stoïk

Sinistres Cyber

Rapport Stoïk 2024

Sommaire

Avant-propos

Par Jules Veyrat
Président et cofondateur de Stoïk

2024 a été une année paradoxale dans l'évolution de la menace cyber.

À première vue, les tendances semblent rassurantes. La menace, si ce n'est contenue, a été globalement maîtrisée. Les attaques par ransomware, longtemps symbole de l'insécurité numérique, ont reculé en début d'année grâce notamment au démantèlement de certains groupes cybercriminels majeurs. Même les Jeux de Paris 2024, fortement redoutés, se sont déroulés sans incidents majeurs.

Pourtant, cette apparente accalmie ne doit pas masquer une réalité vertigineuse : l'extrême fragilité de l'écosystème numérique mondial. Les événements de 2024 nous ont rappelé le niveau considérable d'interdépendance de nos systèmes informatiques à travers le monde, et laissé présager de la gravité de la menace systémique qui pèse sur nos économies. La vulnérabilité critique Fortinet a laissé craindre le pire en début d'année, tandis que le bug de Crowdstrike, durant l'été, a permis de percevoir l'ampleur des dégâts potentiels.

Face à une telle menace, et en particulier dans un contexte géopolitique aussi incertain, il faut faire front commun, car la réponse ne peut qu'être collective.

La cybersécurité est une responsabilité partagée entre États, entreprises, experts et individus. Ce deuxième rapport de Stoïk s'inscrit dans cette dynamique. En partageant les données et les enseignements tirés des incidents gérés en 2024 pour nos plus de 5000 assurés en Europe, nous souhaitons contribuer à l'intelligence collective face au risque cyber.

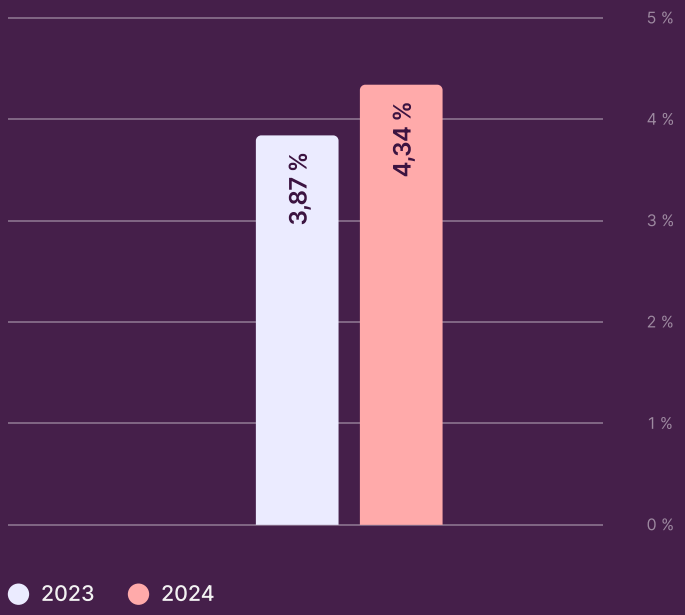
Cette démarche, aussi modeste soit-elle, vise à tracer un chemin : celui d'une transparence accrue, d'une mutualisation des connaissances et d'une action concertée. C'est en conjuguant nos efforts que nous pourrons espérer protéger notre capacité à vivre, travailler et innover dans un monde numérique de plus en plus complexe et incertain.

Vue d'ensemble de l'année 2024

En 2024, la fréquence des sinistres* sur notre portefeuille d'assurés s'est établie à 4,34 %, une augmentation mineure par rapport à l'année précédente, qui traduit une certaine stabilité globale. Cependant, la décomposition de ces attaques révèle une évolution notable des menaces, témoignant des changements dans leur nature et leurs modes opératoires d'une année à l'autre.

Figure 1.1

Fréquence des sinistres déclarés



*Donnée basée sur les sinistres déclarés entre le 1er janvier 2024 et le 31 décembre 2024 en France, Allemagne, Autriche, Monaco.
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.
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.

Fréquence des sinistres déclarés par type d'évènement

Figure 1.2.a

Fréquence des sinistres de type ransomware

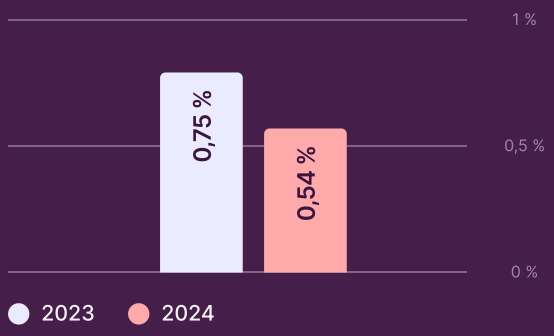


Figure 1.2.b

Fréquence des sinistres de type fraude

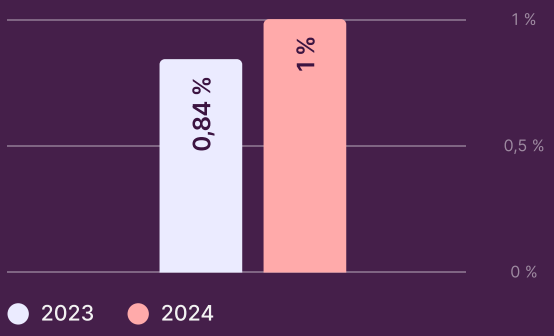


Figure 1.2.c

Fréquence des sinistres de type compromission de messagerie

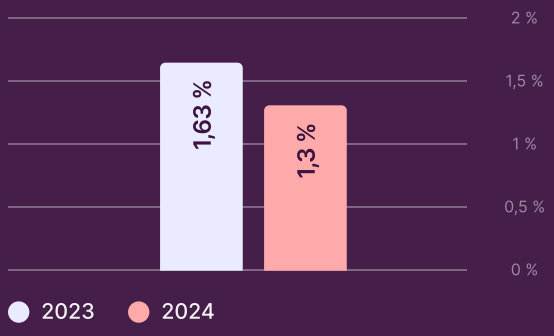


Figure 1.2.d

Fréquence des sinistres de type compromission d'un actif interne

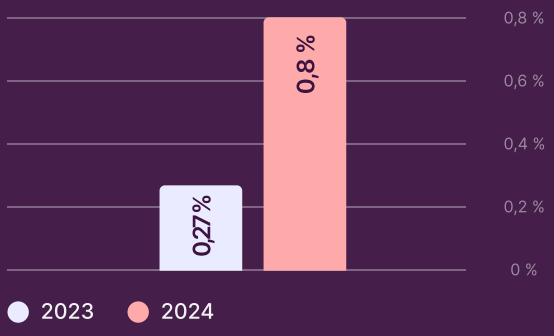


Figure 1.2.e

Fréquence des sinistres de type compromission d'actifs exposés sur Internet

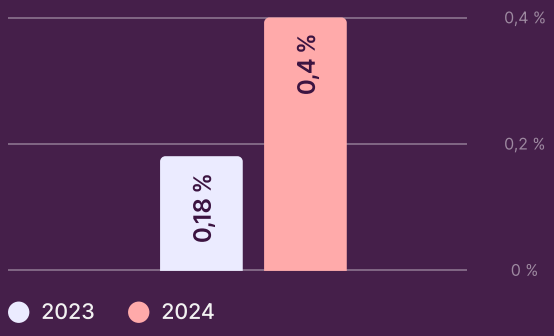


Figure 1.2.f

Fréquences des autres types de sinistres

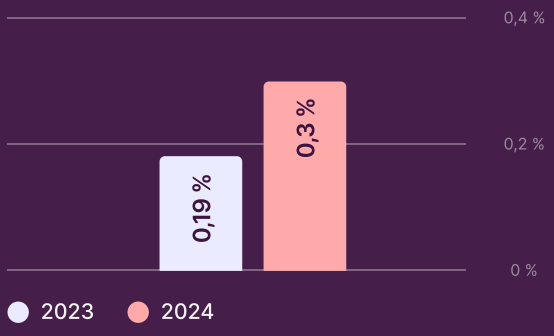
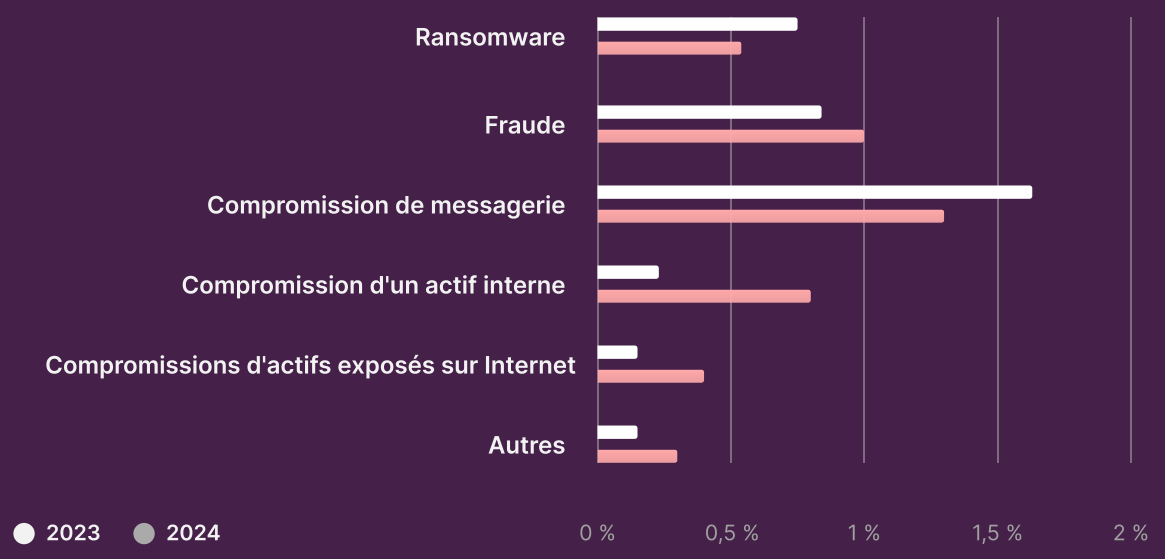


Figure 1.2 Fréquence des sinistres déclarés par type d'évènement



Définition de chaque catégorie :

Ransomware
Logiciel malveillant qui chiffre les données d'un système d'information et exige une rançon pour les déchiffrer, aussi appelé rançongiciel.

Fraude
Réalisation d'un détournement de fonds suite à une intrusion via une compromission de messagerie, un site internet ou un actif ou suite à une ingénierie sociale.

Compromission de messagerie
Accès non autorisé à des comptes de messagerie qui n'a pas abouti à une fraude ou à un ransomware.

Compromission d'un actif interne
Infection par un logiciel malveillant ciblant des systèmes internes pour voler, altérer ou détruire des données.

Compromissions d'actifs exposés sur Internet
Compromission de systèmes ou applications accessibles via Internet, souvent par exploitation de vulnérabilités.

Une année marquée par les manifestations du potentiel systémique du risque cyber

2024 a illustré plus que jamais auparavant à quel point notre dépendance à certaines technologies créait une menace systémique à l'échelle mondiale. En juillet 2024, l'incident CrowdStrike a révélé le potentiel systémique du risque cyber lorsqu'un bug a généré le redémarrage et blocage de nombreux systèmes Windows à l'échelle mondiale. Même s'il ne s'agissait pas d'une cyberattaque, ce dysfonctionnement a affecté des millions d'organisations dans le monde entier, perturbant leurs opérations. L'ampleur de l'incident a mis en évidence à quel point une défaillance technique dans une infrastructure centrale peut avoir des répercussions massives sur des écosystèmes entiers. Cet épisode souligne la dépendance accrue aux technologies, il rappelle que le risque cyber dépasse les seules menaces humaines et inclut aussi les erreurs techniques systémiques.

Exemple de moindre ampleur mais tout aussi révélateur du caractère systémique du risque cyber, la cyberattaque contre l'ESN Axido en juin 2024 en est une parfaite illustration. Dépassant l'entreprise ciblée, elle a également affecté ses clients et partenaires, dont elle gère les infrastructures IT. Victime d'une attaque par ransomware, Axido a subi les effets directs du chiffrement d'une partie de ses systèmes et a dû, en parallèle, isoler l'ensemble de ses systèmes d'information pour protéger ses clients.

Pour bon nombre d'organisations clientes, Axido représentait un maillon essentiel de leur chaîne d'approvisionnement numérique, ce qui a généré un effet domino : l'indisponibilité des services et infrastructures d'Axido rendant à leur tour les services de leurs clients indisponibles et incapables d'assurer leurs fonctions et métiers, aussi critiques soient-ils.

Étude de cas

En 2024, Axido a été la cible d'une attaque par ransomware ayant contraint l'entreprise à couper l'ensemble de son système d'information, impactant ainsi l'ensemble de ses clients pendant près de deux semaines. Pendant cette période, les entreprises dépendantes ont dû fonctionner en mode dégradé, subissant des pertes de données critiques et des interruptions de service prolongées.

Notre CERT-Stoïk a accompagné trois entreprises assurées touchées par cet incident. Pour l'une d'entre elles, l'impact a été particulièrement sévère, car l'ensemble de son infrastructure numérique était géré par Axido. La perte de données et les délais nécessaires pour réimporter celles-ci ont engendré plusieurs semaines de perturbations, entraînant des coûts significatifs. Les deux autres assurés, moins dépendants, ont subi des conséquences plus limitées, mais non négligeables. Ce cas met en lumière la dépendance des entreprises aux fournisseurs tiers et les effets domino qu'une cyberattaque sur un prestataire peut avoir sur un large écosystème. Il souligne également la nécessité pour les entreprises de diversifier leurs fournisseurs, de s'assurer de leur résilience et de renforcer leurs plans de continuité d'activité pour réduire leur exposition au risque systémique.

Par ailleurs, une seule vulnérabilité sur une seule technologie peut mettre à mal des milliers d'organisations si elle est exploitée efficacement par un groupe malveillant. Entre la détection et la résolution de ces failles, une fenêtre de vulnérabilité persiste, exposant les entreprises à des attaques ou à des dysfonctionnements.

Plusieurs événements de ce type se sont produits durant les dernières années : Log4Shell en 2021 et ESXiargs en 2023. En 2024, trois vulnérabilités "zero-day" notables ont eu un impact significatif :

- **Fortinet FortiOS**
  La vulnérabilité CVE-2024-21762, activement exploitée, permettait à un attaquant non authentifié d'exécuter du code arbitraire à distance. Cette faille a compromis des milliers d'appareils, exposant des données sensibles telles que des adresses IP et des configurations d'équipements.
- **OpenSSH**
  La vulnérabilité CVE-2024-6387, surnommée "RegreSSHion", permettait à un attaquant non authentifié d'exécuter du code arbitraire à distance avec des privilèges root. Cette faille affectait les versions 8.5p1 à 9.7p1 d'OpenSSH.
- **Ivanti / Pulse Connect Secure**
  La vulnérabilité CVE-2024-22024, la première d'une longue lignée chez Ivanti, découverte en février 2024, permettait à un attaquant non authentifié d'exécuter du code arbitraire à distance sur les passerelles VPN Pulse Connect Secure. Exploitée activement, cette faille a compromis de nombreuses organisations, exposant des données sensibles et permettant des accès non autorisés à des réseaux internes.

Ces vulnérabilités illustrent le potentiel destructeur des failles techniques à l'échelle mondiale. **Nous avons accompagné plusieurs milliers de nos assurés dans la gestion proactive de ces vulnérabilités pour y faire face** en les notifiant des vulnérabilités détectées sur leur système d'information dès l'annonce ou la découverte de la faille par nos équipes et en apportant un accompagnement personnalisé pour la mise en place de correctifs ou de mesures de contournement le plus rapidement possible. Lors de la souscription, nous veillons à identifier les hébergeurs utilisés par nos assurés afin de diversifier les profils technologiques de notre portefeuille. Ainsi, nous pouvons contrôler la dépendance de nos assurés à certains fournisseurs ou solutions, et adapter notre veille pour être proactif en cas de vulnérabilité identifiée.

99 ↘

Notre dépendance croissante aux technologies interconnectées exacerbe un risque systémique d'une ampleur inédite. Une seule faille peut provoquer des répercussions majeures à l'échelle mondiale. L'année 2024 a une fois de plus démontré que les enjeux cyber transcendent les frontières, rendant indispensable une approche globale et internationale pour y faire face.

Alexandre Andreini
Directeur des risques et cofondateur de Stoïk

Une fin d'année marquée par une recrudescence des ransomwares et des exfiltrations de données

Le calme relatif observé au début de l'année 2024 en matière d'attaques par ransomware s'explique principalement par le démantèlement du groupe cybercriminel LockBit. Le 20 février 2024, une opération internationale baptisée "Opération Cronos", impliquant notamment le FBI, l'ANSSI, la Gendarmerie nationale et Europol, a permis de démanteler une partie significative de l'infrastructure de LockBit, considéré comme l'un des groupes cybercriminels les plus actifs au monde. Par ailleurs, le groupe REvil, connu pour exiger des rançons particulièrement élevées, avait déjà été démantelé en janvier 2022. Cette opération avait conduit à l'arrestation de 14 membres présumés du groupe, réduisant ainsi leur activité.

Suite à ces démantèlements, le paysage des ransomwares a été marqué par une diminution des attaques sophistiquées menées par des groupes organisés. Cependant, des cybercriminels isolés ont continué à lancer des attaques moins élaborées, souvent accompagnées de demandes de rançon moins élevées. Cette fragmentation a contribué à une baisse générale de l'intensité des attaques par ransomware au début de l'année 2024.

Durant l'été, la tenue des Jeux Olympiques et Paralympiques de Paris 2024 a suscité de nombreuses inquiétudes, notamment en matière de cybersécurité. Si aucun incident majeur n'a été signalé, les cybercriminels ont exploité l'engouement autour de l'événement pour diffuser massivement des emails de phishing, souvent générés à l'aide d'intelligences artificielles, imitant fidèlement les communications officielles. En proposant des billets à des tarifs attractifs, ils ont joué sur l'appât du gain, les émotions et la rareté de cet événement exceptionnel, incitant les victimes à divulguer des informations personnelles.

Nous avons également observé un taux de réussite particulièrement élevé des emails de phishing aux couleurs des Jeux que nous avons envoyés à nos assurés durant cette période :

45%

de nos faux emails de phishing sur le modèle des Jeux ont été ouverts chez les collaborateurs de nos assurés.

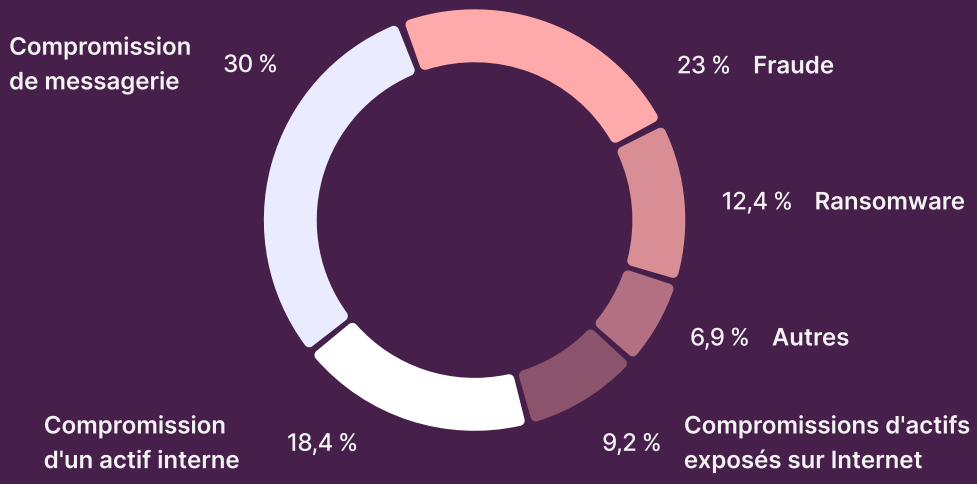
33%

de ceux ayant ouvert l'email ont communiqué leurs données personnelles contre 10% sur les autres modèles.

Ainsi, on estime que des milliers de données ont été dérobées durant les Jeux, sans impact direct sur leur déroulement. Comme anticipé, les conséquences se sont manifestées ultérieurement :

- **À partir de mi-septembre, une augmentation notable des attaques par ransomware avec des impacts significatifs a été observée.**
- **Plusieurs entreprises européennes, telles que Auchan, Free, Boulanger, Cultura, Le Point, Direct Assurance, SFR, Mediboard et Norauto en France, Volkswagen, Medion, AEP GmbH, Thyssenkrupp, KaDeWe et Varta en Allemagne, CNMC (Commission nationale des marchés et de la concurrence) et INIA (Institut national de recherche et de technologie agronomique et alimentaire) en Espagne ont été victimes de fuites de données, largement médiatisées.**

Figure 1.3 Répartition des sinistres déclarés par type d'évènement



Le ransomware : le type de sinistre le plus redouté

Le ransomware, bien qu'il ne soit pas le type de sinistre le plus fréquent, demeure une priorité majeure pour les assureurs en raison de son impact financier disproportionné. En effet, ces attaques entraînent des pertes d'exploitation significatives pour les entreprises touchées, tout en générant des coûts élevés liés à la réponse aux incidents, tels que la gestion de crise et la restauration des systèmes. Cette combinaison en fait une menace particulièrement redoutée dans le paysage des risques cyber.

Corrélation entre l'impact financier et la durée de réponse aux incidents

Le chiffrement complet des systèmes d'information peut provoquer un arrêt brutal de l'activité, ce qui entraîne des pertes d'exploitation significatives et des coûts élevés pour relancer l'activité. En comparaison, les compromissions de boîtes mail, beaucoup plus fréquentes, engendrent des pertes plus limitées, car elles entraînent rarement un arrêt total des activités.

Nouveauté unique en Europe : l'assistance garantie

Nous souhaitons que nos assurés sachent qu'ils pourront toujours compter sur Stoïk, et nous savons à quel point il peut être désagréable de solliciter l'assistance cyber sans savoir si elle sera prise en charge par l'assureur.

Avec Stoïk, il n'y a jamais de déchéance de garantie pour la réponse aux incidents et celle-ci sera toujours prise en charge. Parce qu'une cyberattaque est avant tout un drame, nos assurés bénéficient de notre soutien en toute circonstance.

stoïk

Corrélation entre configuration des sauvegardes et l'impact des sinistres

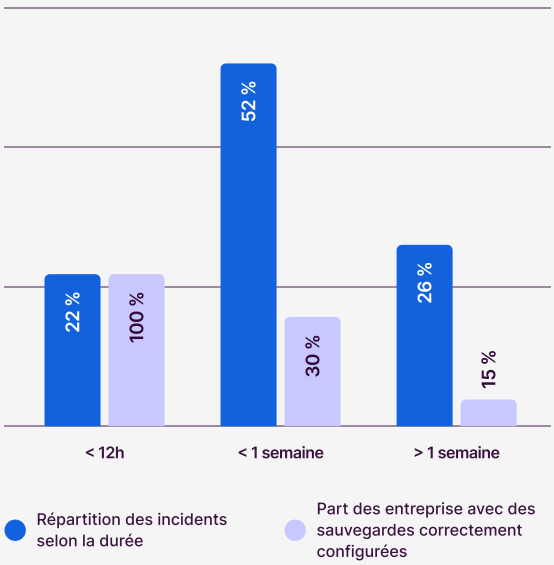
Cette année, nous observons que dans **74%** des cas de ransomwares, nos équipes ont réussi à relancer l'activité de l'entreprise en moins d'une semaine dont **22%** des cas en moins de 12h. Comme l'an passé, nous observons une corrélation marquée entre la présence de sauvegardes correctement configurées* et la durée de réponse aux incidents. Ainsi, nous avons constaté que dans **100%** des cas de gestion du ransomware en moins de 12h, l'entreprise disposait de sauvegardes restaurables (copie de sauvegarde immuable ou complètement déconnectée de tout réseau informatique).

Dans toutes les situations dans lesquelles la durée a excédé une semaine, à l'inverse, les sauvegardes de l'assuré n'avaient soit pas été correctement configurées, soit elles l'étaient mais les équipes informatiques n'étaient pas en capacité de restaurer l'ensemble des fichiers nécessaires au redémarrage du système, un défi encore trop souvent sous-estimé par les entreprises de taille intermédiaire.

Encore trop d'entreprises pensent avoir des sauvegardes correctement configurées et restaurables alors qu'elles ne sont en capacité de restaurer qu'une partie des fichiers de sauvegardes. Concrètement, si restaurer un fichier ou une machine virtuelle est rapide, restaurer tout un serveur de fichiers ou toutes les machines virtuelles de tous les hyperviseurs prend généralement quelques heures en plus que ce qui est prévu dans le PCA. Nous continuons d'encourager vivement nos assurés de réaliser deux tests par an de restauration de sauvegarde intégrale des fichiers pour être en capacité de redémarrer rapidement après un ransomware.

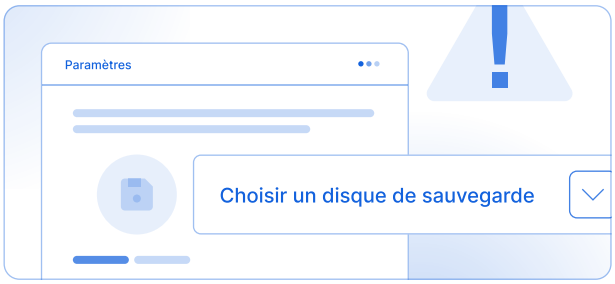
Figure 2

Durée de réponse à incident par ransomware



Étude de cas

Début octobre 2024, une entreprise assurée en Allemagne et spécialisée dans l'intégration d'ERP fait face à un ransomware qui chiffre tout son parc informatique. À cela s'ajoute l'absence de l'authentification multifacteur qui a permis à l'attaquant de se propager très rapidement vers les environnements infogérés d'une quarantaine de ses clients. Le dirigeant de l'entreprise est persuadé de disposer de sauvegardes correctement configurées, ce qui ne s'avère finalement pas exact. Notre CERT-Stoïk fait appel à Databack, spécialiste de la récupération de données, et relance partiellement le système d'information au bout de 3 semaines seulement. Pendant ce laps de temps, l'assuré n'a pas été en capacité de livrer ses services à ses 40 clients qui, pour certains, n'ont pas pu clôturer leurs comptes de fin d'année à temps.



* Nous considérons que les sauvegardes sont correctement configurées, lorsqu'elles sont disponibles sur des supports déconnectés du reste du SI et restaurables sans difficulté car elles étaient testées et que le catalogue de sauvegarde était également sauvegardé.

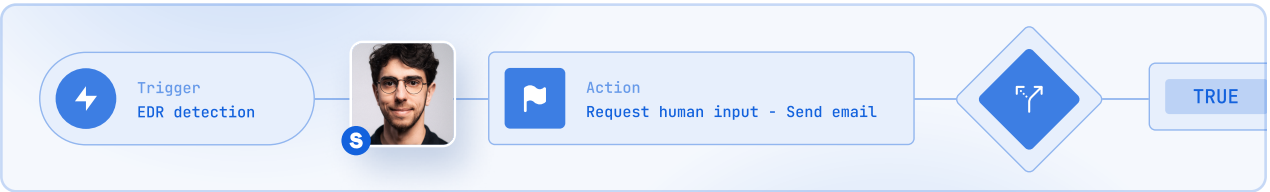
Corrélation entre présence d'un EDR managé et réduction de la fréquence des sinistres

La présence d'un EDR (Endpoint Detection and Response) managé est directement corrélée à une réduction significative de la fréquence des ransomware, grâce à ses capacités de détection proactive, d'isolation rapide et d'investigation avancée. Aucun sinistre par ransomware n'a été déclaré sur les entreprises assurées qui ont installé la solution d'EDR managé proposée et déployée par Stoïk depuis mai 2024.

L'EDR managé de Stoïk c'est :

672
alertes traitées entre juillet et décembre 2024

0
ransomware n'a été déclenché sur les périmètres couverts par notre MDR



L'EDR managé pour réduire la durée des sinistres

Le **CERT-Stoïk** déploie systématiquement un EDR chez les assurés victimes de ransomware qui n'en disposent pas déjà. La solution déployée permet alors de :

- **Protéger les systèmes qui ne sont pas encore touchés et limiter la propagation de l'attaquant.**
- **Détecter les machines sur lesquelles il y a des comportements suspects pour intervenir rapidement et de manière ciblée.**
- **Nettoyer les systèmes compromis et s'assurer que l'attaquant a bien été exclu du système avant de procéder à la restauration des sauvegardes et de redémarrer les services de l'entreprise.**

> *L'EDR est un outil clé pour faire face aux ransomwares : il nous permet de relancer rapidement et en toute confiance les services informatiques de nos assurés tout en limitant les risques. En cas de nouvelle tentative d'intrusion, il nous alerte immédiatement et isole le réseau pour prévenir toute propagation.*

Jannik Stuckstätte
CERT analyst chez Stoïk

La fraude au faux virement

En 2024, le montant détourné chez nos assurés ayant déclaré un sinistre de ce type s'est élevé en moyenne à 54 876 € et la médiane est de 15 727 €.

Parmi tous les cas de fraude aux virements notifiés à notre CERT, nous distinguons trois types de situations :

37,1% Dans 37,1 % des cas, la fraude est réalisée **sans qu'il y ait intrusion dans le système d'information de l'assuré**, par le simple moyen d'un email ou d'un appel téléphonique externe frauduleux.

28,6% Dans 28,6 % des cas, la fraude est réalisée **suite à la compromission du système d'information de l'assuré lui-même**.

34,3% Dans 34,2 % des cas, la fraude est réalisée **suite à la compromission du système informatique d'un tiers** (par exemple, le cabinet comptable de l'assuré).

La fraude au virement est un enjeu majeur qui révèle la vulnérabilité des systèmes d'information, qu'ils appartiennent à nos assurés ou à leurs partenaires. Les chiffres de 2024 montrent l'importance de rester vigilants face à des méthodes d'attaque toujours plus sophistiquées, tout en rappelant qu'un simple email ou un appel peut suffire à détourner des sommes considérables.

Madeleine Motte
Responsable du département gestion de sinistres chez Stoïk

Les secteurs d'activités dans le viseur

Le secteur de l'hôtellerie
Nous avons observé des compromissions des comptes Booking où l'attaquant avait pu accéder au compte de l'établissement et changer les coordonnées bancaires des réservations par les siennes.

Le secteur du commerce de gros
Ces entités manipulent beaucoup de factures au quotidien. Les fraudes arrivent le plus souvent via des mails frauduleux contenant des factures qui ressemblent à s'y méprendre à ceux des prestataires ou via la compromission de la messagerie qui permet d'intervertir les RIB.

Nos recommandations pour faire face à la fraude

1/ Faire face aux emails frauduleux

Il est de plus en plus difficile d'anticiper une tentative de fraude au virement. Les attaquants peuvent désormais créer des emails d'apparence professionnelle, exempts de fautes et imitant avec une précision troublante les communications officielles d'entreprises ou d'institutions. Pour faire face à ces emails plus élaborés, il est nécessaire de renforcer les techniques de sensibilisation avec toujours ces trois réflexes à adopter :

Mettre en place l'authentification multifacteur (MFA) sur les boîtes de messagerie pour minimiser le risque d'intrusion dans la messagerie.

Mettre en place une campagne de sensibilisation au phishing auprès de tous les employés pour s'entraîner à reconnaître les emails frauduleux.

Mettre en place un processus de double validation des paiements au-delà d'un certain montant pour éviter les fraudes d'un montant trop élevé.

Se doter de capacités permettant la détection de tentatives de fraude.
Chez Stoïk, nous développons dans notre technologie XDR (eXtended Detection & Reponse) des scénarios de détection d'emails frauduleux sur la base des informations collectées au sein des messageries SaaS de nos assurés (e.g. demande de changement de RIB, ajout d'une nouvelle adresse email externe dans une boucle de mails existante, etc.).

2/ Récupération des montants détournés

Si certaines entreprises arrivent à récupérer les montants détournés, ce n'est pas parce que l'attaquant a rendu l'argent, mais parce que l'entreprise a pu alerter sa banque rapidement et bloquer le virement. Ici aussi, la corrélation entre réactivité de l'assuré et réduction de la sévérité d'une attaque est frappante.

Étude de cas

Pas besoin d'IA pour réaliser une fraude ! Un simple appel téléphonique pour relancer une facture en se faisant passer pour un prestataire peut aboutir. Le directeur financier d'une entreprise assurée s'est même fait piéger par un message vocal reçu sur son Whatsapp. Le tout sans utilisation de l'IA, sans deepfake ni modification de la voix.

La compromission des boîtes mail

La compromission d'une boîte mail peut mener à trois types de sinistres :

Le vol de données : celles qui sont accessibles dans la boîte mail.

Le détournement de fonds (fraude) via un changement de RIB, comme vu précédemment.

Le rebond : l'attaquant se sert de la messagerie compromise pour obtenir des informations ou droits d'accès supplémentaires, et amplifier son pouvoir de nuisance jusqu'à déployer un ransomware. S'il n'en est pas capable lui-même, il pourra aussi revendre ses accès à des attaquants plus aguerris.

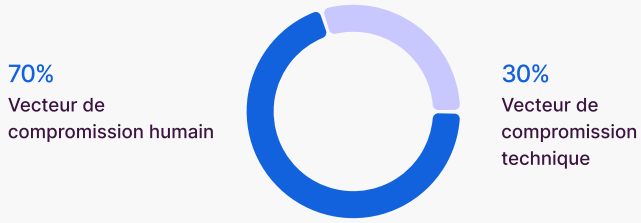
Dans notre analyse, nous observons que la compromission de boîte mail est le 1er vecteur d'intrusion chez nos assurés.

1er vecteur d'intrusion

Nous distinguons deux grandes catégories de vecteurs de compromission : les vecteurs humains, principalement liés au phishing et à l'ingénierie sociale, et les vecteurs techniques, incluant les vulnérabilités des systèmes exposés sur Internet et les défauts de configuration des services d'accès à distance. Parmi les sinistres observés dans notre portefeuille d'assurés, la répartition est la suivante :

Figure 3

Vecteurs de compromission



Cette année, nous constatons une légère progression des compromissions par vecteurs techniques, attribuable à une explosion du nombre de vulnérabilités publiées. Cette augmentation complique considérablement la gestion des correctifs pour les victimes, en raison de la fréquence élevée des mises à jour nécessaires et du rythme soutenu des patchs à appliquer.

Cette situation souligne l'importance cruciale d'une stratégie proactive en gestion des vulnérabilités et en sensibilisation humaine pour limiter les risques.

Il est intéressant de comparer nos chiffres à ceux du dernier rapport de l'InterCERT France* qui observe "un équilibre presque parfait entre ces deux canaux d'attaque, soulignant que les attaques ciblent autant les utilisateurs que les systèmes techniques." Aussi, la différence marquée entre nos deux rapports s'explique notamment par la présence de notre scan externe**, actif en continu chez tous nos assurés. Cet outil leur permet d'être notifié en cas de nouvelle vulnérabilité détectée et d'être accompagné par notre équipe d'experts en cybersécurité dans la résolution des failles, des plus mineures au plus critiques. Ainsi, les compromissions via un canal technique sont moins nombreuses chez nos assurés.

÷2

La fréquence des incidents est divisée par deux chez nos assurés qui ont activé les outils de la plateforme **Stoïk Protect.**

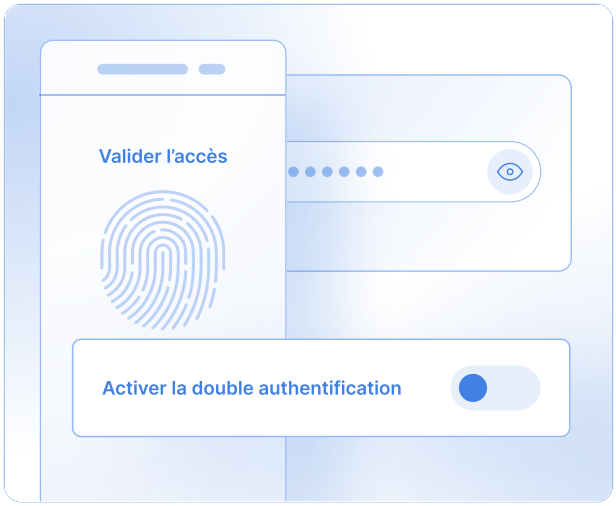
Analyse des compromissions de boîte mail

En 2024, **95 %** des compromissions de boîtes aux lettres électroniques traitées concernaient des environnements Microsoft 365 (M365), tandis qu'aucun cas n'a été recensé sur des environnements Google Workspace ou des messageries on-premises. Les **5 %** restants concernaient des messageries en ligne telles qu'OVH ou Orange/Wanadoo.
Cependant, ces chiffres doivent être analysés avec précaution : la majorité des organisations assurées utilisent M365, alors que les solutions on-premises deviennent rares.

Un point crucial est que dans **100 %** des cas de compromission, l'authentification multifacteur (MFA) n'était pas déployée, voire pas déployable, notamment dans certains environnements comme Orange.

En outre, la réactivité est essentielle pour les investigations sur M365, car les logs utiles ne sont disponibles que durant 7 jours. Grâce à notre CERT internalisé, nous pouvons intervenir sans délai dès l'alerte de la victime. À l'inverse, les interventions impliquant des fournisseurs IT externes s'avèrent souvent complexes et chronophages, faute de SLA ou de clauses d'incident/crise adéquates dans les contrats.

Enfin, les compromissions sont souvent détectées plusieurs semaines ou mois après leur occurrence, laissant aux attaquants le temps de subtiliser des données, créer des comptes malveillants avec des noms de domaine similaires, et perpétrer des attaques plus ou moins sophistiquées d'usurpation d'identité sans éveiller les soupçons immédiats de leurs victimes.



* https://www.intercert-france.fr/rapport-dincidentologie-2024/
** Outils de la plateforme Stoïk Protect

Nos recommandations pour protéger les boîtes mail

Mettre en place les outils de la plateforme Stoïk Protect :

Scan externe

Utiliser le scan externe pour recevoir les alertes en cas de nouvelle vulnérabilité détectée sur les serveurs de messagerie exposés sur Internet.

Simulation de phishing

Activer le module de simulation de phishing pour renforcer la sensibilisation des collaborateurs face aux emails frauduleux.

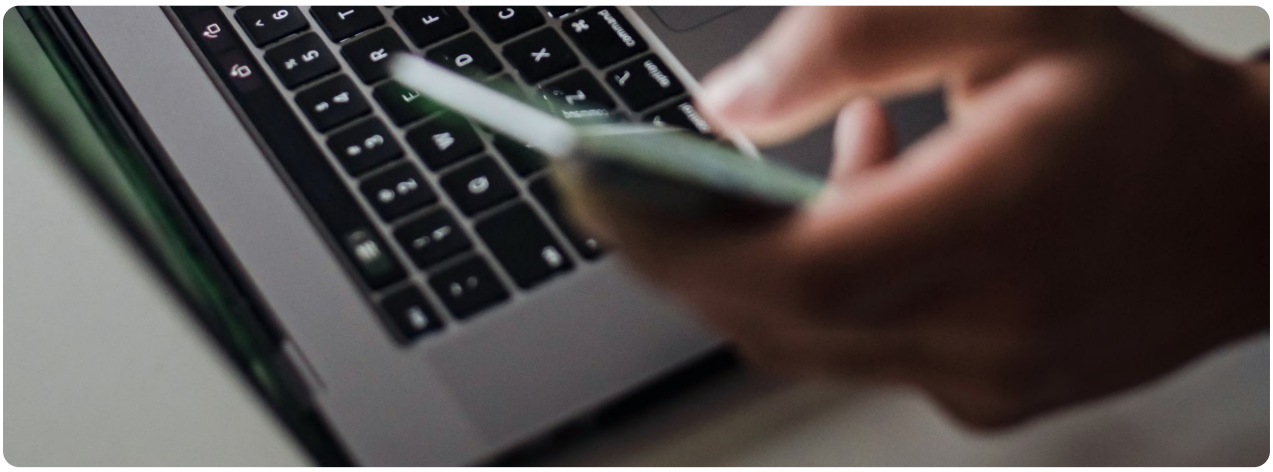
Scan de Cloud

Pour les messageries hébergées sur M365 ou Google Workspace, **activer le scan de services Cloud** (couvrant également les technologies AWS) afin d'évaluer quotidiennement la configuration globale de ces services.

Nos conseils supplémentaires :

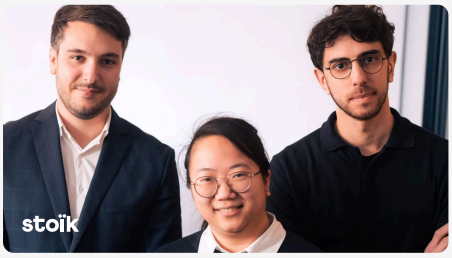
Mettre en place un système de double validation pour tout changement d'information bancaire ou paiement à partir d'un certain seuil.

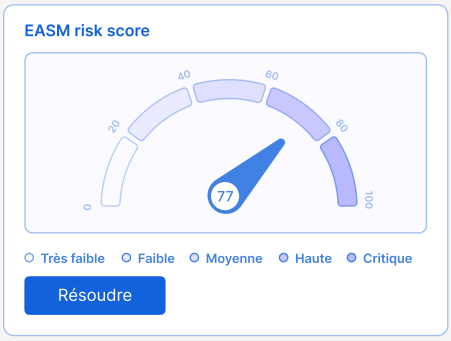
Mettre en place un puits de logs (journaux) afin de conserver les traces utiles et faciliter l'investigation suite à une intrusion.



L'assurance active s'adapte continuellement au risque cyber

Chez Stoïk, nous avons conçu une offre innovante pour répondre aux défis croissants du risque cyber. En combinant technologie de pointe, expertise humaine et adaptabilité, nous apportons une protection complète et proactive à nos assurés.





La technologie et l'expertise cyber au service de l'assurance

Notre plateforme **Stoïk Protect** joue un rôle central dans la prévention des risques. Grâce à des outils automatisés comme le scan externe, la simulation de phishing et l'audit des configurations Cloud et Active Directory, nos assurés sont en capacité d'identifier et de corriger les vulnérabilités avant qu'elles ne soient exploitées. Cette prévention active contribue à diviser par deux la sinistralité cyber chez nos assurés.

Par ailleurs, notre solution **Stoïk MDR** offre une surveillance 24/7 des systèmes d'information avec une réponse immédiate en cas d'incident. Accessible aux entreprises de toute taille, elle associe la technologie EDR des meilleures solutions du marché et l'expertise cyber du CERT-Stoïk pour garantir une remédiation rapide et efficace en cas d'alerte.

Notre **CERT-Stoïk**, composé d'ingénieurs et d'experts cyber 100% internalisés, est disponible 24h/24 et 7j/7 pour intervenir dès les premières minutes d'un incident. Cette proximité garantit une reprise d'activité rapide et sécurisée : comme nous l'avons vu dans ce rapport, 74% de nos assurés relancent leur activité en moins d'une semaine après une attaque.

Un parfait alignement des intérêts

L'assuré, son courtier et Stoïk partagent un même objectif : éviter qu'un incident ne survienne. Ainsi :

- L'accès à la plateforme est i**nclus gratuitement** avec le produit d'assurance.
- La franchise sur la couverture d'assurance **est réduite de 25%** dès lors que l'assuré a implémenté les outils à sa disposition.
- **Nos experts sont en permanence à disposition** pour aider les assurés à corriger leurs vulnérabilités au plus vite.
- En cas d'alerte critique, nos experts interviennent de manière personnalisée **24h/24 7j/7** pour aider l'entreprise à y répondre.

> *La plateforme Stoïk Protect nous permet de monitorer notre risque cyber au quotidien. Je mets un point d'honneur à traiter les vulnérabilités dès leur découverte par le scan externe. On utilise aussi l'outil de simulation de phishing et on a remarqué une forte diminution des identifiants soumis.*

Dimitri Longo
DSI de Ligerio, Assuré Stoïk

En 2025, la cybersécurité s'impose plus que jamais comme un effort collectif

Par Vincent Nguyen
Directeur cybersécurité chez Stoïk

L'année 2025 marque une étape cruciale pour la cybersécurité, avec une montée des risques systémiques, un cadre réglementaire renforcé et une évolution rapide des technologies d'attaque et de défense. **Les chaînes d'approvisionnement et les infogérants resteront des cibles privilégiées** des cybercriminels, rendant indispensable une collaboration renforcée entre entreprises privées, secteur public et associations spécialisées. Le partage structuré des informations sur les menaces sera un levier stratégique pour une réponse collective efficace.

Les entreprises devront intégrer la cybersécurité comme un enjeu stratégique à haut niveau. Le contexte géopolitique instable influencera les menaces, ciblant certains secteurs et régions. Par ailleurs, les réglementations comme NIS 2 et DORA exigeront des niveaux de maturité accrus en cybersécurité, transformant la conformité en avantage concurrentiel.

Les infrastructures *legacy*, notamment dans les environnements OT, resteront un défi critique. Face à leur vulnérabilité croissante, les organisations devront allier modernisation et isolation des systèmes critiques tout en maintenant la continuité opérationnelle. La gestion des vulnérabilités sera une priorité, avec l'exploitation croissante de failles comme le témoigne déjà le début de l'année avec les vulnérabilités sur Ivanti et Fortinet.

L'intelligence artificielle jouera un rôle central des deux côtés du cyberconflit : si elle permettra d'accélérer les attaques, elle restera davantage un outil d'optimisation qu'un vecteur d'attaque principal. En défense, son adoption massive renforcera la cybersécurité tout en étendant la surface d'attaque.

La cybersécurité s'impose comme un effort collectif, impliquant des **exercices communs et des simulations de crise pour améliorer la préparation**. Dans cette dynamique, les cyberranges deviendront des outils clés. Cependant, la surcharge des équipes cyber, exacerbée par les évènements de 2024 (Jeux Olympiques, élections, tensions géopolitiques), nécessitera des mesures de soutien et des ressources adaptées pour assurer leur résilience.

Enfin, après les investissements de 2024, les budgets cybersécurité seront contraints en 2025, obligeant les organisations à prioriser leurs actions en fonction des risques les plus critiques. **L'optimisation des ressources sera essentielle pour maintenir un haut niveau de protection** face à des menaces toujours plus sophistiquées.

www.stoik.com | contact@stoik.io

Prêt à maîtriser le risque cyber ?

N° ORIAS : 24000772

stoïk