Présenté par

Trellix ADVANCED RESEARCH CENTER

RAPPORT SUR LE PAYSAGE DES MENACES

Février 2023

SOMMAIRE

VUE D'ENSEMBLE SUR LES MENACES – T4 2022

Les cybercriminels se sont à nouveau avérés des adversaires redoutables pendant les derniers mois de l'année 2022. Trellix Advanced Research Center a répliqué en intégrant encore plus de ressources de Threat Intelligence à notre équipe composée de centaines d'analystes et de chercheurs chevronnés en sécurité.

« Nous avons optimisé notre Threat Intelligence. Allégez le stress des SecOps grâce à une sécurité plus simple. Renforcez votre niveau de sécurité en toute sérénité. Les menaces ne cessent d'évoluer. Faites-en de même. »

Ce rapport de premier plan passe en revue les cybercriminels, familles de menaces, campagnes et techniques qui ont dominé au cours du dernier trimestre. Mais ce n'est pas tout. Nous avons également élargi nos sources afin de recueillir des données issues des sites de divulgation des ransomwares et de divers rapports publiés par le secteur de la sécurité. L'augmentation des ressources Trellix entraîne l'apparition de nouvelles catégories d'informations sur les menaces, y compris du contenu concernant la sécurité réseau, les incidents cloud, les incidents sur les terminaux et les opérations de sécurité.

Depuis notre dernier rapport sur le paysage des menaces, Trellix Advanced Research Center a mené des études et des observations à l'échelle mondiale. Notre équipe a notamment mis en lumière le lien entre Gamaredon et la multiplication des cyberattaques ciblant l'Ukraine au 4e trimestre, corrigé 61 000 projets open source vulnérables et publié ses prévisions 2023 en matière de menaces.

Le récapitulatif ci-dessous illustre la grande variété d'informations glanées par Trellix Advanced Research Center pour soutenir les clients et le secteur de la sécurité dans la lutte contre les cybermenaces :

Ransomwares

- LockBit 3.0 a été le groupe de ransomware le plus actif au 4e trimestre.
- Les ransomwares sont restés prévalents dans le monde entier, en particulier aux États-Unis.
- Ils ont ciblé des secteurs comme les biens et services industriels.

Attaques étatiques

- Ces attaques ont ciblé des secteurs comme l'administration publique ainsi que les transports et la logistique.
- Les entreprises américaines ont été les plus touchées.

Exploitation des ressources locales

- La méthodologie de traque de Trellix Advanced Research Center a permis d'en apprendre davantage sur l'utilisation de Cobalt Strike en environnement réel.
- Un grand nombre de serveurs Cobalt Strike sont hébergés auprès de fournisseurs cloud chinois.
- Windows Command Shell représente près de la moitié des 10 fichiers binaires de systèmes d'exploitation les plus prévalents utilisés dans les campagnes identifiées.

Cybercriminels

- La Chine, la Corée du Nord et la Russie arrivent en tête de la liste des pays d'origine des cybercriminels.

Tendances en matière de sécurité e-mail

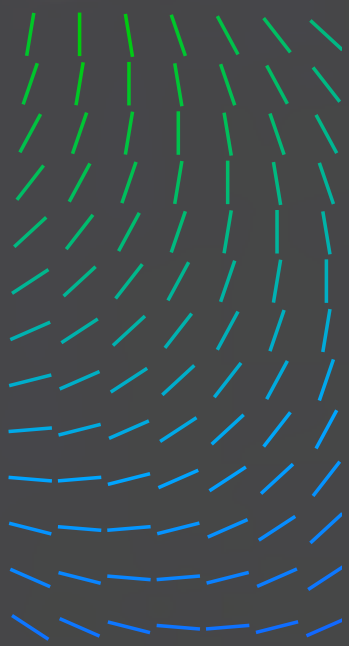
- Forte croissance du volume d'e-mails malveillants dans les pays arabes pendant la Coupe du monde de football
- Informations sur les campagnes de phishing et de vishing, notamment les techniques d'usurpation d'identité et les principaux thèmes utilisés pour le vishing

Sécurité réseau

- Attaques, webshells, outils et techniques les plus efficaces, significatifs et pertinents du trimestre

Données télémétriques sur les opérations de sécurité recueillies par Trellix XDR

- Alertes de sécurité, exploits, sources de journalisation et techniques MITRE ATT&CK prévalents
- Incidents cloud
- Techniques et détections pour Azure, AWS et GCP
- Principales techniques et détections



LETTRE DE NOTRE DIRECTEUR DE LA THREAT INTELLIGENCE

L'équipe Trellix Advanced Research Center est heureuse de partager avec vous le premier Rapport sur le paysage des menaces du 4e trimestre 2022. Ce rapport associe désormais de nouvelles données issues de nos capteurs produits aux informations provenant d'autres sources, telles que les sites de divulgation des ransomwares et notre suivi des infrastructures en environnement réel. Chez Trellix, nous restons résolus à protéger nos clients contre les menaces face à des cybercriminels tenaces et motivés, qui se réinventent sans cesse. Dans un contexte géopolitique et économique complexe marqué par de fortes incertitudes, une Threat Intelligence mondiale s'avère de plus en plus essentielle.

Partout dans le monde, le climat d'incertitude économique généré par la guerre en Ukraine a entraîné la plus forte hausse des prix de l'énergie jamais observée depuis les années 1970, qui pèse lourd sur l'économie mondiale. Le retour de la guerre en Europe a également agi comme un révélateur chez ceux qui remettaient en question l'approche de l'UE en matière de sécurité et de défense ainsi que sa capacité à défendre ses intérêts, en particulier dans le cyberespace. Par ailleurs, aux États-Unis, les pouvoirs publics ont reconnu la nécessité de répondre à la concurrence géostratégique, de protéger les infrastructures critiques et de lutter contre la manipulation d'informations et l'interférence de puissances étrangères. SolarWinds, Hafnium, l'Ukraine et d'autres événements ont déclenché une action bipartite de l'administration et du Congrès concernant de nouvelles normes et politiques de financement de sécurité qui reposent en grande partie sur les engagements de la nation et le travail des gouvernements antérieurs. Quel est donc l'impact de cette incertitude sur la cybersécurité de nos entreprises, de nos institutions publiques et privées et de nos valeurs démocratiques ?

Au cours du dernier trimestre, notre équipe a observé l'utilisation active de cyberattaques à des fins d'espionnage, de cyberguerre et de désinformation au service d'ambitions politiques, économiques et territoriales. La guerre en Ukraine a également entraîné l'émergence de nouvelles formes de cyberattaques, et les cyberactivistes se sont montrés plus sophistiqués et plus audacieux dans leurs actions : dégradation de sites web, divulgation d'informations et attaques DDoS. Les formes traditionnelles de cyberattaques n'ont pas été abandonnées pour autant. Les stratagèmes d'ingénierie sociale visant à tromper et à manipuler les individus pour les pousser à divulguer des informations confidentielles ou personnelles, comme le phishing, restent prévalents.

Les ransomwares ont continué à semer le chaos dans de nombreuses entreprises à travers le monde. Tout comme nous l'avons observé pendant la pandémie de COVID-19, les cybercriminels cherchent à tirer profit de cette période de crise et d'incertitude. Nos recherches suivent l'évolution du paysage des menaces. Nous continuons à concentrer nos efforts sur l'amélioration continue de l'efficacité de nos produits et la mise à disposition d'informations exploitables à nos parties prenantes afin qu'elles puissent protéger leurs ressources les plus précieuses. Dans ce rapport, vous découvrirez l'importance de notre travail pour tous les membres de l'équipe Trellix Advanced Research Center. Nos chercheurs et experts abordent tous les projets avec une motivation sans faille.

N'hésitez pas à nous faire part de vos commentaires sur ce rapport détaillé. Si vous souhaitez que notre équipe se penche sur des aspects spécifiques, contactez-moi ou notre équipe @TrellixARC sur Twitter. Nous nous réjouissons de vous retrouver à l'occasion de la conférence RSA qui se tiendra à San Francisco en avril.

John Fokker
Directeur de la Threat Intelligence

MÉTHODOLOGIE

Les systèmes principaux de Trellix fournissent des données télémétriques sur lesquelles nous nous appuyons pour élaborer nos rapports trimestriels sur le paysage des menaces. Nous combinons ces données télémétriques avec une Threat Intelligence open source et nos propres investigations sur les menaces prévalentes telles que les ransomwares et les cyberattaques étatiques.

Lorsque nous employons le terme « données télémétriques », nous faisons référence aux détections, pas aux infections. Une détection est enregistrée lorsqu'un fichier, une URL, une adresse IP ou un autre indicateur est détecté par l'un de nos produits et que nous en sommes alertés.

Par exemple, nous savons qu'un nombre croissant d'entreprises utilisent des infrastructures de test de l'efficacité qui déploient de vrais échantillons de malwares. Cette utilisation apparaîtra comme une détection, mais ne constitue en aucun cas une infection.

Le processus d'analyse et de filtrage des faux positifs dans les données télémétriques est en constant développement, ce qui peut entraîner l'apparition de nouvelles catégories de menaces par rapport aux éditions précédentes.

De nouvelles catégories de menaces seront également ajoutées à mesure que davantage d'équipes Trellix contribueront à ce rapport trimestriel.

La confidentialité de nos clients est essentielle. Elle est respectée lors de la collecte des données télémétriques et lors de la mise en correspondance de ces données avec les pays et secteurs d'activité de nos clients. Comme notre base clients varie selon les pays, les évolutions sont analysées de manière approfondie afin d'identifier les facteurs qui entrent en jeu. À titre d'exemple, le secteur des télécommunications affiche souvent des scores élevés en matière de menaces. Cela ne signifie pas nécessairement qu'il est fortement ciblé en tant que tel. Le secteur des télécommunications comprend des FAI qui possèdent des espaces d'adressage IP pouvant être achetés par d'autres entreprises. Qu'est-ce que cela signifie ? Les envois à partir de l'espace d'adressage IP d'un FAI apparaissent comme des détections dans le secteur des télécommunications, mais pourraient en réalité provenir de clients de ce FAI qui opèrent dans un autre secteur.

RANSOMWARES – T4 2022

Cette section regroupe les informations que nous avons collectées sur l'activité des groupes spécialisés dans le ransomware. Ces informations proviennent de plusieurs sources, ce qui nous permet de dresser un tableau plus complet du paysage des menaces, de réduire le biais d'observation et de déterminer la famille de ransomwares la plus marquante au 4e trimestre 2022. La première source est quantitative. Elle illustre les statistiques des campagnes de ransomware découlant de la mise en corrélation des indicateurs de compromission (IOC) et des données télémétriques des clients de Trellix. La deuxième source est qualitative. Elle montre l'analyse des différents rapports publiés par le secteur de la sécurité qui sont validés et analysés par le groupe Threat Intelligence. Enfin, la troisième source est une nouvelle catégorie qui regroupe les informations sur les victimes de ransomwares tirées des divers « sites de divulgation » (leak sites) des groupes d'auteurs de ransomware ; ces informations sont normalisées, enrichies puis analysées pour obtenir une version anonymisée des résultats.

En proposant ces différents points de vue, nous espérons vous donner les clés pour comprendre le paysage actuel des menaces. Aucun d'entre eux n'est suffisant, car chacun présente ses propres limites. Personne n'a accès à tous les journaux de tous les systèmes connectés à Internet, les incidents de sécurité ne sont pas tous signalés et toutes les victimes ne font pas forcément l'objet d'extorsions ou de publication sur des sites de divulgation. Toutefois, l'association de ces différents points de vue permet de mieux comprendre le paysage des menaces, tout en limitant nos propres angles morts.

Une combinaison de données quantitatives et qualitatives provenant de diverses sources permet de porter un jugement éclairé, tout en tenant compte des potentiels inconvénients et angles morts.

L'actualité des ransomwares – T4 2022

Groupe de ransomware ayant le plus d'impact au 4e trimestre : LockBit 3.0

Par l'observation des diverses sources de Trellix, nous pouvons conclure que LockBit 3.0 a été le groupe de ransomware le plus marquant au 4e trimestre 2022. La réputation de LockBit 3.0 repose sur les caractéristiques suivantes :

3e LockBit 3.0 a été le troisième groupe de ransomware le plus prévalent au cours du trimestre, d'après l'analyse des données télémétriques sur les ransomwares collectées par les capteurs de Trellix déployés dans le monde entier.

2e LockBit 3.0 a été le deuxième groupe de ransomware le plus signalé par le secteur de la sécurité avec Cuba, d'après l'analyse des différentes campagnes identifiées par le groupe Threat Intelligence.

1er Le site de divulgation de LockBit 3.0 a répertorié le plus de victimes parmi tous les groupes de ransomware au cours du trimestre. Cela fait de LockBit le groupe le plus enclin à avoir recours à la dénonciation publique comme moyen de pression.

Voici d'autres catégories et observations liées à LockBit pour le 4e trimestre 2022 :

SECTEURS TOUCHÉS PAR LOCKBIT 3.0 – T4 2022

29 %

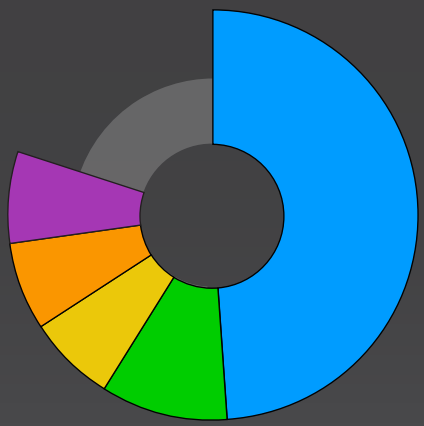
D'après le site de divulgation de LockBit 3.0, les biens et services industriels ont été le secteur le plus touché par LockBit 3.0 au 4e trimestre 2022.

- Biens et services industriels
- Vente au détail
- Technologies
- Santé
- Construction et matériaux
- Biens personnels et domestiques
- Administration publique

PAYS DES ENTREPRISES TOUCHÉES PAR LOCKBIT 3.0 – T4 2022

49 %

D'après le site de divulgation de LockBit 3.0, les entreprises américaines ont été les plus touchées (49 %) par LockBit 3.0 au 4e trimestre 2022, suivies par les entreprises britanniques.



- États-Unis
- Royaume-Uni
- Canada
- France
- Brésil

Outils et exploits LockBit 3.0

VULNÉRABILITÉS CONNUES POUR ÊTRE EXPLOITÉES PAR LOCKBIT 3.0

CVE-2018-13379
CVE-2020-0787
CVE-2021-20028
CVE-2021-34473
CVE-2021-34523

OUTILS MALVEILLANTS UTILISÉS PAR LOCKBIT 3.0

Amadey	Hakops
Blister	Neshta
BloodHound	SocGholish
Cobalt Strike	StealBit
GrabFF	WinPEAS

OUTILS NON MALVEILLANTS UTILISÉS PAR LOCKBIT 3.0

BCDEdit	MiniDump	NSIS	Schtasks.exe
Cmd	MpCmdRun.exe	PCHunter	VSSAdmin
Fltmc.exe	Mshta	PowerShell	wevtutil
Fsutil	MSTSC	Process Monitor	WMIC
GMER	Netsh	Rundll32	RCLONE
MEGASYNC	Nltest		

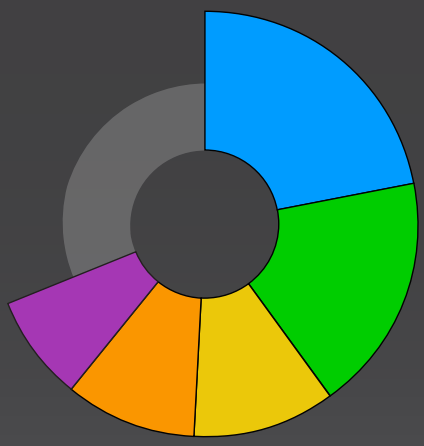
Les ransomwares par le prisme de nos données télémétriques

Les statistiques suivantes reposent sur la mise en corrélation de nos données télémétriques et de notre base de connaissances de Threat Intelligence. Après une phase d'analyse, nous identifions un ensemble de campagnes à partir des données recueillies sur la période sélectionnée et extrayons leurs caractéristiques. Les statistiques affichées sont celles des campagnes, et non des détections en elles-mêmes. Nos données télémétriques mondiales révèlent des indicateurs de compromission (IOC) qui appartiennent à plusieurs campagnes lancées par divers groupes cybercriminels. Les familles de ransomwares suivantes, avec leurs outils et techniques respectifs, ont été les plus prévalentes dans les campagnes identifiées. De même, les pays et secteurs ci-dessous ont été les plus touchés par les campagnes identifiées.

FAMILLES DE RANSOMWARES LES PLUS PRÉVALENTES – T4 2022

22 %

Cuba a été la famille de ransomwares la plus prévalente au 4e trimestre 2022. Zeppelin a souvent été utilisé par Vice Society. En savoir plus sur les fuites de communication de Yanluowang



- Cuba
- Hive
- LockBit
- Zeppelin
- Yanluowang

OUTILS MALVEILLANTS LES PLUS PRÉVALENTS UTILISÉS PAR LES GROUPES DE RANSOMWARE – T4 2022

41 %

Cobalt Strike a été l'outil malveillant le plus prévalent utilisé par les groupes de ransomware au 4e trimestre 2022.

1.	Cobalt Strike	41 %
2.	Mimikatz	23 %
3.	BURNTCIGAR	13 %
4.	VMProtect	12 %
5.	POORTRY	11 %

TECHNIQUES MITRE ATT&CK LES PLUS UTILISÉES PAR LES GROUPES DE RANSOMWARE – T4 2022

1.	Chiffrement de données pour impact	17 %
2.	Découverte des informations système	11 %
3.	PowerShell	10 %
4.	Transfert d'outils à l'entrée	10 %
5.	Windows Command Shell	9 %

OUTILS NON MALVEILLANTS LES PLUS PRÉVALENTS UTILISÉS PAR LES GROUPES DE RANSOMWARE – T4 2022

21 %

Cmd a été l'outil non malveillant le plus prévalent utilisé par les groupes de ransomware au 4e trimestre 2022.

1.	Cmd	21 %
2.	PowerShell	14 %
3.	Net	10 %
4.	Reg	8 %
5.	PsExec	8 %

PAYS LES PLUS TOUCHÉS PAR LES GROUPES DE RANSOMWARE – T4 2022

29 %

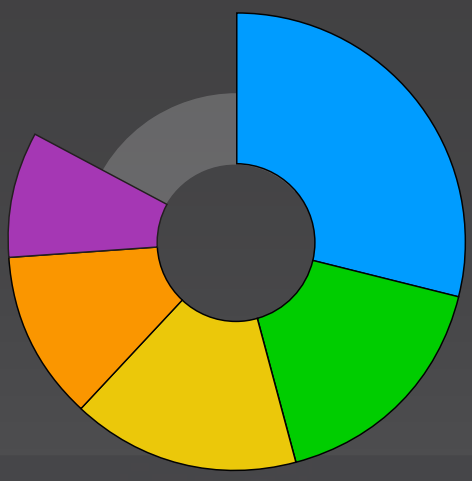
D'après les données télémétriques de Trellix, les États-Unis ont été le pays le plus touché par les groupes de ransomware au 4e trimestre 2022.

- États-Unis
- Chine
- Qatar
- Japon
- Indonésie

SECTEURS LES PLUS TOUCHÉS PAR LES GROUPES DE RANSOMWARE – T4 2022

29 %

D'après les données télémétriques de Trellix, le secteur de l'externalisation et de l'hébergement a été le plus touché par les groupes de ransomware au 4e trimestre 2022. Cela concorde avec la taille moyenne des entreprises des victimes répertoriées sur les sites de divulgation des ransomwares. Ces entreprises ne disposent généralement pas de leur propre bloc IP attribué et ont recours à des fournisseurs d'hébergement tiers.



- Externalisation et hébergement
- Banques/Finance/ Gestion de patrimoine
- Administration publique
- Vente en gros
- Pharmaceutique

Ransomwares identifiés par le secteur de la sécurité

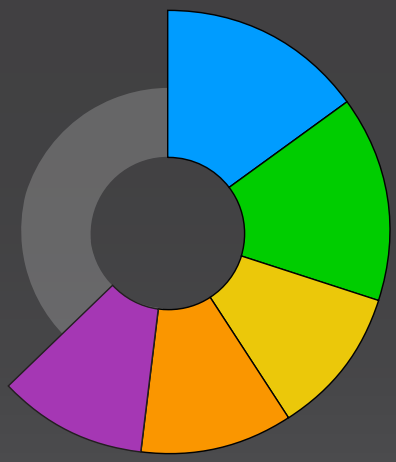
Les statistiques suivantes se basent sur des rapports publics et des recherches internes. Il convient de noter que les incidents liés aux ransomwares ne sont pas tous signalés. De nombreuses familles de ransomwares sont actives depuis longtemps et sont naturellement moins remarquables que les nouvelles familles au cours de trimestres spécifiques. Selon ces critères, ces mesures sont un indicateur des familles de ransomwares que le secteur de la sécurité a identifiées comme étant les plus pertinentes et marquantes au cours du trimestre.

FAMILLES DE RANSOMWARES LES PLUS SIGNALÉES - T4 2022

15 %

D'après les rapports publiés par le secteur de la sécurité, les familles de ransomwares Black Basta et Magniber ont été les plus signalées au 4e trimestre 2022.

- Black Basta
- Magniber
- Cuba
- LockBit
- Quantum



PRINCIPALES TECHNIQUES D'ATTAQUE UTILISÉES PAR LES FAMILLES DE RANSOMWARES - T4 2022

19 %

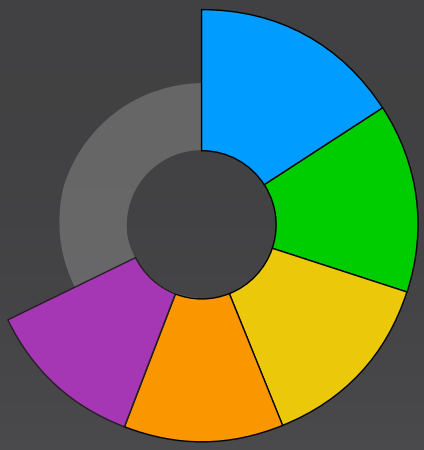
D'après les rapports publiés par le secteur de la sécurité, le chiffrement de données pour impact a été la technique d'attaque utilisée par les familles de ransomwares la plus signalée au 4e trimestre 2022.

1.	Chiffrement de données pour impact	19 %
2.	Windows Command Shell	11 %
3.	Découverte des informations système	10 %
4.	Transfert d'outils à l'entrée	10 %
5.	PowerShell	10 %

PRINCIPAUX SECTEURS CIBLÉS PAR LES FAMILLES DE RANSOMWARES – T4 2022

16 %

D'après les rapports publiés par le secteur de la sécurité, la santé a été le secteur le plus ciblé par les familles de ransomwares au 4e trimestre 2022.



- Santé
- Finance
- Administration publique
- Fabrication
- Transports

PAYS LES PLUS CIBLÉS PAR LES FAMILLES DE RANSOMWARES – T4 2022

19 %

D'après les rapports publiés par le secteur de la sécurité, les États-Unis ont été le pays le plus ciblé par les familles de ransomwares au 4e trimestre 2022.

- États-Unis
- Allemagne
- Brésil
- Argentine
- Canada
- Inde
- Pays-Bas
- Corée du Sud
- Suisse
- Royaume-Uni

CVE UTILISÉES PAR LES FAMILLES DE RANSOMWARES – T4 2022

1.	CVE-2021-31207	16 %
	CVE-2021-34474	16 %
	CVE-2021-34523	16 %
2.	CVE-2021-34527	13 %
3.	CVE-2021-26855	9 %
	CVE-2021-27065	9 %

OUTILS MALVEILLANTS UTILISÉS PAR LES FAMILLES DE RANSOMWARES – T4 2022

44 %

D'après les rapports publiés par le secteur de la sécurité, Cobalt Strike a été l'outil malveillant le plus utilisé par les familles de ransomwares signalées au 4e trimestre 2022.

1.	Cobalt Strike	44 %
2.	QakBot	13 %
3.	IcedID	9 %
4.	BURNTCIGAR	7 %
5.	Carbanak SystemBC	7 % 7 %

OUTILS NON MALVEILLANTS UTILISÉS PAR LES FAMILLES DE RANSOMWARES – T4 2022

21 %

D'après les rapports publiés par le secteur de la sécurité, PowerShell a été l'outil non malveillant le plus utilisé par les familles de ransomwares signalées au 4e trimestre 2022.

1.	PowerShell	21 %
2.	Cmd	18 %
3.	Rundll32	11 %
4.	VSSAdmin	10 %
5.	WMIC	9 %

Victimes répertoriées sur les « sites de divulgation » des ransomwares – T4 2022

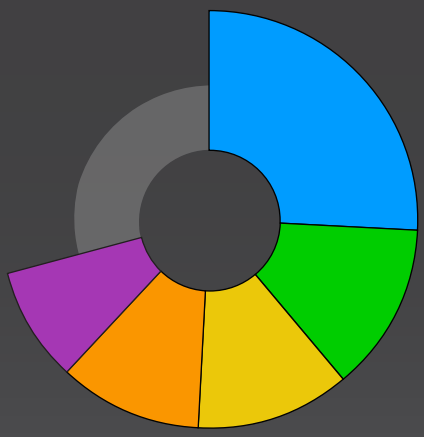
Les données de cette section ont été compilées en analysant les « sites de divulgation » (leak sites) de divers groupes de ransomware. Ces sites constituent un moyen de pression supplémentaire : lorsque les négociations piétinent ou que les victimes refusent de payer la rançon à l'échéance, les groupes de ransomware y divulguent les informations volées lors de leur attaque. Nous utilisons l'outil open source RansomLook pour collecter les diverses publications, puis nous traitons les données en interne pour normaliser et enrichir les résultats afin d'obtenir une version anonymisée de l'analyse de la victimologie.

Il est important de souligner que les victimes de ransomwares ne sont pas toutes répertoriées sur les sites de divulgation concernés. Bon nombre de victimes paient la rançon et ne sont pas comptabilisées. Ces mesures sont un indicateur des victimes ayant fait l'objet d'extorsion ou de représailles, à ne pas confondre avec le nombre total de victimes.

GROUPES DE RANSOMWARE COMPTABILISANT LE PLUS DE VICTIMES – T4 2022

26 %

LockBit 3.0 représente 26 % des 10 principaux groupes de ransomware comptabilisant le plus de victimes sur leurs sites de divulgation respectifs au 4e trimestre 2022.

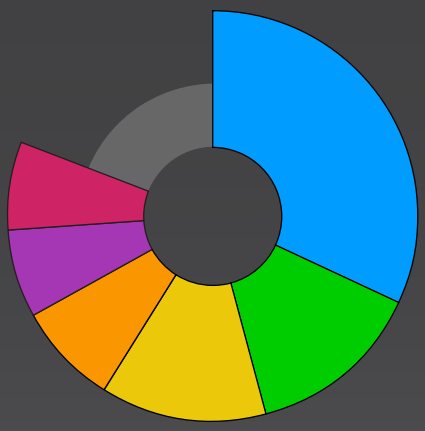


- LockBit 3.0
- ALPHV
- Royal
- Black Basta
- Cuba

SECTEURS TOUCHÉS PAR DES GROUPES DE RANSOMWARE SELON LEURS SITES DE DIVULGATION – T4 2022

32 %

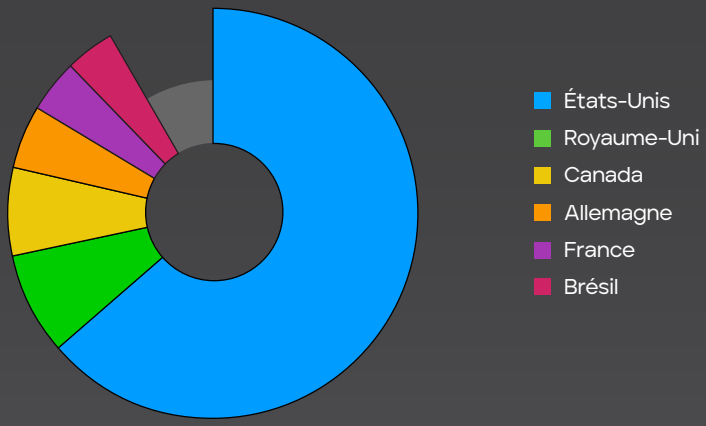
Le secteur des biens et services industriels a été le secteur le plus prévalent touché par des groupes de ransomware selon leurs sites de divulgation au 4e trimestre 2022. Les biens et services industriels désignent tous les produits matériels et services intangibles principalement utilisés pour la construction et la fabrication.



- Biens et services industriels
- Vente au détail
- Technologies
- Construction et matériaux
- Santé
- Administration publique

PAYS DES ENTREPRISES TOUCHÉES PAR DES GROUPES DE RANSOMWARE SELON LEURS SITES DE DIVULGATION – T4 2022

63 % des 10 principales entreprises répertoriées par divers groupes de ransomware sur leurs sites de divulgation respectifs au 4e trimestre 2022 étaient basées aux États-Unis. Elles sont suivies par le Royaume-Uni (8 %) et le Canada (7 %).



STATISTIQUES SUR LES ATTAQUES ÉTATIQUES – T4 2022

Cette section comprend des informations que nous avons collectées sur l'activité des groupes cybercriminels étatiques. Ces informations proviennent de plusieurs sources, ce qui nous permet de dresser un tableau plus complet du paysage des menaces et de réduire le biais d'observation. Premièrement, nous utilisons les statistiques extraites de la mise en corrélation des indicateurs de compromission (IOC) des groupes étatiques et des données télémétriques des clients de Trellix. Deuxièmement, nous fournissons des informations tirées de différents rapports publiés par le secteur de la sécurité, qui sont validés et analysés par le groupe Threat Intelligence.

L'actualité des attaques étatiques – T4 2022

- Les États-Unis et l'Allemagne ont enregistré une hausse significative du nombre d'attaques étatiques.
- La Chine et le Vietnam ont fait leur entrée dans le classement des pays les plus touchés par ce type d'attaques au 4e trimestre.

Statistiques sur les attaques étatiques par le prisme de nos données télémétriques mondiales

Ces statistiques reposent sur la mise en corrélation de nos données télémétriques et de notre base de connaissances de Threat Intelligence. Après une phase d'analyse, nous identifions un ensemble de campagnes à partir des données recueillies sur la période

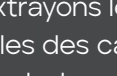
sélectionnée et extrayons leurs caractéristiques. Les statistiques affichées sont celles des campagnes, et non des détections en elles-mêmes. Compte tenu de l'agrégation de différents journaux, de l'utilisation d'infrastructures de simulation de menaces par nos clients et de la mise en corrélation de haut niveau avec la base de connaissances de Threat Intelligence, les données sont filtrées manuellement pour répondre aux critères souhaités.

Nos données télémétriques mondiales révèlent des indicateurs de compromission (IOC) qui appartiennent à plusieurs campagnes lancées par des groupes APT. Les pays et cybercriminels suivants, ainsi que leurs outils et techniques, ont été les plus prévalents dans les campagnes identifiées. De même, les données concernant les pays et les secteurs représentent ceux qui sont les plus touchés par les campagnes identifiées.

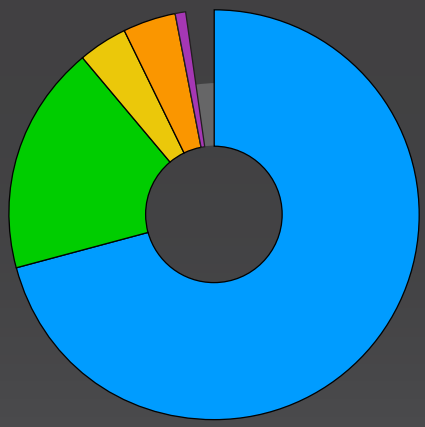
Données télémétriques sur les attaques étatiques

PAYS D'ORIGINE LES PLUS PRÉVALENTS DES CYBERCRIMINELS IMPLIQUÉS DANS LES ATTAQUES ÉTATIQUES – T4 2022

71 %



La Chine est le pays d'origine d'où émanent le plus grand nombre de cybercriminels à l'origine d'attaques étatiques au 4e trimestre 2022.

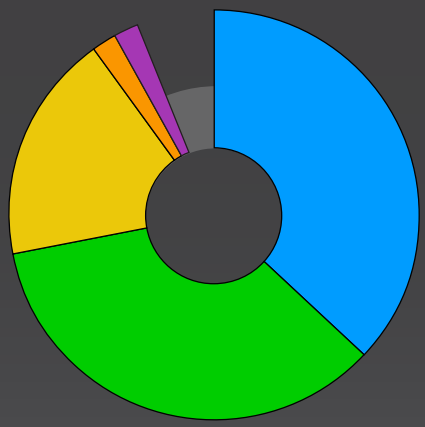


- Chine
- Corée du Nord
- Russie
- Iran
- Liban

GROUPES CYBERCRIMINELS LES PLUS PRÉVALENTS – T4 2022

37 %

D'après les données télémétriques sur les attaques étatiques, Mustang Panda a été le groupe cybercriminel le plus prévalent au 4e trimestre 2022.



- Mustang Panda
- UNC4191
- Lazarus
- MuddyWater
- Kimsuky

TECHNIQUES MITRE ATT&CK LES PLUS PRÉVALENTES UTILISÉES DANS DES ATTAQUES ÉTATIQUES – T4 2022

1.	Chargement latéral de DLL	14 %
2.	Rundll32	13 %
3.	Obfuscation de fichiers ou d'informations	12 %
4.	Windows Command Shell	11 %
5.	Clés d'exécution du Registre/ dossier de démarrage	10 %

OUTILS MALVEILLANTS LES PLUS PRÉVALENTS UTILISÉS DANS DES ATTAQUES ÉTATIQUES – T4 2022

1.	PlugX	24 %
2.	BLUEHAZE	23 %
3.	DARKDEW	23 %
4.	MISTCLOAK	23 %
5.	JSX (cheval de Troie d'accès à distance)	2 %

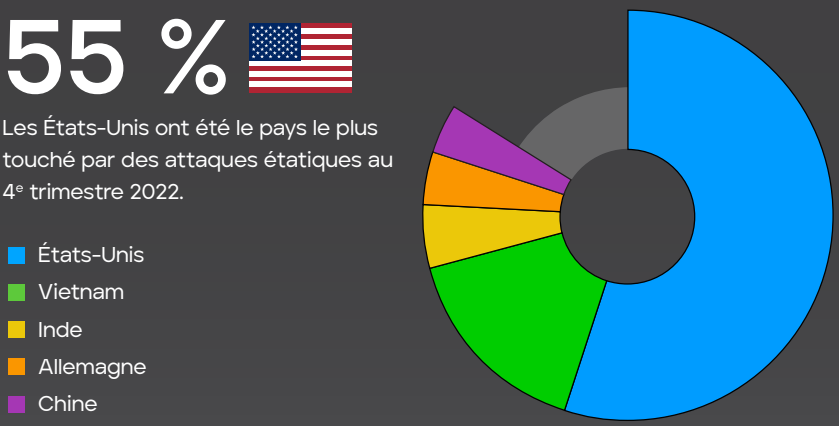
OUTILS NON MALVEILLANTS LES PLUS PRÉVALENTS UTILISÉS DANS DES ATTAQUES ÉTATIQUES – T4 2022

1.	Rundll32	22 %
2.	Cmd	19 %
3.	Reg	17 %
4.	Ncat	12 %
5.	Regsvr32	6 %

PAYS LES PLUS TOUCHÉS PAR DES ATTAQUES ÉTATIQUES – T4 2022

55 %

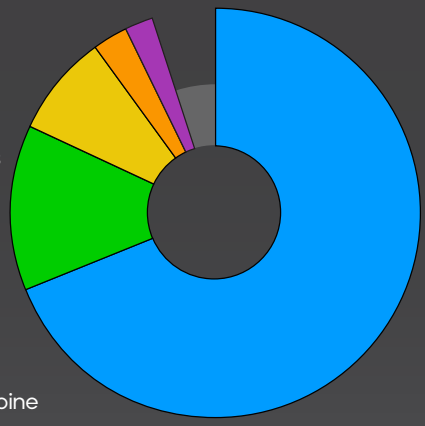
Les États-Unis ont été le pays le plus touché par des attaques étatiques au 4e trimestre 2022.



SECTEURS LES PLUS TOUCHÉS PAR DES ATTAQUES ÉTATIQUES – T4 2022

69 %

Les transports et la logistique ont été le secteur le plus touché par des attaques étatiques au 4e trimestre 2022.



Incidents d'attaques étatiques selon les rapports publics – T4 2022

Ces statistiques se basent sur des rapports publics et des recherches internes, et non sur les données télémétriques issues des journaux des clients. Il convient de noter que les cyberattaques étatiques ne sont pas toutes notifiées. De nombreuses campagnes suivent des tactiques, techniques et procédures (TTP) déjà connues et sont donc moins intéressantes à analyser. Le secteur a tendance à se concentrer sur des campagnes plus récentes où un cybercriminel a introduit une nouveauté ou commis une erreur. Ces mesures sont un indicateur de ce que le secteur a trouvé utile et pertinent au 4e trimestre 2022.

PAYS OÙ LE PLUS DE CAMPAGNES D'ATTAQUES ÉTATIQUES ONT ÉTÉ SIGNALÉES – T4 2022

37 %

des campagnes d'attaques étatiques rendues publiques au 4e trimestre 2022 ont été lancées depuis la Chine.

1.	Chine	37 %
2.	Corée du Nord	24 %
3.	Iran	1 %
4.	Russie	1 %
5.	Inde	1 %

CYBERCRIMINELS LES PLUS PRÉVALENTS À L'ORIGINE D'ATTAQUES ÉTATIQUES SIGNALÉES – T4 2022

33 %

Lazarus est l'acteur d'attaques étatiques signalées qui a été le plus prévalent au 4e trimestre 2022.

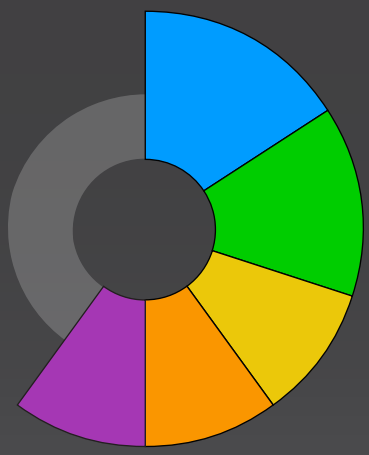
1.	Lazarus	33 %
2.	Mustang Panda	17 %
3.	APT34 APT37 APT41 COLDRIVER Patchwork Polonium SideWinder Winnti Group	1 % chacun

PAYS LES PLUS CIBLÉS PAR DES CAMPAGNES D'ATTAQUES ÉTATIQUES SIGNALÉES – T4 2022

16 %

Les États-Unis ont été le pays le plus ciblé par des campagnes d'attaques étatiques signalées au 4e trimestre 2022.

- États-Unis
- Royaume-Uni
- Pakistan
- Russie
- Ukraine

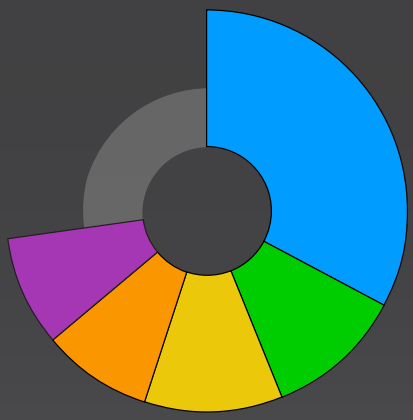


SECTEURS LES PLUS CIBLÉS PAR DES CAMPAGNES D'ATTAQUES ÉTATIQUES SIGNALÉES – T4 2022

33 %

L'administration publique a été le secteur le plus ciblé par des campagnes d'attaques étatiques signalées au 4e trimestre 2022, suivie par le secteur militaire (11 %) et les télécommunications (11 %).

- Administration publique
- Militaire
- Télécommunications
- Énergie
- Finance



OUTILS MALVEILLANTS LES PLUS UTILISÉS DANS LES CAMPAGNES D'ATTAQUES ÉTATIQUES SIGNALÉES – T4 2022

1.	PlugX	22 %
2.	Cobalt Strike	17 %
3.	Metasploit	13 %
4.	BlindingCan	9 %
5.	Scanbox ShadowPad ZeroCleare	9 % chacun

OUTILS NON MALVEILLANTS LES PLUS UTILISÉS DANS DES CAMPAGNES D'ATTAQUES ÉTATIQUES – T4 2022

1.	Cmd	32 %
2.	Rundll32	20 %
3.	PowerShell	14 %
4.	Reg	8 %
5.	Schtasks.exe	7 %

TECHNIQUES MITRE ATT&CK LES PLUS UTILISÉES DANS LES CAMPAGNES D'ATTAQUES ÉTATIQUES SIGNALÉES – T4 2022

1.	Transfert d'outils à l'entrée	13 %
2.	Découverte des informations système	13 %
3.	Obfuscation de fichiers ou d'informations	12 %
4.	Protocoles web	11 %
5.	Désobfuscation/décodage de fichiers ou d'informations	11 %

VULNÉRABILITÉS EXPLOITÉES PAR LES CAMPAGNES D'ATTAQUES ÉTATIQUES SIGNALÉES – T4 2022

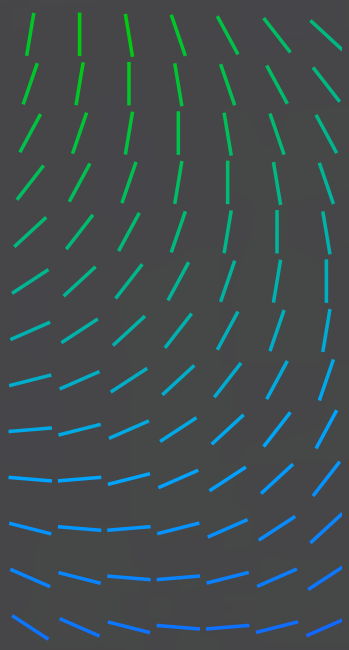
CVE-2017-11882
CVE-2021-44228
CVE-2018-0802
CVE-2021-26855
CVE-2021-27065
CVE-2021-34473
CVE-2021-34523
CVE-2015-2545
CVE-2017-0144
CVE-2018-0798
CVE-2018-8581
CVE-2019-0604
CVE-2019-0708
CVE-2019-16098
CVE-2020-0688
CVE-2020-1380
CVE-2020-1472
CVE-2020-17141
CVE-2020-17143
CVE-2021-21551
CVE-2021-26606
CVE-2021-26857
CVE-2021-26858
CVE-2021-28480
CVE-2021-28481
CVE-2021-28482
CVE-2021-28483
CVE-2021-31196
CVE-2021-31207
CVE-2021-40444
CVE-2021-45046
CVE-2021-45105
CVE-2022-1040
CVE-2022-30190
CVE-2022-41128

EXPLOITATION DES RESSOURCES LOCALES ET OUTILS TIERS – T4 2022

Les observations et le suivi par le biais de la plate-forme Global Threat Intelligence de Trellix Insights ont permis d'obtenir les informations et la visibilité suivantes sur le paysage des menaces du 4e trimestre 2022.

L'ACTUALITÉ DE L'EXPLOITATION DES RESSOURCES LOCALES – T4 2022

- L'exploitation des ressources locales continue à jouer un rôle lors de toutes les phases d'une attaque : accès initial, exécution, découverte, persistance et impact.
- Dans les données collectées au 4e trimestre 2022, l'exécution de commandes et de scripts via Windows Command Shell ou PowerShell s'impose comme la technique la plus utilisée.



- Le recours à l'exploitation des ressources locales est prévalent parmi les cybercriminels, y compris les groupes APT chevronnés, les collectifs motivés par l'appât du gain et les cyberactivistes.

Les nouveaux venus, les cybercriminels ponctuels et les pirates amateurs qui font des incursions dans le paysage des menaces utilisent également les fichiers binaires déjà utilisés dans le cadre d'exploits dans l'espoir de passer inaperçus et de pirater un système ou d'exploiter une vulnérabilité.

Les techniques d'exploitation des ressources locales continuent à être utilisées pour réaliser des tâches malveillantes lors de toutes les phases d'une attaque : accès initial, exécution, découverte, persistance et impact. Dans les données collectées au 4e trimestre 2022, l'exécution de commandes et de scripts via Windows Command Shell ou PowerShell s'impose comme la technique la plus utilisée.

FICHIERS BINAIRES DE SYSTÈMES D'EXPLOITATION LES PLUS PRÉVALENTS – T4 2022

47 %

Windows Command Shell représente près de la moitié (47 %) des 10 fichiers binaires de systèmes d'exploitation les plus prévalents au 4e trimestre 2022, suivi par PowerShell (32 %) et Rundl32 (27 %).

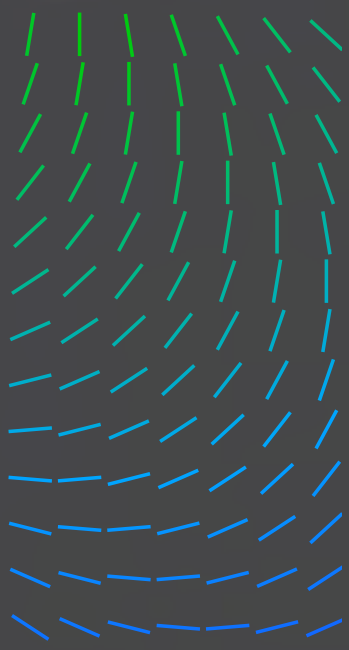
1.	Windows Command Shell	47 %
2.	PowerShell	32 %
3.	Rundl32	27 %
4.	Schtasks	23 %
5.	WMI	21 %

Le recours à l'exploitation des ressources locales est prévalent parmi les cybercriminels, y compris les groupes APT chevronnés, les collectifs motivés par l'appât du gain et les cyberactivistes.

Les événements traités par le biais de la plate-forme Trellix Insights et pour lesquels les cybercriminels ont utilisé des fichiers binaires Windows ont entraîné le déploiement de malwares supplémentaires tels qu'un outil d'exfiltration d'informations, un cheval de Troie d'accès à distance ou un ransomware. Les fichiers binaires tels que MSHTA, WMI et WScript peuvent avoir été exécutés pour récupérer les charges actives supplémentaires à partir des ressources contrôlées par les attaquants.

PRINCIPAUX OUTILS TIERS – T4 2022

1.	Outils d'accès à distance	58 %
2.	Transfert de fichiers	22 %
3.	Outils de post-exploitation	20 %
4.	Découverte du réseau	16 %
5.	Découverte d'Active Directory	10 %



Les outils d'accès et de contrôle à distance font systématiquement partie des outils les plus exploités par les cybercriminels. De même, les outils employés par les professionnels de la sécurité continuent à être détournés à des fins malveillantes. Les cybercriminels peuvent s'en servir pour initier des balises de connexion active, automatiser l'exfiltration ou collecter et compresser des informations ciblées.

Parmi les outils gratuits et open source, les programmes de compression sont exploités par les cybercriminels pour recompresser un logiciel légitime afin d'y inclure du contenu malveillant ou pour compresser des malwares dans l'espoir d'empêcher leur détection et leur analyse.

OBSERVATIONS SUR COBALT STRIKE – T4 2022

Le groupe Threat Intelligence de Trellix Advanced Research Center surveille l'utilisation des serveurs Cobalt Strike (C2 Cobalt Strike) en environnement réel en combinant des méthodologies de traque des charges actives et des infrastructures. Dans cette section, nous vous présentons nos observations tirées de l'analyse des balises Cobalt Strike collectées :

15 %
LICENCES D'ÉVALUATION DE COBALT STRIKE

Seulement 15 % des balises Cobalt Strike identifiées en environnement réel disposaient d'une licence d'évaluation de Cobalt Strike. Cette version de Cobalt Strike inclut la plupart des fonctionnalités connues de ce framework de post-exploitation. Toutefois, elle ajoute des « signaux » et désactive le chiffrement des données en transit pour rendre la charge active facilement détectable par les produits de sécurité.

87 %
RUNDLL32.EXE

Rundll32.exe, le processus par défaut utilisé pour générer des sessions et exécuter des tâches de post-exploitation, a été détecté dans 87 % des balises identifiées.

5 % EN-TÊTE HTTP HOST

Au moins 5 % des balises Cobalt Strike identifiées utilisaient l'en-tête HTTP Host, une option qui permet le domain fronting avec Cobalt Strike. Le domain fronting est une technique qui exploite des réseaux de distribution de contenu (CDN) hébergeant plusieurs domaines. Les attaquants dissimulent une requête HTTPS envoyée à un site web malveillant sous une connexion TLS à un site web légitime.

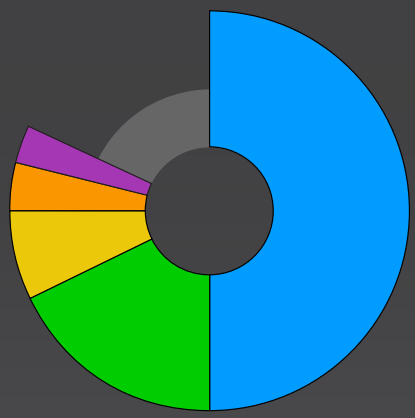
22 % BALISES DNS

Les balises DNS représentent 22 % des balises Cobalt Strike identifiées. Ce type de charge active communique avec le serveur Cobalt Strike de l'attaquant, qui est le serveur de référence du domaine, via des requêtes DNS pour dissimuler son activité.

PRINCIPAUX PAYS HÉBERGEANT DES SERVEURS COBALT STRIKE – T4 2022

50 %

La moitié des serveurs Cobalt Strike détectés au 4e trimestre 2022 étaient hébergés en Chine, ce qui s'explique en grande partie par la capacité d'hébergement cloud disponible dans ce pays.



GOOTLOADER – T4 2022

Gootloader est un malware modulaire parfois appelé « GootKit » ou « GootKit Loader ». À l'heure actuelle, les fonctionnalités modulaires du malware Gootloader sont utilisées pour distribuer des charges actives supplémentaires comme REvil, Kronos, Cobalt Strike et IcedID.

Lors d'événements récents, Gootloader a eu recours à l'optimisation pour les moteurs de recherche (SEO) pour inciter des utilisateurs trop confiants à se rendre sur un site compromis ou frauduleux utilisé pour héberger un fichier d'archive contenant une charge active JavaScript. Cette technique exige toutefois que l'utilisateur trop confiant ouvre l'archive et en exécute le contenu, qui exécute à son tour le code JavaScript malveillant via Windows Scripting Host. Une fois l'exécution réussie, Gootloader initie des communications C2 et récupère d'autres malwares.

On soupçonne Gootloader d'être un service MaaS (Malware-as-a-Service) permettant aux cybercriminels abonnés de déployer plusieurs charges actives supplémentaires. Il constitue donc une menace majeure pour les environnements d'entreprise.

Grâce à notre outil de suivi interne de Gootloader, nous avons identifié une variante récente, observée en environnement réel le 18 novembre 2022, ainsi que des variantes plus anciennes silencieuses depuis le 13 novembre 2022. Les modifications apportées à la dernière variante sont les suivantes :

- Suppression de la fonctionnalité de manipulation du Registre
- Augmentation des requêtes réseau distantes à 10 URL plutôt que trois

- Capacité d'invoquer directement des scripts PowerShell via CScript
- Persistance pour chaque connexion utilisateur

Notre processus de suivi de Gootloader

La nouvelle variante de Gootloader utilise plusieurs couches d'obfuscation. Chaque phase imbriquée après la décompression a recours à des variables chargées à un stade précoce qui compliquent l'analyse. Les échantillons collectés grâce à nos efforts de traque YARA sont chargés dans un analyseur JavaScript et PowerShell statique pour extraire des indicateurs de compromission (IOC) tels que des serveurs de commande et de contrôle (C&C, C2) et des signatures d'identification uniques. Ces indicateurs permettent d'identifier et de suivre des instances spécifiques de Gootloader en environnement réel.

Les indicateurs extraits sont ensuite traités en interrogeant la base de données de l'équipe Trellix chargée de la réputation des URL pour identifier les URL malveillantes, les domaines légitimes potentiellement compromis et les domaines légitimes utilisés comme leurres pour perturber l'analyse.

Données télémétriques sur Gootloader

Les statistiques affichées sont celles des campagnes identifiées par la mise en corrélation des indicateurs de compromission (IOC) extraits et des journaux de nos clients, et non des détections en elles-mêmes. Dans le cas de Gootloader, la plupart des détections sont basées sur les accès aux domaines. Étant donné que Gootloader utilise des domaines leurres, les statistiques doivent être interprétées comme malveillantes avec un degré de confiance modéré.

PAYS LES PLUS AFFECTÉS PAR GOOTLOADER – T4 2022

37 %

Les États-Unis ont été le pays le plus affecté par Gootloader au 4e trimestre 2022.

1.	États-Unis	37 %
2.	Italie	19 %
3.	Inde	11 %
4.	Indonésie	9 %
5.	France	5 %

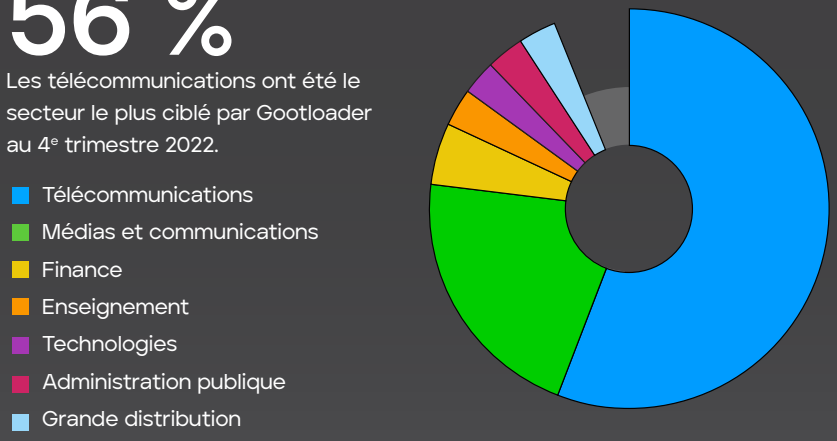
TECHNIQUES MITRE ATT&CK LES PLUS UTILISÉES PAR GOOTLOADER – T4 2022

1. Désobfuscation/ décodage de fichiers ou d'informations
2. JavaScript
3. Obfuscation de fichiers ou d'informations
4. PowerShell
5. Vidage de processus

SECTEURS LES PLUS CIBLÉS PAR GOOTLOADER – T4 2022

56 %

Les télécommunications ont été le secteur le plus ciblé par Gootloader au 4e trimestre 2022.



Techniques MITRE ATT&CK les plus utilisées par Gootloader – T4 2022

Désobfuscation/décodage de fichiers ou d'informations

JavaScript

Obfuscation de fichiers ou d'informations

PowerShell

Vidage de processus

Chargement réflexif de code

Clés d'exécution du Registre/dossier de démarrage

Rundll32

Tâche planifiée

INFORMATIONS SUR LES VULNÉRABILITÉS – T4 2022

Notre tableau de bord des vulnérabilités compile l'analyse des dernières vulnérabilités à fort impact. L'analyse et le tri sont effectués par les experts en vulnérabilités de Trellix Advanced Research Center. Ces chercheurs spécialisés dans l'ingénierie inverse et l'analyse des vulnérabilités surveillent constamment les dernières vulnérabilités et la façon dont les cybercriminels les utilisent dans leurs attaques pour fournir des conseils de correction. Ces conseils concis et très techniques vous permettent de filtrer les signaux des bruits parasites et de vous concentrer sur les vulnérabilités les plus dangereuses pour votre entreprise, afin de pouvoir réagir rapidement.

L'ACTUALITÉ DES VULNÉRABILITÉS – T4 2022

41 % Lanner représente 41 % des produits vulnérables et des fournisseurs affectés par des CVE uniques au 4e trimestre 2022.

29 % La version 1.10.0 du microprogramme d'IAC-AST2500A a été la CVE la plus signalée utilisée par des produits au 4e trimestre 2022.

PRODUITS VULNÉRABLES, FOURNISSEURS ET CVE AYANT LE PLUS D'IMPACT – T4 2022

1.	Lanner	41 %
2.	Microsoft	19 %
3.	Boa	15 %
4.	Oracle	8 %
5.	Apple Chrome Citrix Fortinet Linux	5 % chacun

CVE SIGNALÉES PAR PRODUITS – T4 2022

29 %

La version 1.10.0 du microprogramme d'IAC-AST2500A a été la CVE la plus signalée utilisée par des produits au 4e trimestre 2022, suivie par le serveur Boa (10 %), IAC-AST2500A (6 %) et Exchange (6 %).

Produits avec CVE signalées	CVE uniques
IAC-AST2500A, version 1.10.0 du microprogramme	9
Serveur Boa	3
Exchange	3
IAC-AST2500A	2
tvOS	1
iPadOS	1
iOS	1
Windows	1
Safari	1
SQLite version 3.40.0 et antérieures	1
Oracle Access Manager, 11.1.2.3.0, 12.2.1.3.0, 12.2.1.4.0	1
macOS	1
Noyau Linux avant la version 5.15.61	1
Internet Explorer	1

Produits avec CVE signalées	CVE uniques
FortiOS (sslvpnd)	1
Citrix ADC/Citrix Gateway	1
Chrome avant la version 108.0.5359.94/.95	1
Serveur Boa, Boa 0.94.13	1

CVE SIGNALÉES – T4 2022

CVE-2022-1786
CVE-2022-26134
CVE-2022-27510
CVE-2022-27518
CVE-2022-31685
CVE-2022-32917
CVE-2022-32932
CVE-2022-33679
CVE-2022-34718
CVE-2022-35737
CVE-2022-3602
CVE-2022-3786
CVE-2022-37958
CVE-2022-40684
CVE-2022-41040
CVE-2022-41080
CVE-2022-41082
CVE-2022-41128
CVE-2022-41352
CVE-2022-42468
CVE-2022-42475
CVE-2022-4262
CVE-2022-42856
CVE-2022-42889
CVE-2022-43995
CVE-2022-46908
CVE-2022-47939

TENDANCES EN MATIÈRE DE SÉCURITÉ E-MAIL – T4 2022

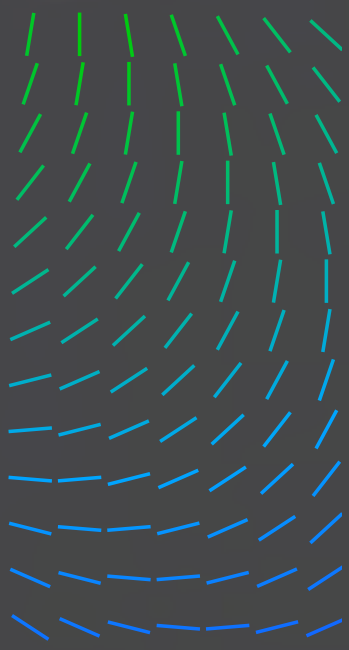
Ces statistiques se basent sur les données télémétriques générées par diverses appliances de sécurité e-mail déployées sur les réseaux de nos clients partout dans le monde. Les journaux de détection sont agrégés et analysés pour produire les informations suivantes :

L'ACTUALITÉ DES TENDANCES EN MATIÈRE DE SÉCURITÉ E-MAIL – T4 2022

100 % Le volume d'e-mails malveillants dans les pays arabes a augmenté de 100 % en octobre par rapport à août et à septembre.

40 % Qakbot a été la tactique de malware la plus utilisée. Il représente 40 % des campagnes ciblant les pays arabes.

42 % Les télécommunications ont été le secteur le plus touché par des e-mails malveillants au 4e trimestre 2022, avec 42 % des campagnes e-mail malveillantes ciblant l'ensemble des secteurs.



87 % Les e-mails de phishing utilisant des URL malveillantes ont été de loin le vecteur d'attaque le plus prévalent au 4e trimestre 2022.

64 % Le nombre d'usurpations d'identité a bondi de 64 % entre le 3e et le 4e trimestre 2022.

82 % des e-mails de fraude au PDG ont été envoyés à l'aide de services e-mail gratuits.

78 % des attaques par piratage de la messagerie en entreprise (BEC) utilisaient des expressions couramment employées par les PDG.

142 % Les attaques de vishing ont progressé de 142 % entre le 3e et le 4e trimestre 2022.

MALWARES E-MAIL LES PLUS PRÉVALENTS – T4 2022

40 %

Qakbot a été le malware e-mail le plus prévalent au 4e trimestre 2022.

1.	Qakbot	40 %
2.	Emotet	26 %
3.	Formbook	26 %
4.	Remcos	4 %
5.	QuadAgent	4 %

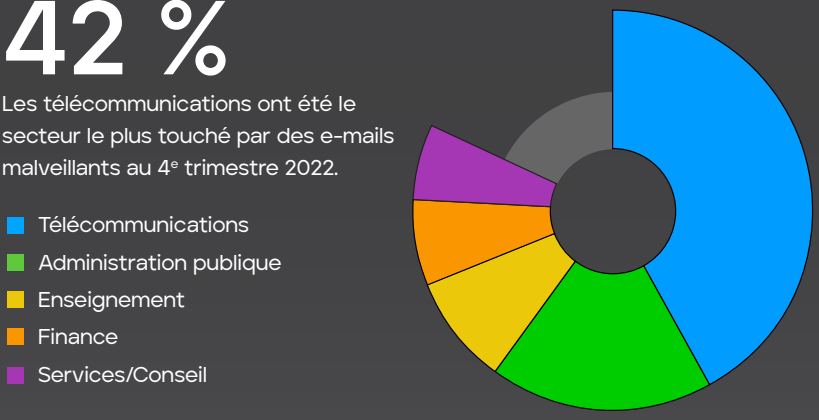
PRODUITS ET MARQUES LES PLUS CIBLÉS PAR DES E-MAILS DE PHISHING – T4 2022

1.	Générique	62 %
2.	Outlook	13 %
3.	Microsoft	11 %
4.	Ekinet	8 %
5.	Cloudfare	3 %

SECTEURS LES PLUS TOUCHÉS PAR DES E-MAILS MALVEILLANTS – T4 2022

42 %

Les télécommunications ont été le secteur le plus touché par des e-mails malveillants au 4e trimestre 2022.



TENDANCES EN MATIÈRE D'USURPATION D'IDENTITÉ PAR E-MAIL – T4 2022

82 % des e-mails de fraude au PDG ont été envoyés à l'aide de services e-mail gratuits.

78 % des attaques par piratage de la messagerie en entreprise (BEC) utilisaient des expressions couramment employées par les PDG.

64 % Augmentation du nombre d'e-mails malveillants usurpant l'identité de PDG et d'autres dirigeants entre le 3e et le 4e trimestre 2022

Expressions de PDG/dirigeants les plus utilisées dans les attaques BEC – T4 2022

« Je vais vous confier une tâche que je vous demande de réaliser immédiatement. »

« Je dois vous confier une tâche, veuillez me communiquer votre numéro de téléphone. »

« Envoyez-moi votre numéro de téléphone, je dois vous confier une tâche à exécuter immédiatement. »

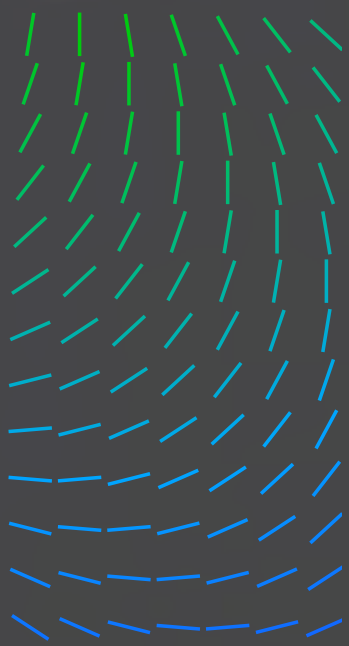
« Veuillez m'envoyer votre numéro de téléphone et attendre mon SMS. Je dois vous confier une tâche. »

« Veuillez vérifier et confirmer votre numéro de téléphone et attendre mon SMS d'instructions. »

« Avez-vous reçu mon précédent e-mail ? J'ai une offre rentable à vous proposer. »

ÉVOLUTION DES USURPATIONS D'IDENTITÉ – T4 2022

64 % Le nombre d'usurpations d'identité a bondi de 64 % entre le 3e et le 4e trimestre 2022.



OBSERVATIONS SUR LES CAMPAGNES DE PHISHING – T4 2022

Les fournisseurs d'hébergement web sont de plus en plus exploités lors d'escroqueries et de vols

Au 4e trimestre, nous avons constaté une augmentation de l'utilisation de fournisseurs d'hébergement web légitimes pour escroquer des utilisateurs et voler des identifiants. Trois fournisseurs de services ont été largement exploités : dweb.link, ipfs.link et translate.goog. Nous avons également noté des volumes importants provenant des domaines d'autres fournisseurs de services comme ekinet, storageapi_fleek et selcdn.ru. Les attaquants utilisent des services d'hébergement nouveaux et populaires pour héberger des pages de phishing et contourner les moteurs antiphishing. Ces services ne peuvent être mis sur la liste noire d'aucun système de détection, étant donné que leur principal objectif est d'héberger des fichiers légitimes et de partager du contenu. C'est l'une des raisons pour lesquelles les attaquants portent un intérêt accru aux fournisseurs d'hébergement web légitimes.

VECTEURS D'ATTAQUE LES PLUS UTILISÉS DANS LES E-MAILS DE PHISHING

87 %

Les e-mails de phishing utilisant des URL malveillantes ont été de loin le vecteur d'attaque le plus prévalent au 4e trimestre 2022.

1.	URL	87 %
2.	Pièce jointe	7 %
3.	En-tête	6 %

FOURNISSEURS D'HÉBERGEMENT WEB FORTEMENT EXPLOITÉS – T4 2022

154 %

Si Dweb a été le fournisseur d'hébergement web le plus exploité au 4e trimestre, c'est Google Traduction qui a enregistré la hausse la plus importante (154 %) entre le 3e et le 4e trimestre 2022.

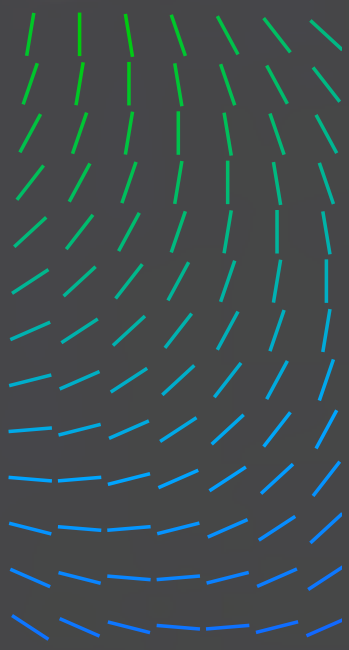
1.	Dweb	81 %
2.	Ipfs	17 %
3.	Google Traduction	10 %

TECHNIQUES DE CONTOURNEMENT LES PLUS UTILISÉES DANS LES ATTAQUES DE PHISHING – T4 2022

63 %

Les attaques par contournement basé sur une redirection 302 ont été les plus nombreuses au 4e trimestre 2022.

- Les attaques de phishing par contournement basé sur la géolocalisation ont fortement augmenté au 4e trimestre.
- Les attaques basées sur les CAPTCHA ont également progressé au 4e trimestre.



OBSERVATIONS SUR LE VISHING – T4 2022

Le vishing est une forme de phishing conçue pour inciter les victimes à interagir avec les attaquants principalement par le biais d'e-mail, SMS, appel téléphonique ou chat en direct.

142 % Les attaques de vishing ont progressé de 142 % entre le 3e et le 4e trimestre 2022.

85 % Les services e-mail gratuits ont gagné les faveurs des auteurs d'attaques de vishing. Un pourcentage élevé des attaques de phishing détectées au 4e trimestre (85 %) ont été envoyées à l'aide d'un service e-mail gratuit.

Norton, McAfee, Geek Squad, Amazon et PayPal ont été les thèmes les plus populaires utilisés dans ces campagnes au 4e trimestre.

SÉCURITÉ RÉSEAU – T4 2022

L'équipe de recherche réseau de Trellix Advanced Research Center se concentre sur la détection et le blocage des attaques réseau qui menacent nos clients. Nous inspectons différentes étapes de la chaîne de frappe (reconnaissance, compromission initiale, communication avec le serveur C&C et TTP de déplacement latéral). Notre capacité à tirer parti des atouts de nos technologies nous offre une visibilité permettant de mieux détecter les menaces inconnues.

Techniques MITRE ATT&CK les plus utilisées pour contourner la sécurité réseau – T4 2022

- T1083 - Découverte des fichiers et des répertoires
- T1573 - Canal chiffré
- T1020 - Exfiltration automatisée
- T1210 - Exploitation de services distants
- T1569 - Services système
- T1059 - Interpréteur de commandes et de scripts : Windows Command Shell
- T1047 - Infrastructure de gestion Windows
- T1087 - Découverte des comptes
- T1059 - Interpréteur de commandes et de scripts
- T1190 - Exploitation d'applications publiques

Attaques ayant le plus d'impact contre des services externes – T4 2022

De nombreuses analyses réseau sont effectuées chaque jour pour sonder les machines avec accès externe afin de trouver un point d'accès potentiel à un environnement client. Les anciens exploits cherchent constamment des systèmes non corrigés par des patchs.

- Détection d'une tentative d'accès au fichier /etc/passwd
- Possible attaque du type exécution de scripts intersites
- Analyseur de sécurité SIPVicious
- Trafic de l'analyseur Nmap détecté
- Activité d'analyse - Shellshock, sondage des serveurs web
- Exécution de code à distance Bash (Shellshock) CGI HTTP (CVE-2014-6278)
- Vulnérabilité d'exécution de code à distance CVE-2020-14882 Oracle WebLogic
- Tentative de traversée de répertoires
- Injection de script OGNL ConversionErrorInterceptor Apache Struts 2
- Exécution de code à distance CVE-2021-44228 Apache Log4j

Principaux webshells utilisés pour l'implantation sur le réseau – T4 2022

Les webshells suivants sont généralement utilisés pour tenter de contrôler un serveur web vulnérable.

- Webshell China Chopper
- Webshell JFolder
- Webshell ASPXSpy
- Webshell C99
- Webshell Tux
- Webshell B374K/Famille RootShell

Outils, techniques et procédures les plus pertinents une fois à l'intérieur du réseau – T4 2022

Les webshells suivants sont généralement utilisés pour tenter de contrôler un serveur web vulnérable.

Nous avons observé un volume élevé de TTP utilisées par les attaquants lors du déplacement latéral, y compris d'anciennes vulnérabilités et des outils comme SCShell et PSExec.

- SCShell : déplacement latéral sans fichier via le Gestionnaire de services
- Appel de processus à distance Windows WMI
- Invocation du shell CMD avec WMIEXEC via SMB
- Exploit EternalBlue détecté
- Tentative CVE-2020-0796 Microsoft SMBv3
- RCE CVE-2021-44228 Apache Log4j
- Énumération des comptes d'administration d'entreprise/de domaine à distance
- Exécution de scripts PowerShell suspects à distance
- Reconnaissance des réseaux suspects avec WMIC
- Commande d'énumération détectée dans le fichier de commandes
- Activité PsExec SMB

DONNÉES TÉLÉMÉTRIQUES SUR LES OPÉRATIONS DE SÉCURITÉ RECUEILLIES PAR TRELLIX XDR

Ces statistiques se basent sur les données télémétriques générées par divers capteurs déployés par nos clients. Les journaux de détection sont agrégés et analysés pour produire les informations suivantes :

Incidents de sécurité ayant le plus d'impact – T4 2022

La section ci-dessous indique les alertes de sécurité les plus prévalentes au 4e trimestre 2022 :

EXPLOIT - LOG4J [CVE-2021-44228]

OFFICE 365 ANALYTICS [Connexion anormale]

OFFICE 365 [Phishing autorisé]

EXPLOIT - FORTINET [CVE-2022-40684]

EXPLOIT - APACHE SERVER [Tentative CVE-2021-41773]

WINDOWS ANALYTICS [Attaque en force réussie]

EXPLOIT - ATLASSIAN CONFLUENCE [CVE-2022-26134]

EXPLOIT - F5 BIG-IP [Tentative CVE-2022-1388]

TECHNIQUES MITRE ATT&CK LES PLUS UTILISÉES – T4 2022

1.	Exploitation d'applications publiques (T1190)	29 %
2.	Protocole de la couche Application : DNS (T1071.004)	14 %
	Phishing (T1566)	14 %
3.	Manipulation de comptes (T1098.001) Attaque en force brute (T1110) Compromission par téléchargement à l'insu de l'utilisateur (T1189) Exécution par l'utilisateur : Fichier malveillant (T1204.002) Comptes valides : Comptes locaux (T1078.003)	7 % chacun

RÉPARTITION DES PRINCIPALES SOURCES DE JOURNALISATION – T4 2022

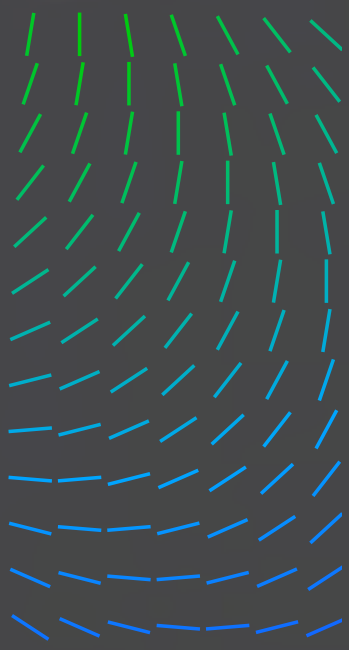
1.	Réseau	40 %
2.	E-mail	27 %
3.	Terminal	27 %
4.	Pare-feu	6 %

EXPLOITS IDENTIFIÉS – T4 2022

EXPLOITS LES PLUS PRÉVALENTS IDENTIFIÉS – T4 2022

30 % Log4j a été l'exploit le plus prévalent identifié au 4e trimestre 2022.

1.	Log4j (CVE-2021-44228)	30 %
2.	Fortinet (CVE-2022-40684)	16 %
3.	Apache Server (CVE-2021-41773)	15 %
4.	Atlassian Confluence (CVE-2022-26134)	14 %
5.	F5 Big-IP (tentative CVE-2022-1388)	13 %
6.	Microsoft Exchange (tentative d'exploit ProxyShell)	11 %



INCIDENTS CLOUD – T4 2022

Les attaques visant l'infrastructure cloud poursuivent leur essor, car de nombreuses entreprises délaissent leur infrastructure sur site au profit du cloud. Selon les analystes de Gartner, plus de 85 % des entreprises auront adopté une approche axée sur le cloud d'ici 2025.

Lors de l'analyse des données télémétriques collectées au 4e trimestre 2022, nous avons observé ce qui suit :

- Les détections liées à AWS ont été les plus nombreuses, peut-être en raison de la position de leader d'AWS sur le marché cloud.
- La plupart des attaques se concentraient sur l'obtention d'un accès initial à des comptes valides via une attaque en force brute ou la pulvérisation de mots de passe (passwordspray), ce qui laisse croire que le vecteur d'infection initial se trouve au niveau de la surface d'attaque du cloud.
- Étant donné que la majorité des comptes d'entreprise ont activé l'authentification multifacteur (MFA), les cybercriminels à l'origine d'attaques en force réussies sont passés par des plates-formes MFA, ce qui a entraîné un pic des détections associées.

Les sections ci-dessous décrivent brièvement les données télémétriques sur les attaques cloud issues de notre base clients, réparties selon le fournisseur de services cloud.

RÉPARTITION DES TECHNIQUES MITRE ATT&CK POUR AWS – T4 2022

1.	Comptes valides (T1078)	18 %
2.	Modification de l'infrastructure de service de calcul du compte cloud (T1578)	12 %
3.	Manipulation de comptes (T1098)	9 %
4.	Comptes cloud (T1078.004)	8 %
5.	Attaque en force brute (T1110) Perturbation des défenses (T1562)	6 % chacun

PRINCIPALES TECHNIQUES MITRE ATT&CK POUR AZURE – T4 2022

1.	Comptes valides (T1078)	23 %
2.	Authentification multifacteur (T1111)	19 %
3.	Attaque en force brute (T1110)	14 %
4.	Proxy (T1090)	14 %
5.	Manipulation de comptes (T1098)	5 %

PRINCIPALES DÉTECTIONS AWS PAR TECHNIQUES MITRE ATT&CK – T4 2022

Technique MITRE ATT&CK	Règle
Manipulation de comptes (T1098)	Stratégie privilégiée AWS liée à l'identité IAM AWS S3 - Suppression de la stratégie de compartiment
Comptes valides (T1078)	AWS Analytics - Connexion anormale à la console AWS Analytics - Utilisation anormale des clés API AWS GuardDuty - Comportement anormal des utilisateurs AWS GuardDuty - Accès anonyme octroyé
Perturbation des défenses (T1562)	AWS CloudTrail - Modifications des stratégies AWS CloudTrail - Suppression du journal de suivi
Informations d'identification dans des fichiers (T1552.001)	Alerte sur un potentiel vol de clés secrètes AWS
Modification de l'infrastructure de service de calcul du compte cloud (T1578)	AWS CloudTrail - Suppression du compartiment S3 AWS CloudTrail - Chargement de l'ACL d'un compartiment S3 AWS CloudTrail - Chargement de l'ACL d'un objet

PRINCIPALES DÉTECTIONS AZURE PAR TECHNIQUES MITRE ATT&CK – T4 2022

Technique MITRE ATT&CK	Règle
Comptes valides (T1078)	Azure AD - Connexion à risque Azure - Connexion à partir d'un emplacement inhabituel Azure - Connexion d'un compte inactif pendant 60 jours
Attaque en force brute (T1110)	Azure - Plusieurs échecs d'authentification Graph - Attaque en force brute contre le portail Azure Graph - Tentatives de craquage du mot de passe distribué

Authentification multifacteur (T1111)	Azure - Authentification multifacteur refusée car alerte de fraude Azure - Authentification multifacteur refusée car utilisateur bloqué Azure - Authentification multifacteur refusée car code frauduleux Azure - Authentification multifacteur refusée car application frauduleuse
Services distants externes (T1133)	Azure - Connexion à partir du réseau Tor
Manipulation de comptes (T1098)	Azure - Réinitialisation inhabituelle d'un mot de passe utilisateur

RÉPARTITION DES TECHNIQUES MITRE ATT&CK POUR GCP – T4 2022

1.	Comptes valides (T1078)	36 %
2.	Exécution via une API (T0871)	18 %
3.	Découverte de comptes (T1087.001) Manipulation de comptes (T1098) Perturbation des défenses (T1562) Modification de l'infrastructure de service de calcul du compte cloud (T1578) Services distants (T1021.004)	9 % chacun

PRINCIPALES DÉTECTIONS GCP PAR TECHNIQUES MITRE ATT&CK – T4 2022

Technique MITRE ATT&CK	Règle
Comptes valides (T1078)	GCP - Création d'un compte de service GCP Analytics - Activité anormale GCP - Création de la clé du compte de service
Services distants (T1021.004)	GCP - Règle de pare-feu autorisant tout le trafic sur le port SSH
Manipulation de comptes (T1098)	GCP - Modification de la stratégie IAM de l'entreprise
Découverte des comptes (T1087.001)	Alerte [gcps net user]
Transfert de données vers un compte cloud (T1527)	GCP - Modification du récepteur de journalisation
Modification de l'infrastructure de service de calcul du compte cloud (T1578)	GCP - Désactivation de la protection contre la suppression

RÉDACTION ET RECHERCHES

Alfred Alvarado
Henry Bernabe
Adithya Chandra
Phuc Duy Pham
Sarah Erman
John Fokker
Lennard Galang
Sparsh Jain
Daksh Kapoor
Maulik Maheta
João Marques
Tim Polzer
Srini Seethapathy
Rohan Shah
Vihar Shah
Swapnil Shashikantpa
Shyava Tripathi
Leandro Velasco

RESSOURCES

Pour suivre l'évolution des menaces les plus récentes et de celles ayant le plus d'impact identifiées par l'équipe Trellix Advanced Research Center, consultez ces ressources :

TWITTER

Trellix ARC

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER

Trellix Advanced Research Center possède la charte la plus complète du secteur de la cybersécurité et est à l'avant-garde de l'étude des méthodes, tendances et groupes cybercriminels émergents dans le paysage des menaces. Partenaire incontournable des équipes en charge des opérations de sécurité partout dans le monde, Trellix Advanced Research Center propose une Threat Intelligence et des contenus de tout premier ordre aux analystes en sécurité, tout en alimentant en parallèle notre plate-forme XDR de pointe.

À PROPOS DE TRELLIX

Trellix est une société d'envergure internationale qui a pour vocation de redéfinir l'avenir de la cybersécurité. Sa plate-forme XDR (eXtended Detection and Response) ouverte et native aide les entreprises confrontées aux menaces actuelles les plus évoluées à renforcer leur confiance dans la sécurité et la résilience de leurs opérations. Trellix, soutenu par un vaste écosystème de partenaires, accélère l'innovation technologique grâce à l'apprentissage automatique et à l'automatisation afin de renforcer la protection de plus de 40 000 clients des secteurs privé et public au moyen d'une sécurité évolutive. Pour en savoir plus, consultez notre site à l'adresse www.trellix.com/fr-fr/.

Pour en savoir plus, visitez le site Trellix.com/fr-fr/.

Trellix

À propos de Trellix

Trellix est une société d'envergure internationale qui a pour vocation de redéfinir l'avenir de la cybersécurité. Sa plate-forme XDR (eXtended Detection and Response) ouverte et native aide les entreprises confrontées aux menaces actuelles les plus évoluées à renforcer leur confiance dans la sécurité et la résilience de leurs opérations. Les experts en sécurité de Trellix, soutenus par un vaste écosystème de partenaires, accélèrent l'innovation technologique grâce à l'apprentissage automatique et à l'automatisation afin de renforcer la protection de plus de 40 000 clients des secteurs privé et public.

072022-05