proofpoint.

PROOFPOINT THREAT RESPONSE AUTO-PULL

MISE EN QUARANTAINE AUTOMATIQUE DES E-MAILS DANGEREUX

AVANTAGES CLÉS

- Réduisez le temps nécessaire à la mise en quarantaine et au confinement des menaces associées à la messagerie.
- Limitez les temps d'exposition aux e-mails malveillants.
- Placez en quarantaine les messages transmis aux listes de distribution ou à certains destinataires.
- Obtenez un historique auditable des mesures de riposte afin d'accélérer le retour sur investissement de l'infrastructure existante.
- Limitez la dépendance au code personnalisé.
- Recevez des notifications électroniques en cas d'évolution de l'incident ou de confirmation de mise en quarantaine.
- Facilitez l'intégration aux systèmes de gestion des incidents en définissant un contenu de notification flexible.
- Surveillez et vérifiez automatiquement le caractère risqué des messages présents dans les boîtes aux lettres surchargées.
- Restaurez les messages mis en quarantaine via la fonction 'annuler'.
- Nettoyez les groupes de messages à l'aide de fichiers CSV ou des résultats SmartSearch.

Proofpoint Threat Response™ est la première plateforme de gestion des menaces à même d'élargir l'orchestration et l'automatisation pour éliminer les e-mails malveillants qui aboutissent dans la boîte de réception des utilisateurs. Version d'entrée de gamme de la plateforme, Threat Response Auto-Pull retire les e-mails malveillants des mains de l'utilisateur et implémente une logique métier supplémentaire pour identifier et supprimer les éventuelles copies internes des messages transférés.

Dans de nombreux cas, la réaction des entreprises aux incidents est à la fois lente et laborieuse. Comme le nettoyage manuel des e-mails peut être une véritable corvée, réagir aux incidents de sécurité associés à la messagerie peut prendre des heures voire des jours. Le traitement des e-mails reçus contenant des malware, des URL dangereuses ou du phishing d'identifiants comprend de nombreuses étapes :

- Association de chaque adresse e-mail à une identité interne
- Recherche et localisation des messages malveillants désignés dans le serveur
- Suppression du message malveillant dans la boîte de réception de l'utilisateur ou dans d'autres dossiers
- Identification et mise en quarantaine des messages malveillants déjà transmis

Répéter ces mêmes procédures pour chaque incident peut prendre des heures chaque jour, et surcharger encore davantage les équipes en charge de la sécurité et de la messagerie, déjà réduites.

« PIÈGES » LIÉS AU NETTOYAGE DE LA MESSAGERIE

Généralement manuel, le nettoyage des e-mails malveillants commence par une alerte voire la réclamation d'un utilisateur se plaignant d'en avoir reçu un.

À première vue, résoudre un tel incident semble assez facile, mais supposer qu'il suffit d'examiner la boîte de réception et de supprimer le message peut vous coûter cher. Outre le fait de ne pas tenir compte du volume de messages, les maladresses associées au nettoyage vont de la simplification excessive à tous les cas complexes. Les autres éléments importants à prendre en compte sont notamment les suivants :

- Le message présent dans la boîte de réception est-il le seul exemplaire ou a-t-il été déplacé vers un autre dossier ?
- Est-il nécessaire de rechercher d'éventuelles copies de ce message dans d'autres dossiers ?
- Ce message a-t-il été transmis en interne ? Si oui, à qui et en combien d'exemplaires ?
- Existe-t-il un moyen de vérifier dans le détail toutes les actions effectuées ?

D'autres variables, également susceptibles d'affecter le nettoyage de la messagerie, ont conduit au « bricolage » et à la création de scripts développés en interne. Ces derniers présentent toutefois aussi des risques.

DANGERS ASSOCIÉS AU « BRICOLAGE » ET AU CODE PERSONNALISÉ

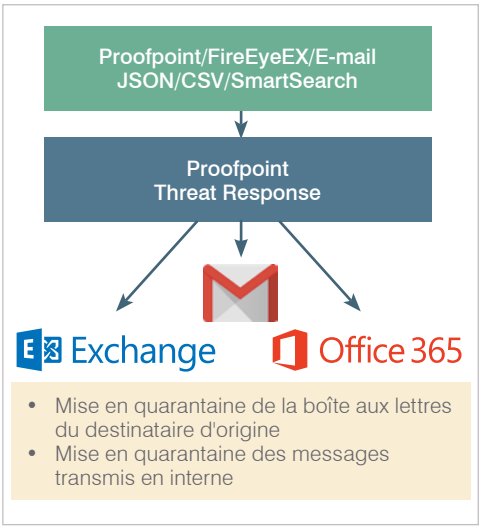
En matière de nettoyage des e-mails malveillants reçus, la création et l'exécution d'un code personnalisé permettant de nettoyer la messagerie est devenue la solution de facto.

Bien que cette méthode n'ait rien de mauvais en soi, la création et l'exécution de code personnalisé soulève toutefois des questions, notamment liées au développement logiciel :

- Ce code personnalisé nécessite-t-il des précisions ou n'exécute-t-il qu'une seule fonction, sans demander de spécifications détaillées ?
- Comment ce script est-il géré ? Est-il associé à un propriétaire à même de réagir et de corriger les éventuels problèmes ? Que se passe-t-il en l'absence de ce développeur ?
- Si le script s'applique à des produits tiers, qui supervise la version du produit, les tests, les changements d'interface ou d'API associés à ces produits tiers ?

Outre ces préoccupations techniques évidentes, l'aspect métier implique que le code personnalisé soit en accord avec la logique métier et les objectifs de visibilité. En général, ces derniers comprennent :

- Surveillance des opérations réalisées en continu par le code
- Mesure ou suivi de l'efficacité du code
- Certitude que toutes les versions malveillantes du message sont traitées, y compris celles qui ont été transmises



OPTEZ POUR THREAT RESPONSE AUTO-PULL !

Version d'entrée de gamme de Threat Response, Threat Response Auto-Pull assure la mise en quarantaine des e-mails lorsqu'il est connecté à Proofpoint Targeted Attack Protection (TAP) et à Office 365 ou Exchange sur site. La plateforme accepte également les fichiers CSV FireEye EX et les alertes SmartSearch et JSON.

La procédure est simple : en cas de détection d'un e-mail malveillant, le système envoie une alerte à Threat Response, accompagnée des informations relatives à ce message. Threat Response accède alors à Exchange, Office 365 et/ou Gmail pour placer le message en quarantaine. Auto-Pull recherche également les éventuelles copies du message déjà transmises, ainsi que les destinataires du message dans les autres boîtes aux lettres stockées dans le même serveur pour les placer en quarantaine avec accès limité.

INTÉGRATIONS MODÉLISÉES

Threat Response Auto-Pull est doté d'adaptateurs qui lui permettent de se connecter aux sources Exchange, Office 365, Gmail, CSV, SmartSearch, TAP, FireEye EX et JSON en quelques minutes. Il n'est donc pas nécessaire d'acheter d'autres systèmes ou connecteurs. Pour pouvoir récupérer les e-mails via Exchange et O365, l'administrateur a seulement besoin des identifiants appropriés. Par ailleurs, Threat Response Auto-Pull surveille aussi les boîtes aux lettres surchargées et vérifie automatiquement la réputation des messages qui y sont envoyés et les informations qui s'y rapportent.

THREAT RESPONSE AUTO-PULL OU VERSION COMPLÈTE

Bien que la version Auto-Pull soit à même de traiter les incidents de sécurité associés à la messagerie, les professionnels de la sécurité peuvent également envisager d'opter pour la version complète de Threat Response qui, grâce à ses capacités, va bien au-delà de la simple mise en quarantaine :

- Orchestration de la sécurité et automatisation de la réaction aux incidents
- Mise en contexte et ajout de renseignements accélérant le tri des incidents
- Collecte et vérification des informations obtenues via les terminaux par rapport à celles du sandbox
- Acceptation et application des renseignements donnés par des tiers à tous les incidents
- Mise en quarantaine et confinement de la menace via les pare-feu, les proxy et Active Directory
- Génération de rapports en temps réel sur les campagnes, les utilisateurs, les incidents, les menaces et les cibles

« En deux heures à peine, la solution était déjà intégrée à TAP et AD, et purgeait automatiquement les messages. »

Client anonyme, Secteur de la santé

RÉCAPITULATIF

Threat Response Auto-Pull est à même de mettre en quarantaine et d'endiguer les e-mails malveillants qui parviennent jusqu'à la boîte aux lettres, de façon automatisée et proactive, en éliminant également les messages transmis en interne. Pour gagner du temps, se montrer plus efficaces et bénéficier de capacités allant bien au-delà du simple traitement des incidents associés à la messagerie, les professionnels de la sécurité peuvent également opter pour la version complète de Threat Response.

À PROPOS DE PROOFPOINT

Proofpoint Inc. (NASDAQ:PFPT), leader spécialisé dans la cybersécurité nouvelle génération, permet aux organisations de protéger leurs données contre les menaces avancées, et de se conformer aux réglementations en vigueur. Grâce à Proofpoint, les professionnels de la cybersécurité sont en mesure d'accéder à des renseignements et outils capables de protéger les utilisateurs et leurs données contre les attaques menées par courrier électronique, sur les réseaux sociaux ou les appareils mobiles. De nombreuses entreprises de toutes tailles, dont plus de la moitié de celles figurant dans le classement Fortune 100, exploitent des solutions Proofpoint. Celles-ci sont conçues spécialement pour les environnements mobiles et de réseaux sociaux. Elles tirent parti de la puissance du cloud et d'une plateforme d'analyse pilotée par les Big Data pour lutter contre les menaces avancées modernes.