RAPPORT : PRÈS DE 100 % DES ATTAQUES PAR COURRIELS SONT DUES AUX UTILISATEURS FINAUX QUI CLIQUENT SUR DES LIENS

Devolutions

LES UTILISATEURS FINAUX SONT DE LOIN LE MAILLON LE PLUS FAIBLE DE LA CHAÎNE DE SÉCURITÉ

Un nouveau rapport de la société de cybersécurité Proofpoint fait écho à ce que les professionnels des TI et de la sécurité de l'information disent depuis des années : les utilisateurs finaux sont de loin le maillon le plus faible de la chaîne de sécurité.

À quel point la situation est-elle devenue alarmante? Selon le rapport, plus de 99 % des attaques par courriels sont déclenchées par des utilisateurs finaux qui cliquent sur des liens malveillants, ouvrent des documents, acceptent des avertissements de sécurité et adoptent d'autres comportements non sécuritaires. Les attaques restantes – qui représentent une infime partie des attaques – utilisent des kits d'exploitation (EX) et des vulnérabilités logicielles pour attaquer des systèmes. Voici d'autres informations clés tirées du rapport :

Méthodes d'hameçonnage

Les 10 méthodes les plus courantes (alias les leurres) utilisées par les pirates informatiques pour mener leurs attaques sont les suivantes :

1. Récolte d'identifiants de courriel
2. Hameçonnage de compte Office 365
3. Hameçonnage par institution financière
4. Hameçonnage par Microsoft OWA
5. Hameçonnage par OneDrive
6. Hameçonnage par American Express
7. Hameçonnage générique Chalbhai (les détails à ce sujet ci-dessous)
8. Hameçonnage de compte Adobe
9. Hameçonnage par DocuSign
10. Hameçonnage par Netflix

Le kit d'hameçonnage Chalbhai

Pour ceux qui ne connaissent pas Chalbhai, cette menace implique l'envoi de courriels incitant les utilisateurs finaux à consulter divers sites web courants comme Bank of America, OneDrive, Outlook, Wells Fargo, LinkedIn, Comcast, Yahoo, Chase, etc., puis à entrer leurs informations d'identification. Une fois que c'est fait, les pirates informatiques drainent des fonds et ont un accès direct à leurs services d'infrastructure. L'hameçonnage Chalbhai fait référence à des campagnes associées à des modèles créés et vendus par un groupe appelé Chalbhai selon les artefacts contenus dans les modèles.

Objet des courriels

Comment les pirates informatiques incitent-ils les victimes à prêter attention aux faux messages plutôt qu'à les détruire? Voici les 10 catégories d'objet les plus courantes dans le courriel des imposteurs :

1. Autre
2. Paiement
3. Demande
4. Urgent
5. Salutations
6. Où es-tu?
7. W2
8. PVI
9. Cadeau
10. Document

Industries ciblées

Bien que tous les secteurs des entreprises soient sur l'écran radar des hackers, ils sont particulièrement intéressés par ceux-ci :

1. Finances
2. Manufacturier
3. Technologie (pas les TI)
4. Santé
5. Commerce de détail
6. Construction
7. Automobile
8. TI

9. Industriel
10. Éducation

Les personnes ciblées

Le rapport met également en évidence les VAPs - pour « Very Attacked People » en anglais - qui sont des utilisateurs finaux qui représentent un risque élevé dans leurs organisations respectives. Ces utilisateurs ont souvent des identités facilement reconnaissables via des sites web d'entreprise, des réseaux sociaux, des sites web gouvernementaux ou éducatifs, des médias, des recherches sur Google, des fuites sur le web, des données piratées, etc. Cependant, les VAPs ne sont pas nécessairement des utilisateurs finaux de haut niveau, comme les cadres ou les dirigeants. Les pirates ciblent les employés à tous les niveaux, y compris le personnel aux postes d'entrée ou d'échelon intermédiaire.

Les bonnes pratiques pour limiter l'impact du facteur humain

Bien sûr, ce ne sont pas tous les utilisateurs finaux qui sont négligents, même parmi ceux qui cliquent sur des liens inappropriés, ouvrent des documents inconnus ou acceptent des avertissements de sécurité. Comme mentionné dans notre sondage de septembre, il est de plus en plus difficile de repérer les faux courriels et les faux sites web. Certains sont très authentiques, avec seulement de légères différences entre le vrai et le faux. De plus, ces écarts ne sont souvent révélés que lorsque vous survolez un lien ou que vous contactez directement l'expéditeur pour en confirmer l'authenticité.

Pour minimiser les erreurs humaines et le risque de piratage, Proofpoint conseille aux entreprises de mettre en œuvre les bonnes pratiques suivantes :

- Adoptez une posture de sécurité centrée sur l'individu qui permet de savoir qui sont les personnes attaquées, la manière dont elles ont été attaquées et si elles ont cliqué sur un lien ou une pièce jointe.
- Faites des simulations d'attaques et autres méthodes pour former les utilisateurs finaux afin qu'ils puissent identifier les courriels malveillants ou potentiellement malveillants, puis pour signaler rapidement et de manière appropriée les préoccupations de l'utilisateur final.
- Déployez une technologie qui détecte et contient les menaces entrantes avant qu'elles n'atteignent la boîte de réception d'un utilisateur final; isole les URL non vérifiées ou suspectes dans les courriels; bloque les menaces qui utilisent le domaine d'une organisation pour cibler ses clients; et offre de solides capacités de défense contre la fraude par courriel.

- Déployez un outil de sécurité des médias sociaux qui analyse tous les comptes et réseaux sociaux et identifie les activités frauduleuses.
- Travaillez avec un fournisseur de renseignements sur les menaces qui combinent des techniques dynamiques et statiques pour trouver de nouveaux outils, cibles et tactiques d'attaque, et qui apprend de ce processus pour devenir toujours plus intelligent et plus fort.

En plus des bonnes pratiques ci-dessus, nous vous recommandons d'implanter une solution de gestion de mots de passe comme Devolutions Password Server, qui applique une gestion robuste et conforme des accès privilégiés (PAM) et prend en charge le stockage et le partage de données sensibles.

Nous suggérons également d'utiliser une solution infonuagique comme Devolutions Password Hub pour les utilisateurs professionnels non techniques. Plusieurs de ces utilisateurs sont qualifiés de « personnes très attaquées » (VAPs) et constituent donc une cible intéressante pour les pirates qui cherchent à faire intrusion dans un point d'extrémité et à infecter des réseaux.

Conseils de notre Chef de la sécurité, Martin Lemay

« Je suis surpris que le rapport ne mentionne pas l'authentification multi-facteur (AMF) comme technique d'atténuation de l'hameçonnage. Si vous êtes victime d'une intrusion, vous devez tenir compte du fait que les informations d'identification peuvent avoir été compromises par les pirates. Vos utilisateurs risquent de ne pas avertir votre service informatique ou de sécurité lorsque cela se produit, car ils pourraient même ne pas être en mesure d'identifier la supercherie au départ. L'AMF protégera vos comptes contre les informations d'identification volées.

Là encore, vous avez besoin de contrôles déployés au niveau des points d'extrémité pour détecter, contenir et signaler les menaces à votre équipe d'intervention. La technologie Microsoft LAPS (Local Administrator Password Solution) empêche les mouvements latéraux effectués à l'aide des informations d'identité volées si un utilisateur télécharge et exécute un programme malveillant. Les technologies de protection des points d'extrémité peuvent être utilisées pour mieux répondre à ce type de menace. Ce sont des contrôles de base qui auraient dû figurer dans les recommandations du rapport, car ils doivent être effectués bien avant de déployer un outil de sécurité des médias sociaux. Ce n'est pas une chasse aux sorcières : présumez qu'il y aura des violations de sécurité et protégez votre environnement en conséquence. »