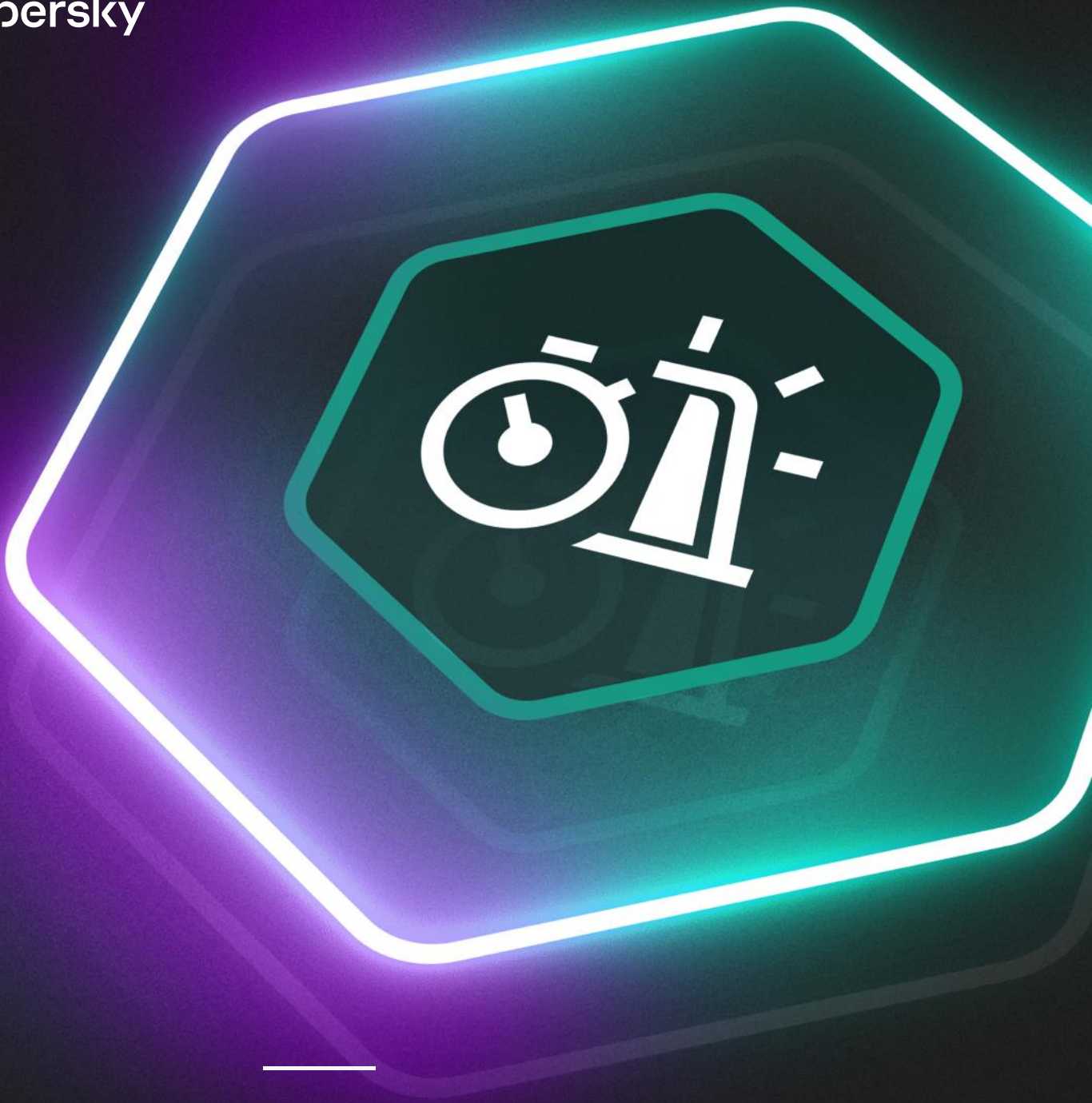
kaspersky



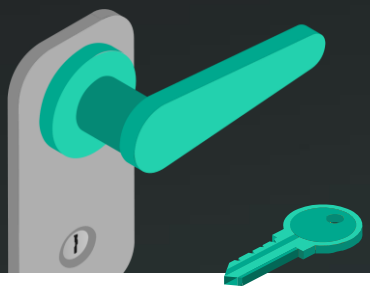
La nature des cyberincidents

Basé sur les enquêtes des attaques informatiques menées par Kaspersky Global Emergency Response Team.

2022

Comment les attaquants ont obtenu un premier accès

2019 2020 2021



Exploitation des applications destinées au public

37,0 % 31,5 % 53,6 %

Comptes compromis

13,0 % 31,6 % 17,9 %

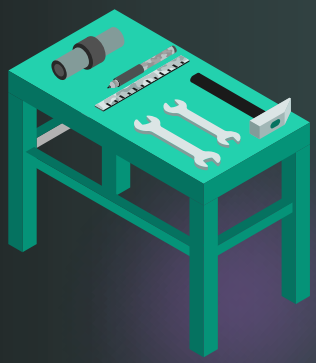
Emails malveillants

30,0 % 23,7 % 14,3 %

Les outils de prédilection des pirates informatiques

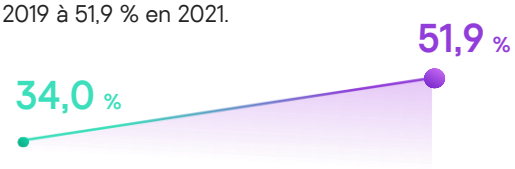
La tendance de l'utilisation des fichiers binaires LOLBins (Living Off The Land Binaries) persiste. PowerShell reste l'un des outils les plus populaires parmi les pirates informatiques utilisé durant la phase de la latéralisation.

PsExec, Mimikatz et Cobalt Strike restent les d'outils de piratage informatique les plus populaires de ces dernières années. En 2021, ces outils ont été impliqués dans respectivement 10,8 %, 9,7 % et 9,7 % de toutes les attaques.



Impact des attaques

Pendant trois années consécutives, l'attaque par chiffrement des fichiers a été le problème numéro un de nos clients. Le nombre d'entreprises ayant fait face à des rançonneurs dans leur infrastructure est passé de 34 % en 2019 à 51,9 % en 2021.



Principales entités ciblées

Le secteur industriel, les Gouvernements et le secteur de la finance restent les trois principales entités ciblées.

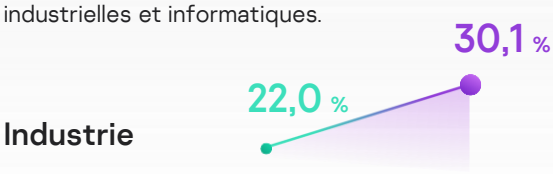
- Industrie
- Gouvernements
- Finance

Les 3 zones géographiques les plus attaquées

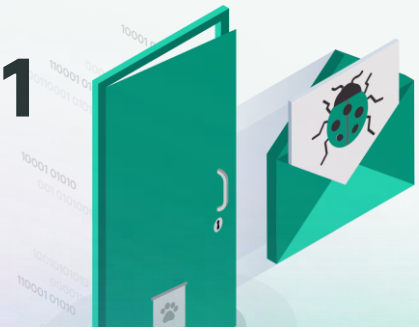
3 zones géographiques sont principalement concernées par la demande des services de Kaspersky Incident Response,

Europe	Arrivée en tête en 2021 avec 30,1 %.
CEI	Première place en 2020
Moyen-Orient	La région n° 1 en 2019

En 2021, nous avons remarqué une croissance importante des demandes de réponse à incidents de la part des entreprises industrielles et informatiques.



Tendances en 2021



Cas de rançongiciels

Répartition des attaques par durée en fonction du vecteur initial

Vecteur d'attaque initial	Heures	Semaines	Mois	Total
Exploitation des applications destinées au public	12,5 %	0,0 %	25,0 %	37,5 %
Emails malveillants	0,0 %	0,0 %	25,0 %	25,0 %
Comptes compromis	12,5 %	12,5 %	12,5 %	37,5 %
Total	25,0 %	12,5 %	62,5 %	100 %

Selon les données de recherche, lors des attaques associées aux rançongiciels, les mêmes méthodes de base similaire à d'autres types d'attaques ont été utilisées pour l'intrusion initiale. L'exploitation de vulnérabilités et de comptes d'utilisateurs compromis en amont de l'attaque a été pratiquée dans **37,5 %** des cas, tandis que l'envoi d'emails malveillant a été utilisé dans un cas sur quatre avec des chiffreurs.

Toutefois, dans un certain nombre d'attaques, l'objectif des pirates informatiques n'était pas l'extorsion ni le chiffrement des données, mais les données de l'entreprise, les données personnelles, la propriété intellectuelle et d'autres informations confidentielles. Il est presque impossible de gérer les dommages causés par ce type d'attaques. Cette situation entraine une perte de réputation ainsi que des sanctions potentielles de la part des régulateurs et des poursuites judiciaires. Tous ces éléments sont utilisés comme une incitation supplémentaire pour faire du chantage.

Nous avons observé une fuite de données dans 10 % des cas impliquant des chiffreurs. De plus, l'utilisation de chiffreurs a parfois pour but de cacher les traces initiales d'une attaque et de compliquer les enquêtes sur les incidents.

En analysant la durée des attaques avec des chiffreurs, on peut conclure qu'une période considérable s'écoule entre la compromission initiale du réseau et la phase finale de l'attaque. Dans **62,5 %** des attaques, les pirates informatiques passent plus d'un mois à l'intérieur du réseau avant de chiffrer les données. Un processus correctement organisé de détection d'attaques et de réponses réduit le temps nécessaire à la détection d'attaquants dans le réseau et à l'élimination des dommages définitifs.

Après l'intrusion initiale, les pirates informatiques utilisent PowerShell pour collecter des données, Mimikatz pour escalader les privilèges, PsExec pour exécuter des commandes à distance ou des frameworks, comme Cobalt Strike, pour toutes les étapes de l'attaque.

Exploitation des vulnérabilités

Dans tous les cas où l'exploitation de vulnérabilités a été utilisée comme vecteur initial, le principal dommage est le chiffrement des données.

La vulnérabilité la plus répandue dans notre ensemble de données est la vulnérabilité CVE-2021-26855 Microsoft Exchange SSRF dans Microsoft Exchange Server qui permet aux pirates informatiques d'envoyer des requêtes HTTP arbitraires et de s'authentifier en tant que serveur Exchange (vulnérabilité utilisée par le groupe Hafnium). Cette vulnérabilité a été exploitée dans 22,7 % des cas.

Bien que les mesures de protection contre ce vecteur d'attaque soient simples (mise à jour de sécurité), l'exploitation des vulnérabilités 1-day est loin devant les autres méthodes d'attaque utilisées pour l'accès initial.

Aperçu des réponses à incident en 2021

Et les recommandations des experts

Vue sur la cybermenace

Les statistiques de réponse à incident se basent sur les investigations de 2021

Vecteur d'attaque initial

1. Mettre en œuvre une politique de mot de passe solide et une authentification multifacteurs
2. Éliminer l'accès public aux ports de gestion
3. Définir une stratégie de tolérance zéro pour la gestion des correctifs ou les mesures de compensation pour les applications destinées au public
4. Assurer une forte sensibilisation des employés à la sécurité

53,6 % Exploitation des applications destinées au public

14,3 % Emails malveillants

17,9 % Comptes compromis

5. Mettre en œuvre des règles de détection des outils d'attaque utilisés par les adversaires
6. Mettre en place une chaine d'outils de sécurité avec des données télémétriques comme celles générées avec les EDR
7. Tester constamment les temps de réaction des opérations de sécurité en mettant en place des exercices offensifs
8. Assurer une sensibilisation élevée des employés à la sécurité

Se latéraliser et exécuter des actions

Dans 39,7 % des cas, des outils légitimes ont été utilisés

9,7 %	9,7 %	8,6 %	10,8 %
Cobalt Strike	Mimikatz	PowerShell	PsExec

Impact

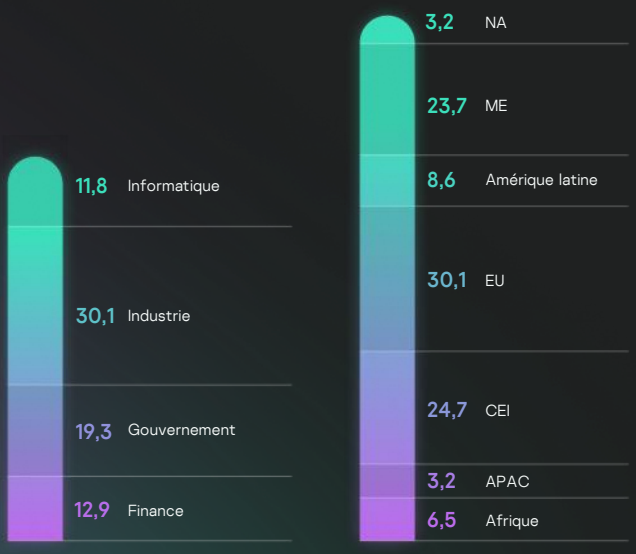
9. Sauvegarder vos données
10. Collaborer avec un partenaire chargé de la gestion des incidents pour traiter les incidents avec des accords de niveau de service rapides
11. Former en permanence votre équipe de réponse aux incidents afin de préserver son expertise et de suivre l'évolution du paysage des menaces
12. Mettre en place des programmes de sécurité stricts pour les applications contenant des données personnelles

16,0 % Fuites de données

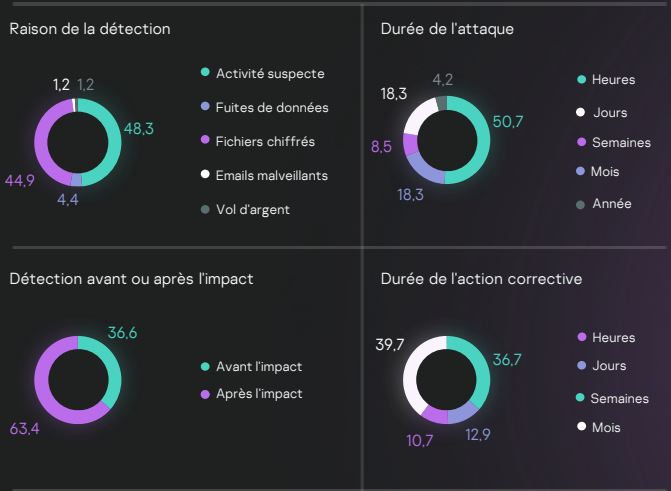
51,9 % Fichiers chiffrés

11,1 % Active Directory compromise

Entités et régions, en %



Vue indicatrice des opérations de sécurité, en %



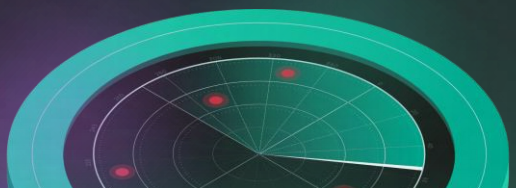
Comprendre le profil des adversaires qui ciblent votre secteur et votre zone géographique afin de hiérarchiser les opérations de sécurité à mettre en œuvre

Introduction

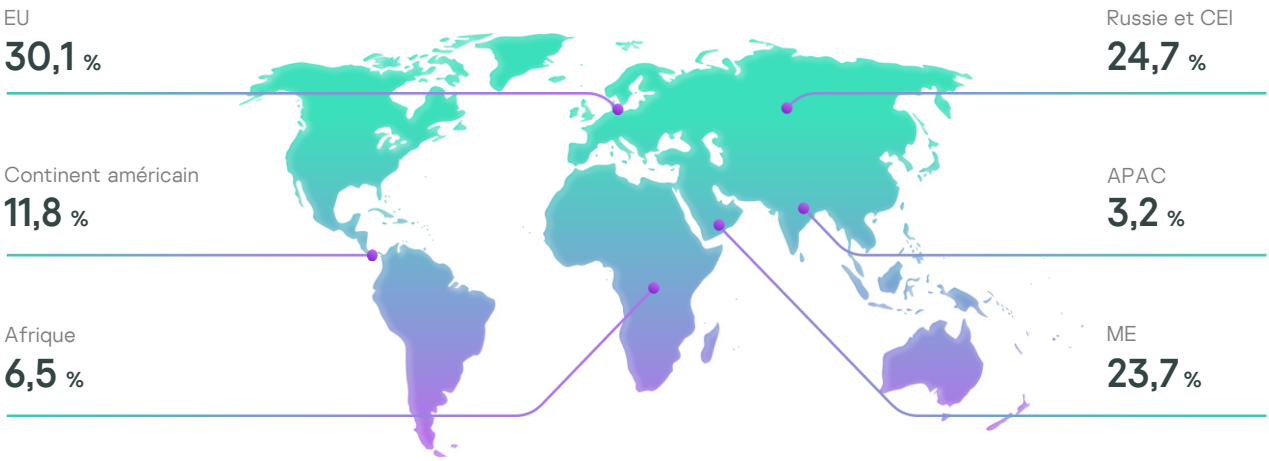
Le Rapport Analytique concernant les Réponses aux Incidents contient des renseignements sur les incidents analysés par le service d'investigation de Kaspersky en 2021. Nous proposons une gamme de services pour aider les entreprises au moment où elles en ont le plus besoin : réponse à incident, investigation numérique et analyse des logiciels malveillants. Les données du rapport sont issues de nos pratiques quotidiennes auprès des entreprises qui font appel à nous pour obtenir une réponse complète aux incidents ou des services spécialisés complémentaires pour leurs équipes de réponse aux incidents[1].

En 2021, bien que les principales tendances en matière de menaces soient restées les mêmes, notre approche du service est passée à une prestation à distance quasi-complète, dans 98 % des cas. Les opérations d'Investigation Numérique et de Réponse à Incident de Kaspersky sont gérées par notre équipe Global Emergency Response Team (GERT)[2] avec des experts en Europe, en Asie, en Amérique du Nord et du Sud, au Moyen-Orient ainsi qu'en Afrique.

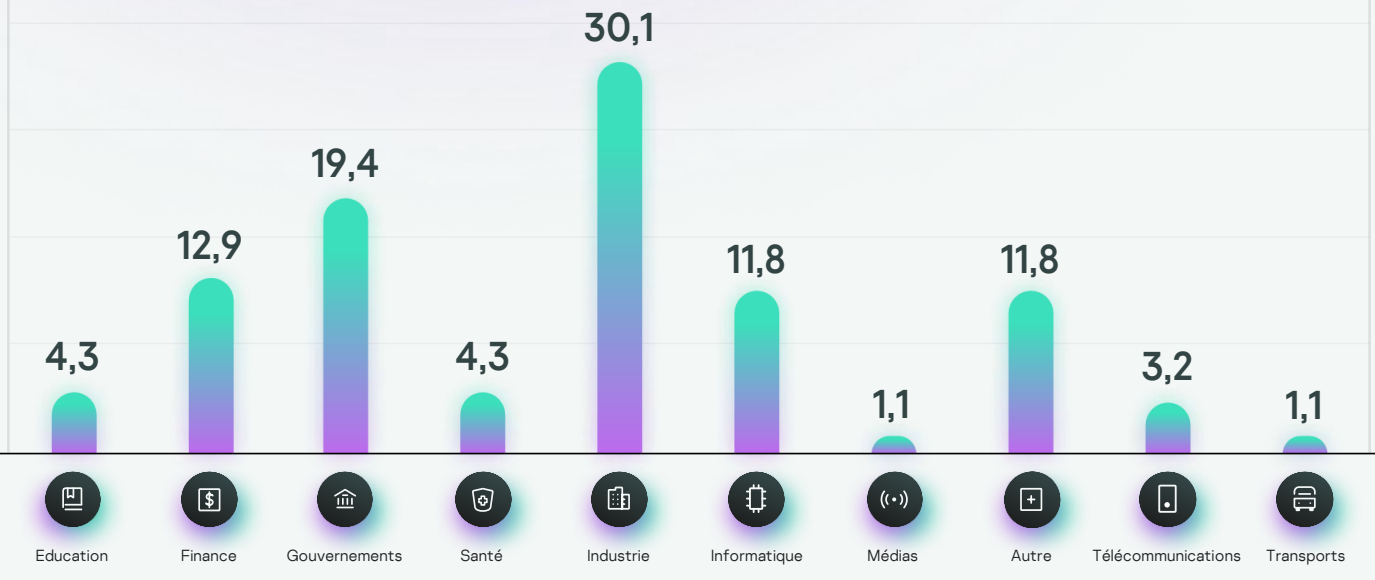
En 2020, la pandémie de COVID-19 a obligé les entreprises à restructurer leurs pratiques de sécurité de l'information pour s'adapter au travail à distance.



Géographie de la réponse aux incidents



Secteurs et entités



1. Les analyses reposent sur des cas de réponse à des incidents commerciaux réalisés par Kaspersky.
2. https://www.kaspersky.fr/enterprise-security/incident-response

Pourquoi la réponse à incident est-elle si importante ?

Les rançongiciels sont en train de rattraper les vols d'argent et autres fraudes, car ils constituent des mécanismes de monétisation plus efficaces, avec une couverture sectorielle beaucoup plus large (pas uniquement le secteur financier). Nous pouvons classer en toute confiance la plupart des incidents dont les causes sont antérieures à l'impact (évènements suspects, alertes d'outils, etc.) comme des rançongiciels.

Vrais positifs

Depuis de nombreuses années, les attaques par rançongiciels ont conservé un rôle dominant dans le paysage des menaces de cybersécurité. Nous vous conseillons fortement de vous informer constamment des dernières nouveautés concernant les attaques de rançongiciels en consultant nos publications et le projet NoRansom.

5,1 %	1,3 %	50,6 %	1,3 %	41,7 %
Fuites de données	Emails malveillants	Fichiers chiffrés	Vol d'argent	Activité suspecte

Faux positifs

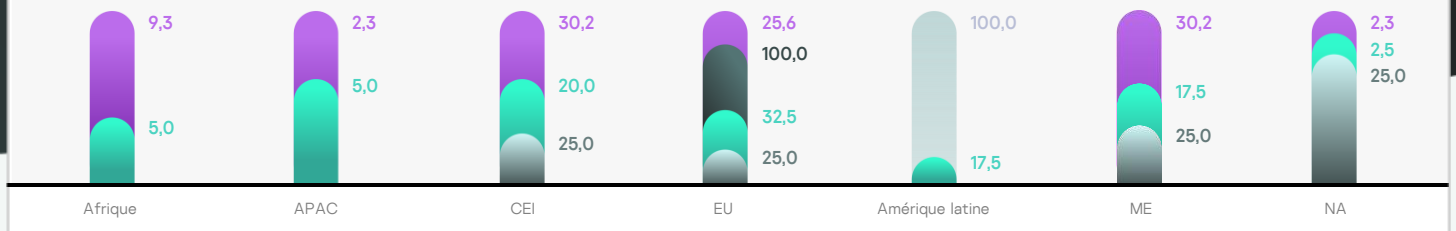
12,9 % de toutes les demandes de réponse aux incidents concernent des faux positifs. L'activité suspecte[3] signalée par les sondes réseau (NIDS, pare-feu) et la protection des terminaux (EPP) génère la plupart des faux positifs.

Une demande sur deux basée sur l'activité suspecte détectée par une sonde réseau ou un terminal s'avérait être un faux positif. Les cas de faux positif de fuites de données sont généralement des doublons ou des fuites provenant d'autres entreprises.

18,2 %	9,1 %	9,1 %	27,3 %	36,3 %
Alerte des outils de sécurité	Emails suspects	Fichier suspect	Activité réseau suspecte	Activité suspecte des terminaux

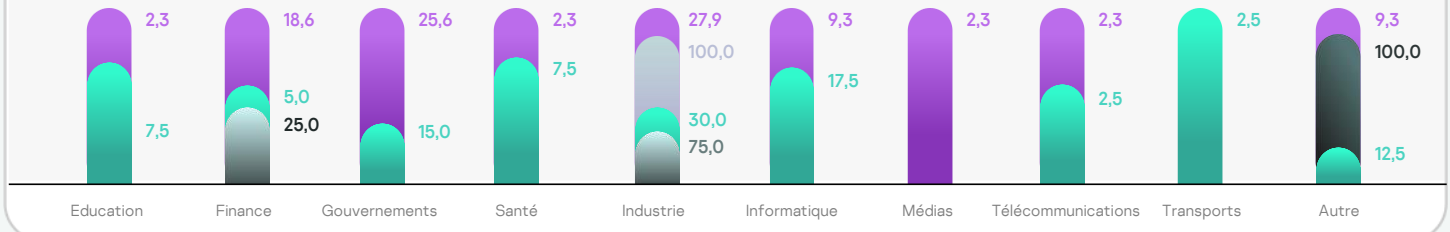
Raisons par zone géographique

Dans la plupart des zones géographiques, les attaques par rançongiciels et une activité suspecte constituent les raisons principales pour déclencher une enquête.



Raisons par secteur d'activité

Même lorsqu'ils ciblent le secteur financier, l'argent n'est plus l'objectif des attaquants. Les données sont la cible. La moitié de nos enquêtes sont menées sur des fuites de données dans ce secteur.



Fuites de données | Fichiers chiffrés | Emails malveillants | Vol d'argent | Activité suspecte

3. L'activité suspecte est une catégorie désignant une alerte générée par une série d'outils de sécurité ou un comportement anormal signalé par un utilisateur.

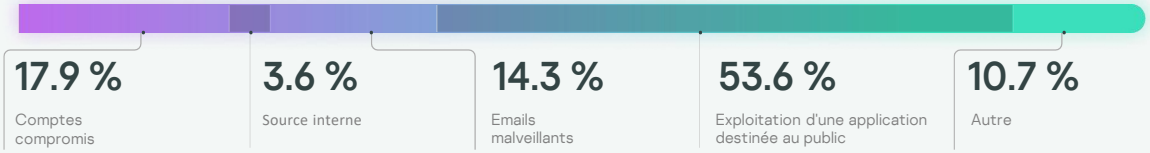
Vecteurs initiaux

Ou comment les cybercriminels arrivent à s'introduire dans les systèmes

D'année en année, les problèmes de sécurité liés aux mots de passe, les vulnérabilités logicielles et l'ingénierie sociale se combinent pour constituer une majorité écrasante de vecteurs d'accès initial[4] au cours des attaques. La mise en place et le contrôle des politiques de mot de passe, la gestion des correctifs et la sensibilisation des employés ainsi que les mesures anti-phishing minimisent substantiellement les capacités des cybercriminels. Lorsque les cybercriminels préparent leurs attaques, ils recherchent les cibles les plus faciles à atteindre telles que les serveurs publics contenant des vulnérabilités et des exploits bien connues.

La mise en place d'une politique de gestion des correctifs appropriée réduira à elle seule de 50 % la probabilité de devenir une victime.

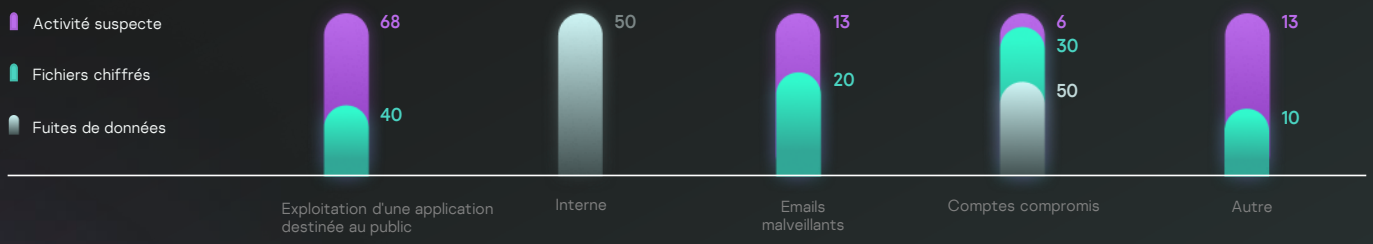
En 2021, des vulnérabilités ont été découvertes dans MS Exchange. En raison de l'omniprésence des serveurs Exchange et de la disponibilité publique d'exploits pour ces vulnérabilités, il en résulte un nombre considérable d'incidents.



17.9 %	3.6 %	14.3 %	53.6 %	10.7 %
Comptes compromis	Source interne	Emails malveillants	Exploitation d'une application destinée au public	Autre

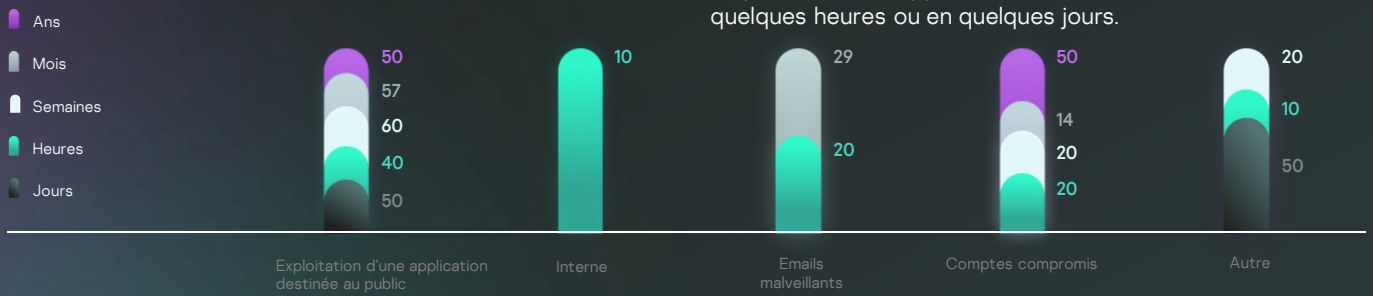
Principaux vecteurs de compromission initiale et mode de détection des incidents

Les adversaires utilisant des rançongiciels exploitent quasiment tous les scénarios courants d'accès initial. De nombreuses attaques utilisent des informations d'identification connues pour commencer l'attaque sur des infrastructures déjà compromises. Il est à noter qu'il n'est pas possible d'enquêter sur la façon dont ces informations ont été divulguées.



Durée de l'attaque avant sa détection et principaux vecteurs initiaux

La plupart des cas dont l'accès initial n'a pas été identifié ont duré plus d'un an avant d'être détectés par l'organisation. À ce moment-là, il ne restait plus aucun artéfact à analyser en raison des politiques de rotation des journaux. Plus de la moitié de toutes les attaques ayant commencé par des emails malveillants, le vol d'informations d'identification et l'exploitation des applications externes sont détectées en quelques heures ou en quelques jours.



4. Nous avons identifié le vecteur initial de l'attaque dans 30 % des cas. Les incidents très anciens, les journaux indisponibles, les destructions de preuves volontaires ou non par l'entreprise de la victime et les attaques contre les chaînes d'approvisionnement font partie des nombreuses raisons qui empêchent de révéler des causes de l'implantation initiale des adversaires dans le réseau

Outils et exploits

40 %

de tous les incidents sont liés à des outils

Quasiment la moitié de tous les incidents reposent sur l'utilisation d'**outils existants de systèmes d'exploitation** (tels que LOLbins)[5], d'outils offensifs connus de GitHub (p.ex. Mimikatz, AdFind, Masscan) et des frameworks commerciaux spécialisés (Cobalt Strike).

Comme il est très difficile de les détecter avec les contrôles de sécurité traditionnels, une autre approche est nécessaire. Kaspersky Managed Detection and Response détecte l'utilisation de tels logiciels.

Distribution et fréquence des outils dans les cas d'incidents

Régulièrement

5–8[6] %

Cobalt Strike, Mimikatz, PowerShell, PsExec

Moyen

3–4 %

Advanced IP Scanner, Bitlocker, ProcDump, ProcessHacker

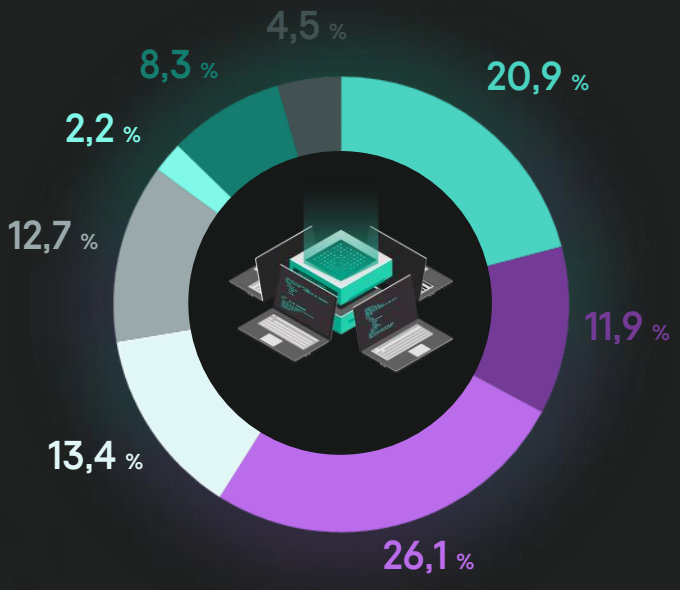
Rarement

1–2 %

AnyDesk, DiskCryptor, Everything, Fast Reverse Proxy FRP, Meterpreter, reg.exe, RMS, SMBExec et WebBrowserPassView.exe

La distribution et la fréquence des outils utilisés dans le cadre des tactiques ATT&CK démontrent un ciblage clair et évident de tous les aspects entre l'accès initial et l'impact. Ces outils devraient renforcer la détection des incidents pendant que les adversaires explorent le réseau.

- **Exécution**
  - PowerShell
  - PsExec
  - SmbExec
- **Contournement des défenses**
  - ProcessHacker
  - PCHunter
  - PowerTool
- **Accès aux identifiants**
  - Mimikatz
  - PowerTool
  - ProcDump
- **Détection**
  - Advanced IP Scanner
  - nbtscan wmic
- **Collecte**
  - Everything
  - 7zip
- **Mouvement latéral**
  - Cobalt Strike
  - Impacket
  - PowerSploit
  - Empire_Powershell
- **Commande et contrôle**
  - RDP
  - AnyDesk
  - RMS
- **Impact**
  - DiskCryptor
  - BitLocker



5. https://lolbas-project.github.io
6. Chaque outil a été identifié dans 5 à 8 % des cas d'incident

L'utilisation d'exploits a été détectée dans 14 % de l'ensemble des incidents

En 2021, des vulnérabilités pour des logiciels largement utilisés ont été publiées et ont touché de nombreuses entreprises. Les stratégies de gestion des correctifs restent un point très important du point de vue de la sécurité.

Microsoft Exchange — CVE-2021-34523

Vulnérabilité d'élévation de privilège (EoP). Cette vulnérabilité permet aux pirates informatiques d'augmenter leurs permissions. Fait partie de la chaîne des vulnérabilités de ProxyShell.

Microsoft Exchange — CVE-2021-34473

Vulnérabilité d'exécution de code à distance (RCE). Cette vulnérabilité est dans le service Autodiscover d'Exchange Server. Des pirates informatiques non authentifiés peuvent accéder à ses ressources restreintes et l'exploiter en conjonction avec d'autres vulnérabilités pour exécuter du code arbitraire. Fait partie de la chaîne des vulnérabilités de ProxyShell.

Microsoft Exchange — CVE-2021-31207

Vulnérabilité de contournement des fonctions de sécurité. La vulnérabilité permet aux attaquants de contourner le processus d'authentification. Fait partie de la chaîne des vulnérabilités de ProxyShell.

Microsoft Exchange — CVE-2021-27065

Vulnérabilité en écriture de fichier arbitraire après authentification. Les pirates informatiques doivent s'authentifier à l'aide d'autres exploits ou d'informations d'identification volées. Cette vulnérabilité permet aux pirates informatiques d'exécuter du code arbitraire et d'écrire des fichiers arbitraires. Utilisée par le groupe Hafnium.

Microsoft Exchange — CVE-2021-26858

Vulnérabilité en écriture de fichier arbitraire après authentification. Les pirates informatiques doivent s'authentifier à l'aide d'autres exploits ou d'informations d'identification volées. Cette vulnérabilité permet aux pirates informatiques d'exécuter du code arbitraire et d'écrire des fichiers arbitraires. Utilisée par le groupe Hafnium.

Microsoft Exchange — CVE-2021-26857

Une vulnérabilité de désérialisation non sécurisée dans le service de messagerie unifiée de Microsoft Exchange. Les pirates informatiques doivent s'authentifier à l'aide d'autres exploits ou d'informations d'identification volées. Cette vulnérabilité permet aux pirates informatiques d'exécuter du code arbitraire et d'écrire des fichiers arbitraires. Utilisée par le groupe Hafnium.

Microsoft Exchange — CVE-2021-26855

Vulnérabilité SSRF dans Microsoft Exchange Server. Les pirates informatiques sont capables d'envoyer des requêtes HTTP arbitraires et de s'authentifier en tant que serveur Exchange. Utilisée par le groupe Hafnium.

Apache Solr — CVE-2019-17558

L'exploitation des vulnérabilités d'exécution de codes à distance permet aux cybercriminels d'exécuter un code arbitraire sans authentification dans Apache Solr par le biais de VelocityResponseWriter.

Pilotes Gigabyte — CVE-2018-19320

Vulnérabilité des pilotes de bas niveau GDrv. Les pirates informatiques utilisent les fonctions exposées dans gdrv.sys qui permettent à un utilisateur de bas niveau d'allouer et d'écrire des données dans la mémoire afin d'élever les privilèges à SYSTEM.

Fortinet FortiOS — CVE-2018-13379

Une vulnérabilité de traversement de répertoires dans le portail Web du FortiOS SSL VPN permet à des pirates informatiques non authentifiés de télécharger des fichiers système via des demandes de ressources HTTP spécialement conçues.

Durée de l'attaque

Les incidents peuvent être classés en trois catégories caractérisées par la durée de l'attaque, la durée de la réponse aux incidents et l'impact de l'attaque.

Furtive	Moyen	Longue durée
52,7 %	6,5 %	17,2 %
Des heures et des jours	Semaines	Des mois et plus longtemps

Durée moyenne d'une attaque

1 jour	14 jours	94,5 jours

Impact représentatif

Rançongiciels

Rançongiciels et vol d'argent

Fuite de données et rançongiciel

Durée de réponse aux incidents

Temps consacré à l'enquête

Attaques qui ont duré jusqu'à une semaine	Attaques qui ont duré jusqu'à un mois	Attaques qui ont duré plus d'un mois
29,4 heures	48,3 heures	60,13 heures
Les grandes attaques de rançongiciel furtives présentent les plus grands défis, même pour les opérations de sécurité matures. Les comportements de « voisin bruyant » portant sur des proies faciles (problèmes de sécurité facilement identifiables et publiquement connus).	A cause des rançongiciels, il est impossible de distinguer la plupart des attaques des attaques rapides (attaques éclair). Pour de nombreux incidents de ce groupe, un laps de temps important s'écoule entre l'accès initial et les phases d'attaque suivantes.	Périodes irrégulières de phases actives et passives au cours de l'attaque. La durée des phases actives est très similaire à celle du groupe précédent (moyenne).

Contacts

- Pour les demandes d'informations commerciales et les nouvelles demandes d'intervention en cas d'incident :
  intelligence@kaspersky.com

- Pour une assistance en cas d'urgence :

  gert@kaspersky.com

kaspersky