RAPPORT SUR LE PAYSAGE DES CYBERMENACES

Juin 2023

Informations recueillies auprès d'un réseau mondial d'experts, de capteurs, de données télémétriques et de Threat Intelligence

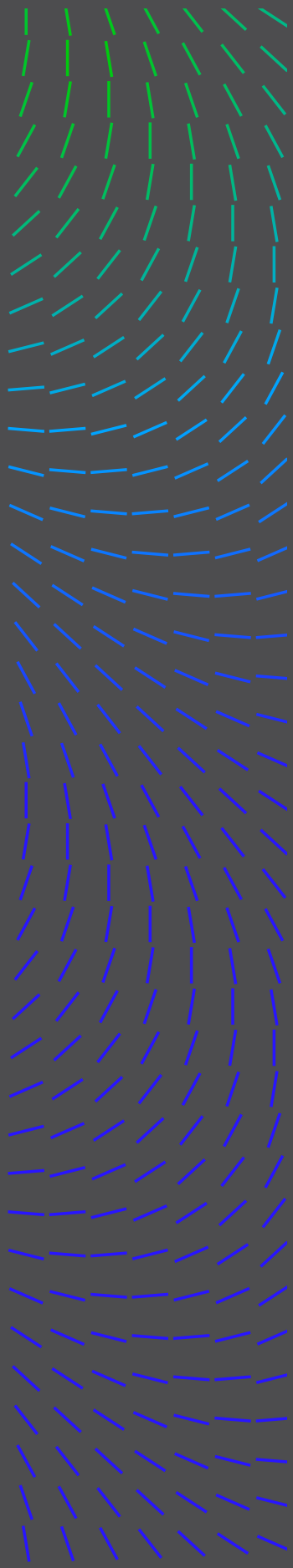


Présenté par

Trellix ADVANCED RESEARCH CENTER

RAPPORT SUR LE PAYSAGE DES CYBERMENACES

Rédigé par notre équipe Trellix Advanced Research Center, ce rapport (1) met en lumière les informations, la Threat Intelligence et les conseils recueillis auprès de plusieurs sources de données critiques sur les menaces de cybersécurité, et (2) propose des interprétations expertes, rationnelles et raisonnables de ces données pour informer et favoriser de bonnes pratiques de cyberdéfense. Cette édition se concentre sur les données et informations collectées entre le 1er janvier 2023 et le 31 mars 2023.



Les cybermenaces continuent à évoluer et à se multiplier rapidement et à grande échelle.

Les équipes SecOps mettent tout en œuvre pour défendre les informations, les actifs et l'activité, mais aucune ne bénéficie d'une visibilité complète sur le paysage des menaces.

En effet, une telle visibilité nécessite une large perspective, un grand nombre de sources, des flux de données multiples, une cyberveille brute et d'importants volumes de données télémétriques.

Pour obtenir des informations exploitables, il est nécessaire de disposer d'une vision stratégique sur un grand nombre d'entreprises, de secteurs, de régions et de surfaces d'attaque.

Bienvenue dans l'édition de juin 2023 du Rapport sur le paysage des cybermenaces.

COMPRENDRE LES RISQUES, LES MENACES ET LES VULNÉRABILITÉS DANS LE VISEUR DES ATTAQUANTS

Je passe beaucoup de temps à échanger avec des membres de conseils d'administration, des PDG, des RSSI, des DSI, des directeurs des technologies et d'autres responsables chargés de la cyberdéfense de nations, d'organismes publics et d'entreprises privées dans de nombreux secteurs.

Nous abordons un large éventail de sujets, de la recherche mondiale et de l'innovation à la Threat Intelligence, en passant par les dernières pratiques de cyberdéfense de leurs équipes SecOps. Nous évoquons les obstacles qu'ils rencontrent, récemment relevés par Trellix dans son rapport « The Mind of the CISO » : un trop grand nombre de sources d'informations différentes (35 %), l'évolution des obligations légales et réglementaires (35 %), l'élargissement des surfaces d'attaque (34 %), la pénurie de personnel compétent (34 %) et le manque de soutien d'autres départements de l'entreprise (31 %)[1].

Pratiquement toutes ces interactions abordent, directement ou indirectement, la nature du paysage des menaces. Quels types d'attaques sont prévalentes ? Quels sont les groupes de ransomware les plus dangereux ? Quelles vulnérabilités sont ciblées ? Quelles nations semblent les plus actives ? Quelles tendances en matière de menaces surveillons-nous via nos dispositifs de sécurité e-mail et réseau ?

« Ces connaissances, disponibles dans ce rapport et dans la riche bibliothèque de ressources de Trellix, sont souvent essentielles à la mission des dirigeants, PDG, RSSI, DSI, directeurs des technologies et équipes SecOps. »

Chez Trellix, nous avons beaucoup à partager, car nous sommes chaque jour en première ligne dans la lutte contre la cybercriminalité. Nous nous appuyons sur un vaste référentiel de Threat Intelligence, d'analyses et de données sur la sécurité collectées par plus d'un milliard de capteurs à travers le monde. Ces connaissances, disponibles dans ce rapport et dans la riche bibliothèque de ressources de Trellix, sont souvent essentielles à la mission des dirigeants, PDG, RSSI, DSI, directeurs des technologies et équipes SecOps.

Mon collègue John Fokker, responsable de la Threat Intelligence au sein de l'équipe chevronnée Trellix Advanced Research Center, a compilé ici un excellent rapport. Aidez-vous de ces informations riches et pertinentes pour concentrer les efforts de votre équipe, renforcer vos processus et mettre en place les bonnes technologies XDR. N'hésitez pas à nous faire part de vos centres d'intérêt : nous en tiendrons compte lors de nos futures éditions pour vous aider à assurer la sécurité et la prospérité de votre entreprise.



Joseph (Yossi) Tal
SVP, DIRECTEUR DE TRELLIX ADVANCED RESEARCH CENTER

EN SOUTIEN AUX HÉROS EN PREMIÈRE LIGNE DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ

Je travaille avec des héros. Je ne parle pas des membres de mon équipe, malgré leurs brillantes carrières dans les secteurs public et privé.

Je parle de vous. Je parle des individus et des équipes du monde entier qui utilisent les fonctionnalités de recherche avancée de Trellix – nos systèmes, nos informations et notre Threat Intelligence – pour protéger leur entreprise contre les cyberattaques. Les RSSI, directeurs des technologies et DSI, mais aussi nos collègues d'agences telles qu'Europol, le FBI et la NSA, la CISA (Cybersecurity and Infrastructure Security Agency), l'ACSC (Australian Cybersecurity Centre) et le NCSC (National Cyber Security Centre) au Royaume-Uni. Tout aussi important, si ce n'est plus, je parle de chaque membre de votre équipe SecOps.

« Comme vous le constatez dans votre travail quotidien, la cybersécurité évolue à vitesse grand V : avancées technologiques, adoption du XDR (...) »

Selon vous, qu'est-ce qui change la donne de votre mission SecOps ? Les responsables de la cybersécurité du monde entier ont partagé leur point de vue dans le rapport Trellix mentionné ci-dessus par mon collègue Yossi. Ils ont cité une visibilité accrue (44 %), une meilleure priorisation (42 %), une collaboration plus étroite pour contrer les attaques multivectorielles (40 %) et une précision améliorée (37 %)[2].

Chacun de ces facteurs repose fondamentalement sur des informations et des données précises, comme le contenu de ce rapport.

Comme vous le constatez dans votre travail quotidien, la cybersécurité évolue à vitesse grand V : avancées technologiques, adoption du XDR, évolution des réglementations et des législations, mutations du paysage des menaces, etc. Une révolution est en cours et transforme la manière dont les équipes SecOps peuvent garder une longueur d'avance sur la prochaine génération de cyberattaques. Tout commence par l'information et par une compréhension fine de la situation actuelle.

Unissons nos forces. Vous pouvez compter sur Trellix. Ce rapport vous est destiné.



John Fokker
DIRECTEUR DE LA THREAT INTELLIGENCE
ET INGÉNIEUR EN CHEF
TRELLIX ADVANCED RESEARCH CENTER

[1] Trellix, « 2023 Report : The Mind of the CISO », 2023
[2] Trellix, « 2023 Report : The Mind of the CISO », 2023

INTRODUCTION

Contexte stratégique : un monde en quête de stabilité

Pour interpréter les données de ce rapport, il est nécessaire d'appréhender la conjoncture à l'échelle mondiale. En effet, les cybermenaces ciblant les entreprises du monde entier n'existent pas en vase clos. Parmi les principaux facteurs de cyberrisque, on retrouve les guerres et autres cas de force majeure, les mutations économiques et les nouvelles vulnérabilités qui peuvent émerger à chaque fois qu'une équipe apporte des changements à des éléments tels que les modèles de gestion, les partenaires clés, les processus de base, l'adoption de technologies et la conformité réglementaire. Voici quelques-uns des facteurs influençant nos données sur les menaces du 1er trimestre 2023 :

L'invasion de l'Ukraine par la Russie et la guerre asymétrique contre l'Occident – Les cyberattaques lancées par des acteurs étatiques à des fins d'espionnage, de guerre et de désinformation au service d'ambitions politiques, économiques et territoriales continuent à s'intensifier. Les hackers ciblent des entreprises, des infrastructures et des organes publics occidentaux avec des cyberattaques de plus en plus sophistiquées.

La mainmise de Xi Jinping sur la Chine et ses aspirations géopolitiques – Les objectifs nationalistes, la politique étrangère affirmée et les pratiques d'espionnage industriel de la Chine continuent à accroître les cyberrisques, tandis que les groupes APT affiliés à la Chine dominent le paysage mondial des menaces.

Les économies en développement et l'expansion rapide des infrastructures – Alors que de nombreuses régions en développement étendent leurs infrastructures et leurs technologies à mesure de la croissance de leur économie, la cybersécurité est souvent négligée, ce qui engendre de nombreuses vulnérabilités cyber dans les infrastructures critiques.

L'inflation mondiale et ses retombées économiques et politiques – Ce trimestre a été synonyme de marchés volatils, de crises financières et politiques, ainsi que de pressions sur les priorités en matière de dépenses et les budgets de cybersécurité.

La chaîne logistique toujours perturbée post-COVID – L'apparition de nouvelles voies d'accès aux marchés dans toutes les régions a engendré des changements au niveau des partenaires, des réseaux de transport, du partage d'informations et, par ricochet, des cyberrisques. Les cybermenaces ayant une incidence quotidienne sur la chaîne logistique, le besoin de fonctionnalités Zero Trust ne faiblit pas dans l'ensemble des secteurs.

Le mythe de la supériorité de l'environnement de sécurité d'Apple – Cette légende persiste alors que les environnements macOS ne peuvent plus être considérés comme sûrs, car les cybercriminels utilisent désormais des malwares en Golang à grande échelle et multiplient les vecteurs d'attaque afin de couvrir de nombreux systèmes d'exploitation.

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

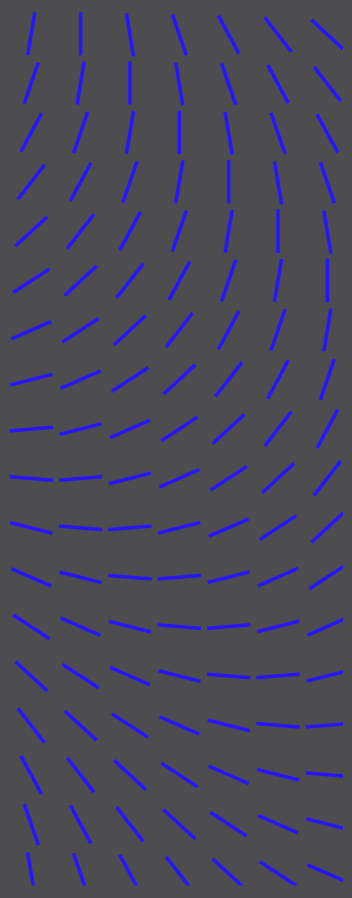
SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX



L'irruption de l'intelligence artificielle sur le devant de la scène mondiale, promettant des perturbations – L'apprentissage automatique optimisé, le traitement du langage naturel et d'autres avancées du même genre ont un impact à la fois positif et négatif sur la cyberdéfense. Face à l'évolution des cybermenaces mondiales à un rythme beaucoup trop rapide pour les équipes humaines, les solutions d'intelligence artificielle deviennent essentielles à la cyberdéfense des entreprises.

Cybersécurité : les défis pour les RSSI et la révolution SecOps

Quel est l'un des défis les plus critiques pour les professionnels de la cybersécurité et les équipes SecOps ? Assimiler la Threat Intelligence rapidement et à grande échelle et transmettre immédiatement des informations exploitables aux équipes de traque des menaces et aux forces opérationnelles au sein des entreprises.

L'objectif de Trellix ? Simplifier ces processus.

Comment ? En fournissant le niveau d'automatisation nécessaire pour parvenir aux réponses sur lesquelles les entreprises doivent se concentrer, à l'aide de nos fonctionnalités de Threat Intelligence, de traque des menaces et de sécurité de pointe, intégrées à nos produits XDR, de protection des hôtes, de sécurité réseau et de sécurité e-mail.

Le paysage des menaces du 1er trimestre 2023 a également été influencé par des facteurs internes, dont bon nombre reflètent les turbulences auxquelles sont confrontés les responsables de la cybersécurité et les équipes de première ligne.

Technologies obsolètes – De nombreuses entreprises continuent d'utiliser des technologies héritées comme des outils SOAR et SIEM. En effet, 96 % des RSSI déclarent avoir besoin de solutions plus adaptées pour protéger leur entreprise contre les cybermenaces[3].

Multitude d'outils de sécurité – Les équipes SecOps sont submergées d'alertes et ne parviennent pas à établir les priorités nécessaires pour gérer efficacement leur temps. En moyenne, les entreprises utilisent pas moins de 25 solutions et outils de sécurité[4].

Désensibilisation aux alertes – Inondées d'alertes, les équipes SecOps éprouvent des difficultés en termes de priorisation, de faux positifs et d'alertes manquées. Selon IDC, 35 % des analystes ignorent les alertes – ce qui s'explique en partie par le fait que 45 % d'entre elles sont des faux positifs[5].

Ressources insuffisantes – Compte tenu de leurs ressources et de leur expertise limitées, les équipes SecOps ont du mal à contrer efficacement les menaces. Il faut savoir par exemple qu'en moyenne, un analyste SOC reste à son poste environ deux ans[6].

Méthodologie : comment nous collectons et analysons les données

Trellix et les experts de l'équipe de classe mondiale Trellix Advanced Research Center recueillent les statistiques, les tendances et les résultats d'analyses qui composent ce rapport auprès d'un large éventail de sources mondiales, à la fois captives et ouvertes. Les données agrégées alimentent nos plates-formes Insights et ATLAS. Grâce à l'apprentissage automatique, à l'automatisation et à l'acuité humaine, l'équipe effectue une série de processus intensifs, intégrés et itératifs afin de normaliser les données, d'analyser les informations et de développer des renseignements pertinents pour les responsables de la cybersécurité et les équipes SecOps de première ligne dans le monde entier. Pour une description plus détaillée de notre méthodologie, consultez la fin de ce rapport.

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

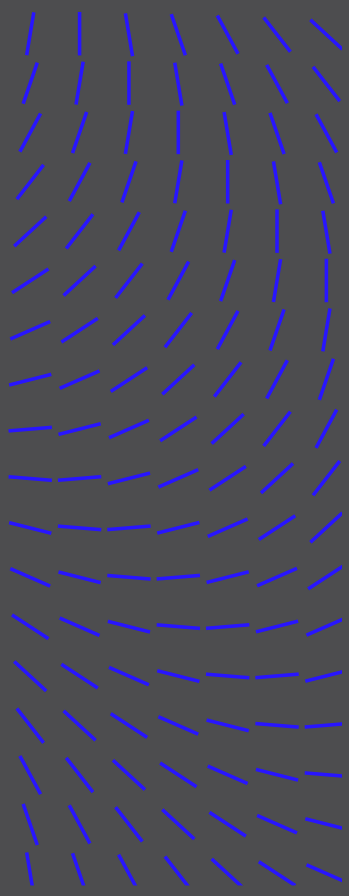
SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX



Application : comment utiliser ces informations

Il est indispensable que chaque équipe d'évaluation de premier plan comprenne, reconnaisse et, si possible, réduise l'effet de biais, c'est-à-dire la tendance naturelle, intériorisée ou imperceptible à accepter, rejeter ou manipuler les faits et leur signification. Il en va de même pour les consommateurs du contenu.

Contrairement à une expérience ou à un test mathématique structurés, ce rapport est par nature un échantillon de commodité — un type d'étude non probabiliste souvent utilisé dans les tests médicaux, psychologiques et sociologiques qui s'appuie sur des données disponibles et accessibles.

En bref, nos conclusions sont basées sur ce que nous pouvons observer et n'incluent pas de preuves relatives à des menaces, attaques ou tactiques ayant échappé à la détection, au signalement et à la capture de données.

En l'absence d'informations « complètes » ou de visibilité « parfaite », il s'agit du type d'étude le plus adapté à l'objectif de ce rapport : identifier des sources connues de données critiques sur les menaces de cybersécurité et proposer des interprétations rationnelles, expertes et éthiques de ces données qui informent et favorisent de bonnes pratiques de cyberdéfense.

Voici les éléments centraux de cette éthique d'investigation :

Instantané ponctuel – 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'extorsion ou de publication sur des sites de divulgation. Toutefois, la surveillance et le traçage des éléments dont nous disposons permettent de mieux comprendre les différentes menaces, tout en réduisant les angles morts dans les analyses et les investigations.

Faux positifs et faux négatifs – Parmi les caractéristiques techniques performantes des systèmes télémétriques et de suivi spéciaux de Trellix visant à collecter des données, on retrouve des mécanismes, des filtres et des tactiques qui contribuent à réduire ou à éliminer les faux positifs et les faux négatifs. Ceux-ci permettent de renforcer le niveau d'analyse et la qualité de nos observations.

Détections, et non infections – Lorsque nous employons le terme « données télémétriques », nous faisons référence aux détections, et non 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.

Capture de données irrégulière – Certains ensembles de données nécessitent une interprétation minutieuse. Les données de télécommunications, par exemple, incluent des données télémétriques de FAI opérant dans de nombreux autres secteurs.

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

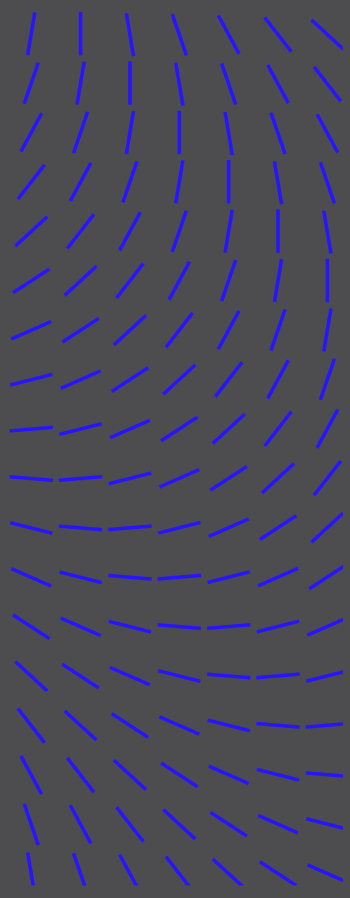
SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX



Attribution des attaques étatiques – De même, attribuer la responsabilité de différentes cyberattaques et menaces à des groupes étatiques peut être très difficile, étant donné que ces groupes ont tendance à usurper l'identité d'un autre collectif ou à faire croire que leurs activités malveillantes proviennent d'une source approuvée.

Perspectives d'avenir : conseils et ressources

Que signifient les informations figurant dans ce rapport pour les héros en première ligne de la lutte contre la cybercriminalité ? Les informations et données de cybersécurité ne sont utiles que si elles se transforment en actions et permettent de réduire les risques, d'améliorer la prise de décision ou de renforcer l'efficacité des activités SecOps. Pour plus de conseils et de ressources, rendez-vous sur le site www.trellix.com.

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

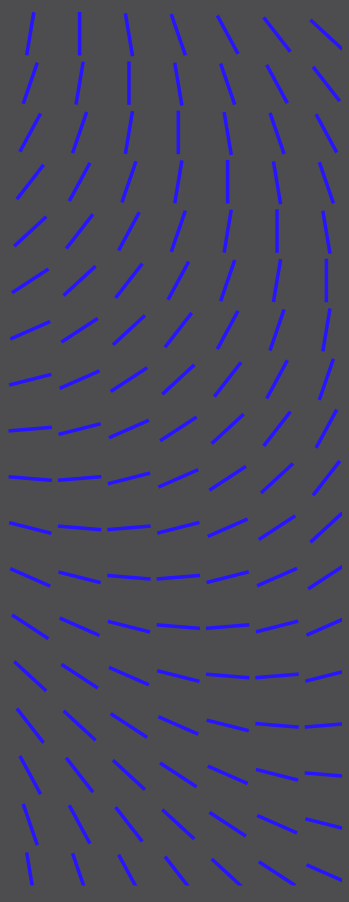
SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX



[3] Trellix, « 2023 Report : The Mind of the CISO », 2023

[4] Trellix, « 2023 Report : The Mind of the CISO », 2023

[5] IDC, The Voice of the Analysts, 2021

[6] Ponemon Institute, 2020

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

Le paysage des ransomwares

- **La vague de ransomwares –** Les ransomwares continuent à dominer le paysage mondial des cyberattaques. 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, sont plus prévalents et sophistiqués que jamais.
- **La prédominance de Cuba et de Play –** Bien que nous ayons observé un recul des activités cybercriminelles liées aux ransomwares au début de l'année, les familles de ransomwares les plus prévalentes au 1er trimestre étaient Cuba (9 %) et Play (7 %).
- **La persistance de LockBit –** Malgré une baisse d'activité pendant deux trimestres consécutifs, LockBit demeure le ransomware le plus agressif vis-à-vis de ses victimes, fortement mises sous pression pour qu'elles paient la rançon exigée.
- **L'essor potentiel de Magecart Group –** D'après les signalements publics, les activités de ce groupe spécialisé dans le vol de données de carte de crédit et d'escroqueries d'e-commerce ont explosé au 1er trimestre 2023. Il opère rarement à la même échelle que les autres grands groupes APT étatiques, ce qui peut indiquer une réémergence de Magecart Group dans le monde entier.

L'évolution des tactiques de ransomware

- **Appât du gain –** Il n'est pas surprenant que les motivations des ransomwares restent principalement pécuniaires. Les secteurs des assurances (20 %) et des services financiers (17 %) sont ceux qui ont enregistré le plus de détections d'attaques potentielles.
- **Impact majeur sur les entreprises de taille moyenne –** L'analyse des données associées aux sites de divulgation révèle que les victimes de ces attaques sont majoritairement des entreprises de taille moyenne ne comptant que 51 à 200 collaborateurs (32 %) et entre 10 et 50 millions de dollars de chiffre d'affaires (38 %).
- **Les États-Unis, pays le plus ciblé –** Les États-Unis (15 %) ont été le pays le plus ciblé par des groupes de ransomware. Il s'agit également du pays ayant enregistré le pourcentage le plus important d'entreprises victimes (48 %) qui ont décidé de « racheter leurs données » aux attaquants — un chiffre six fois plus élevé que le deuxième pays du classement, le Royaume-Uni.
- **Cobalt Strike comme arme de prédilection –** Les données télémétriques de Trellix identifient cet outil comme fortement plébiscité par les groupes de ransomware (28 % des incidents). Il semble gagner en popularité et en utilisation parmi ces groupes, malgré les efforts déployés au 4e trimestre 2022 par le fournisseur Fortra pour compliquer son utilisation par des cybercriminels.

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

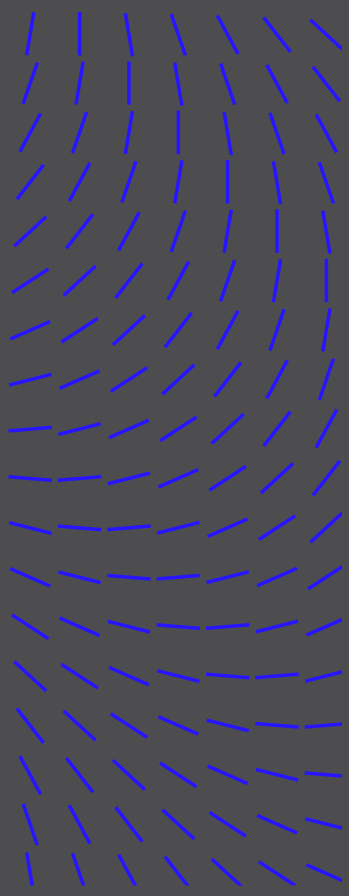
SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX



Attaques étatiques

- **Principaux acteurs –** Les groupes APT affiliés à la Chine, y compris Mustang Panda et UNC4191, ont été les plus actifs lors des attaques visant des États au 1er trimestre. Les collectifs à la solde de la Chine ont dominé le paysage mondial des menaces, générant 79,3 % des attaques étatiques, suivis par les cybercriminels liés à la Corée du Nord, à la Russie et à l'Iran.
- **Groupe APT le plus actif –** Mustang Panda a conservé son titre de groupe APT le plus actif au monde (72 %) pour le troisième trimestre consécutif, illustrant les efforts continus et croissants déployés par la Chine à des fins d'espionnage et de perturbation.

Vulnérabilités

- **Défaut de correction des vulnérabilités connues –** La plupart des vulnérabilités les plus critiques du trimestre étaient des vulnérabilités connues qui n'avaient pas encore été corrigées.
- **Vulnérabilités anciennes –** Pour une vulnérabilité Apple signalée en février 2023, le bug avait des racines remontant à l'exploit FORCEDENTRY, utilisé par NSO Group dans le cadre de son logiciel espion Pegasus rendu public en 2021.

Sécurité e-mail

- **Nouveaux vecteurs d'attaque –** Bien que Microsoft ait commencé à bloquer les macros dans les pièces jointes pour la plate-forme Office, les cybercriminels ont rapidement adopté d'autres vecteurs d'infection pour continuer de cibler des équipements Windows, comme l'empoisonnement SEO, OneNote et les pièces jointes ZIP.
- **Marques non fiables –** En plus des e-mails de phishing génériques, les acteurs malveillants usurpent de plus en plus de noms de marque et de services légitimes, comme ceux de PayPal, Google, DWeb et IPFS, pour escroquer des victimes et dérober leurs informations d'identification en ligne.

Accès non autorisé au cloud

- **Évolution des tactiques –** Les attaques visant les infrastructures cloud ne cessent de se multiplier à mesure qu'un nombre croissant d'entreprises migrent d'une infrastructure sur site à des options plus abordables et évolutives proposées par Amazon, Microsoft, Google et d'autres.
- **Comptes valides –** Malgré la prolifération des attaques plus sophistiquées ayant recours à l'authentification multifacteur (MFA), à des proxys et à l'exécution d'API, la technique d'attaque dominante reste les comptes valides, avec une fréquence plus de deux fois supérieure à celle du deuxième vecteur d'attaque le plus utilisé. Cela prouve que le risque d'accès non autorisé est bien réel, car les cybercriminels accèdent à des identifiants de comptes ou de sites web légitimes pour s'infiltrer et lancer des attaques.

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

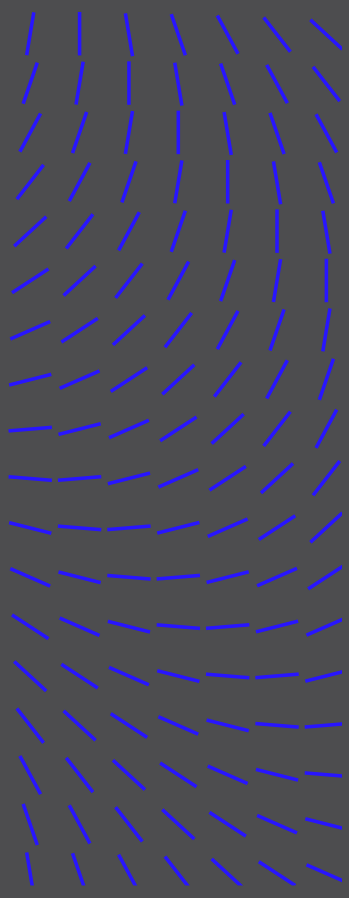
SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX



SIGNALEMENTS, DONNÉES ET ANALYSES

Incidents de sécurité

Les incidents de sécurité évoqués dans cette section se basent sur des signalements publics. Au 1er trimestre 2023, les fichiers binaires Windows, les outils tiers, les malwares personnalisés et les outils de test d'intrusion ont continué d'avoir un impact sur les opérations alors que les cybercriminels exploitaient des vecteurs d'attaque plus faciles. PowerShell et Windows Command Shell sont toujours exploités pour générer des tâches menant à la persistance, au déploiement et à l'extraction.

PRINCIPAUX FICHIERS BINAIRES WINDOWS UTILISÉS – T1 2023

1. PowerShell
2. Windows CMD
3. Tâche planifiée
4. RunDLL32
5. WMIC

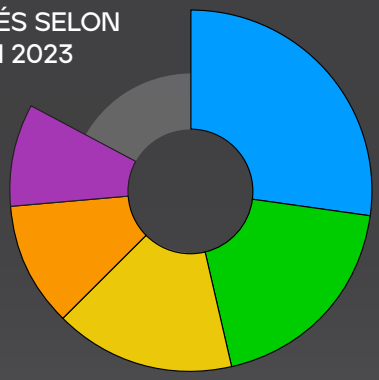
Les tâches planifiées, l'insertion de fichiers DLL malveillants et l'exécution de commandes par le biais de l'infrastructure de gestion Windows (WMI) viennent compléter le top 5. Que ce soit par le biais de l'exécution de scripts ou d'une saisie manuelle au clavier, les cybercriminels ont continué d'utiliser les fichiers binaires non protégés et non surveillés déjà à leur disposition.

Souvent, les outils tiers, les freewares et les outils de test d'intrusion jouent un rôle dans le cycle de vie d'une attaque en aidant les cybercriminels à établir une persistance, à exécuter des scripts, à identifier et à collecter des informations ciblées et à élever des privilèges pour accéder à des actifs ou à des données qui seraient autrement inaccessibles aux comptes restreints. En outre, un attaquant peut, à des fins d'élévation de privilèges, exécuter des processus d'installation avec des privilèges élevés et accéder à des zones, à des actifs ou à des données qui seraient autrement inaccessibles aux comptes restreints.

PRINCIPAUX OUTILS TIERS UTILISÉS SELON LES SIGNALEMENTS PUBLICS – T1 2023

CATÉGORIES D'OUTILS

- Transfert de fichiers
- Programmes de compression
- Outils de post-exploitation
- Outils d'accès à distance
- Utilitaires d'archivage



INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

SIGNALEMENTS, DONNÉES ET ANALYSES

INCIDENTS DE SÉCURITÉ

RANSOMWARES

ATTAQUES ÉTATIQUES

VULNÉRABILITÉS

SÉCURITÉ E-MAIL

SÉCURITÉ RÉSEAU

INCIDENTS CLOUD

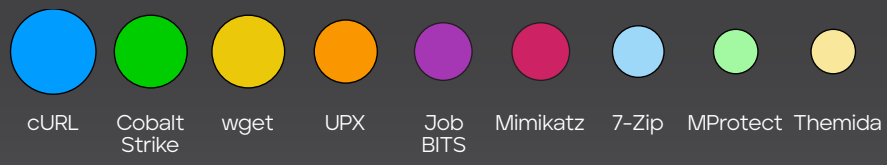
MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX

OUTILS TIERS UTILISÉS SELON LES SIGNALEMENTS PUBLICS – T1 2023

OUTILS SPÉCIFIQUES



Les outils tiers plus dangereux comme Cobalt Strike, Mimikatz et SharpHound sont utilisés à la fois de manière légitime et par des cybercriminels pour collecter des mots de passe, définir des jetons ou élever des privilèges. Une fois qu'un attaquant a compromis un environnement, il peut utiliser des outils de transfert de fichiers comme cURL pour accéder à des charges actives à distance ou Rclone pour exfiltrer des données vers un stockage cloud.

Au 1er trimestre 2023, Magecart Group, APT29 et APT41 ont été les trois collectifs cybercriminels les plus actifs pour cibler des utilisateurs selon leur géolocalisation et leur secteur afin de gagner de l'argent, de voler des secrets gouvernementaux ou d'empêcher l'utilisation d'infrastructures. Nous avons été surpris de constater que Magecart Group arrive en tête du classement, car il opère rarement à la même échelle que les autres grands groupes APT étatiques. Nous allons surveiller l'activité du groupe au cours des mois à venir pour déterminer si les données de la période actuelle indiquent une réémergence du groupe dans le monde entier.

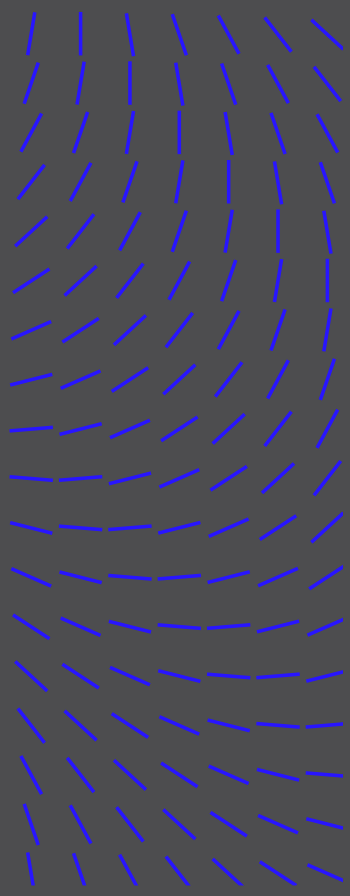
PRINCIPAUX GROUPES CYBERCRIMINELS ACTIFS SELON LES SIGNALEMENTS PUBLICS – T1 2023

1.	Magecart Group	5 %
2.	APT29	4 %
3.	APT41	4 %
4.	Blind Eagle	4 %
5.	Gamaredon Group	4 %
6.	Lazarus	4 %
7.	Mustang Panda	4 %
8.	Sandworm Team	4 %

Lors de précédentes campagnes mondiales, des techniques moins sophistiquées de type « spray-and-pray » conçues pour tenter les utilisateurs susceptibles de cliquer sur un lien malveillant ou de télécharger un fichier dangereux ont semé le chaos dans divers secteurs. Les attaques ciblées ont gagné en sophistication et sont plus persistantes contre les secteurs de la fabrication, de la finance et de la santé. Si les deux secteurs restants, les télécommunications et l'énergie, semblent avoir été moins souvent ciblés lors d'événements mondiaux, ils sont tout aussi importants et il est possible que les entreprises associées n'aient pas signalé les compromissions ou n'aient pas détecté les incidents dont elles ont été victimes.

PRINCIPAUX SECTEURS CIBLÉS SELON LES SIGNALEMENTS PUBLICS – T1 2023

1.	Fabrication	8 %
2.	Finance	7 %
3.	Santé	6 %
4.	Télécommunications	5 %
5.	Énergie	5 %



Les événements signalés qui ont été analysés et vérifiés par notre équipe de recherche contiennent une mine d'informations, de corrélations ou d'attributions d'un cybercriminel, d'un groupe cybercriminel ou d'un collectif APT plus sophistiqué. Les outils, techniques et procédures ainsi que les familles de malwares employés incluent les malwares chargeurs et téléchargeurs, les outils d'administration à distance (RAT), les outils d'exfiltration d'informations et les ransomwares. D'après les événements analysés et disponibles via Insights pour le 1er trimestre 2023, nous avons déterminé que l'Ukraine a été le pays le plus ciblé, suivi de près par les États-Unis.

Les familles de ransomwares Royal Ransom, Trigona et Maui ont été les plus utilisées au 1er trimestre 2023. Trellix a récemment publié une analyse détaillée de Royal Ransom et de son mode opératoire avec des fichiers exécutables Windows et Linux. Bien que les statistiques représentées émanent spécifiquement de notre plate-forme Insights, de nombreux autres événements se sont produits au sein de l'infrastructure connectée à l'échelle mondiale, y compris des événements connus ayant été signalés ou étant restés confidentiels, ainsi que des événements qui n'ont pas encore été identifiés et corrigés.

PRINCIPAUX PAYS CIBLÉS SELON LES SIGNALEMENTS PUBLICS – T1 2023

7 %

D'après les événements rendus publics et disponibles pour analyse, nous avons déterminé que l'Ukraine a été le pays le plus ciblé par des cybercriminels, suivi de près par les États-Unis.

1.	Ukraine	7 %
2.	États-Unis	7 %
3.	Allemagne	4 %
4.	Corée du Sud	3 %
5.	Inde	3 %

PRINCIPAUX RANSOMWARES UTILISÉS SELON LES SIGNALEMENTS PUBLICS – T1 2023

1.	Royal Ransom	7 %
2.	Trigona	4 %
3.	Maui	4 %
4.	Magniber	3 %
5.	LockBit	3 %

Ransomwares

Les statistiques affichées ci-dessous 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.

Il est assez courant d'observer une baisse des activités cybercriminelles au début de l'année, en particulier en janvier. Cette tendance pourrait expliquer la diminution notable des activités associées aux ransomwares Hive et Cuba. Par ailleurs, il ne serait pas étonnant que la perturbation des activités de Hive par le FBI et Europol à la fin du mois de janvier ait considérablement interféré avec ses opérations. LockBit demeure une famille de ransomwares prévalente. Elle est particulièrement agressive et semble réussir à inciter ses victimes à payer les rançons.

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX

PRINCIPAUX RANSOMWARES UTILISÉS – T1 2023

8 %

Cuba a été le groupe de ransomware le plus actif, suivi par Play et LockBit.

- Cuba
- Play
- LockBit 3.0
- Clop
- Hive

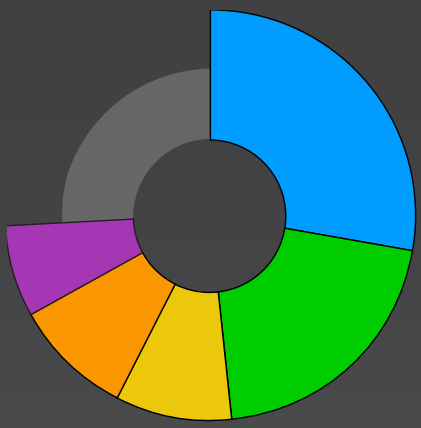


OUTILS DE RANSOMWARE UTILISÉS – T1 2023

28 %

Cobalt Strike a été utilisé dans près d'un tiers des attaques de ransomware du trimestre. Sa popularité ne fait que croître, malgré les récentes mises à jour visant à compliquer son utilisation par des cybercriminels.

- Cobalt Strike
- Mimikatz
- Empire
- BloodHound
- SystemBC



PAYS LES PLUS TOUCHÉS PAR DES GROUPES DE RANSOMWARE – T1 2023

15 %

Ce trimestre, les États-Unis restent le pays le plus touché par des groupes de ransomware, suivi de près par la Turquie.

1.	États-Unis	15 %
2.	Turquie	14 %
3.	Portugal	10 %
4.	Inde	9 %
5.	Canada	9 %

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

SIGNALEMENTS, DONNÉES ET ANALYSES

INCIDENTS DE SÉCURITÉ

RANSOMWARES

ATTAQUES ÉTATIQUES

VULNÉRABILITÉS

SÉCURITÉ E-MAIL

SÉCURITÉ RÉSEAU

INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX

SECTEURS LES PLUS TOUCHÉS PAR DES GROUPES DE RANSOMWARE – T1 2023

1.	Assurances	20 %
2.	Services financiers	17 %
3.	Industrie pharmaceutique	7 %
4.	Télécommunications	4 %
5.	Externalisation et hébergement	4 %

Les groupes de ransomware extorquent de l'argent à leurs victimes en publiant leurs informations sur des sites web appelés « sites de divulgation » (leak sites) pour relancer les négociations ou en cas de refus de paiement de la rançon. Les experts Trellix utilisent RansomLook, un outil open source, pour collecter des données à partir des publications, puis normaliser et enrichir les résultats afin de procéder à une analyse anonymisée 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. Les mesures ci-dessous sont un indicateur des victimes ciblées par des groupes de ransomware à des fins d'extorsion ou de représailles, à ne pas confondre avec le nombre total de victimes.

GROUPES DE RANSOMWARE COMPTABILISANT LE PLUS DE VICTIMES SELON LEURS SITES DE DIVULGATION – T1 2023

1.	LockBit	30 %
2.	Hive	22 %
3.	Clop	12 %
4.	Royal Ransom	7 %
5.	ALPHV	5 %

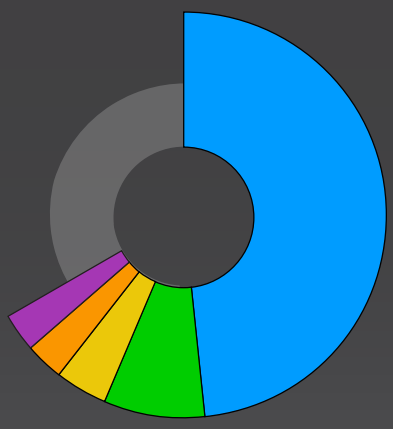
SECTEURS LES PLUS TOUCHÉS PAR DES GROUPES DE RANSOMWARE SELON LEURS SITES DE DIVULGATION – T1 2023

1.	Biens et services industriels	25 %
2.	Vente au détail	14 %
3.	Technologies	11 %
4.	Santé	8 %
5.	Services financiers	6 %

PRINCIPAUX PAYS DES ENTREPRISES RÉPERTORIÉES SUR LES SITES DE DIVULGATION – T1 2023

48 %

des entreprises victimes répertoriées sur les sites de divulgation des groupes de ransomware étaient basées aux États-Unis.



- États-Unis
- Royaume-Uni
- Allemagne
- Canada
- Inde

TAILLE DES ENTREPRISES RÉPERTORIÉES SUR LES SITES DE DIVULGATION – T1 2023

NOMBRE DE COLLABORATEURS		CHIFFRE D'AFFAIRES ANNUEL	
1. 51-200	32 %	1. 10-50 Mio $	38 %
2. 1 001-5 000	22 %	2. 1-10 Mds $	23 %
3. 11-50	15 %	3. 1-10 Mio $	21 %
4. 201-500	15 %	4. 100-250 Mio $	11 %
5. 501-1 000	15 %	5. 500 Mio-1 Md $	7 %

Attaques étatiques

Les informations sur les attaques étatiques 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 groupes étatiques, des indicateurs de compromission (IOC) 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 vérifiés et analysés par le groupe Threat Intelligence.

Comme mentionné ci-dessus, ces statistiques 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 à nos objectifs d'analyse.

Les collectifs affiliés à la Chine continuent à dominer le paysage mondial des menaces. Mustang Panda est d'ailleurs à l'origine d'une grande majorité des détections au 1er trimestre 2023. Étant donné qu'ils font une utilisation massive du transfert local direct (« sideloading ») et d'autres techniques furtives, il est possible que les groupes APT à la solde de la Chine changent moins souvent d'outils de malware que les autres cybercriminels. Si tel est le cas, cette pratique pourrait se traduire par un « biais de projection » ou par une estimation gonflée des détections des hachages affiliés à la Chine.

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

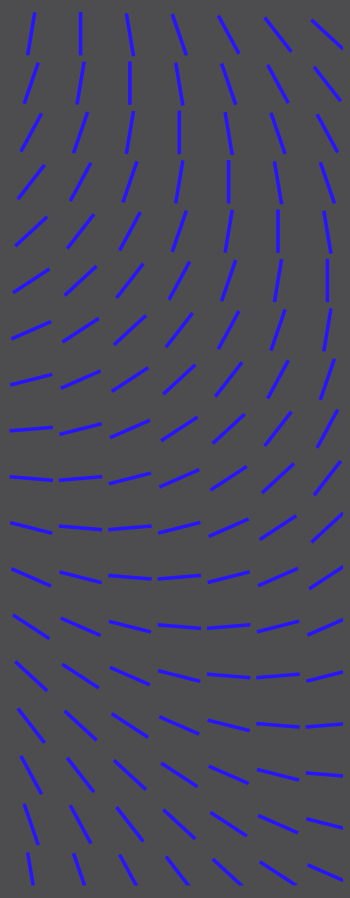
SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX

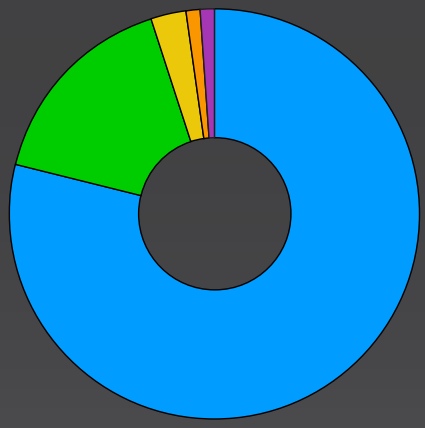


PAYS D'ORIGINE LES PLUS PRÉVALENTS DES CYBERCRIMINELS IMPLIQUÉS DANS DES ATTAQUES ÉTATIQUES – T1 2023

79 %

La Chine est à l'origine d'une grande majorité des attaques étatiques au 1er trimestre 2023.

- Chine
- Corée du Nord
- Russie
- Iran
- Pakistan



GROUPES CYBERCRIMINELS LES PLUS PRÉVALENTS – T1 2023

1.	Mustang Panda	72 %
2.	Lazarus	17 %
3.	UNC4191	1 %
4.	Common Raven	1 %
5.	APT34	1 %

TECHNIQUES MITRE ATT&CK LES PLUS PRÉVALENTES UTILISÉES DANS DES ATTAQUES ÉTATIQUES – T1 2023

1.	Chargement latéral de LDLL	14 %
2.	Désobfuscation/décodage de fichiers pour trouver des informations	11 %
3.	Transfert d'outils à l'entrée	10 %
4.	Données extraites d'un système local	10 %
5.	Découverte des fichiers et des répertoires	10 %

OUTILS MALVEILLANTS LES PLUS PRÉVALENTS UTILISÉS DANS DES ATTAQUES ÉTATIQUES – T1 2023

38 %

PlugX représente 38 % des attaques étatiques au 1er trimestre 2023.

1.	PlugX	38 %
2.	Cobalt Strike	35 %
3.	Raspberry Robin	14 %
4.	BLUEHAZE/DARKDEW MISTCLOAK	3 %
5.	Mimikatz	3 %

L'Inde fait partie des principaux pays d'Asie et des régions voisines disposant de programmes de cybersécurité efficaces. Certains groupes, principalement des collectifs liés à la Chine, ont manifesté un vif intérêt pour les développements technologiques, militaires et politiques de l'Inde. Un nombre considérable de détections effectuées en Inde peuvent être attribuées à Mustang Panda.

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

SIGNALEMENTS, DONNÉES ET ANALYSES

INCIDENTS DE SÉCURITÉ

RANSOMWARES

ATTAQUES ÉTATIQUES

VULNÉRABILITÉS

SÉCURITÉ E-MAIL

SÉCURITÉ RÉSEAU

INCIDENTS CLOUD

MÉTHODOLOGIE

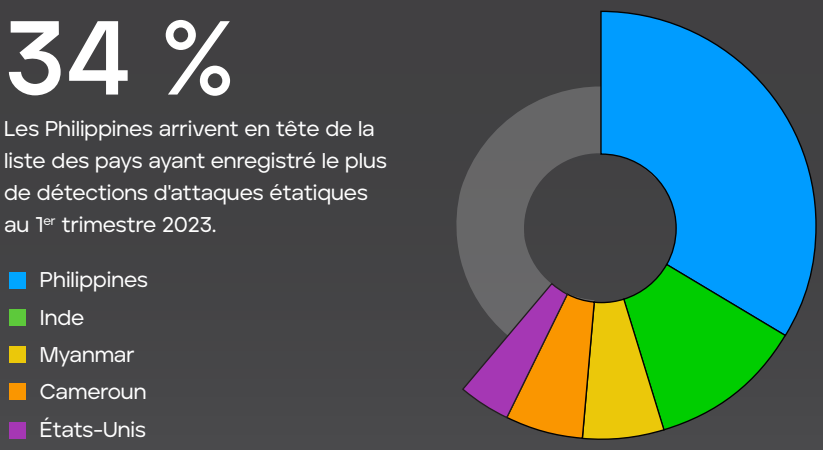
RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX

PAYS AYANT ENREGISTRÉ LE PLUS DE DÉTECTIONS D'ATTAQUES ÉTATIQUES – T1 2023

34 %

Les Philippines arrivent en tête de la liste des pays ayant enregistré le plus de détections d'attaques étatiques au 1er trimestre 2023.



SECTEURS AYANT ENREGISTRÉ LE PLUS DE DÉTECTIONS D'ATTAQUES ÉTATIQUES – T1 2023



Vulnérabilités

Les experts en ingénierie inverse et en analyse des vulnérabilités de Trellix Advanced Research Center surveillent en permanence les dernières vulnérabilités afin d'expliquer aux clients comment les cybercriminels les exploitent et comment réduire la probabilité et l'impact de ces attaques.

L'une de nos observations les plus intéressantes, bien que prévisibles, sur le 1er trimestre 2023 est que bon nombre des vulnérabilités critiques de cette période correspondaient à des contournements de patchs d'anciennes CVE, à des bugs de la chaîne logistique dus à l'utilisation de bibliothèques obsolètes ou à des vulnérabilités corrigées depuis longtemps qui persistent bien après leurs quinze minutes de gloire.

Prenons comme exemple CVE-2022-47966, une vulnérabilité critique (9.8) identifiée dans les produits ManageEngine de Zoho qui a circulé en janvier. ManageEngine est utilisé par des milliers d'entreprises à travers le monde. Nous n'avons donc pas été surpris que l'exploitation de cette vulnérabilité soit détectée en environnement réel. Ce qui nous a étonnés, c'est la cause première : l'utilisation d'Apache Santuario 1.4.1, une version très ancienne qui contenait un problème connu autorisant l'injection de XML. Zoho a corrigé la vulnérabilité dans sa suite de produits en octobre et, près de trois mois plus tard, au 1er trimestre, la CISA a publié un avis de sécurité signalant son exploitation en environnement réel et incitant les fournisseurs à appliquer un patch.

CVE-2022-44877 est un autre exemple. Il s'agit d'une vulnérabilité critique présente dans Control Web Panel (CWP). Bien qu'elle ne soit pas directement liée, cette vulnérabilité présente bon nombre des caractéristiques de notre précédent exemple : il s'agit également d'une RCE 9.8 qui a été largement exploitée en janvier malgré la publication d'un patch en octobre. La cause première n'était pas digne d'une conférence Black Hat non plus, car il s'agissait d'une injection de commande utilisant une expansion de variable shell standard dans un paramètre d'URL.

Comme troisième exemple, on peut citer CVE-2021-21974, une vulnérabilité identifiée dans le service OpenSLP de VMware ESXi, corrigée en février 2021, soit presque exactement deux ans avant sa soudaine résurgence en raison d'une exploitation en environnement réel. Lorsque nous avons mentionné cette vulnérabilité dans notre Rapport sur les bugs de février, nous avons constaté que, selon Shodan, près de 48 000 serveurs accessibles par Internet exécutaient toujours des versions vulnérables d'ESXi. Aujourd'hui, ce chiffre reste supérieur à 38 000, soit une baisse de moins de 22 %.

Date	Nombre de serveurs ESXi vulnérables selon Shodan
Fin février 2023	48 471
Fin avril 2023	38 047

Nous avons nous-mêmes trouvé quelques exemples lors de nos recherches sur les équipements Apple au début de l'année : CVE-2023-23530 et CVE-2023-23531. Ces deux vulnérabilités diffèrent des exemples précédents, car leur impact est limité à l'élévation locale de privilèges et elles n'ont pas recours à l'exécution de code à distance. Ce n'est toutefois pas une raison pour les négliger, étant donné qu'une vulnérabilité très similaire a été employée par l'exploit FORCEDENTRY, utilisé par NSO Group pour déployer son logiciel espion Pegasus en 2021. En effet, les deux vulnérabilités que nous avons découvertes utilisent la primitive qui a servi de base à l'exploit FORCEDENTRY : une classe inoffensive appelée NSPredicate. Malheureusement, l'approche d'Apple pour la prévention de FORCEDENTRY impliquait l'utilisation d'une longue liste de blocage afin d'empêcher l'exploitation de NSPredicate – une prévention qui n'a pas résolu le problème sous-jacent et nous a permis de la contourner.

Il est tentant de montrer du doigt des tendances telles que celles-ci et de conclure que les fournisseurs ne prennent pas la sécurité au sérieux ou de se plaindre de la régurgitation d'anciens exploits par des cybercriminels et des chercheurs, mais ce n'est pas le bon comportement à adopter. Les chercheurs sur les vulnérabilités procèdent à l'analyse des variantes, car un chercheur efficace émule les priorités des véritables cybercriminels et la découverte d'un mécanisme de contournement de la prévention ou d'une ancienne CVE dans un produit rarement corrigé produit systématiquement un meilleur retour sur investissement que la réinvention de la roue. Les entreprises qui ont conscience de cette tendance doivent tirer l'enseignement suivant : si ces technologies de détection des menaces de pointe sont irremplaçables dans le paysage des menaces actuel, de nombreuses victoires peuvent être remportées au niveau des fondamentaux, comme l'application de patchs aux processus et la vérification de la chaîne logistique.

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

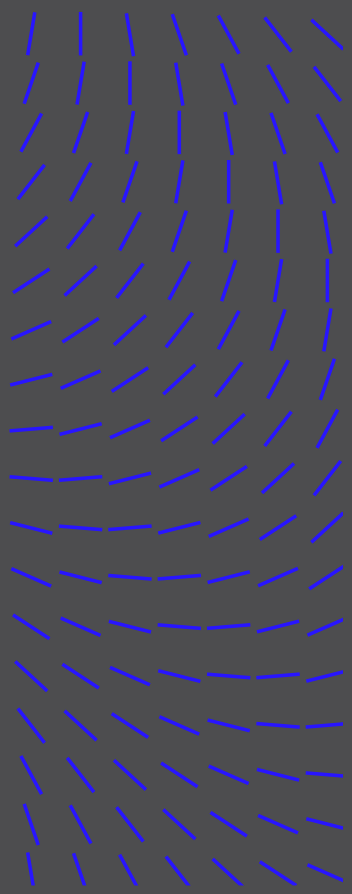
SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX



Sécurité e-mail

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 attaques de phishing qui détournent des marques légitimes pour escroquer des utilisateurs et subtiliser leurs informations d'identification sont en plein essor. DWeb, IPFS et Google Traduction sont largement utilisés dans les attaques par e-mail. Les attaquants ont également exploité des messageries gratuites et d'autres services comparables, comme les applications PayPal Invoicing et Google Forms, pour lancer des attaques de vishing et échapper à toute détection. De nouvelles marques telles que Scribd et LesMills ainsi que les cartes cadeaux Google Play ont aussi été prises pour cible pendant cette période.

Par ailleurs, si l'on s'intéresse au malware spécifique utilisé pour ces attaques, Formbook et Agent Tesla ont tous deux connu une augmentation significative au 1er trimestre 2023 par rapport à la fin de l'année dernière. Cela peut s'expliquer par le fait que ces deux malwares sont plus faciles à acquérir et à déployer que Rembos, Emotet et Qakbot.

MALWARES E-MAIL LES PLUS PRÉVALENTS – T1 2023

44 %

Formbook représente près de la moitié des malwares e-mail au 1er trimestre, suivi de près par Agent Tesla.



INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX

PAYS LES PLUS CIBLÉS PAR DES E-MAILS DE PHISHING – T1 2023

30 %



Les États-Unis et la Corée ont été les pays les plus touchés par des tentatives de phishing par e-mail au 1er trimestre. Ils ont en effet reçu près de deux tiers des tentatives de phishing à l'échelle mondiale.

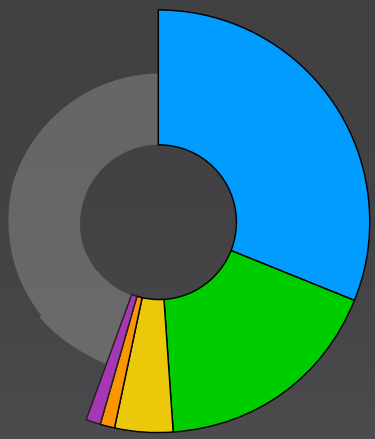
1.	États-Unis	30 %
2.	Corée du Sud	29 %
3.	Taïwan	10 %
4.	Brésil	8 %
5.	Japon	7 %

PRODUITS ET MARQUES LES PLUS CIBLÉS PAR DES E-MAILS DE PHISHING – T1 2023

38 %

Bien que des centaines de marques aient été ciblées, les produits Microsoft ont été de loin les plus exploités au 1er trimestre 2023.

- Microsoft
- Google Captcha
- Outlook
- GCash
- USPS



SECTEURS LES PLUS TOUCHÉS PAR DES E-MAILS MALVEILLANTS – T1 2023

1.	Organismes publics	11 %
2.	Services financiers	8 %
3.	Fabrication	6 %
4.	Technologies	6 %
5.	Divertissement	5 %

HÉBERGEURS WEB FORTEMENT EXPLOITÉS – T1 2023

1.	IPFS	41 %
2.	Google Traduction	33 %
3.	DWeb	16 %
4.	Amazon AWS Appforest	3 %
5.	Firebase OWA	3 %

TECHNIQUES DE CONTOURNEMENT LES PLUS UTILISÉES DANS DES ATTAQUES DE PHISHING – T1 2023

79 %

Les attaques par contournement basé sur une redirection 302 ont constitué la technique de contournement la plus prévalente utilisée dans les attaques de phishing au 1er trimestre 2023.

46 %

Les attaques basées sur les CAPTCHA ont beaucoup progressé au 1er trimestre 2023 par rapport au 4e trimestre 2022.

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX

Sécurité réseau

En parallèle de la détection et du blocage des attaques basées sur le réseau qui menacent nos clients, l'équipe de recherche réseau de Trellix Advanced Research Center inspecte différentes étapes de la chaîne de frappe (reconnaissance, compromission initiale, communication avec le serveur C&C et TTP de mouvement latéral).

TENDANCES LES PLUS MARQUANTES EN MATIÈRE DE MALWARES – T1 2023

L'activité du ransomware STOP a chuté de	94 %
La distribution du ransomware LockBit par Amadey a bondi de	25 %
L'activité des malwares Android a progressé de	12,5 %
L'activité d'Ursnif a augmenté de	10 %
L'activité de Smoke Loader a été multipliée par un facteur	X7
L'activité d'Amadey a été multipliée par un facteur	X4
L'activité de Cobalt Strike a été multipliée par un facteur	X3
L'activité d'Emotet a été multipliée par un facteur	X2

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

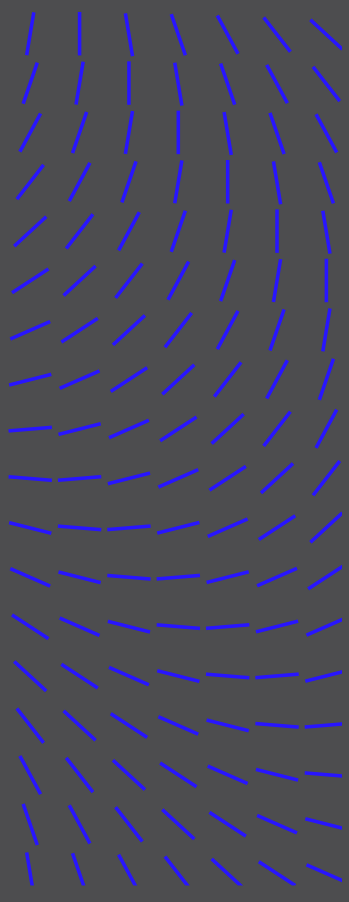
SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

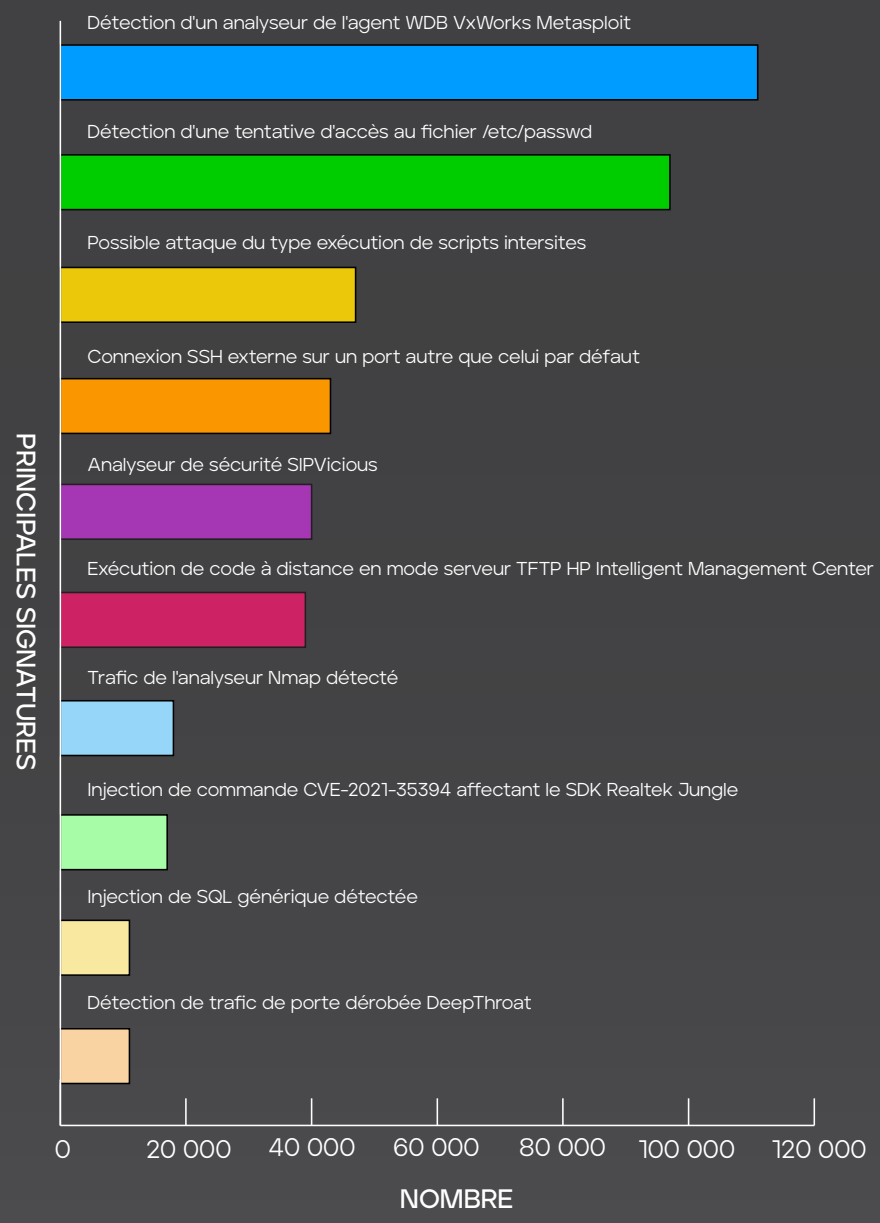
MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX



ATTAQUES AYANT LE PLUS D'IMPACT CONTRE DES SERVICES ACCESSIBLES DE L'EXTÉRIEUR – T1 2023



INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX

Incidents cloud

Les attaques visant des infrastructures cloud sur des services développés et distribués par Amazon, Microsoft, Google et d'autres ne cessent de se multiplier. Le tableau ci-dessous reprend les données télémétriques sur les attaques cloud, réparties selon le client et le fournisseur de services cloud.

DÉTECTIONS PAR TECHNIQUES MITRE ATT&CK – T1 2023

	AWS	Microsoft Azure	GCP
Comptes valides	3 437	4 312	997
Modification de l'infrastructure de service de calcul du compte cloud	4 268	0	17
Port non standard	115	0	17
Authentification multifacteur	190	1 534	22
Découverte des services réseau	141	93	0
Attaque en force brute	25	1 869	22
Proxy	299	2 744	135
Découverte des comptes	264	68	787
Règle de transfert d'e-mail	25	0	22
Exécution via une API	1 143	0	252

MÉTHODOLOGIE

Collecte – Trellix et les experts chevronnés de l'équipe de classe mondiale Trellix Advanced Research Center recueillent les statistiques, les tendances et les résultats d'analyses qui composent ce rapport auprès d'un large éventail de sources mondiales.

- **Sources captives –** Dans certains cas, les données télémétriques sont générées par les solutions de sécurité Trellix sur les réseaux de cybersécurité des clients et les dispositifs de défense déployés dans le monde entier sur les réseaux des secteurs public et privé, y compris ceux distribuant des services technologiques, d'infrastructure ou de données. Ces systèmes, qui se comptent en millions, génèrent des données à partir d'un milliard de capteurs.
- **Sources ouvertes –** Dans d'autres cas, Trellix s'appuie sur une combinaison d'outils brevetés, propriétaires et open source pour analyser des sites, des journaux et des référentiels de données sur Internet ainsi que sur le Dark Web, par exemple les « sites de divulgation » où les groupes de ransomware publient des informations sur ou appartenant à leurs victimes.

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

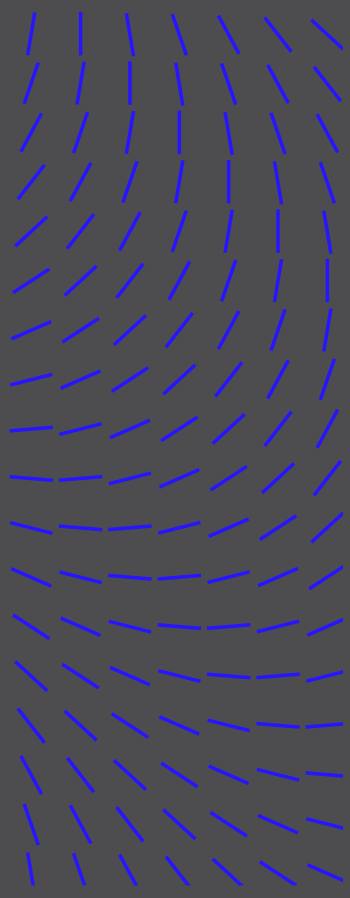
SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX



Normalisation – Les données agrégées alimentent nos plates-formes Insights et ATLAS. Grâce à l'apprentissage automatique, à l'automatisation et à l'acuité humaine, l'équipe effectue une série de processus intensifs, intégrés et itératifs afin de normaliser les données, d'enrichir les résultats, de supprimer les informations personnelles et d'identifier les corrélations entre les méthodes d'attaque, les agents, les secteurs, les régions, les stratégies et les résultats.

Analyse – Ensuite, Trellix analyse ce vaste référentiel d'informations, en le comparant à (1) son importante base de données de Threat Intelligence, (2) des rapports du secteur de la cybersécurité provenant de sources accréditées et respectées, et (3) l'expérience et les connaissances de ses analystes en cybersécurité, spécialistes en investigation, en ingénierie inverse et en investigation numérique, et experts en vulnérabilités.

Interprétation – Enfin, l'équipe Trellix extrait, examine et valide les informations pertinentes qui peuvent aider les responsables de la cybersécurité et les équipes SecOps (1) à comprendre les tendances les plus récentes du paysage des cybermenaces et (2) à utiliser cette perspective pour améliorer leur capacité à anticiper, prévenir et bloquer les cyberattaques à l'avenir.

RESSOURCES

Archives des Rapports sur le paysage des menaces

The Mind of the CISO

Trellix Advanced Research Center Discovers a New Privilege Escalation Bug Class on macOS and iOS

A Royal Analysis of Royal Ransom

Feeding Gophers to Ghidra

TWITTER

Trellix ARC

Consulter les éditions précédentes du Rapport sur le paysage des cybermenaces

Trellix Advance Research Center

INTRODUCTION

RÉSUMÉ DE L'ACTUALITÉ DES MENACES – T1 2023

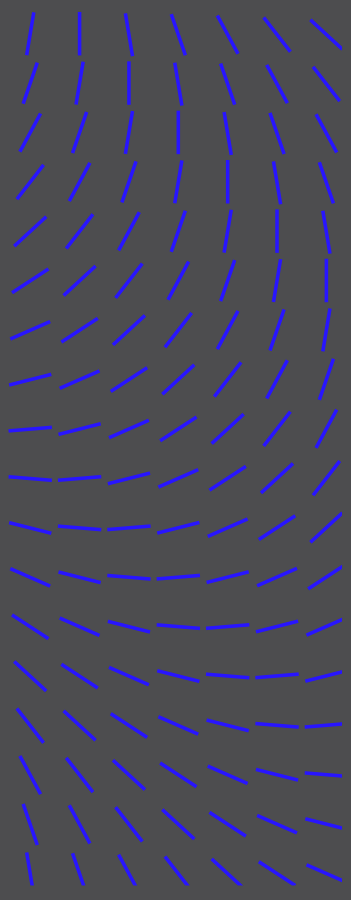
SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX



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 mondial des menaces. Partenaire incontournable des équipes responsables 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. Par ailleurs, le groupe Threat Intelligence de Trellix Advanced Research Center propose des produits et services de Threat Intelligence aux clients dans le monde entier.

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.

INTRODUCTION

L'ACTUALITÉ DES MENACES EN RÉSUMÉ – T1 2023

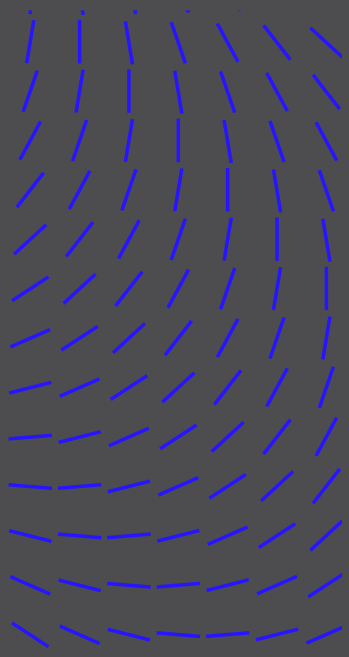
SIGNALEMENTS, DONNÉES ET ANALYSES

- INCIDENTS DE SÉCURITÉ
- RANSOMWARES
- ATTAQUES ÉTATIQUES
- VULNÉRABILITÉS
- SÉCURITÉ E-MAIL
- SÉCURITÉ RÉSEAU
- INCIDENTS CLOUD

MÉTHODOLOGIE

RESSOURCES

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER ET TRELLIX



Ce document et les renseignements qu'il contient concernent des recherches dans le domaine de la sécurité informatique. Ils ne sont fournis qu'à titre informatif, au bénéfice des clients de Trellix. Trellix mène ses recherches conformément à sa Politique de divulgation responsable des vulnérabilités. L'utilisateur assume pleinement les risques liés à toute tentative de reproduction de tout ou partie des activités mentionnées, dont Trellix et ses sociétés affiliées ne pourront en aucun cas être tenus responsables.

Trellix est une marque commerciale ou une marque commerciale déposée de Musarubra US LLC ou ses sociétés affiliées aux États-Unis et dans d'autres pays. Les autres noms et marques sont la propriété de leurs détenteurs respectifs.

Pour en savoir plus, visitez le site Trellix.com.

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.

Copyright © 2023 Musarubra US LLC

072022-05