proofpoint.

FICHE MENACE

Attaques de la chaîne logistique

En bref

DESCRIPTION

Les attaques de la chaîne logistique relèvent de deux catégories : la fraude par email et les logiciels tiers. Lors de ces attaques, les cybercriminels compromettent les comptes de messagerie de fournisseurs ou de prestataires de services dans le but d'attaquer leurs clients et leurs partenaires. La compromission initiale s'effectue souvent par le biais d'une attaque de phishing ou d'un malware. Une fois introduit dans le système du fournisseur, le cyberattaquant peut usurper des comptes de messagerie pour lancer une attaque de phishing, une fraude aux factures ou d'autres types d'attaque à l'encontre des clients. Dès lors que le cyberattaquant parvient à infiltrer les systèmes de clients, il peut voler des données confidentielles, installer un ransomware ou utiliser l'accès ainsi obtenu pour déclencher ultérieurement une vague d'attaques de phishing ou de fraude par email.

ARSENAL

Les attaques de la chaîne logistique recourent généralement au phishing à des fins de vol d'identifiants de connexion (prise de contrôle de comptes), à des malwares (Stuxnet, NotPetya, Sunburst, Kwampirs) et à des menaces d'imposteurs, telles que le piratage de la messagerie en entreprise (BEC, Business Email Compromise).

TYPES

- **Piratage de la messagerie en entreprise (BEC, ou fraude par email).** Le cyberattaquant se fait passer pour une personne en qui le destinataire a confiance – généralement un partenaire commercial, un fournisseur ou un revendeur. Le destinataire est invité à transférer des fonds, à régler une facture factice ou modifiée, à détourner des salaires ou à modifier des informations bancaires en vue de l'exécution ultérieure de paiements. Dans certaines campagnes de fraude par email, le cyberattaquant peut compromettre le compte de messagerie réel du fournisseur pour usurper son identité et même exploiter des conversations email existantes.
- **Attaques logicielles de la chaîne logistique.** Le cyberattaquant obtient un accès aux systèmes d'un éditeur de logiciels ou d'un fournisseur de services managés et infecte les nouvelles builds qui sont ensuite distribuées aux clients et partenaires. Ces attaques sont plus rares que les attaques décrites ci-dessus, mais une seule compromission peut faire de nombreuses victimes.

FACTEURS DE RISQUE

- Recours à des fournisseurs pour des services professionnels et des consultations
- Utilisation d'une solution de cybersécurité inadéquate
- Octroi d'un accès à des collaborateurs négligents ou non sensibilisés à la sécurité informatique
- Complexité de la chaîne logistique – les entreprises s'appuient de plus en plus sur un éventail de services SaaS et de plates-formes cloud

Les attaques de la chaîne logistique dans l'actualité

En 2013, Target a dû verser une rançon de 18,5 millions de dollars à la suite d'une compromission de données ayant affecté 41 millions de clients

Grâce aux identifiants de compte volés à un des fournisseurs de Target, des cyberattaquants ont réussi à infiltrer les système sde ce géant de la vente au détail et à dérober les informations financières sensibles de plus de 41 millions de clients.

Des hackers s'attaquent à la chaîne d'approvisionnement en vaccins contre la COVID-19

Une attaque de phishing a ciblé les cadres de 44 entreprises sur plusieurs continents dans une tentative pour compromettre la chaîne d'approvisionnement mondiale en vaccins contre la COVID-19.

Une association à but non lucratif de logements communautaires perd 1,2 million de dollars dans une attaque BEC

Des cyberattaquants ont usurpé le domaine d'un fournisseur pour voler près d'1 million de livres sterling de loyers à une association de logements communautaires près de Londres.

Anatomie d'une attaque de la chaîne logistique

1. **Infiltration**

   Les cyberattaquants utilisent diverses méthodes pour la compromission initiale :

- Attaques par force brute au moyen d'outils automatisés pour tester des paires d'identifiant et de mot de passe jusqu'à trouver une concordance

- Usurpation de l'identité d'un contact de confiance pour envoyer un email de phishing ou d'imposteur ou des liens/pièces jointes contenant un malware, tel qu'un enregistreur de frappe ou un voleur d'identifiants de connexion

- Prise de contrôle du compte d'un fournisseur de confiance

2. **Reconnaissance**

- Après avoir volé des identifiants de connexion valides, le cyberattaquant peut commencer à exploiter le réseau et à entacher la réputation du fournisseur. Il surveille les communications entre ce dernier et ses clients afin de trouver des cibles.

3. **Attaque**

- Au terme de la phase de reconnaissance, le cyberattaquant peut utiliser les systèmes compromis du fournisseur pour pirater des identifiants de connexion, envoyer des factures frauduleuses ou distribuer des malwares à des clients.

Le point sur la recherche

Sur une période d'une semaine en février 2021, Proofpoint a analysé les données de 3 000 entreprises de divers secteurs aux États-Unis, au Royaume-Uni et en Australie. La grande majorité de ces entreprises ont été victimes d'attaques de la chaîne logistique au cours de cette période.

98 % ont reçu une menace d'un fournisseur dont l'identité avait été usurpée ou le compte compromis.

Le nombre d'attaques était à peu près identique dans tous les pays et secteurs couverts par l'échantillon.

Près des trois quarts de ces menaces impliquaient une attaque de phishing ou l'usurpation d'identité.

Plus de 30 % des emails envoyés depuis des domaines de fournisseur contenaient un malware.

LA CYBERCRIMINALITÉ EN TANT QUE SERVICE A FAVORISÉ LES ATTAQUES DE LA CHAÎNE LOGISTIQUE

Le Dark Web est une place de marché bien connue de kits d'exploitation et de malwares personnalisés utilisés pour vendre des services, tels que des botnets à louer et des ransomwares. À l'instar de la plupart des fournisseurs SaaS, les cybercriminels proposent des outils et des plates-formes pour mener des attaques de la chaîne logistique et de ransomware, ainsi que d'autres activités cybercriminelles. Les cybercriminels qui ne disposent pas de compétences techniques poussées peuvent désormais lancer ce type d'attaque sans difficulté.

Comment protéger votre entreprise

Pour lutter contre les fraudes et les attaques logicielles de la chaîne logistique, voici quelques contrôles de sécurité à mettre en place.

Fraude dans la chaîne logistique

Face à la fraude aux factures fournisseurs, les entreprises doivent adopter une approche globale et multicouche, car les cyberattaquants combinent souvent usurpation d'identité et compromission de comptes fournisseur.

Les attaques BEC commencent souvent par un email envoyé par un cybercriminel se faisant passer pour une personne de confiance ou usurpant son identité après avoir compromis son compte. Dans la mesure où elles sont dépourvues de charge virale malveillante, elles sont difficiles à détecter pour les passerelles d'ancienne génération qui se fient uniquement à la réputation et à l'analyse des malwares en environnement sandbox.

Voici comment neutraliser les attaques de la chaîne logistique les plus courantes et les plus coûteuses.

Visibilité sur le risque de fraude par email de vos fournisseurs

Pour mieux comprendre, communiquer et réduire les risques, posez-vous les questions suivantes :

- Quels sont les risques d'attaques BEC auxquels nous sommes exposés ?
- Quels sont les utilisateurs les plus vulnérables ?
- Quels fournisseurs mettent en péril nos activités ?
- Que devons-nous faire pour réduire les risques ?

Vous devez identifier vos utilisateurs les plus ciblés par des menaces d'imposteurs et ceux qui sont les plus susceptibles de tomber dans le piège.

Grâce à une visibilité granulaire sur les détails des menaces BEC et à l'identification des thèmes habituellement utilisés dans ces attaques (fraude aux factures fournisseurs et détournement de salaires, par exemple), vous pourrez mieux comprendre les risques BEC et communiquer plus efficacement à ce sujet.

Détection et blocage des menaces d'imposteurs avant qu'elles n'infiltrent votre environnement

Pour bloquer les fraudes aux fournisseurs qui utilisent la messagerie, vous devez identifier toutes les tactiques en la matière, notamment l'usurpation du nom d'affichage, les domaines similaires et les fraudes sophistiquées aux factures fournisseurs. Pour ce faire, vous avez besoin d'une solution qui analyse de façon dynamique les messages pour identifier les nombreuses tactiques associées aux fraudes aux factures fournisseurs, notamment :

- Détournement d'adresses de réponse
- Utilisation d'adresses IP malveillantes
- Utilisation de domaines de fournisseurs dont l'identité a été usurpée
- Mots ou expressions couramment employés dans les fraudes aux fournisseurs

Face à la fraude aux factures fournisseurs, les entreprises doivent adopter une approche globale et multicouche, car les cyberattaquants combinent souvent usurpation d'identité et compromission de comptes fournisseur.

(La plupart des solutions de protection de la messagerie s'appuient exclusivement sur des règles statiques ou des données contextuelles limitées nécessitant une optimisation manuelle.)

Renforcement de la résilience des utilisateurs face aux attaques BEC

Les attaques BEC ciblent des utilisateurs et les incitent à se livrer à des activités malveillantes. Étant donné que ces attaques d'imposteurs ont recours à l'ingénierie sociale et à l'usurpation d'identité, vos utilisateurs constituent souvent votre dernière ligne de défense. C'est la raison pour laquelle la réduction des risques d'attaques BEC requiert à la fois des technologies et des formations.

Formez vos utilisateurs à identifier et à signaler les emails d'imposteurs suspects. Vos utilisateurs disposeront ainsi des connaissances et des compétences nécessaires pour protéger votre entreprise contre ces menaces déclenchées par des humains.

L'affichage d'avertissements en cas d'emails suspects permet d'évaluer le risque associé à chaque email. Par exemple, l'affichage d'un avertissement lorsqu'un message est envoyé par un expéditeur externe ou un domaine récemment enregistré permettra aux utilisateurs de prendre des décisions plus éclairées en cas d'email suspect.

Prévention de l'usurpation de votre marque dans le cadre de fraudes par email

Si vous vous inquiétez des risques posés par vos fournisseurs, sachez que vos propres clients peuvent avoir les mêmes inquiétudes vous concernant.

Les cybercriminels peuvent utiliser le nom et la marque de votre entreprise pour piéger vos clients et vos partenaires commerciaux. Bien qu'elle n'entraîne pas forcément de pertes financières directes pour votre entreprise, l'usurpation de marque peut porter atteinte à votre réputation, éroder la confiance de vos clients et avoir des conséquences négatives sur vos activités.

Pour prévenir l'envoi d'emails frauduleux directement depuis votre compte ou par l'intermédiaire d'un tiers désigné, utilisez le protocole DMARC d'authentification des emails.

Attaques logicielles de la chaîne logistique

Outre les attaques de la chaîne logistique les plus courantes examinées ci-avant, la généralisation des logiciels tiers ou managés fait peser un risque supplémentaire sur la chaîne logistique.

Si un fournisseur compromis propose un logiciel ou des services cloud, les cyberattaquants peuvent modifier le code source et injecter un malware dans le processus de développement et de mise à jour. Les programmes ou services infectés par la charge virale malveillante ajoutée par le cyberattaquant sont ensuite distribués aux clients et partenaires.

Les utilisateurs n'ont pas toujours la possibilité d'inspecter les programmes tiers qu'ils utilisent, de sorte qu'ils sont tributaires de la fiabilité des contrôles de sécurité mis en place par leurs fournisseurs et éditeurs de logiciels. La distribution d'un logiciel compromis à une entreprise peut exposer celle-ci à un large éventail d'attaques, du vol de données à l'infection par des ransomwares.

Ce type d'attaque est particulièrement difficile à prévenir. Les vulnérabilités logicielles non corrigées constituent l'un des principaux vecteurs de cyberattaque. La mise à niveau vers la version la plus récente du logiciel reste donc la meilleure défense, mais constitue désormais aussi un vecteur d'attaque.

En savoir plus

Compte tenu du nombre d'attaques de la chaîne logistique qui font désormais les gros titres, il est clair que les services de tiers, les fournisseurs et les sous-traitants font courir un risque de sécurité majeur aux entreprises. Une solution de sécurité centrée sur les personnes capable de détecter les nouveaux outils, cibles et tactiques peut contribuer à atténuer ce risque.

Pour découvrir comment lutter efficacement contre les attaques de la chaîne logistique, consultez le site **www.proofpoint.com/fr**.

proofpoint.

1207-002-01-01 05/22