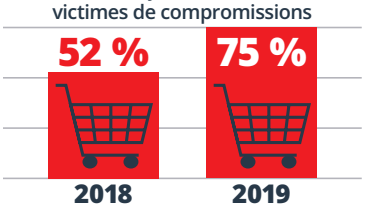
THREATQUOTIENT™

# ThreatQ™ pour le commerce de détail et l'hôtellerie

Les compromissions de cybersécurité dans les secteurs du commerce de détail et de l'hôtellerie, qui sont peut-être les plus médiatisées, se produisent à une fréquence alarmante. Selon un rapport de Thales, près de 75 % des commerçants américains affirment avoir été victimes d'une compromission, contre 52 % l'année précédente[1]. Les commerçants et les fournisseurs de services hôteliers investissent massivement dans la cybersécurité pour protéger les données des cartes de paiement et les autres informations d'identification personnelle. Cependant, certaines des mesures les plus efficaces que les commerçants puissent prendre pour éviter que leurs marques ne fassent la une des journaux reposent sur l'adage suivant : « Ceux qui ne tirent pas les leçons de l'histoire sont condamnés à la répéter ». En effet, les cybercriminels utilisent fréquemment les mêmes tactiques, techniques et procédures. Ce faisant, ils laissent toute une série d'indicateurs ou de traces identifiables offrant des informations précieuses sur les menaces.

Pourtant, il ne suffit pas de s'abonner à des feeds pour se protéger. Les entreprises doivent pouvoir regrouper et dédupliquer toutes les données externes et internes sur les menaces, réduire le bruit, évaluer et prioriser les données de Threat Intelligence, et exploiter concrètement ces dernières afin d'optimiser le délai de détection et de remédiation. Une rationalisation rapide de la capacité à importer, enrichir, déployer et opérationnaliser ces informations permet aux acteurs de la cybersécurité d'exercer une pression accrue sur les adversaires, favorisant ainsi les erreurs et les négligences au cours des attaques. L'opérationnalisation des données de renseignement sur la menace permet également aux équipes de cybersécurité de tirer parti de leur expérience et de celle de leurs homologues pour identifier les tactiques, techniques et procédures des adversaires, et de réévaluer et renforcer les défenses de façon proactive afin de contrer plus efficacement les attaques à venir.

Commerçants américains victimes de compromissions




Selon un rapport publié par Thales en 2018, près de 75 % des commerçants américains affirment avoir été victimes d'une compromission, contre 52 % l'année précédente[2].

Cyberattaques par secteur


Les commerçants font l'objet de trois fois plus d'attaques que le secteur des services financiers[3].

Attaques ciblant des grandes entreprises de distribution américaines


Aux États-Unis, le coût moyen d'une attaque de cybersécurité visant une grande entreprise de distribution est estimé à 12,69 millions de dollars[4].

## PRINCIPAUX DÉFIS

### INFORMATIONS D'IDENTIFICATION PERSONNELLE ET INFORMATIONS DE PAIEMENT

Les informations d'identification personnelle et les données des cartes de paiement jouent un rôle vital dans le secteur du commerce de détail. Chaque transaction implique l'échange d'informations d'une grande valeur, et cet énorme volume de données fait de ces organisations des cibles particulièrement lucratives pour les acteurs malveillants. Bien sûr, les technologies de paiement sécurisé contribuent à renforcer les défenses, mais elles n'offrent pas une solution miracle. Une étude réalisée par Visa indique que lorsque les attaques parviennent à déjouer les dispositifs de protection, l'impact des compromissions est plus important. Il faut également noter que si la technologie à puce EMV (Europay, Mastercard et Visa) améliore la sécurité des transactions aux points de vente, elle ne protège en rien les transactions sans présentation de carte, typiques du commerce électronique.

### SPEAR PHISHING

Un grand nombre des menaces visant le secteur du commerce de détail et de l'hôtellerie reposent sur des e-mails de spear phishing qu'il est presque impossible de distinguer des e-mails légitimes. Si certaines campagnes privilégient les attaques rapides à grande échelle pour cibler plusieurs commerçants simultanément en les mitraillant plus ou moins à l'aveuglette, d'autres ciblent le fournisseur ou l'intégrateur du point de vente du commerçant pour accéder aux données recherchées.

Une fois à l'intérieur du réseau, elles exploitent des vulnérabilités permettant l'usurpation d'informations d'identification ou l'escalade de privilèges pour voler les données des cartes de paiement ou lancer des attaques par ransomware.

### CORRECTION DES VULNÉRABILITÉS

Les attaquants profitent du fait que les équipes informatiques et de sécurité ont du mal à assurer la correction régulière de leurs systèmes de point de vente, de leurs applications de paiement électronique et de l'infrastructure interne sous-jacente. Pour tenter de rester compétitifs, les commerçants, quant à eux, investissent dans des canaux numériques, des applications et des technologies supplémentaires qui accroissent la complexité de l'environnement et génèrent de nouvelles contraintes de correction. Une pénurie de spécialistes en cybersécurité et la bureaucratie organisationnelle expliquent souvent l'incapacité à appliquer les correctifs en temps utile.

## RATIONALISATION DES OPÉRATIONS DE SÉCURITÉ DANS LES SECTEURS DU COMMERCE DE DÉTAIL ET DE L'HÔTELLERIE

Une plate-forme de Threat Intelligence robuste fournit aux commerçants et aux fournisseurs de services hôteliers 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. R-CISC) 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.
- **PRIORISATION** des mesures et ressources primordiales pour votre environnement.
- **TRAQUE PROACTIVE** des activités malveillantes pouvant indiquer une fraude à la carte de paiement ou des attaques par déni de service, 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 systèmes de point de vente, les applications de commerce électronique, 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] Rapport 2018 de Thales sur les menaces informatiques — Édition Commerce de détail (https://www.thalesesecurity.com/2018/data-threat-report-retail)

[2] Rapport 2018 de Thales sur les menaces informatiques — Édition Commerce de détail (https://www.thalesesecurity.com/2018/data-threat-report-retail)

[3] Étude de référence 2018 de Cisco sur les fonctionnalités de sécurité (https://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/retail-security-infographic.pdf)

[4] Livre blanc Symantec — Cyber Security for Retail Services: Strategies that Empower your Business, Drive Innovation and Build Customer Trust (La cybersécurité pour les services de vente au détail : stratégies qui dynamisent votre entreprise, stimulent l'innovation et renforcent la confiance des clients) (https://www.symantec.com/content/dam/symantec/docs/white-papers/cybersecurity-retail-en.pdf)

### 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 en Virginie du Nord, et possède des filiales chargées des opérations internationales en Europe et en Asie-Pacifique. Pour plus d'informations, consultez le site https://threatquotient.com.



TQ_ThreatQ-for-Retail-and-Hospitality_Rev1

THREATQUOTIENT™

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