Offrir aux employés une formation sur mesure en cybersécurité (ITSAP.10.093)
- Communiquez directement avec l'expéditeur pour s'assurer de la légitimité des messages non sollicités. Règle générale, les institutions financières et les organismes gouvernementaux ne communiquent jamais par téléphone, message texte ou courriel pour demander à une personne de modifier de l'information sensible ou de la divulguer.
- Vérifiez les liens avant de cliquer sur ceux-ci en passant le curseur sur le lien pour voir l'expéditeur ou les détails sur le site Web.
- Signalez sans délai à l'équipe des TI ou de gestion toute situation laissant croire à une attaque.
- Limitez les renseignements que vous affichez dans les comptes de médias sociaux personnels et professionnels. Pour en savoir plus, consultez Utilisation de comptes personnels de médias sociaux au travail (ITSAP.00.066)
- Filtrez les pourriels et enlevez les macros intégrées. Pour en savoir plus, consultez Reconnaître les courriels malveillants (ITSAP.00.100) et Protection d'un organisme contre les macros malveillantes (ITSAP.00.200)
- Pour mettre en œuvre les listes d'applications, consultez Liste d'applications autorisées (ITSAP.10.095) ou pour bloquer les adresses IP, les noms de domaine et les types de fichiers reconnus pour être malveillants, consultez Système d'adressage par domaine de protection (ITSAP.40.019)
- Installez des outils de sécurité comme un antivirus, un antimaliciel et un logiciel anti-hameçonnage, ainsi que des pare-feu provenant de fournisseurs de confiance. Pour en savoir plus, consultez Les outils de sécurité préventive (ITSAP.00.058)
- Activez des mises à jour et des correctifs automatiques pour les outils de sécurité et les systèmes d'exploitation de vos dispositifs. Pour en savoir plus Information, consultez Application des mises à jour sur les dispositifs (ITSAP.10.096)
- Élaborez et mettez en œuvre un plan d'intervention en cas d'incident qui couvre les cyberincidents, dont les attaques par piratage psychologique. Pour en savoir plus, consultez Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003)
- Sauvegardez les renseignements hors ligne pour vous assurer que votre sauvegarde est déconnectée de vos systèmes et du réseau. Pour en savoir plus, consultez Sauvegarder et récupérer vos données (ITSAP.40.002).

Centre de la sécurité des télécommunications
Communications Security Establishment

 No de cat.D97-1/00-166-2023F-PDF ISBN 978-0-660-68095-8

Canada