THREATQUOTIENT™

ThreatQ™ pour les services financiers

Le secteur des services financiers constitue une cible à la fois attrayante et lucrative pour les cybercriminels. Depuis trois ans, il s'agit du secteur le plus ciblé[1]. En effet, les clients des services financiers sont victimes de 65 % de cyberattaques en plus que n'importe quel autre secteur[2].

Malgré le fait qu'ils effectuent des simulations et des tests réguliers des fonctions de réponse à incident, et qu'ils enregistrent certains des taux de détection et de réponse les plus rapides, les établissements financiers continuent à être victimes de failles de sécurité et de compromissions. Le coût moyen de la cybercriminalité pour les entreprises de services financiers est de 18,37 millions de dollars, soit le montant le plus élevé de tous les secteurs[3]. En plus des fonds volés, ce chiffre inclut la détection des menaces, la réponse à incident et la notification des failles de sécurité, les amendes et frais de contentieux, ainsi que les pertes de revenus. En réalité, suite aux failles de sécurité, le secteur enregistre le deuxième taux de perte de clientèle le plus élevé après le secteur de la santé[4].

PRINCIPAUX DÉFIS

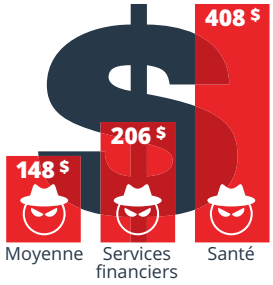
ÉLARGISSEMENT DES SURFACES D'ATTAQUE

D'un côté, les clients attendent des services qu'ils soient disponibles 24 h/24 et 7 j/7 depuis n'importe quel appareil et en tout lieu. De l'autre, les acteurs malveillants perturbent les activités des entreprises en lançant des attaques par déni de service distribué (DDoS). Si ces campagnes sont relativement simples à exécuter à l'aide d'outils et de services tiers, elles comptent parmi les attaques les plus coûteuses à neutraliser pour les entreprises. En outre, les acteurs malveillants ciblent de plus en plus les réseaux sociaux et mobiles que les entreprises utilisent pour interagir avec les clients et leur fournir une assistance, ainsi que mener des opérations commerciales. Étant donné que peu d'établissements financiers intègrent ces vecteurs à leur modèle de menaces, les cybercriminels utilisent des escroqueries par phishing, des techniques d'ingénierie sociale et des logiciels malveillants pour commettre des fraudes financières, porter atteinte à la réputation des marques et même faire peser des menaces physiques. Pour protéger leurs surfaces d'attaque de plus en plus larges, les établissements financiers doivent bénéficier d'une visibilité sur l'ensemble de leur infrastructure, ainsi qu'adopter une approche proactive pour combler les failles de leurs systèmes de défense.

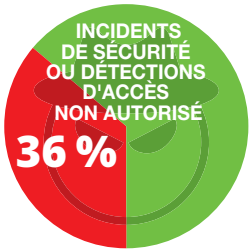
CIBLES ATTRAYANTES

Si les cybercriminels s'en prennent aux établissements financiers, c'est parce qu'ils représentent une cible lucrative. Ils exploitent activement les vulnérabilités des distributeurs automatiques, tandis que des réseaux tels que SWIFT (Society for Worldwide Interbank Financial Telecommunication) permettent aux groupes criminels de voler directement des banques ou de détourner subrepticement de l'argent volé ailleurs. En outre, les informations de compte bancaire, les données de carte de paiement et les autres informations d'identification personnelle des clients peuvent être rapidement monétisées. La plupart des analystes en sécurité sont submergés d'alertes. Ils doivent donc pouvoir se concentrer sur les menaces pertinentes et prioritaires, ainsi qu'améliorer leurs capacités de Threat Hunting.

COÛT PAR DOSSIER COMPROMIS



Le secteur des services financiers enregistre le deuxième coût le plus élevé par dossier compromis, soit 206 $, contre 148 $ en moyenne[4].



Près de 36 % des établissements financiers ont été victimes d'un incident de sécurité ou ont détecté un accès non autorisé en 2018, contre 24 % en 2017[5].

Les banques et les entreprises de services financiers ont été la cible de 25,7 % des attaques par logiciel malveillant l'année dernière, plus que n'importe quel autre secteur[6].

ATTAQUES VIA DES APPLICATIONS WEB

Les entreprises de services financiers utilisent des applications web pour fournir toutes sortes de services numériques et en ligne à leurs employés et à leurs clients. Ces applications permettent aux utilisateurs d'envoyer et de récupérer des données issues de bases de données à l'aide de leur navigateur. Les acteurs malveillants exploitent les vulnérabilités de ces applications et des appareils utilisés pour y accéder afin d'infiltrer des réseaux et des systèmes en vue de voler des données confidentielles ainsi que de l'argent. Il existe tout un éventail d'attaques exécutées via des applications web. Les établissements financiers ont donc besoin de connaissances en temps réel sur le mode opératoire des cybercriminels et des campagnes ainsi que l'infrastructure utilisée, afin de pouvoir accélérer la réponse à incident et renforcer la prévention.

« Les données des indicateurs de compromission issues de sources fiables sont désormais envoyées de manière proactive aux listes de surveillance de détection qu'utilisent divers contrôles de sécurité internes, sans que le personnel de l'équipe ne doive assurer une surveillance quotidienne. « Qui plus est, comme nous exportons de façon sélective les données vers l'outil spécifiquement conçu pour les utiliser, nous ne transmettons pas de gros volumes de données sur le réseau et nous ne ralentissons donc pas les opérations. »

— Directeur de l'équipe Réponse aux menaces d'une entreprise de services financiers du Fortune 500

RATIONALISATION DES OPÉRATIONS DE SÉCURITÉ DES SERVICES FINANCIERS

Une plate-forme de Threat Intelligence robuste offre aux entreprises de services financiers le contexte et la priorisation dont ils ont besoin pour prendre des décisions plus avisées, accélérer la détection et la réponse à incident, et favoriser l'apprentissage et la collaboration entre équipes pour une amélioration continue. Dans la mesure où tous les outils et technologies s'intègrent et fonctionnent en toute transparence avec l'architecture ouverte de ThreatQ, il n'est pas nécessaire de modifier l'infrastructure ou les workflows de sécurité existants.

PRINCIPAUX ATOUTS DE THREATQ :

- **CONSOLIDATION** au sein d'un référentiel central de toutes les sources de données de Threat Intelligence et sur les vulnérabilités, tant les sources externes (p. ex. FS-ISAC) qu'internes (p. ex. SIEM).
- **ÉLIMINATION** des nombreuses données parasites, pour mieux cibler les renseignements sur les menaces pertinents et se concentrer sur les ressources et les vulnérabilités critiques.
- **HIÉRARCHISATION** des mesures et ressources primordiales pour votre environnement.
- **TRAQUE PROACTIVE** des activités malveillantes pouvant indiquer une compromission des données de compte bancaire, une fraude à la carte de paiement ou des attaques par déni de service (DDoS), ou susceptibles de porter atteinte aux consommateurs et aux commerçants.
- **PRIORISATION** des vulnérabilités de sécurité connues et exploitées de manière active, risquant d'affecter la conformité réglementaire et la sécurité.
- **ANALYSE ET RÉPONSE ACCÉLÉRÉES** permettant de contrer plus rapidement les attaques visant plusieurs cibles, y compris les distributeurs automatiques, le réseau SWIFT, les applications web, les nouveaux canaux numériques et l'infrastructure sous-jacente.
- **DIFFUSION AUTOMATIQUE** des données de Threat Intelligence vers les outils de détection et de réponse à incident.

Rendez-vous sur threatq.com/demo pour demander une démonstration en direct de la plate-forme ThreatQ et de ThreatQ Investigations.

1 IBM, « IBM X-Force Threat Intelligence Index 2019 », https://www.ibm.com/account/reg/fr-fr/signup?formid=urx-36763

2 The World Bank, « Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision », 2018, http://www.worldbank.org/en/topic/financialsector/brief/cybersecurity-cyber-risk-and-financial-sector-regulation-and-supervision

3 Accenture, « The Cost of Cybercrime », 2019 https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

4 IBM, « 2018 Ponemon Cost of a Data Breach Study », https://www.ibm.com/security/data-breach

5 Security Boulevard, « Cybersecurity Investment to Shoot Up in Financial Industry in 2019; Top Firms Already Spend $1 Billion », https://securityboulevard.com/2018/12/cybersecurity-investment-to-shoot-up-in-financial-industry-in-2019-top-firms-already-spend-1-billion/

6 Helpnetsecurity, « Which cyber threats should financial institutions be on the lookout for? », https://www.helpnetsecurity.com/2019/04/30/2019-cyber-threats-finance/

À PROPOS DE THREATQUOTIENT™

ThreatQuotient s'est donné pour mission d'améliorer l'efficacité des opérations de sécurité à l'aide d'une plate-forme entièrement axée sur les menaces. En intégrant les processus et technologies existants d'une entreprise dans une architecture de sécurité unique, ThreatQuotient accélère et simplifie les investigations et la collaboration, non seulement au sein des équipes mais également entre les outils. Grâce à l'automatisation, la priorisation et la visualisation, les solutions ThreatQuotient réduisent le bruit et mettent en évidence les menaces prioritaires afin de permettre aux ressources souvent limitées de se concentrer sur les événements à haut risque et de prendre des décisions avisées. ThreatQuotient est basé dans le Nord de la Virginie, et possède des filiales chargées des opérations internationales en Europe et en Asie-Pacifique. Pour plus d'informations, consultez le site https://threatquotient.com.

ThreatQ-for-Financial-Services_Rev1

THREATQUOTIENT™

11400 Commerce Park Drive, Suite 200, Reston, VA 20191, États-Unis • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885