HISCOX

CYBERCLEAR®

Evolution de la sinistralité
Avril à juin 2020

La fréquence des sinistres a baissé alors que les ransomware ont augmenté

chiffres d'affaires

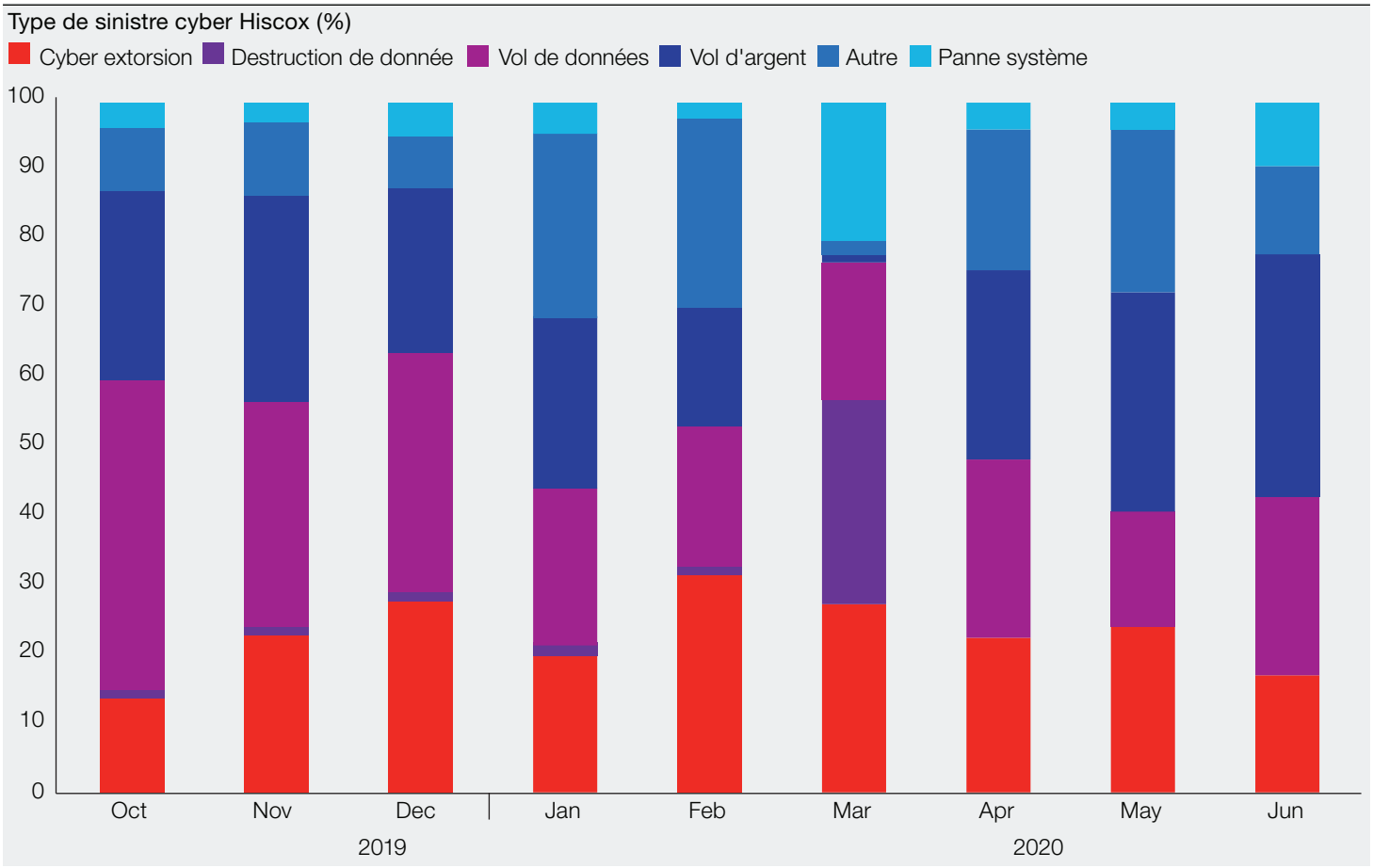
On peut noter sur les données depuis juin 2020 l'impact immédiat et continu du COVID-19 sur les sinistres cyber. Dans l'ensemble, les sinistres Hiscox cyber pour les entreprises de moins de €8.6 million de ~~chiffre d'affaire~~ on baissé aux USA, au UK et en Europe de 17% entre le premier et le deuxième trimestre. On observe le changement le plus significatif au UK avec une baisse de 25%, suivi par les USA avec 15% et l'Europe avec 12%. En complément, les grands organismes publics (4,3 milliards de chiffre d'affaire et plus, listés sur la bourse des US) on vu plus d'incidents par ransomware sur le premier semestre 2020 que sur l'ensemble de 2019 et nous nous attendons à ce que cela double encore d'ici la fin de l'année.

Certains types d'incidents ont eu impact significatif sur les sinistres du second trimestre, plus particulièrement la fraude financière. La fraude financière a eu le plus grand impact sur l'ensemble des géographies au deuxième trimestre avec une très forte progression de 67% par rapport au premier trimestre. L'Europe a connu trois fois plus de sinistres avec vol d'argent qu'au premier trimestre, alors que les USA ont connu une hausse de 29%. La premiere tactique utilisée dans les tentatives de fraude réussies a été la fraude par détournement de paiement, et le télétravail lié au COVID-19 a sans doute joué un role clé dans ce phénomène. Les processus et procédures habituels pour l'approbation et le réglement des fournisseurs ont peut etre été moins respectés dans le contexte actuel. De plus, des tiers attaqués peuvent aussi avoir été à l'origine des cyber attaques.

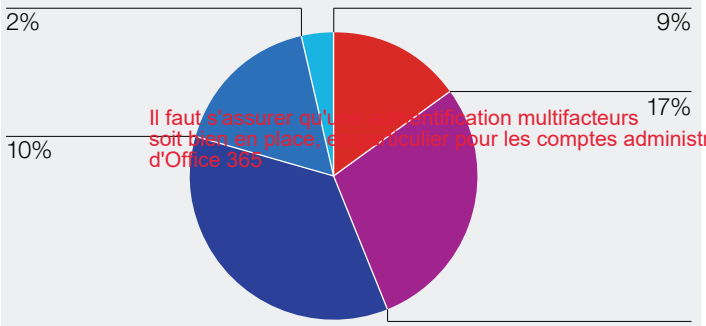
De nouveaux gangs de ransomware ont aussi émergé. au second trimestre 2020, le type de ransomware dominant dans les sinistres Hiscox aux USA et en Europe a été Dharma. D'autres types fréquents étaient Snatch, Maze, LockBit et Medusa. La pandémie semble avoir affecté les sinistres par ransomware à la fois positivement et négativement. Par exemple, un hotel a subi une attaque par ransomware qui a eu un impact très mineur du fait que l'activité était stoppée du fait du confinement, entrainant une absence de perte d'exploitation. Pour un autre assuré, cependant, malchanceux suite à un incident par ransomware parce que leurs sauvegardes dataient de deux mois. Les restrictions d'accès au local où les sauvegardes se situaient ont en effet empêché de pouvoir les utiliser. Mais il ne s'agit pas juste de quelques entreprises isolées faisant face à des ransomwares. Comme pour la fraude financière, il est très important de sécuriser les fournisseurs et les structures de supply chain. En avril, 44% des sinistres par ransomware aux USA étaient liés à des attaques des fournisseurs affectant par rebond nos assurés.

neuf

Vue par géographie sur ~~nueve~~ mois

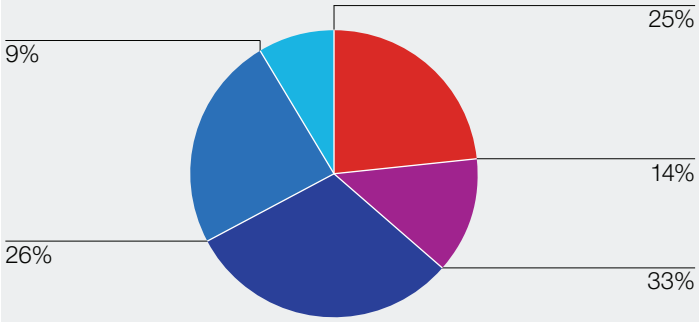


Sinistres UK T2 2020 (%)

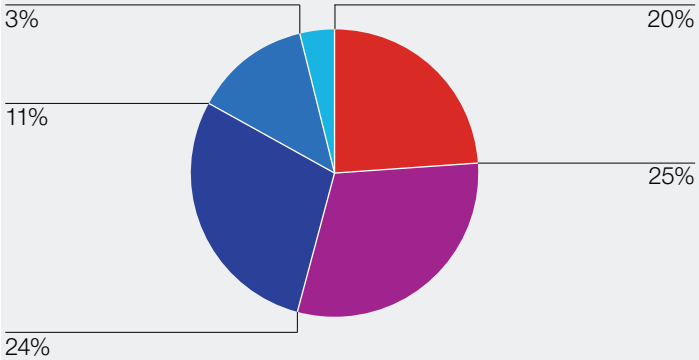


Il faut s'assurer qu'une authentification multifacteurs soit bien en place, en particulier pour les comptes administrateurs d'Office 365

Sinistres Europe T2 2020 (%)



Sinistres USA T2 2020 (%)



Réduire votre risque

- Les failles de Microsoft Office 365 sont toujours un problème, causant de nombreuses compromission d'email professionels (business email compromise) et des détournements de fonds au second trimestre aux USA et en Europe. S'assurer une authentification multifacteurs est bien en place, en particulier pour les comptes administrateurs d'Office 365.
- RDP et VPN restent des points d'entrée habituels dans les attaques par ransomware. Ce sont des technologies sur lesquelles on compte beaucoup, en particulier pour le télétravail. De tels incidents peuvent être évités par l'application régulière des patchs.
- Au dernier trimestre, les assurés d'Europe ont été vraiment bons pour notifier tôt les sinistres potentiels. Ils commencent maintenant à faire de même aux USA et au UK. Il est important pour une entreprise de signaler à leur assureur dès qu'ils détectent un malware ou une activité suspicieuse sur leur réseau, une équipe support peut ainsi les assister immédiatement pour éviter de futures attaques. D'après le rapport Hiscox 2020 sur la gestion des risques Cyber, qu'une rançon soit payée ou pas, la perte moyenne pour les compagnies soumises à une attaque par ransomware étaient à peu près du double pour celles qui devaient se débattre seule avec la leur – 781 000€ contre 415 000€. Comme les cas de vols de données continuent d'augmenter, les sauvegardes ne sont plus infaillibles pour réduire le risque contre les attaques par ransomware, chacun veut éviter qu'un malware devienne un ransomware.

Attaques dans la vraie vie

E-commerce
Revenue: €1.7 million
Impact: vol de données

Une plateforme d'e-commerce offrant des articles de décoration d'intérieur a été attaquée, et le criminel a obtenu des accès valides à leur système Magento, la plateforme d'ecommerce qui opérait leur site. Le hacker a placé un script dans le menu qui déclenchait.

E-commerce
Revenue: €132 million
Impact: vol de données

Une marketplace en ligne de services d'art et de design graphique a appris via les média qu'un groupe de hackers avait acquis des données de différentes compagnies, eux compris. Les données étaient vendues sur le dark web. Les hackers ont obtenu les données de millions d'utilisateurs de plateformes, comprendant leurs noms, login et mots de passes. Pour certains utilisateurs, les informations volées inclueaient les dates de naissances, numéros de téléphones, facturations et adresses de livraisons.

Media
Revenue: €14.3 million
Impact: cyber extorsion

Une agence média a subi une attaque par ransomware de type RagnarLocker. Pendant une revue par un expert, on a découvert que les criminels avaient aussi volé les informations personnelles des clients de notre assuré. La demande de rançonn d'un million d'euros a été négociée à 191 000€ et payée.

Fournisseur B to B
Revenue: €5 million – €10 million
Impact: fraude financière

Un fournisseur de pièces détachées automobile a subi un détournement de fond après qu'un email d'employé ait été compromis et utilisé pour envoyer des emails aux clients contenant des demandes de réglement falsifiées. Au total, les clients ont réglé 51 000€ aux hackers.

Alimentation en gros
Revenue: €19.4 million
Impact: cyber extorsion

Un grossiste fournisseur alimentaire a subi une attaque par ransomware de type Dopplepaymer. La rançon demandée et payée était de 76 000€. Deplus, l'assuré a subi plus de 84 000€ de perte de revenus qui ont pu être indemnisés.

Finance
Revenue: €3 million
Impact: cyber extorsion

Une agence de recouvrement a subi une attaque par ransomware avec vol de données. Les hackers on réclamé une rançon de 44.9 bitcoins (379 000€) pour restaurer les systèmes et ne pas laisser fuiter les données exfiltrées. Il y avait des informations très sensibles (données personnelles médicales et financières) qui étaient dans la base de données de notre assuré pour environ 350 000 individus.

Educational services
Revenue: €1.8 million
Impact: détournement de fonds

Un établissement de formation a subi une compromission d'email assortie de détournement de fonds pour 17 000€. Les hackers pouvaient aussi accéder à des données personnelles sensibles relatives à des mineurs. Les investigations initiales ont révélé que six emails frauduleux ont été envoyés par les hackers pour tenter de convaincre les récipiendaires de verser des droits d'inscription à un compte bancaire frauduleux, et offrant une réduction pour les premiers inscrits.

Glossaire

Les termes cyber sont souvent compliqués à comprendre. Nous sommes là pour vous aider.

Cyber extorsion
Cyber criminels encryptant les données/systèmes de leur victime (ransomware), menaçant de publier les données volées, prenant en otage les données/systèmes, etc. jusqu'à ce que leurs victimes satisfassent leurs demandes de raçon.

Email professionnel compromis (business email compromise)
Accès et contrôle non autorisé d'un compte email professionnel pouvant servir à des vols de données ou du détournement de fonds.

Fraud par détournement de réglement
Cyber criminels détournant des paiements vers un compte bancaire frauduleux.

Remote desktop protocol (RDP)
Outil propriétaire développé par Microsoft qui founit à un utilisateur une interface de connection à un autre ordinateur par connection réseau.

Vol d'argent
Cyber crime impliquant le vol d'argent.

Vol de données
Accès non autorisé à des données, dans la plupart des cas, extraction ou copie des données du réseau de la victime.

VPN (virtual private network)
Communément utilisé pour autoriser des personnes en télétravail en dehors du reseau d'entreprise d'accéder de façon sécurisée au réseau d'entreprise de leur domicile ou lors de leurs déplacements.

Hiscox France
38 av de l'Opéra
75002 Paris
France

T +33 (0)1 53 21 82 82
E hiscox.communication@hiscox.fr
www.hiscox.fr

20538c 10/20

A propos d'Hiscox en France

En France, Hiscox Assurances s'appuie sur l'expertise de 135 collaborateurs pour proposer ses produits d'assurances spécialisés à travers trois canaux de distribution (Courtage, Direct et Partenariats). Cette organisation reflète la volonté d'Hiscox de placer les besoins du client au centre de son développement en lui offrant une approche multicanale. L'agilité et les valeurs d'Hiscox définissent son activité, avec un accent sur l'humain, le courage et l'excellence dans l'exécution au service de ses clients. C'est ce qu'illustre sa signature de marque « Penser à tout, et surtout à vous ».

HISCOX ASSURANCES | Penser à tout, et surtout à vous