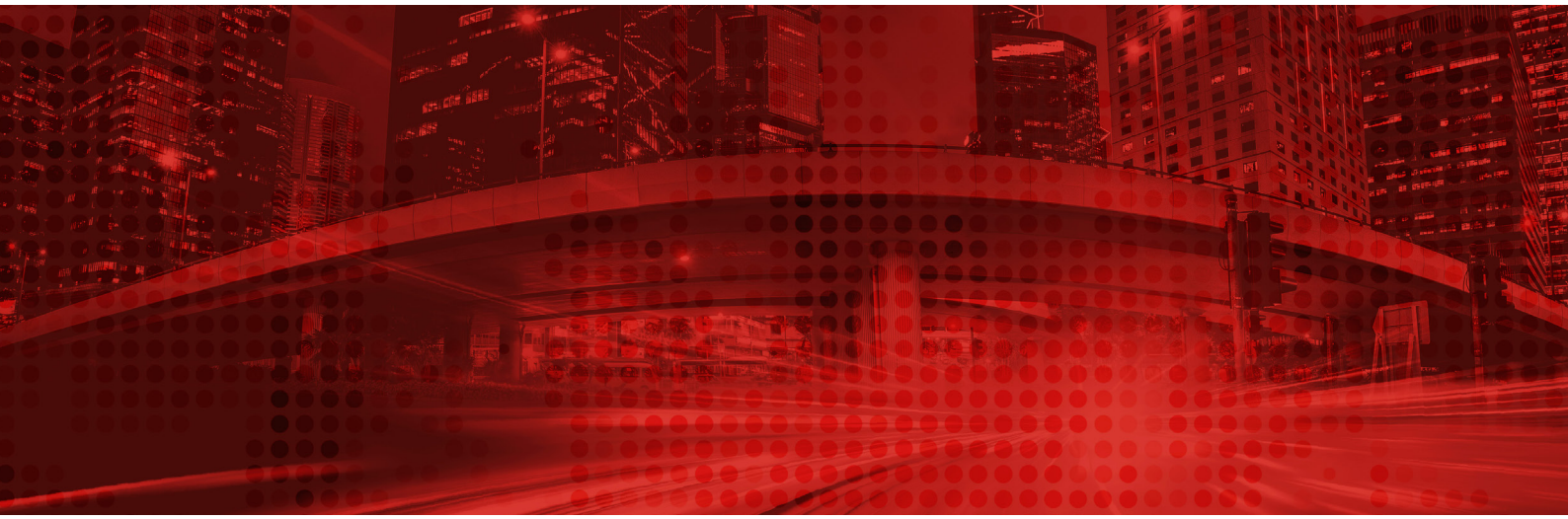
RSA® FRAUDACTION™ 360



INTRODUCTION

Le canal en ligne n'a jamais été confronté à un réseau criminel aussi novateur et intégré à l'échelle mondiale que celui auquel il fait face actuellement. Les criminels disposent des technologies les plus avancées et alimentent une économie souterraine élaborée :

- Le phishing continue de croître.
- Les chevaux de Troie sont plus évolués et plus faciles à obtenir.
- Les applications mobiles malveillantes infiltrent les boutiques d'applications publiques.
- Les médias sociaux sont parsemés de fausses pages d'entreprise.

À ce jour, le service RSA® FraudAction™ a permis les actions suivantes :

- arrêter plus de 2 millions de cyberattaques ;
- identifier plus de 1 milliard de cyberattaques dans le monde ;
- restaurer des centaines de millions d'informations d'identification compromises.

EN BREF

Protection de bout en bout contre le phishing, les chevaux de Troie, les applications mobiles malveillantes et les menaces liées aux médias sociaux, de la détection à la mise hors service

Rapports d'intelligence et flux d'informations sur les dernières menaces en ligne, y compris les nouvelles tendances en matière de fraude

Accès à des rapports d'attaque détaillés via le tableau de bord RSA FraudAction, le portail de création de rapports en ligne

Détenir une protection contre ces différents types d'attaques est essentiel, car ces dernières deviennent de plus en plus interdépendantes : les chevaux de Troie, par exemple, intègrent souvent un composant d'application mobile. Les médias sociaux sont devenus le nouveau repaire des fausses pages d'entreprise, créées par des cybercriminels pour tromper les consommateurs.

Pour jouir d'une protection complète contre la fraude, les organisations sont confrontées à plusieurs défis. Il s'agit soit de gérer plusieurs fournisseurs (avec des indicateurs pour plusieurs services, des exigences budgétaires et des relations commerciales variées car les services correspondant aux divers vecteurs de menaces sont vendus par des fournisseurs différents), soit de choisir et donner la priorité à un vecteur de menace plutôt qu'à un autre, et prendre ainsi le risque de devenir vulnérables à certains types d'attaques.

RSA FRAUDACTION 360

Pour vous protéger contre les schémas d'attaque complexes que l'on rencontre aujourd'hui, le service RSA FraudAction 360 réunit tous les vecteurs de menaces dans un service complet de gestion des menaces externes. Vous bénéficiez ainsi d'une protection totale contre les fraudes comme le phishing, les attaques par cheval de Troie, les applications malveillantes et les menaces liées aux médias sociaux. En outre, les clients peuvent accéder à des informations détaillées sur les menaces émergentes grâce aux rapports d'intelligence qui offrent de la visibilité sur les dessous de la cybercriminalité.

LIMITATION DES MENACES EXTERNES

Avec un service global, les organisations peuvent :

- déployer moins de ressources internes pour gérer les menaces externes ;
- bénéficier d'une protection complète contre la fraude sans qu'un seul vecteur de menace reste non identifié ;
- gérer un seul budget fournisseur pour les opérations antifraude 24/7.

Le service de gestion des menaces externes RSA FraudAction 360 propose les composants suivants :

- Protection contre le phishing
- Protection contre les chevaux de Troie
- Protection contre les applications mobiles malveillantes
- Protection contre les menaces liées aux médias sociaux
- Certains flux de données et rapports issus de RSA FraudAction Cyber Intelligence

PROTECTION CONTRE LE PHISHING

Le service RSA FraudAction détecte et limite les attaques par phishing. Il est conçu pour aider les organisations à faire face à une attaque lorsque celle-ci se produit, et pour effectuer une analyse approfondie après chaque attaque.

SURVEILLANCE ET DÉTECTION PRÉCOCE

RSA utilise plusieurs stratégies de détection précoce, notamment la surveillance des domaines nouvellement enregistrés et les journaux Web des clients. Les ressources de détection RSA FraudAction permettent à nos analystes de balayer des milliards d'URL par jour, y compris les boîtes aux lettres électroniques victimes de fraude des clients, et de procéder à la qualification heuristique automatisée et manuelle des URL suspectes.

ALERTES ET CRÉATION DE RAPPORTS EN TEMPS RÉEL

Une fois qu'il a été confirmé qu'une URL constitue une menace, les clients sont avertis instantanément et ont la possibilité de surveiller en temps réel les dernières informations sur cette menace et sur son état par le biais du tableau de bord RSA FraudAction. Le portail de création de rapports en ligne fournit également des échéanciers de mise hors service, ainsi que des tendances sectorielles et géographiques.

RÉSEAU EXCLUSIF DE BLOCAGE DES SITES MALVEILLANTS

RSA est devenu la première ligne de défense pour plus de 96 % du trafic Web mondial avec son flux de blocage pour les utilisateurs des principaux navigateurs Internet, y compris les navigateurs mobiles, et les clients des principaux fournisseurs de sécurité des données et des FAI. Dès qu'une attaque est identifiée, les flux d'informations sur les sites de phishing associés sont envoyés en temps quasi réel à ces organisations, ce qui leur permet de bloquer ces sites quelques minutes seulement après leur détection.

MISE HORS SERVICE DES SITES DE PHISHING

RSA tire parti des relations qu'il entretient de longue date avec plus de 16 000 hébergeurs ainsi que de ses capacités multilingues pour assurer la mise hors service rapide des sites frauduleux à l'échelle mondiale. À ce jour, RSA est responsable de la mise hors service de plus de 1 million de sites frauduleux hébergés dans plus de 187 pays.

PROTECTION CONTRE LES CHEVAUX DE TROIE

Le service RSA FraudAction détecte et limite les dommages causés par les attaques de chevaux de Troie. Ce service est conçu pour identifier les menaces émanant des logiciels malveillants, répondre à une attaque lorsqu'elle survient et minimiser les effets de la menace en bloquant l'accès par les utilisateurs finaux aux ressources en ligne de l'attaque.

RAPPORTS SUR LES MENACES RSA FRAUDACTION

Les clients RSA FraudAction 360 reçoivent des rapports issus des renseignements relatifs aux menaces, portant, par exemple, sur les tendances en matière de fraude, les nouvelles méthodologies d'escroquerie, les nouveaux outils et services de cybercriminalité proposés dans le réseau.

Les rapports sur les menaces RSA FraudAction informent les clients au sujet des nouvelles failles de sécurité détectées ou utilisées par les fraudeurs, des méthodes de retrait d'argent ou toute autre méthode utilisée par les fraudeurs dans leurs tentatives ciblant les organisations.

IDENTIFICATION ET ANALYSE

Le service RSA FraudAction s'appuie sur un réseau de partenaires afin d'atteindre un niveau élevé de détection. Ce réseau se compose d'organisations issues de différents domaines liés aux technologies, notamment les logiciels antivirus grand public, les opérations de renseignement et les passerelles Internet.

Lorsqu'un partenaire RSA FraudAction détecte un logiciel malveillant, les informations relatives au cheval de Troie sont transmises au RSA Anti-Fraud Command Center pour enquête. Les analystes experts effectuent des analyses statiques et dynamiques, qui identifient les déclencheurs, les points de communication et d'autres données, ainsi que le mode opératoire du cheval de Troie sur un système infecté. Dans la mesure du possible, les points de chute du cheval de Troie sont mis sous surveillance pour tenter de restaurer les informations d'identification de l'utilisateur final qui ont été compromises.

MISE HORS SERVICE DES SITES FRAUDULEUX

RSA fait le nécessaire pour le compte des clients pour mettre hors service les sites frauduleux connectés aux points d'infection de chaque attaque. Une fois les sites frauduleux découverts et analysés, l'AFCC RSA initie leur mise hors service par le biais d'une ordonnance de cessation et d'abstention, en collaboration avec les fournisseurs de services Internet et d'hébergement Web, ainsi qu'avec les organismes d'enregistrement de domaine.

PROTECTION CONTRE LES APPLICATIONS MOBILES MALVEILLANTES

Le service RSA FraudAction aide les organisations à réduire les pertes dues aux fraudes en prenant des mesures contre les applications mobiles malveillantes ou non autorisées. Il surveille toutes les principales boutiques d'applications, détecte les applications ciblant les bases de clients des organisations et met hors service les applications non autorisées, ce qui diminue les menaces pour la réputation des organisations et les pertes financières dues à des fraudes sur application mobile.

SURVEILLANCE ET DÉTECTION

Ce service fournit une visibilité constante sur les boutiques d'applications mobiles et offre donc une défense en ligne proactive aux organisations. Cette surveillance continue des boutiques d'applications aide les organisations à conserver une longueur d'avance sur les menaces potentielles, et leur permet d'être averties dès qu'une application non autorisée fait son apparition.

MISE HORS SERVICE DES APPLICATIONS MALVEILLANTES

Après détection et validation de la mise hors service, RSA initie la suppression de l'application malveillante. Ce service permet aux clients de contrôler les applications représentant leur organisation, en autorisant uniquement les applications délivrées et/ou autorisées par l'organisation de figurer sur les marchés d'applications. Il évite également que les clients et des centaines de millions d'utilisateurs d'applications mobiles en ligne n'accèdent à des applications de phishing, contenant des logiciels malveillants et à toute autre application non autorisée, avant même que ces applications malveillantes ne gagnent en visibilité et en popularité dans les boutiques d'applications.

RÉACTIONS DES CLIENTS

« En implémentant le service RSA FraudAction, nous avons fortement réduit le temps nécessaire pour neutraliser les attaques par phishing : il est passé de plusieurs semaines à seulement quelques heures. Nous avons également bloqué des tentatives de fraude portant sur des millions de couronnes tchèques, ce qui est très satisfaisant pour nous, mais aussi pour nos clients, ce qui est encore plus important. »

Une grande institution financière européenne

PROTECTION CONTRE LES MENACES LIÉES AUX MÉDIAS SOCIAUX

Les médias sociaux sont apparus comme une structure de communication à part entière qui réunit la marque de votre organisation et les offres de services associées à vos clients. De nouveaux fils sociaux ayant permis l'émergence de vecteurs de menaces, les cybercriminels ont entrepris de falsifier des pages de médias sociaux pour frauder ou lancer un projet de fraude. Les organisations sont confrontées à la tâche consistant à surveiller constamment les risques sur les canaux numériques, notamment les médias sociaux, car les options manuelles en interne peinent à répondre aux besoins en matière de gestion du risque.

Le service RSA FraudAction est conçu pour fournir une visibilité sur les pages des médias sociaux et aider les organisations à faire la distinction entre les pages professionnelles autorisées et celles potentiellement risquées. En surveillant les médias sociaux, RSA FraudAction identifie les pages qui sont directement liées à des activités frauduleuses ciblant votre organisation, ou qui tentent de tromper vos clients en usurpant l'identité de votre organisation et/ou filiale. RSA FraudAction permet aux organisations de prendre rapidement des mesures correctives contre les menaces de fraude liées aux médias sociaux, avant l'apparition de dommages graves et durables.

RSA FRAUDACTION CYBER INTELLIGENCE

L'opération RSA FraudAction Cyber Intelligence fournit des informations sur les tendances de la cybercriminalité et des enquêtes approfondies sur les méthodes et les opérations de fraude au sein du réseau mondial de cybercriminels.

Des flux d'information et des rapports complémentaires issus du service RSA FraudAction Cyber Intelligence de niveau 1 sont inclus dans RSA FraudAction 360 sans frais supplémentaires. Ces rapports et flux de données sur les menaces peuvent facilement s'intégrer à d'autres systèmes centraux.

PRODUITS RELATIFS AUX RENSEIGNEMENTS RSA FRAUDACTION 360 :

- **Flux IP :** liste quotidienne comprenant des adresses IP à haut risque, telles que des serveurs proxy/SOCKS et RDP
- **Flux d'e-mail :** liste quotidienne des adresses e-mail professionnelles compromises des collaborateurs et des e-mails indésirables
- **Flux de comptes mule :** composé de comptes mule restaurés par les analystes de l'intelligence RSA
- **Flux de points de chute d'articles :** composé d'adresses postales physiques de points de chute auxquelles les « mules de réexpédition » acceptent des articles achetés avec des cartes volées
- **Flux de cartes de crédit :** composé d'informations sur les cartes de crédit/de débit compromises, suivies sur le réseau de cybercriminels
- **Bulletin d'informations trimestriel :** statistiques mondiales relatives au phishing et aux chevaux de Troie, ainsi qu'une présentation des tendances signalées au cours du trimestre écoulé
- **Rapports sur les menaces :** conclusions de rapports sur les nouvelles méthodes d'attaque et les tendances du réseau de cybercriminalité

À PROPOS DE LA SUITE RSA FRAUD AND RISK INTELLIGENCE SUITE

La suite RSA® Fraud and Risk Intelligence Suite permet aux organisations de gérer le risque sur les canaux numériques destinés aux consommateurs, ce qui leur garantit de pouvoir optimiser leur chiffre d'affaires et minimiser les pertes dues aux fraudes. Cette suite, qui fait partie de la gamme RSA des solutions de sécurité orientées métiers, offre une approche unifiée de la gestion des risques numériques qui repose sur une visibilité intégrée, des informations automatisées et des actions coordonnées. RSA protège des millions d'utilisateurs dans le monde entier et aide plus de 90 % des sociétés du classement Fortune 500 à prospérer et à s'adapter en permanence au changement transformationnel. Pour plus d'informations, accédez au site rsa.com/fr-fr/.

©2020 RSA Security LLC ou ses filiales. Tous droits réservés. RSA et le logo RSA sont des marques déposées ou des marques commerciales de RSA Security LLC ou de ses filiales aux États-Unis et dans d'autres pays. Toutes les autres marques sont la propriété de leurs propriétaires respectifs. RSA estime que les informations contenues dans ce document sont exactes. Les informations peuvent faire l'objet de modifications sans préavis. 09/20 Présentation de solution H16793-1 W386667.