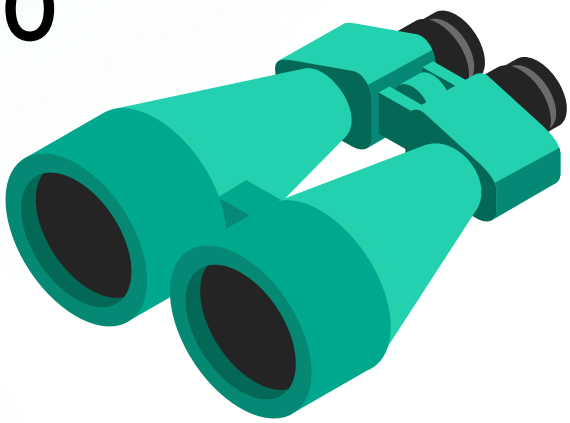
Managed Detection and Response : rapport d'analyste

4ème trimestre 2020



kaspersky

Résumé analytique

* Incidents critiques : incidents de gravité élevée causés par des attaques d'origine humaine. Ils représentent 9 % de l'ensemble des incidents identifiés

Recommandations

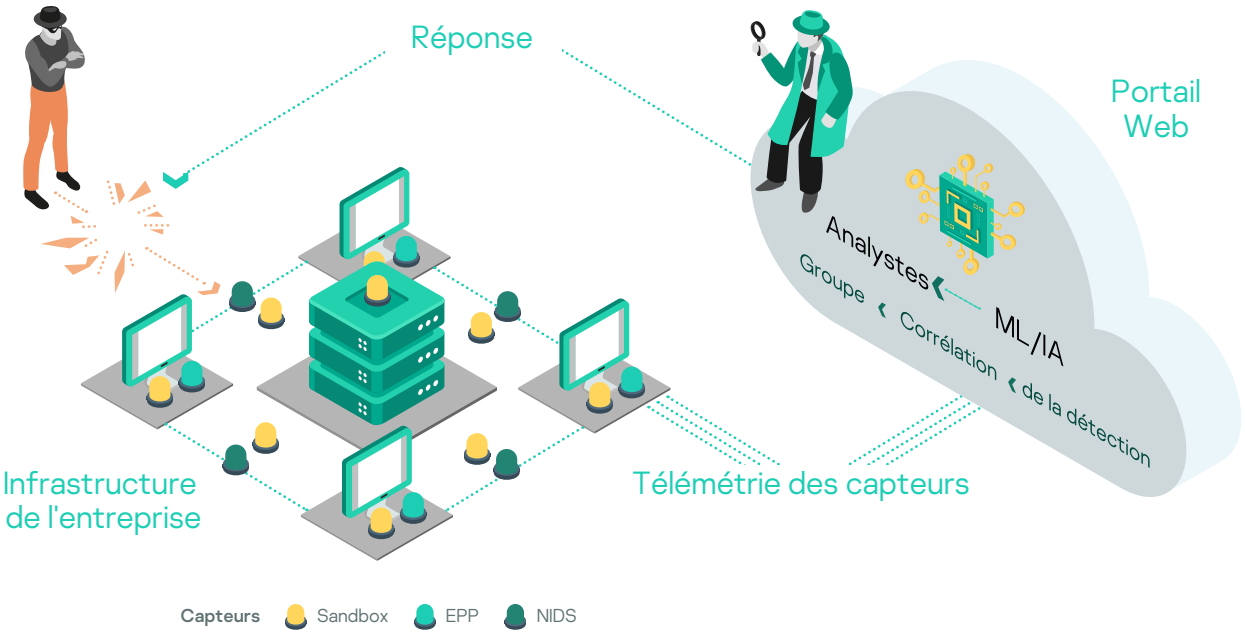
- Un tiers des incidents de gravité élevée sont dus à des attaques ciblées d'origine humaine. Les outils automatisés ne peuvent pas les détecter toutes, et doivent donc être associés à la recherche de menaces manuelle classique à l'aide d'alertes[1].
- Les exercices de sécurité (red team) professionnels[2]. reproduisent fidèlement les conditions d'une attaque avancée et sont un bon moyen d'évaluer l'efficacité opérationnelle d'une entreprise.
- Neuf pour cent des incidents de gravité élevée déclarés résultent d'attaques par social engineering, ce qui démontre la nécessité de sensibiliser les employés aux questions de sécurité[3].
- Préparez-vous à détecter les menaces de tous types de tactiques (phases de la chaîne de frappe de l'attaque). Toutes les attaques, même les plus complexes, reposent sur un enchaînement d'étapes simples (ou techniques). La détection d'une technique particulière peut révéler une attaque dans son ensemble.
- Différentes technologies de détection sont efficaces contre différentes techniques d'attaque. Utilisez un large éventail de technologies de sécurité[4]. pour accroître vos chances de détection.

[1] https://www.kaspersky.fr/enterprise-security/managed-detection-and-response
[2] https://www.kaspersky.fr/enterprise-security/security-assessment
[3] https://www.kaspersky.fr/enterprise-security/security-awareness
[4] https://www.kaspersky.fr/enterprise-security/wiki-section/products/multi-layered-approach-to-security

Introduction

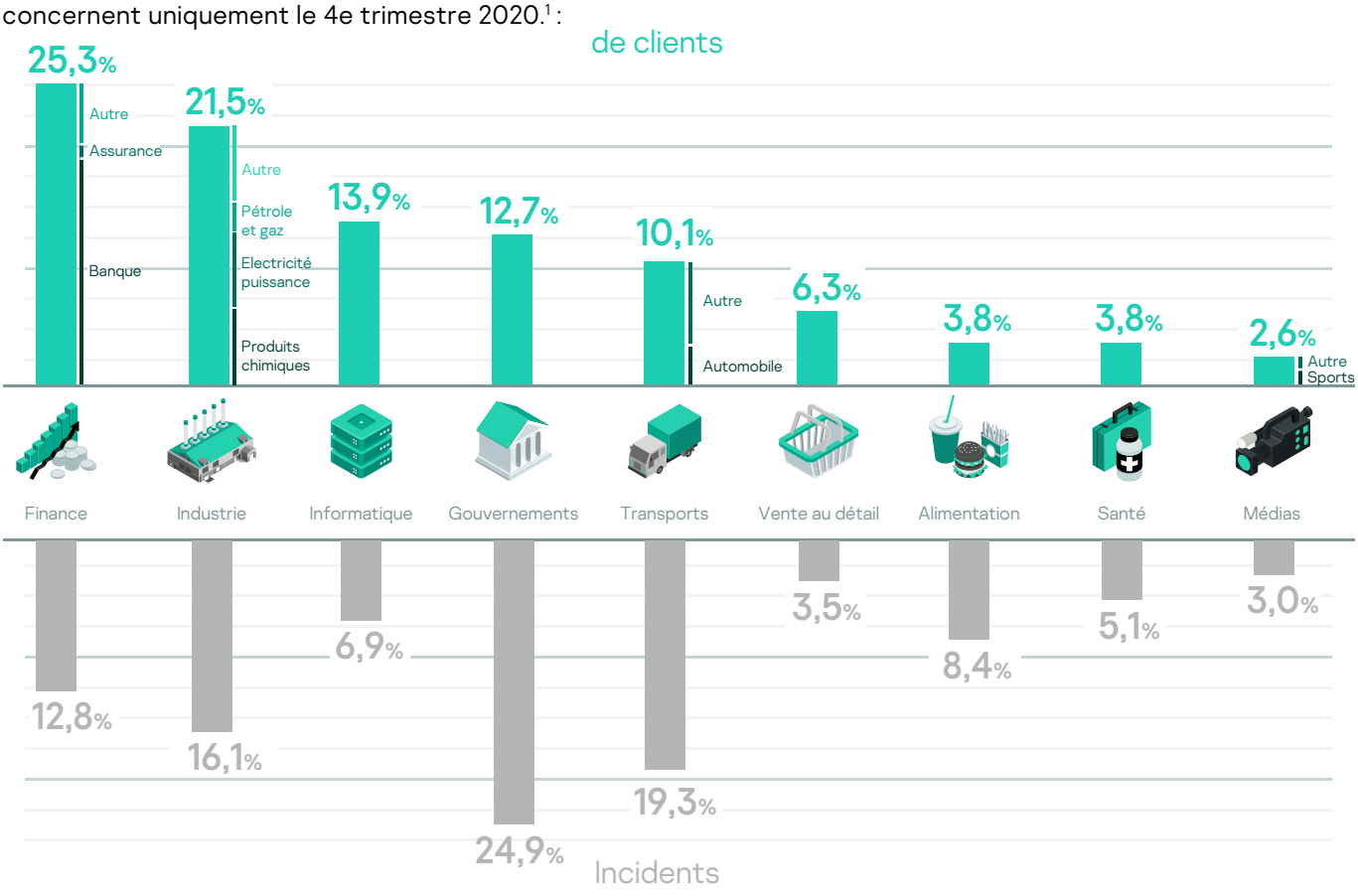
À l'heure où les cyberattaques deviennent de plus en plus sophistiquées et où les solutions de sécurité exigent toujours plus de ressources pour analyser l'énorme quantité de données collectées quotidiennement, de nombreuses entreprises recherchent des services de sécurité avancés capables de gérer cette complexité croissante en temps réel, 24 heures sur 24 et 7 jours sur 7.

Dans son Guide du marché MDR, publié en 2020, Gartner estime que « d'ici 2025, 50 % des entreprises utiliseront des services de détection et de réponse gérés afin de disposer de fonctions de surveillance, de détection et de réponse capables de contenir les menaces ».



Portée du service MDR : secteurs d'activité et marchés

Comme le montre le graphique ci-dessous, notre service MDR est utilisé dans tous les secteurs d'activités. Le pourcentage d'incidents détectés est également précisé pour chaque catégorie. Les données du rapport concernent uniquement le 4e trimestre 2020.[1] :



[1] Le rapport utilise des métadonnées anonymisées que nos clients nous ont communiquées volontairement depuis le 4e trimestre 2020, date de disponibilité du service dans certains pays. Il a été lancé dans le monde entier au premier trimestre 2021.

Routine quotidienne du service MDR

Le service MDR reçoit de grandes quantités de données télémétriques brutes des capteurs, filtre et enrichit ces événements afin de les transformer en alertes. Grâce à ces informations, nos chercheurs expérimentés créent des incidents dans un format pratique qui accélère le temps de réponse humain et peut être réutilisé par d'autres outils de sécurité.

Événements quotidiens sur un seul hôte :

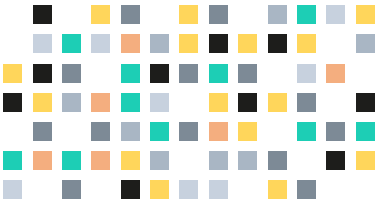
env. 15K

Cette valeur peut varier sensiblement selon l'activité de l'hôte

Dont

65 000 alertes traitées

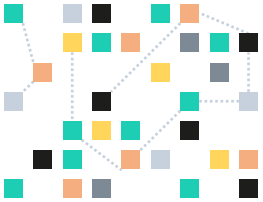
en l'espace de 3 mois par tous les capteurs



43 000 alertes enrichies triées manuellementet 22 000 triées à l'aide del'IA/ML

Soit

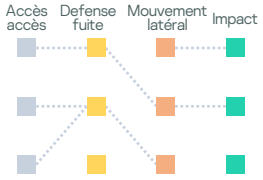
1 506 incidents signalés aux clients



- Nombre d'alertes liées aux incidents signalés : 2 566
- Taux de conversion des alertes en incidents de 5,9 %, soit 94,1 % de faux positifs.

92,9%

d'alertes enrichies avec les données ATT&CK



- 1 400 incidents applicables au cadre MITRE ATT&CK
- Le cadre ne s'applique pas forcément aux autres incidents (incidents de visibilité ou de faible gravité)

Efficacité de la résolution des incidents

Combien d'alertes faut-il pour résoudre un incident ?

1 alerte

pour 80,1 % des incidents

Montre l'efficacité globale des systèmes de détection et de correction des incidents

80,1%

Entre 2 et 4 alertes

pour 15,3 % des incidents

Montre les améliorations à apporter au système de détection des incidents et au processus de correction. Tous ces incidents contribuent à la création d'une nouvelle logique de détection et alimentent les statistiques de détection automatique

15,3%

5 alertes ou plus

pour 4,6 % des incidents

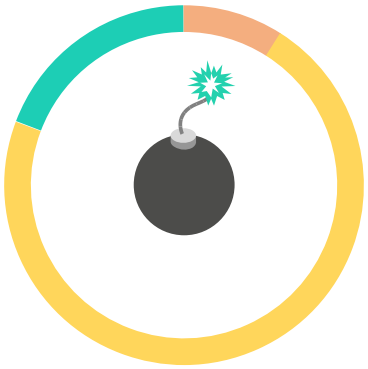
Les incidents présentant un grand nombre d'alertes désignent des cas qui ne peuvent pas être résolus rapidement ni efficacement :

- Nouvelle attaque ciblée/APT découverte
- Surveillance d'attaque sans réponse à la demande du client
- Exercices de sécurité sans réponse (ex. : test de pénétration)

4,6%

1 alerte | Entre 2 et 4 alertes | 5 alertes ou plus

Gravité des incidents



9% **incidents de gravité élevée**

Provoquent de fortes perturbations ou permettent un accès non autorisé aux ressources du client protégées par le service MDR.

Traces identifiées d'une attaque ciblée ou d'une menace inconnue, nécessitant un complément d'enquête grâce au cyberdiagnostic

72% **incidents de gravité moyenne**

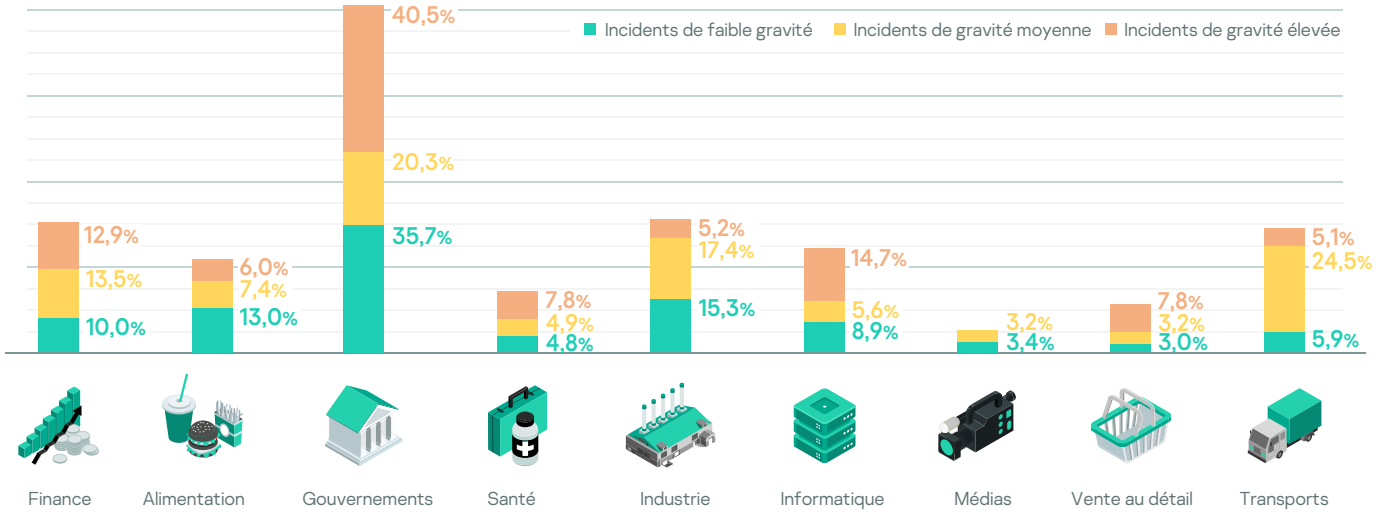
Affectent l'efficacité ou les performances des ressources du client protégées par le service MDR ou entraînent la corruption de certaines données isolées.

19% **incidents de faible gravité**

Peu susceptibles d'affecter le fonctionnement ou les performances des ressources du client protégées par le service MDR, ces incidents ont peu de chances de corrompre les données.

Logiciels potentiellement indésirables identifiés (adwares, programmes potentiellement dangereux, faux positifs, etc.)

Nous avons identifié tous les jours entre 1 et 2 incidents de gravité élevée. Seuls les clients des secteurs des médias et des transports n'ont connu aucun incident de gravité élevée lors du 4e trimestre 2020. Les secteurs gouvernementaux, de la finance et de l'informatique ont été les plus touchés ce trimestre.



Combien de temps faut-il pour identifier un incident ?

En cas d'événement suspect, une alerte débute sa vie dans la file d'attente, où elle attend d'être triée par un analyste humain (les alertes IA/ML - env. 33 % sont traitées en quelques secondes et ne sont pas affichées ici). Les alertes triées sont ensuite transformées en dossiers d'incident, puis examinées par un analyste, qui crée une carte d'incident et la communique au client. L'illustration ci-dessous détaille le processus complet de traitement des alertes, du temps passé dans la file d'attente à la création du rapport d'incident.

52,6 min. **Gravité élevée**

Les incidents les plus graves nécessitent des données supplémentaires et mettent davantage de temps à être détectés

21,1 min. **Gravité moyenne**

Le type d'incident le plus courant en termes de volume. Le temps de traitement plus rapide montre l'efficacité de l'utilisation de modèles pour les cartes d'incidents les plus fréquentes

30,2 min. **Faible gravité**

En raison de leur niveau de priorité peu élevé, ces incidents passent l'essentiel de leur temps dans la file en attendant d'être traités par un analyste

Nature des incidents de gravité élevée

Quelles sont les causes des incidents de gravité élevée ?

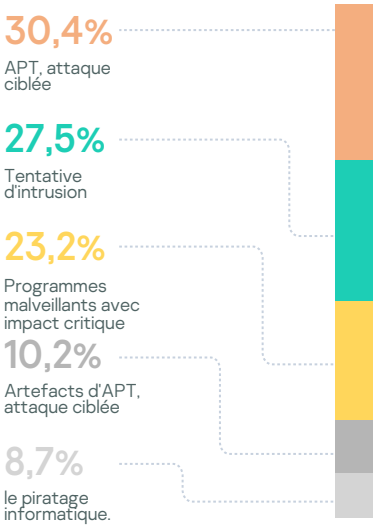
Un tiers (30,4 %) des incidents de gravité élevée correspondent à des attaques ciblées ou des Menaces persistantes avancées (APT)

Un incident de gravité élevée sur 4 est lié à un exercice offensif dirigé par l'homme (test de pénétration, red team, simulation d'adversaire, etc.)

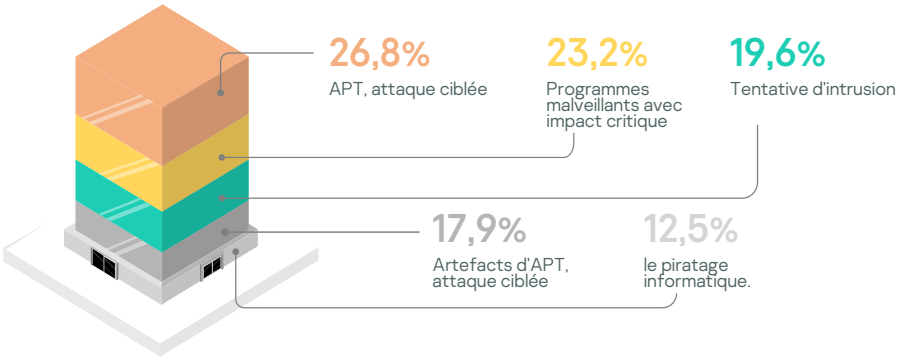
Un incident sur 5 découle de l'apparition de programmes malveillants tels que des ransomwares (ex. : WannaCry) à l'impact significatif, mais d'origine non humaine

10 % des incidents n'entrent dans aucune catégorie, mais montrent des traces d'anciennes attaques ou tentatives d'intrusion
(ex. : dump Lsass, fichiers kirbi, signes d'un système d'exploitation persistant, etc.) Cela peut s'expliquer par l'intégration de nouveaux clients ou l'ajout d'un nouvel hôte au champ de surveillance.

9 % des incidents résultent d'un accès initial par social engineering, dont l'attaque a été déjouée avant qu'elle ne puisse être catégorisée



Combien d'entreprises ont subi des incidents de gravité élevée ?



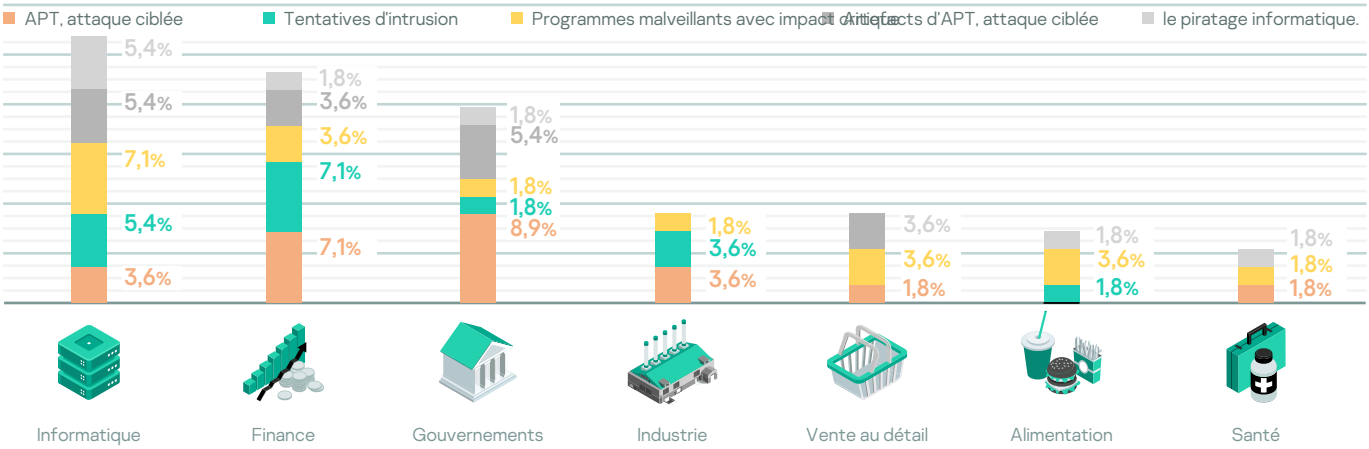
27 % des entreprises ont subi une attaque ciblée ou une APT

23 % d'entre elles ont été victimes de programmes malveillants (tels que des ransomwares)

20 % de nos clients ont simulé des tentatives d'intrusion

Nombre d'entreprises victimes d'incidents graves par secteur d'activité

La quasi totalité des secteurs d'activité ont été confrontés à des incidents de tous types au cours des trois mois de la période d'analyse.



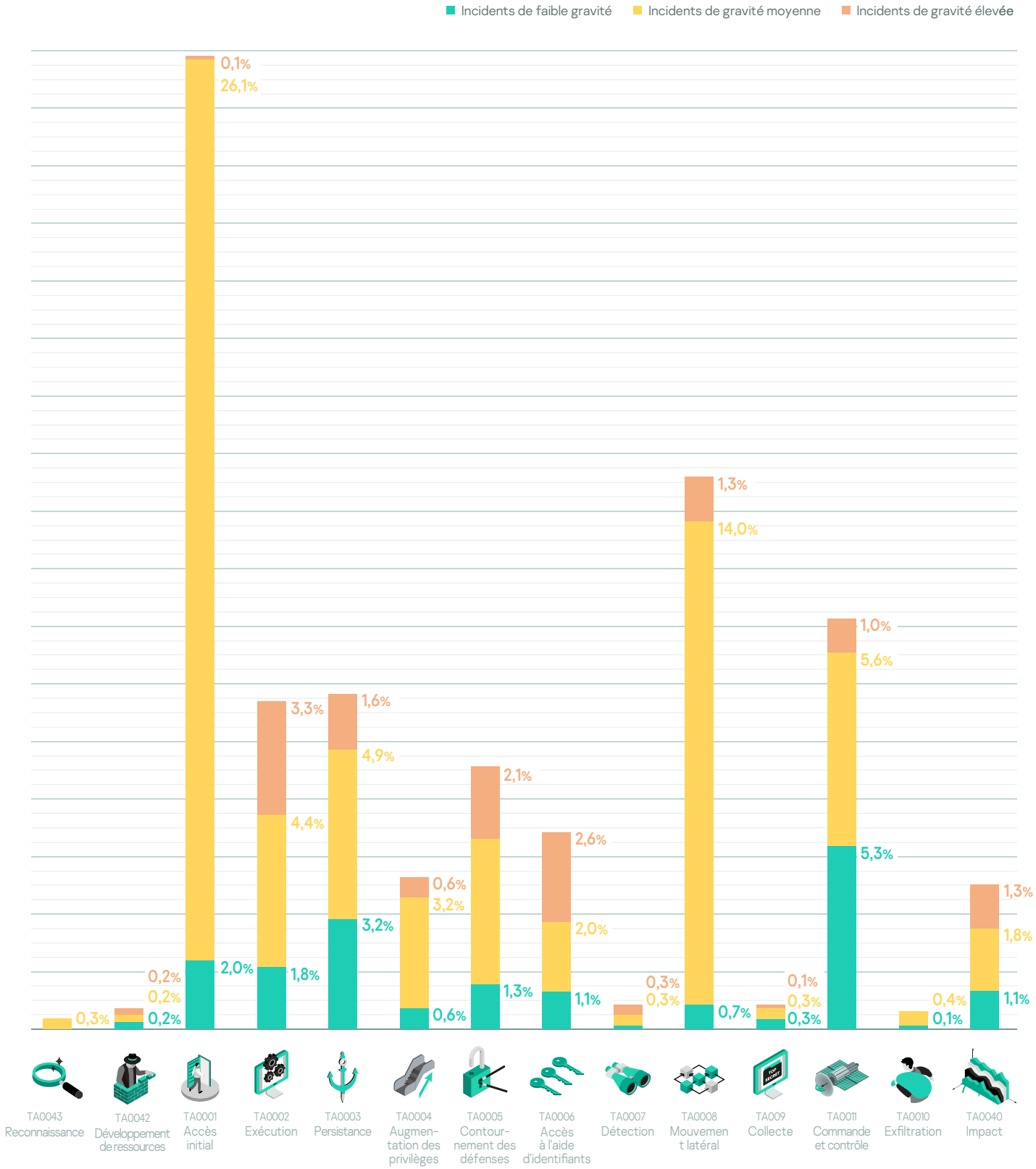
Les APT actives produisent quasi systématiquement des artefacts d'APT (traces d'autres attaques d'origine humaine). Cela indique que les entreprises ayant subi une APT sont souvent à nouveau prises pour cible par le même cybercriminel.

Les secteurs ciblés par des APT organisent des exercices de sécurité (red team) qui leur permettent d'évaluer précisément les risques.

Technologie de détection et tactiques, techniques et procédures (TTP) des adversaires

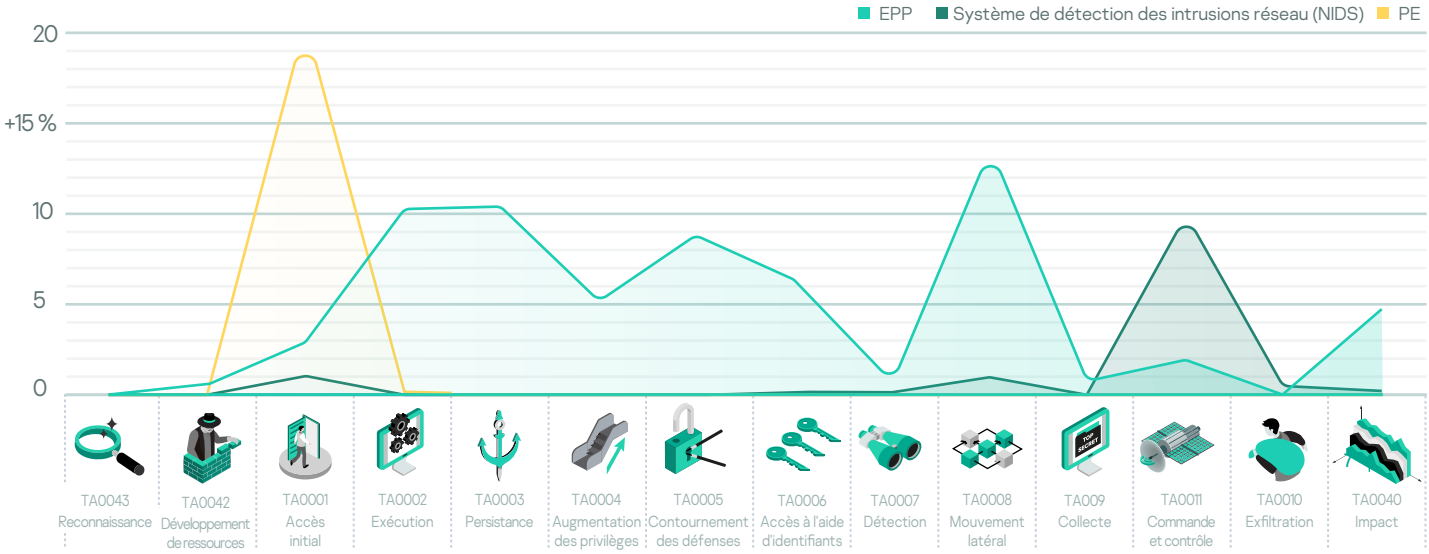
Tactiques des adversaires

La plupart des incidents ont été détectés lors de la phase d'accès initial. L'exécution, la persistance, le contournement des défenses, l'accès à l'aide d'identifiants, le mouvement latéral, la commande et le contrôle sont les sources d'attaque les plus fréquentes. Peu d'incidents ont été détectés lors des phases d'exfiltration et de collecte car ces problèmes ont été correctement classifiés et corrigés en amont. Tous les cas détectés à ces stades avancés sont analysés en détail afin d'améliorer la logique de détection et d'accroître les chances de détecter les menaces dès que possible.



Tactiques et technologies de détection

Le service MDR reçoit des données télémétriques de différents types de capteurs (technologies de détection) : la plateforme de protection des terminaux (EPP), l'environnement sandbox (SB) et le système de détection des intrusions réseau (NIDS). Le système de détection des intrusions réseau et l'environnement sandbox sont des composantes de la plateforme contre les attaques ciblées de Kaspersky.1 :. Notre solution EPP Kaspersky Endpoint Security for Business intègre un système de détection des intrusions réseau hébergé sur l'hôte2. Le graphique suivant montre les techniques MITRE ATT&CK les plus efficaces dans notre service MDR pour chaque capteur et indique la tactique utilisée par l'adversaire lors de la détection de l'incident.



Le graphique suivant montre les techniques MITRE ATT&CK les plus efficaces (classées par pourcentage d'incidents détectés) dans notre service MDR pour chaque capteur

Accès initial

EPP PE — T1566.001
Pièce jointe de phishing ciblé (spearphishing)

PE Système de détection des intrusions réseau (NIDS) — T1566.002
Lien de phishing ciblé

Système de détection des intrusions réseau (NIDS) — T1190
Exploitation d'une application destinée au public

Système de détection des intrusions réseau (NIDS) — T1133
Services externes à distance

Exécution

EPP PE — T1053
Tâche/action planifiée

EPP PE — T1204
Exécution par l'utilisateur

EPP — T1059.001
PowerShell

EPP — T1059
Interprète de commandes et de scripts

PE — T1204.001
Lien malveillant

Persistance

EPP PE — T1053
Tâche/action planifiée

EPP — T1547.001
Clé d'exécution du registre / dossier de démarrage

EPP — T1546.008
Fonctionnalités d'accessibilité

Système de détection des intrusions réseau (NIDS) — T1133
Services externes à distance

Augmentation des privilèges

EPP PE — T1053
Tâche/action planifiée

EPP — T1547.001
Clé d'exécution du registre / dossier de démarrage

EPP — T1546.008
Fonctionnalités d'accessibilité

EPP — T1055
Injection de processus

Contournement des défenses

EPP — T1036
Usurpation d'identité

EPP — T1055
Injection de processus

Accès à l'aide d'identifiants

EPP — T1003
Récupération des identifiants du système d'exploitation

Détection

Système de détection des intrusions réseau (NIDS) — T1083
Détection de fichiers et de répertoires

Mouvement latéral

EPP Système de détection des intrusions réseau (NIDS) — T1210
Exploitation de services à distance

EPP — T1021
Services à distance

Commande et contrôle

Système de détection des intrusions réseau (NIDS) — T1071
Protocole de la couche application

Système de détection des intrusions réseau (NIDS) — T1095
Protocole n'utilisant pas la couche application

Système de détection des intrusions réseau (NIDS) — T1102
Service Web

Exfiltration

Système de détection des intrusions réseau (NIDS) — T1048
Exfiltration via un autre protocole

Impact

EPP — T1496
Détournement de ressources

EPP

- Englobe la plupart des tactiques
- Conçu pour analyser les phases d'attaque les moins discrètes : entre l'accès initial et la compromission avérée avant l'impact

Sandbox

- Permet d'accélérer le tri et de donner davantage de contexte aux analystes
- Résultats focalisés sur le début et la fin de la chaîne de frappe

Système de détection des intrusions réseau (NIDS)

- Privilégie les tactiques avant l'impact
- Complément utile pour identifier les tactiques d'accès initial

1: KATA – https://www.kaspersky.fr/enterprise-security/anti-targeted-attack-platform
2. KESB – https://www.kaspersky.fr/enterprise-security/endpoint-product

Techniques des adversaires

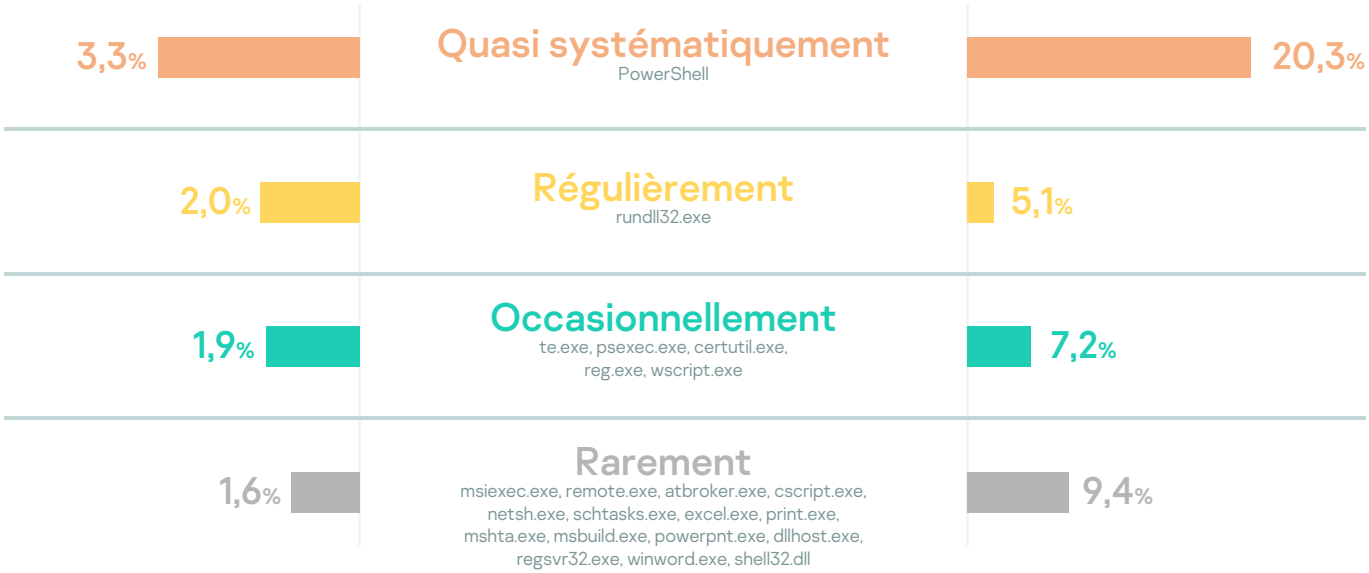
Outils utilisés lors d'incidents

Les malfaiteurs ont tendance à utiliser des outils intégrés au système d'exploitation pour installer leurs instruments en toute discrétion, réduire le coût de développement des boîtes à outils et, surtout, pour donner un aspect légitime à leur travail et ainsi compliquer nettement la tâche du défenseur.

Ces outils sont ce que l'on appelle des fichiers binaires hors sol. Vous pouvez les consulter sur le site Web du projet lolbins. En définitive, même si Microsoft a fait des efforts considérables pour renforcer la sécurité et les contrôles de PowerShell, il reste de loin l'outil le plus utilisé par les acteurs malveillants.

Part des incidents liés aux lolbins sur l'ensemble des incidents

Part des incidents graves liés aux lolbins (sur l'ensemble des incidents graves)



Application des incidents au cadre MITRE ATT&CK

La logique de détection basée sur les techniques MITRE se caractérise par son efficacité. Elle indique la part d'incidents détectée par les règles de recherche de menaces sur l'ensemble des incidents signalés à l'aide de techniques spécifiques.

33 %

T1566 : Phishing

Démontre l'efficacité du service MDR pour contrer cette technique dès le stade de l'accès initial, ainsi que sa popularité parmi les pirates

16,5 %

T1210 : Exploitation services à distance

Correspond à des services à distance (nombreuses failles « EternalBlue »)

10,6 %

T1071 : Protocole de la couche application

Protocole privilégié pour les communications avec l'infrastructure C&C. À titre de comparaison,la technique « T1095 : Protocole n'utilisant pas la couche application » ne représente que 3,79 % des incidents

5,3 %

T1021 : Services à distance

Technique de mouvement latéral largement utilisée par les attaquants (T1021.002 : PME/Partages administrateur Windows et T1021.001 : Remote Desktop Protocol)

4,4 %

T1036 : Usurpation d'identité

Utilisation fréquente de backdoors de fonctionnalités d'accessibilité lorsque des utilitaires comme sethc.exe, narrator.exe, magnify.exe, ultiman.exe, etc. sont remplacés par cmd.exe. D'après les statistiques, les incidents de gravité élevée sont très rares avec cette technique. Dans un petit nombre de cas, les pirates renomment des fichiers malveillants en les faisant passer pour des outils système ou créent des tâches planifiées d'apparence légitime, entraînant ainsi des incidents de gravité moyenne à élevée.

3,3 %

T1204 : Exécution par l'utilisateur

Ingénierie sociale réussie via des pièces jointes de phishing ou tentative d'exécution d'un code téléchargé par le logiciel sur Internet

6,6 %

T1059 : Interprète de commandes et de scripts

Mêle essentiellement les techniques T1059.001 : PowerShell et T1059.004 : Unix Shell

>0 % >5 % >10 % >20 %

TA0043 : Reconnaissance	TA0042 : Développement de ressources	TA0001 : Accès initial	TA0002 : Exécution	TA0003 : Persistance	TA0004 : Augmentation des privilèges	TA0005 : Contournement des défenses
T1595 : Analyse active	T1587 : Développement de fonctionnalités	T1190 : Exploitation d'une application destinée au public	T1059 : Interprète de commandes et de scripts	T1098 : Manipulation de compte	T1548 : Utilisation abusive du mécanisme de contrôle d'augmentation des privilèges	T1140 : Décryptage/décodage de fichiers ou d'informations
	T1588 : Obtention de fonctionnalités	T1133 : Services externes à distance	T1203 : Exploitation pour l'exécution par le client	T1547 : Exécution automatique au lancement ou lors de la connexion	T1134 : Manipulation de jeton d'accès	T1564 : Dissimulation d'artefacts
		T1566 : Phishing	T1559 : Communication interprocessus	T1037 : Scripts d'initialisation au lancement ou lors de la connexion	T1546 : Exécution déclenchée par un événement	T1562 : Affaiblissement des défenses
		T1091 : Réplication via un support amovible	T1053 : Tâche/actio n planifiée	T1554 : Compromission du code binaire d'un logiciel client	T1068 : Exploitation pour augmenter les privilèges	T1070 : Suppression d'indicateurs sur l'hôte
		T1078 : Comptes valides	T1569 : Services système	T1136 : Création de compte	T1574 : Détournement du flux d'exécution	T1036 : Usurpation d'identité
			T1204 : Exécution par l'utilisateur	T1505 : Composant logiciel serveur	T1055 : Injection de processus	T1112 : Modification du registre
			T1047 : Windows Management Instrumentation (WMI)			T1027 : Dissimulation de fichiers ou d'informations
						T1542 : Démarrage avant le système d'exploitation
						T1218 : Exécution de code binaire signé par proxy

TA0006 : Accès à l'aide d'identifiants	TA0007 : Détection	TA0008 : Mouvement latéral	TA0009 : Collecte	TA0011 : Commande et contrôle	TA0010 : Exfiltration	TA0040 : Impact
T1110 : Force brute	T1087 : Détection de compte	T1210 : Exploitation de services à distance	T1123 : Enregistrement du son	T1071 : Protocole de la couche application	T1048 : Exfiltration via un autre protocole	T1485 : Destruction de données
T1555 : Identifiants de banques de mots de passe	T1482 : Détection de l'indice de confiance du domaine	T1570 : Transfert latéral d'outils	T1005 : Données du système local	T1001 : Brouillage de données		T1486 : Données chiffrées pour l'impact
T1556 : Modification du processus d'authentification	T1083 : Détection de fichiers et de répertoires	T1021 : Services à distance	T1056 : Enregistrement de saisie	T1105 : Transfert entrant d'outils		T1565 : Manipulation de données
T1003 : Récupération des identifiants du système d'exploitation	T1046 : Analyse du service réseau	T1550 : Utilisation de méthodes d'authentification alternatives		T1095 : Protocole n'utilisant pas la couche application		T1561 : Effacement de disque
T1552 : Identifiants non sécurisés	T1135 : Détection de partages réseau			T1090 : Proxy		T1496 : Détournement de ressources
	T1069 : Détection de groupes d'autorisation			T1219 : Accès logiciel à distance		
	T1012 : Interrogation du registre			T1102 : Service Web		
	T1018 : Détection de système distant					
	T1033 : Détection du propriétaire du système/de l'utilisateur					
	T1497 : Évasion d'un environnement virtualisé/Sandbox					