Sinistres Cyber

Rapport Stoïk 2023

stoïk

Sommaire

Avant-propos

“Nous sommes tous aveugles face au risque cyber”

Ces dernières années, avec l’explosion des attaques par ransomware et la multiplication des sinistres de petites, moyennes et grandes entreprises, une question s’est imposée dans le monde de l’assurance : le risque cyber est-il vraiment assurable ?

Et pour cause, la complexité de la menace, sa vitesse d’évolution et son potentiel systémique rendent légitime de s’interroger sur la capacité d’un assureur à déterminer de manière fiable et pérenne l’espérance de sinistralité d’une entreprise à partir de sa posture de risque.

C’est pourtant l’ambition d’y parvenir qui nous a poussés à lancer Stoïk il y a maintenant trois ans. Notre projet : maîtriser le risque en accompagnant notre couverture d’assurance d’une grande technicité cyber au niveau de la souscription, de la prévention offerte aux assurés, et bien sûr de la gestion des sinistres.

Depuis, nos courtiers partenaires ont équipé avec le produit Stoïk plusieurs milliers de TPE, PME et ETI allant de 0 à 500 millions de chiffre d’affaires en France et en Allemagne. Et, inévitablement, notre équipe interne dédiée à la gestion des incidents de sécurité de nos assurés a été mobilisée sans relâche pour les assister lors des cyberattaques.

L’un des freins au développement de l’assurance cyber en Europe est l’absence de partage de données sur les sinistres gérés par les assureurs, en partie car l’immense majorité d’entre eux externalise l’expertise d’assistance technique en cas d’incident.

Nous avons, au contraire, le privilège de gérer les sinistres de A à Z, et donc de collecter une donnée dont nous sommes propriétaires. Aussi avons-nous pensé utile pour tous de la partager avec le plus de transparence possible.

Ce rapport présente ainsi un premier aperçu de l’état de la sinistralité cyber chez nos assurés. Nous prévoyons d’en faire un rendez-vous annuel, à travers lequel nous partagerons une donnée de plus en plus granulaire, à mesure qu’augmentera la quantité de données collectées.

J’espère donc que ces quelques pages vous seront utiles, et qu’elles participeront, au moins marginalement, à atténuer notre cécité collective.

Jules Veyrat
Président et cofondateur de Stoïk

Nous avons le privilège de gérer les sinistres de nos assurés de A à Z, et donc de collecter une donnée dont nous sommes propriétaires. Aussi avons-nous pensé utile pour tous de la partager avec le plus de transparence possible.

État de la menace 2023

“Les PME et les ETI toujours en ligne de mire”

Vincent Nguyen
Directeur de la Cybersécurité chez Stoïk

En 2023, nous avons constaté une légère augmentation du volume d’attaques global mais pas d’augmentation drastique telle qu’on a pu la connaître en 2020. L’explosion des cyberattaques tant attendue suite au déclenchement du conflit russo-ukrainien n’a pas eu lieu. Suivant une logique purement lucrative, les cybercriminels continuent d’attaquer de manière opportuniste les entreprises et organisations les plus vulnérables, tous secteurs d’activité confondus. Ainsi, 2023 a confirmé la tendance perçue ces dernières années, les PME et les ETI sont bien les principales victimes de cyberattaques.

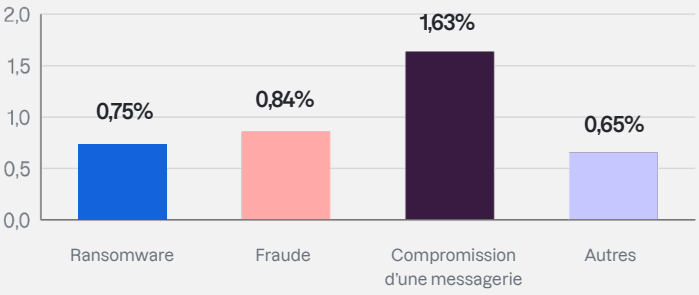
D’après nos observations, les vulnérabilités exploitées par les attaquants en 2023 chez les PME et ETI sont : l’absence d’authentification multifacteur, des combinaisons identifiant et mot de passe faibles, ainsi que des mises à jour non réalisées. La persistance de ces vulnérabilités est majoritairement due à un manque de sensibilisation et de formation, de budget alloué à la cybersécurité et de mise en place de mesures de cybersécurité adéquates.

Si la sensibilisation progresse, le risque cyber reste en 2023 perçu comme complexe, difficilement appréhendable et lorsque l’incident survient, les dommages sont lourds et coûteux.

Les cybercriminels continuent d’attaquer de manière opportuniste les entreprises et organisations les plus vulnérables, tous secteurs d’activité confondus.

Fréquence des sinistres

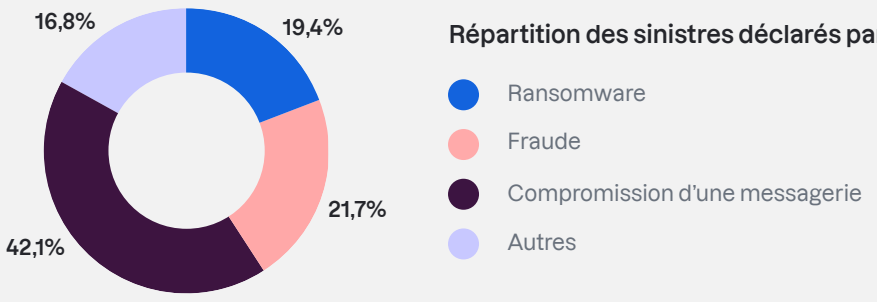
En 2023, nous avons observé une fréquence de sinistres[1] de **3,87%** sur l'ensemble de notre portefeuille d'assurés, avec la catégorisation suivante :



Nous catégorisons les sinistres déclarés de la manière suivante :

- Lorsqu'un événement de compromission de boîte mail est déclaré avant qu'un détournement de fonds (fraude) n'ait lieu ou qu'un ransomware ne soit déployé, celui-ci est catégorisé en tant que **compromission de messagerie.**
- Lorsqu'un événement est déclaré après la réalisation d'un détournement de fonds (fraude), il est catégorisé comme **fraude** même si le vecteur d'attaque était une compromission de boîte mail, d'un site internet ou d'un actif.
- Lorsqu'un événement est déclaré après le déploiement d'un ransomware, il est catégorisé comme **ransomware** même si le vecteur d'attaque était une compromission de boîte mail, de site internet ou d'un actif.

Ainsi, les compromissions de boîtes mails représentent plus de 40% de nos sinistres en volume. Cependant, bien qu'ils soient plus de deux fois moins fréquents, ce sont bien les ransomwares qui ont eu **l'impact financier le plus considérable** sur nos entreprises assurées en 2023.



[1] Donnée basée sur les sinistres déclarés entre le 1er janvier 2023 et le 31 décembre 2023. Par sinistre, nous considérons tout incident de sécurité déclaré par l'un de nos assurés ayant déclenché l'activation d'au moins l'une des garanties de notre contrat d'assurance.

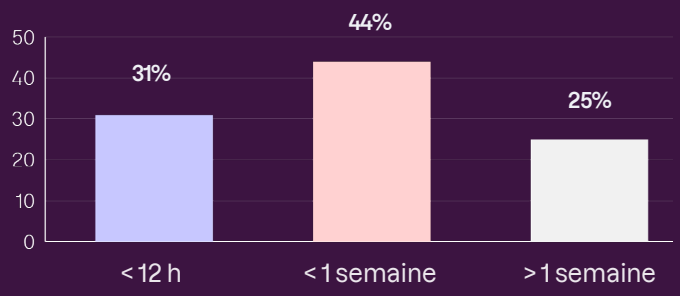
Maîtriser l'impact financier du ransomware

Si l'impact financier potentiel du ransomware fait trembler les assureurs, c'est qu'il engendre quasi systématiquement une perte d'exploitation pour la victime. Passé le délai de franchise (souvent entre 12 et 24 heures), chaque heure qui passe sans que le système d'information ne soit rétabli engendre un coût supplémentaire à indemniser. Aussi, **la vitesse et la qualité de l'intervention des experts en gestion de crise a un impact considérable sur le coût du sinistre.** Les premières heures d'intervention sont particulièrement décisives puisqu'elles visent à interrompre la propagation de l'attaquant au sein du système et donc à limiter les dégâts causés.

Corrélation entre durée du sinistre et configuration des sauvegardes

Dans 75% des cas de ransomwares rencontrés, nos équipes ont réussi à relancer l'activité de l'entreprise en moins d'une semaine. À chaque fois, un point commun parmi les victimes : les sauvegardes de données avaient été correctement configurées, elles étaient disponibles sur des supports déconnectés du reste du système d'information et restaurables sans difficulté car elles étaient testées et que le catalogue des sauvegardes était également sauvegardé. Dans toutes les situations dans lesquelles la durée a excédé une semaine, à l'inverse, les sauvegardes de l'assuré n'avaient pas été correctement déconnectées, ou n'étaient pas immuables.

Durée de réponse à incident par ransomware



Étude de cas

En pleine période de soldes, une veille de week-end, une entreprise de e-commerce a alerté nos experts de l'indisponibilité de son site internet suite à un ransomware. Chaque journée d'interruption du site aurait représenté plusieurs centaines de milliers d'euros de manque à gagner.

Un travail de remédiation a été mené avec le DSI de l'entreprise assurée pour récupérer les sauvegardes et reconstruire l'infrastructure informatique. En parallèle, une seconde équipe s'est attelée à la reconstruction complète du système d'information, dans le cas où ces sauvegardes seraient inutilisables. En quelques heures seulement, l'attaquant a été délogé de l'infrastructure et le système d'information remis en état.

L'épreuve de la négociation

En moyenne, le montant des rançons demandées à nos assurés s'est élevé autour de 700 000 euros en 2023. Souvent, l'attaquant ouvre la porte à une négociation que nos équipes prennent alors en main. Ces phases sont critiques car elles permettent de gagner un temps pendant lequel les équipes peuvent œuvrer à remettre en état le système d'information de l'assuré, sans que l'attaquant n'amplifie les dégâts. Et elles permettent en outre de réduire la facture finale, dans le cas ultime où il faudrait payer : **en moyenne, ces négociations ont abouti à une baisse des demandes de 53% du montant initial.**

La vertu d'un scan externe en prévention des ransomwares

Dans 82% des cas de ransomware subis par nos assurés, les cybercriminels se sont introduits dans le système d'information en récupérant des accès à distance, soit par force brute, soit suite à une tentative réussie de phishing. **Dans 18% des cas seulement, ils ont exploité des vulnérabilités techniques.**

Si l'exploitation de vulnérabilités techniques est plus rare, c'est que toutes les entreprises assurées par Stoïk sont scannées de manière hebdomadaire et alertées lorsqu'une faille apparaît. **Ainsi, notre scan externe a permis de corriger en moyenne 10 vulnérabilités critiques par semaine en 2023 au sein de notre portefeuille d'assurés.**

Pour ces 18% de cas où des vulnérabilités n'ont pas été détectées par notre scan externe, il s'agit de vulnérabilités dites "zero day" (donc pas encore connues) ou de vulnérabilités présentes sur une partie du système d'information non explicitée par l'assuré (par exemple une adresse IP publique non identifiable à partir des domaines ou sous-domaines renseignés), comme ce fut parfois le cas lors de l'attaque par ransomware ESXiargs — une attaque d'ampleur mondiale liée à des milliers de serveurs vulnérables exposés sur Internet.

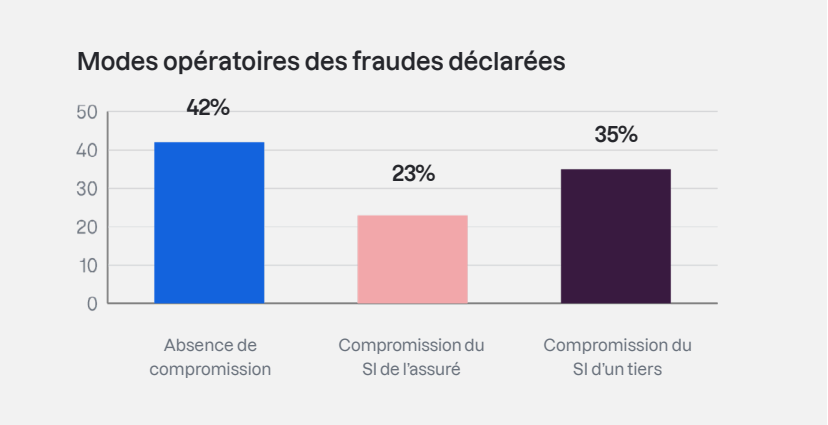
Le ransomware ESXiargs

Dès le début de la campagne d'exploitation massive de la vulnérabilité ESXi, nos experts se sont synchronisés avec l'InterCERT France pour déterminer le meilleur moyen de bloquer l'attaque. Ils ont ensuite alerté tous les assurés pouvant être potentiellement concernés, et réussi ainsi à limiter drastiquement le volume d'attaques subies.

Plusieurs attaques ont cependant eu lieu le même jour chez les assurés les moins réactifs, mais un moyen de déchiffrement efficace a pu être déployé à chaque fois par nos experts, et aucun dégât notable n'a été à déplorer.

La fraude aux faux ordres de virement sous toutes ses formes

Parmi tous les cas de fraude aux virements notifiés à notre CERT[2], on distingue **trois types de situations :**



- Dans 42% des cas, la fraude est réalisée **sans qu'il y ait intrusion dans le système d'information (SI) de l'assuré**, par le simple moyen d'un email ou d'un appel téléphonique externe frauduleux.
- Dans 23% des cas, la fraude est réalisée suite à la **compromission du système d'information de l'assuré lui-même.**
- Dans 35% des cas, la fraude est réalisée suite à la **compromission du système d'information d'un tiers** (par exemple, le cabinet comptable de l'assuré).

En 2023, le montant détourné chez nos assurés ayant déclaré un sinistre de ce type s'est élevé en moyenne à **47 500 €.**

Les métiers du droit et de l'immobilier, dans lesquels les virements sont conséquents et fréquents, ont été particulièrement ciblés. L'attaquant cherche le plus souvent à prendre possession d'une boîte mail et attend le moment opportun pour remplacer le RIB du destinataire (celui du propriétaire d'un logement en location, par exemple, chez les agences immobilières) par le sien.

Les prestataires de service ont également été ciblés à de nombreuses reprises, souvent pour de plus petites sommes qui passent inaperçues.

[2] Computer Emergency Response Team

Étude de cas

Un conflit juridique a eu lieu entre notre assuré et un de ses fournisseurs : depuis plusieurs mois, l'assuré avait payé des factures sur un RIB fourni par un attaquant ayant usurpé l'identité du fournisseur. L'attaquant avait compromis la boîte mail de notre assuré grâce à une attaque par phishing réussie. Suite à cette intrusion, l'attaquant avait mis en place des règles pour automatiquement modifier les factures des fournisseurs arrivant sur la boite mail de notre assuré, en y ajoutant son RIB à la place du RIB légitime.

L'intervention de notre CERT a permis d'identifier la source de la compromission, de sécuriser les boîtes mails de notre assuré tout en sensibilisant l'ensemble de ses équipes aux risques de fraudes financières.

Les leviers d'action pour prévenir le risque :

Il est extrêmement difficile d'anticiper une tentative de fraude au virement. Lorsque l'attaquant accède à la boîte mail, il dispose de tous les mails passés et il lui suffit de relancer une facture en changeant le RIB tout en gardant l'historique de conversation pour tromper son interlocuteur.

Trois réflexes à adopter pour faire face à la fraude aux faux ordres de virement :

Mettre en place **l'authentification multifacteur (MFA)** sur les boîtes de messagerie.

Mettre en place une **campagne de sensibilisation** des employés au phishing.

Mettre en place un processus de **double validation des paiements** au-delà d'un certain montant.

La sécurité des boîtes mails : porte d'entrée privilégiée des attaquants

Un attaquant peut tirer profit de la compromission d'une boîte mail de 3 manières différentes :

- **Le vol de données** : celles qui sont accessibles dans la boîte mail.
- **Le détournement de fonds** via un changement de RIB, comme vu précédemment.
- **L'obtention de moyens d'attaque :** l'attaquant se sert de la messagerie compromise pour obtenir des informations ou droits d'accès supplémentaires, et amplifier son pouvoir de nuisance. S'il n'en est pas capable lui-même, il pourra aussi revendre ses accès à des attaquants plus aguerris.

Notre analyse des déclarations de sinistres liées à la compromission de boîtes mail révèle des différences significatives en fonction des plateformes de messagerie utilisées par nos assurés.

Fréquence des sinistres par compromission de boîte mail en fonction de la plateforme de messagerie utilisée :

x1 Google Workspace

x1,2 Microsoft Office 365

x3 Microsoft Exchange hébergé en interne

D'abord, il est à noter que les utilisateurs de Microsoft Office 365 signalent 1,2 fois plus de cas de boîtes mail compromises que ceux utilisant Google Workspace. Si cela peut laisser penser que les environnements Office 365 présentent des vulnérabilités spécifiques ou sont plus ciblés par les attaquants que les environnements Google Workspace, il est néanmoins important de prendre en compte d'autres facteurs comme la popularité de Microsoft 365 dans le milieu professionnel, qui le rend plus susceptible d'être ciblé. **Surtout, il est crucial de rappeler que la sécurité de toute plateforme de messagerie dépend fortement de la manière dont elle est configurée et gérée.** Cette tendance ne doit donc pas être interprétée comme une indication intrinsèque de la vulnérabilité de Microsoft 365.

De manière encore plus frappante, le nombre de déclarations de sinistres pour les boîtes mail compromises est 3 fois plus élevé chez les utilisateurs hébergeant leur propre serveur mail Exchange comparé à ceux de Google Workspace. Là encore, il convient de ne pas en tirer de conclusion hâtive. Certes, les environnements de messagerie hébergés par les assurés nécessitent une gestion de la sécurité en interne, et peuvent donc être plus exposés à des risques si les pratiques de sécurité ne sont pas rigoureusement appliquées. Mais, il n'empêche que, bien gérées, les solutions hébergées en interne peuvent offrir un très haut niveau de sécurité. L'idée à garder en tête est donc avant tout l'importance d'une gestion et d'une configuration sécurisées, quelle que soit la plateforme choisie.

L'assurance active pour faire face aux cyberattaques

Le risque cyber est un risque nouveau, volatile, imprévisible **mais anticipable**. En 2023, encore trop peu d'entreprises de taille moyenne et intermédiaire sont préparées à faire face à une cyberattaque, et les conséquences peuvent être fatales. Pour l'anticiper et réduire le coût des sinistres, deux aspects nous semblent clé : la qualité de la prévention et la rapidité d'intervention en cas d'attaque.

Une prévention active et continue

Le premier objectif est d'aider les entreprises à éviter les attaques les plus courantes : c'est ce que nous permettons à nos assurés en leur mettant à disposition la plateforme Stoïk Protect qui comprend des outils de scan interne et externe qui repèrent les failles connues avant les attaquants et des outils de sensibilisation au risque cyber (phishing, fraude, etc.) pour tous les collaborateurs et dirigeants.

En complément, nos experts accompagnent les entreprises assurées tout au long de leur contrat dans la mise en place de mesures d'hygiène de cybersécurité :

- **Correction des vulnérabilités** détectées par les scans
- Implémentation de l'**authentification multifacteur**
- Mise en place d'une politique de **sauvegarde hors ligne et déconnectée**
- Mise en place d'une politique de **mots de passe robustes**
- Mise en place d'une politique de **suivi des mises à jour**

Une capacité de réponse aux incidents rapide et efficace

Ensuite, nous avons vu dans ce rapport que les premières heures sont décisives pour minimiser le coût du sinistre, notamment en cas de ransomware. C'est la raison pour laquelle **nous disposons d'une équipe d'experts cyber — le CERT-Stoïk — pour prendre en charge nos assurés le plus rapidement et le plus efficacement possible** lorsqu'une attaque survient.

Les entreprises assurées chez Stoïk disposent ainsi d'un accompagnement technique et humain qui leur permet d'obtenir une visibilité en temps réel de leur niveau de risque et de bénéficier d'une assistance de qualité en cas de sinistre.

Nos prévisions pour 2024

“Les attaquants vont continuer d’exploiter les failles connues”

Vincent Nguyen
Directeur de la Cybersécurité chez Stoïk

En 2024, les attaques via la chaîne d’approvisionnement dont les niveaux de sécurité sont très hétérogènes selon les fournisseurs — rappelons que le niveau de sécurité d’une entreprise est équivalent au niveau de sécurité le plus faible de ses fournisseurs — et notamment les services Cloud émergent comme un risque majeur. Ces derniers sont de plus en plus présents dans les systèmes d’information des entreprises ce qui a pour effet d’augmenter drastiquement la surface d’attaque tout en diminuant fortement la maîtrise interne, mettant en évidence la nécessité impérieuse pour les organisations de tous les secteurs de renforcer leur cybersécurité face à ces menaces de plus en plus sophistiquées et potentiellement dévastatrices.

Les attaques contre les fournisseurs de services Cloud, ont des répercussions considérables. Lorsqu’un de ces fournisseurs est compromis, l’impact ne se limite pas à une seule organisation mais s’étend à l’ensemble de son réseau de clients. Cela peut signifier que **des dizaines, des centaines, voire des milliers d’entreprises peuvent subir les conséquences d’une seule attaque.**

C’est arrivé en 2023

Coaxis, une entreprise de services du numérique, a subi une attaque par ransomware en décembre 2023 qui a mis à l’arrêt la moitié des cabinets d’expertise comptable de France. Lorsqu’un prestataire informatique subit une attaque, c’est tous ses clients qui en subissent les dégâts.

Les tendances annoncées — développement de l’intelligence artificielle, de l’IoT — ne semblent pour le moment pas impacter l’état de la menace qui reste stable. Nous apporterons cependant une vigilance accrue avant et pendant toute la période des **Jeux Olympiques et Paralympiques 2024** en France. La tenue d’un tel événement engendre systématiquement un accroissement de la menace cyber sur l’ensemble des structures du pays hôte, publiques comme privées, et nos coopérations au sein de l’InterCERT France et du FIRST (Forum of Incident Response and Security Teams) nous permettront d’y répondre de la manière la plus efficace.

La **Directive NIS 2**, introduite en Europe et en France, marque une révolution dans le domaine de la cybersécurité, imposant à un large éventail d’organisations de se conformer à des normes strictes en matière de sécurité informatique et de gestion des incidents. Face à ces nouvelles exigences, l’assurance cyber devient un outil crucial, non seulement pour répondre aux obligations réglementaires, mais aussi pour fournir une protection financière et opérationnelle contre les cyberattaques. Ce changement induit une évolution majeure dans la relation entre les entreprises et les assureurs, soulignant la nécessité d’une compréhension approfondie des risques cyber et des meilleures pratiques pour les gérer efficacement.

stoïk

Assurance & Cybersécurité

www.stoik.com

contact@stoik.com

4, rue Euler, 75008 Paris

N° ORIAS 21007462