beazley

Aperçu de l'industrie

La menace du phishing : ce que les organisations doivent savoir

Les attaques de phishing constituent depuis longtemps un défi de cybersécurité pour les organisations ; aujourd'hui, ils sont responsables de plus de 80 % des incidents de sécurité signalés. Selon le rapport 2021 de CISCO sur les tendances des menaces à la cybersécurité, environ 90 % des violations de données sont dues au phishing. Le spear phishing, qui consiste à envoyer des e-mails qui semblent provenir d'un expéditeur de confiance afin d'inciter les cibles à révéler des informations confidentielles, est le type d'attaque de phishing le plus courant, représentant 65 % de toutes les attaques de phishing.

L'une des raisons de la prolifération de ces attaques est peut-être que les campagnes de phishing sont relativement faciles et peu coûteuses à mener en raison de l'automatisation (par exemple, en utilisant la plate-forme de phishing "Caffeine"). Aujourd'hui, phishing peut nécessiter des efforts manuels, mais devient plus facile avec l'abondance de données personnelles qui sont disponibles publiquement. À l’avenir, nous pouvons nous attendre à voir des campagnes de spear phishing automatisées et personnalisées pilotées par l'IA (intelligence artificielle).

L'impact d'une attaque de phishing réussie peut aller de la récupération d'informations privées au déploiement de logiciels malveillants et à l'obtention d'un accès à distance. Comme aucun de ces résultats n'est une intrusion bienvenue, les organisations sont bien avisées d'apprendre à se protéger contre une attaque de phishing. Plusieurs techniques doivent être envisagées.

Réduisez le nombre d'e-mails de phishing auxquels vous êtes exposé

Les organisations doivent sécuriser la configuration de leur solution de messagerie (SPF, DKIM, DMARC et SID) dans le but de bloquer les e-mails reçus de sources inconnues ou suspectes. En outre, il est conseillé de mettre en œuvre une solution de protection contre les menaces de messagerie avec des fonctionnalités telles que le filtrage

du spam, l'analyse des liens, le sandboxing des pièces jointes et le blocage des types de pièces jointes malveillantes courantes (HTA, docm, xlsm, exe, PS1, VBS, js, etc.).

Apprenez à mieux reconnaître les e-mails de phishing

Apprenez et formez vos employés à détecter les domaines usurpés de sites Web et d'adresses e-mail grâce à une sensibilisation à la sécurité et à une formation anti-phishing (ex. services offerts par KnowBe4 et CybeReady). L'usurpation de domaine est une situation dans laquelle un pirate crée un faux site Web ou un faux domaine de messagerie pour se faire passer pour une entreprise ou un individu de confiance. Typiquement, le domaine semble être légitime à première vue, et les différences peuvent être très subtiles et difficiles à repérer (un W qui est en fait deux V, un R et un N minuscules imitant un M, ou un L minuscule qui est en fait un i majuscule).

Un exemple de nom de domaine usurpé est O365.rnicrosoft.fr. Remarquez le « rn » au lieu de « m ». Un autre nom de domaine susceptible de tromper les employés est https://beazley.changepassword.com. Il s'agit d'un sous-domaine qui appartient à changepassword.com et non à Beazley.com. En revanche, https://subscribe.beazley.com est un nom de sous-domaine qui appartient à Beazley.com. Cela peut être contre-intuitif, car nous sommes habitués à lire les phrases de gauche à droite, mais les sites Web et les noms de domaine doivent être lus de droite à gauche.

Les cibles peuvent être amenées à révéler des informations sensibles, à envoyer leur mot de passe (et éventuellement un jeton MFA), à envoyer de l'argent ou à cliquer sur des liens malveillants sans se rendre compte qu'elles interagissent avec une entité inconnue et/ou téléchargent un fichier malveillant.

En plus de sensibiliser les employés à cette menace, l'ajout de l'en-tête « [External] » pour les e-mails reçus d'adresses e-mail externes peut aider à rappeler aux employés d'être plus vigilants face aux adresses e-mail potentiellement usurpées.

Limiter l'impact d'une attaque de phishing

Les e-mails de phishing sont principalement utilisés à deux fins principales. Ils peuvent être employés pour rediriger les utilisateurs vers des sites Web usurpés et voler leurs mots de passe. Alternativement, ils peuvent être utilisés comme moyen de déployer et d'exécuter du code ou des logiciels malveillants sur les postes de travail des utilisateurs. Dans ce cas, le logiciel malveillant est soit attaché à l'e-mail lui-même, soit téléchargé à partir d'un lien ouvert par l'utilisateur ou par une macro intégrée dans un document Word, Excel ou PowerPoint en pièce jointe.

Il y a plusieurs choses qu'une organisation peut faire pour limiter

l'impact d'un utilisateur cliquant sur un lien malveillant ou double-cliquant sur un fichier malveillant. La première étape consiste à disposer d'un logiciel antivirus à jour et à restreindre l'exécution des fichiers téléchargés reconnus comme des logiciels malveillants. Vous pouvez également bloquer les macros qui tentent d'exécuter des commandes sur le système ou d'ouvrir des liens externes. Enfin, le déploiement d'un agent EDR avec la correction automatique activée sur les postes de travail peut aider à détecter et à bloquer l'exécution de nouveaux contenus malveillants (jusqu'alors inconnus).

Mettez en œuvre un renforcement de la sécurité et des restrictions sur les terminaux des utilisateurs, tels que AppLock, pour vous assurer qu'il n'y a pas d'exécution de scripts ou de logiciels non signés, et qu'aucun périphérique USB ne peut être utilisé (par exemple, alignement sur les recommandations de référence CIS). Empêchez l'accès au processus "Lsass" qui stocke les mots de passe des utilisateurs localement sur les terminaux en appliquant la protection des informations d'identification, en réduisant le nombre d'informations d'identification mises en cache localement à 1 et en exécutant Lsass en tant que PPL.

Enfin, créez des procédures et formez votre équipe de sécurité informatique pour mieux répondre aux attaques de phishing réussies.

S'isoler complètement d'Internet serait la solution la plus sûre, mais elle n’est pas une option. Avec un peu de prévoyance, une organisation peut se prémunir contre les attaques de phishing en assumant de manière proactive la responsabilité de la sécurité de ses opérations et des données de ses utilisateurs. Comme les techniques et les protocoles de prévention changent fréquemment, une formation continue et une réévaluation fréquente des procédures de sécurité peuvent souvent être les meilleures défenses d'une organisation.

Jad Nehmé est responsable des cyberservices au sein de l'équipe des cyberservices de Beazley - internationale. Il est basé en France et accompagne les clients de Beazley lors d'un incident de cybersécurité ou d'une violation de données. Il assiste également les clients dans la gestion des risques de confidentialité et de cybersécurité ainsi que dans les contrôles préventifs. Avant de rejoindre Beazley, Jad a occupé des postes chez Alcatel-Lucent et KPMG couvrant à la fois les aspects techniques et organisationnels de la cybersécurité.
Les opinions exprimées ici sont celles de l'auteur.

beazley