RAPPORT SUR LE PAYSAGE DES CYBERMENACES

Juin 2024

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

AU SOMMAIRE :

Présenté par

Trellix ADVANCED RESEARCH CENTER

Un outil de contournement spécifique vient d'être utilisé avec succès pour désactiver les fonctionnalités EDR (Endpoint Detection and Response) d'une entreprise de votre secteur.

La course à la cybersécurité se complique, car il est de plus en plus difficile d'empêcher l'emploi d'outils de sécurité légitimes à des fins malveillantes.

En tant que RSSI, vous devez faire preuve d'agilité, de rapidité, de confiance et de contrôle. Votre PDG et votre conseil d'administration veulent en savoir plus sur vos outils de journalisation et d'alerte. Vous chargez votre équipe d'identifier les failles et vous avez élaboré un plan pour les corriger.

La course à la cybersécurité est un vrai triathlon, dont les disciplines sont le SecOps, les technologies et la Threat Intelligence. L'endurance est essentielle.

> À mesure que les mécanismes de défense gagnent en sophistication, les outils et tactiques d'attaque employés par les cybercriminels et les acteurs étatiques font de même.

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 octobre 2023 et le 31 mars 2024.

1. Mutation rapide et significative du paysage APT
2. L'écosystème des ransomwares secoué par LockBit
3. Émergence d'outils de désactivation d'EDR
4. Escroqueries sur le thème des élections présidentielles américaines
5. L'IA générative et le marché clandestin cybercriminel

AVANT-PROPOS

La Threat Intelligence opérationnelle et la mise en contexte des menaces mondiales en fonction de votre environnement d'entreprise n'ont jamais été aussi importantes pour le rôle du RSSI.

Les RSSI et leurs équipes SecOps ont besoin de la Threat Intelligence pour anticiper les menaces, identifier celles qui sont les plus susceptibles de cibler votre entreprise et s'y préparer, aligner les programmes et le budget sur les menaces et cybercriminels les plus pertinents, et enfin, passer d'une approche réactive à proactive.

En tant que « client zéro » de Trellix, je constate que les renseignements pertinents sur les menaces ont, plus que jamais, le potentiel de transformer la manière dont les équipes de réponse agissent et conçoivent leurs stratégies.

Consultez ces informations, assimilez-les et tenez-en compte pour votre planification stratégique, la rationalisation de votre budget, la collaboration avec le conseil d'administration et le support opérationnel. J'espère que ces pages vous seront utiles et qu'elles vous permettront de mieux orienter votre planification, votre préparation et votre défense contre les menaces APT.

Harold Rivas
CISO, TRELLIX

SOMMAIRE

PRÉFACE

Ce rapport a pour objectif de structurer notre Threat Intelligence et de mettre en contexte nos observations.

Le paysage

Les six derniers mois ont été sans précédent : la polycrise qui perdure a accéléré les activités des cybercriminels dans le monde entier. Nous observons des changements radicaux de comportement, par exemple :

- L'écosystème des ransomwares est atypique à la suite de diverses opérations des forces de l'ordre.
- Des groupes autonomes vendent leurs tests d'intrusion et leurs méthodes d'attaque alternatives à des gangs de ransomware.
- La guerre en Israël a déclenché des attaques et un cyberactivisme étatiques.
- Les acteurs cybercriminels cherchent à gagner en sophistication et ont accès à des outils d'IA générative gratuits ou peu coûteux, qui leur permettent de devenir des experts très rapidement.
- Les outils de contournement et de désactivation d'EDR sont de plus en plus plébiscités par les cybercriminels.

Un jeu du chat et de la souris

Avec l'adoption plus large de l'EDR (Endpoint Detection and Response), le jeu du chat et de la souris qu'est la cybersécurité se complique. L'augmentation du nombre de cybercriminels qui utilisent des outils malveillants pour neutraliser des solutions EDR a éveillé notre intérêt, car il s'agit d'un changement de cap radical par rapport à l'emploi d'outils traditionnels basés sur des malwares.

En tant que professionnels de la sécurité, nous devons suivre cette évolution de très près. Les solutions EDR ont prouvé leur efficacité dans la détection des malwares, ransomwares et activités APT, mais si elles venaient à être désactivées, que doivent faire une entreprise et son RSSI ? Vous avez besoin de la journalisation, des alertes et d'une Threat Intelligence opérationnelle pour bénéficier de visibilité sur les comportements inhabituels au sein de votre environnement. Il faut clairement élever son niveau de jeu.

Trellix s'attache diligemment à partager ses données de Threat Intelligence avec la communauté de la sécurité – l'une de nos valeurs essentielles pour garder une longueur d'avance sur les attaquants – et à suivre les campagnes et les groupes cybercriminels à grande échelle.

Le paysage n'a jamais été aussi mouvant. Notre objectif est de soutenir nos clients et le secteur au sens large en leur fournissant les renseignements pertinents nécessaires pour renforcer leurs défenses, élaborer des contre-mesures et identifier les failles.

Dans ce jeu du chat et de la souris, nous devons jouer pour gagner.

John Fokker
DIRECTEUR DE LA THREAT INTELLIGENCE, TRELLIX

SOMMAIRE

INTRODUCTION : RAPPORT SUR LE PAYSAGE DES CYBERMENACES – JUIN 2024

L'impact des événements géopolitiques sur le cyberdomaine

Les recherches menées par Trellix Advanced Research Center sur la période allant du 1er octobre 2023 au 31 mars 2024 ont révélé une évolution des activités liées aux menaces, dont une hausse notable des cybermenaces à motivation géopolitique. Des événements régionaux et mondiaux majeurs, tels que des exercices militaires, des sommets politiques ou économiques, des congrès politiques et des élections, ont accéléré les activités des cybermenaces.

Les analystes Trellix estiment probable que les cybercriminels se sont concentrés sur ces événements pour collecter des renseignements pertinents sur leurs homologues, sonder activement les réseaux afin d'alimenter leur connaissance situationnelle, ou s'infiltrer stratégiquement sur des réseaux IT en vue de futures attaques.

- **Rencontre entre les présidents Biden et Xi à San Francisco –** En novembre 2023, les données télémétriques de Trellix ont relevé une hausse des activités malveillantes de groupes APT affiliés à la Chine quelques jours seulement avant la rencontre entre le président américain Joe Biden et son homologue chinois Xi Jinping à San Francisco à l'occasion du sommet de la Coopération économique pour l'Asie-Pacifique (APEC). Le nombre d'activités liées aux menaces a nettement diminué après la rencontre et tout au long du sommet.

  Au terme de l'événement, le niveau d'activité des menaces a chuté à son point le plus bas du mois de novembre 2023. Cette évolution des activités des menaces provenant de groupes cybercriminels affiliés à la Chine suggère que ces derniers ont été fortement influencés par des événements géopolitiques tels que le sommet de l'APEC. Il est également possible que les groupes APT attachés à l'État chinois aient délibérément interrompu leurs activités de piratage pendant un événement politique majeur, peut-être pour préserver leur image publique et leur réputation internationale.
- **Guerre Israël-Hamas –** Les menaces émanant de groupes APT affiliés à l'Iran ont également été renforcées par les développements politiques entourant la guerre Israël-Hamas. Aux États-Unis, les données télémétriques mondiales de Trellix montrent des poussées périodiques d'activités malveillantes provenant de groupes APT affiliés à l'Iran au cours des six derniers mois (à l'exception de fin novembre et de décembre 2023). Plus précisément, nos données télémétriques mondiales font état d'une diminution des activités des menaces provenant de groupes APT liés à l'État iranien qui ciblent des entreprises américaines au moment des échanges d'otages israéliens et des accords de cessez-le-feu survenus fin novembre 2023 et en décembre 2023, lorsque les États-Unis ont appelé à un cessez-le-feu humanitaire dans la bande de Gaza, étant donné que l'Iran soutient ouvertement le Hamas. En outre, les données télémétriques mondiales de Trellix révèlent que les groupes APT affiliés à l'Iran ont employé diverses TTP, y compris du phishing, des outils d'exfiltration d'informations, des portes dérobées (backdoors), des téléchargeurs, des webshells malveillants et des vulnérabilités couramment exploitées, pour cibler des organisations israéliennes pendant la période considérée.

SOMMAIRE

- **Exercices militaires –** Par ailleurs, des exercices militaires multinationaux visant à améliorer la préparation au combat peuvent entraîner l'augmentation des activités malveillantes. Dernièrement, en mars 2024, les données télémétriques mondiales de Trellix ont montré des poussées répétées des activités de menaces en Corée du Sud pendant les importants exercices militaires conjoints entre les États-Unis et la Corée du Sud, baptisés Freedom Shield, qui ont eu lieu entre le 4 et le 14 mars. Ces exercices militaires sont conçus pour refléter le théâtre des opérations coréen et contrer la menace nucléaire grandissante de la Corée du Nord. Plus précisément, les détections de menaces en Corée du Sud ont dépassé le seuil des 150 000 le 7 et le 13 mars 2024, respectivement, soit près de sept fois les 20 000 détections quotidiennes habituelles dans le pays.
- **Guerre Russie-Ukraine –** La poursuite de la guerre cinétique dans la région s'accompagne de cyberinitiatives d'envergures diverses. Plus particulièrement, des cybercriminels affiliés à la Russie ont utilisé des malwares effaceurs (wipers) nouveaux et plus avancés pour effacer des milliers de PC et serveurs virtuels en attaquant l'opérateur de télécommunications ukrainien Kyivstar. L'attaque contre Kyivstar fait partie des cyberattaques perturbatrices contre l'Ukraine ayant eu le plus d'impact depuis que la Russie a envahi le pays en 2022.

L'actualité des menaces en résumé

Si ce rapport met en évidence les recherches menées par Trellix, certains thèmes clés restent constants :

1. **Mutation rapide et significative du paysage APT**
    a. **Le collectif Sandworm, affilié à la Russie, intensifie ses activités –** La montée des tensions géopolitiques s'accompagne d'une hausse des activités APT dans l'ensemble de l'écosystème. Bien que les menaces APT progressent de manière globale, le groupe Sandworm lié à Moscou a été détecté beaucoup plus fréquemment (+40 %) sur la période concernée par ce rapport.
    b. **La Chine reste prolifique –** Les groupes cybercriminels liés à l'État chinois restent les auteurs les plus prolifiques d'activités APT. Trellix a en effet observé plus de 21 millions de détections provenant de collectifs affiliés à la Chine. Plus de 23 % des détections d'activités malveillantes sont dirigées contre des organismes publics du monde entier.
    c. **Les activités de Volt Typhoon bondissent –** En tant que groupe APT financé par l'État chinois relativement récent, Volt Typhoon se distingue par son modèle de comportement et ses pratiques de ciblage uniques. Depuis mi-janvier 2024, les données télémétriques de Trellix ont détecté plus de 7 100 activités malveillantes associées à Volt Typhoon, avec des poussées périodiques entre janvier et mars 2024.

SOMMAIRE

2. **L'écosystème des ransomwares secoué par LockBit**
    a. **Les imposteurs nuisent à la réputation des gangs –** Dans le sillage de l'intervention d'une taskforce réunissant des forces de l'ordre de plusieurs pays, Operation Cronos, Trellix a constaté que des imposteurs se faisaient passer pour LockBit, tandis que le groupe essayait laborieusement de sauver les apparences et de restaurer son opération lucrative.
    b. **Les États-Unis toujours en ligne de mire –** Les États-Unis restent le pays le plus ciblé par les groupes de ransomware, suivis de la Turquie, de Hong Kong, de l'Inde et du Brésil.
    c. **Le secteur des transports et de la logistique sous un feu nourri –** Les ransomwares se sont concentrés majoritairement sur le secteur des transports et de la logistique au 4e trimestre 2023 et au 1er trimestre 2024. À l'échelle mondiale, le secteur a généré respectivement 53 % et 45 % des détections de ransomwares, devant le secteur de la finance.
    d. **Une intervention des forces de l'ordre aboutit à une condamnation –** Avant la finalisation de ce rapport, les forces de l'ordre internationales ont révélé la véritable identité du chef du gang LockBit. Une autre opération contre des opérateurs de ransomwares a eu lieu le 1er mai. Un cyberpirate du groupe REvil, qui a attaqué Kaseya et de nombreuses autres entreprises, a été condamné à 13 ans d'emprisonnement et à 16 millions USD de dédommagement.
3. **Émergence d'outils de désactivation d'EDR**
    a. **Apparition du gang de ransomware D0nut –** L'émergence du gang de ransomware D0nut a été particulièrement remarquable à cet égard, en raison de son utilisation innovante d'un outil de désactivation d'EDR – une tactique avancée permettant de contourner la détection sur les endpoints et d'améliorer l'efficacité des attaques.
    b. **Outil de contournement d'EDR de Spyboy utilisé pour cibler les télécommunications –** L'outil de désactivation d'EDR « Terminator » créé par Spyboy a été utilisé dans une nouvelle campagne en janvier 2024. Il permet de contourner les solutions EDR, et 80 % des détections ciblaient le secteur des télécommunications.
4. **Escroqueries sur le thème des élections présidentielles américaines**
    a. **Le phishing reste populaire –** Alors que le monde entier attend les résultats des élections présidentielles américaines de novembre, des escroqueries sur le thème électoral ont vu le jour pour inciter les citoyens à faire des dons.

SOMMAIRE

5. **L'IA générative et le marché clandestin cybercriminel**
    a. **Outils gratuits basés sur l'IA –** Un outil Jabber gratuit basé sur ChatGPT 4.0 et disponible sur le marché clandestin de la cybercriminalité permet au développeur d'aider les acteurs malveillants à intégrer l'IA générative à leurs opérations et de créer une base de connaissances alimentée par l'IA générative pour apprendre des autres cybercriminels, voire voler leurs idées et outils.
    b. **Augmentation de l'adoption des infostealers –** Deux infostealers (outils d'exfiltration d'informations) dotés de fonctionnalités d'IA générative ont été utilisés par des cybercriminels. MetaStealer et LummaStealer s'appuient sur l'IA générative pour échapper à la détection et repérer les bots parmi la liste des journaux, respectivement. L'IA générative rend ces tactiques cybercriminelles plus difficiles à détecter et à bloquer.

Méthodologie : comment nous collectons et analysons les données

Les experts de notre équipe 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.

SOMMAIRE

SIGNALEMENTS, DONNÉES ET ANALYSES

Attaques étatiques et menaces APT

Entre octobre 2023 et mars 2024, Trellix a observé une augmentation de 17 % des détections de menaces APT par rapport aux six mois précédents. Dans notre dernier rapport, nous faisions déjà état d'une hausse impressionnante de 50 % de ces détections. L'écosystème des APT est fondamentalement différent d'il y a un an : il est plus agressif, ingénieux et actif.

Dans le paysage des cybermenaces en perpétuelle mutation, les groupes APT continuent à représenter une menace majeure et sophistiquée pour la cybersécurité mondiale.

Notre but est d'analyser minutieusement les activités associées aux menaces APT (Advanced Persistent Threats) détectées pendant le 4e trimestre 2023 et le 1er trimestre 2024. Cette analyse se concentre sur les origines de ces menaces, leurs principales cibles et les outils utilisés pour leur exploitation. Nous comparons ces résultats aux données collectées au premier semestre 2023 (2e et 3e trimestres) à l'aide de deux métriques clés : la variance du pourcentage et la variance de la contribution proportionnelle.

- Variance du pourcentage : cette métrique nous aide à déterminer si les activités d'un groupe APT spécifique, le ciblage de certains pays ou l'emploi d'outils particuliers ont progressé, ont diminué ou sont restés stables au fil du temps. Nous pouvons ainsi suivre l'évolution des comportements de ces cybercriminels et du paysage des cybermenaces au sens large.
- Variance de la contribution proportionnelle : cette métrique ajoute du contexte en montrant non seulement l'évolution brute des activités, mais aussi comment cette évolution s'inscrit dans l'environnement des cybermenaces dans son ensemble. Par exemple, même si les détections d'un cybercriminel spécifique ont fortement augmenté, il se peut qu'elles ne représentent qu'une petite partie de l'ensemble des cybermenaces si l'environnement de menaces global est devenu nettement plus actif. À l'inverse, si les détections de ce cybercriminel diminuent alors que le reste de l'environnement de menaces connaît un ralentissement encore plus fort, il est alors possible que l'importance relative de cet acteur malveillant augmente.

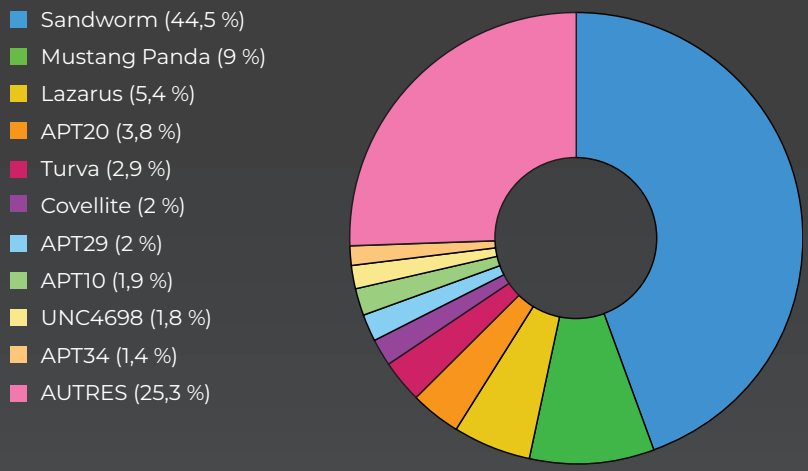
En utilisant ces métriques, nous entendons dresser un tableau nuancé des évolutions des activités APT, ce qui nous permet d'obtenir des informations pertinentes sur leurs objectifs stratégiques, leurs méthodologies de prédilection et les menaces de cybersécurité qu'elles représentent. Les sections suivantes s'attardent sur ces observations en mettant en lumière le monde complexe des APT et les efforts continus qui doivent être déployés pour se défendre contre leurs menaces sophistiquées.

SOMMAIRE

Groupes étatiques et APT actifs

De plus, la période allant d'octobre 2023 à mars 2024 a été le témoin de fluctuations importantes des activités de divers groupes APT. Ces fluctuations soulignent la nature dynamique des cybermenaces et mettent en avant les modifications de l'orientation opérationnelle et des techniques employées par ces cybercriminels sophistiqués.

10 GROUPES APT LES PLUS ACTIFS SELON LES DÉTECTIONS ENTRE LE 4E TRIM. 2023 ET LE 1ER TRIM. 2024



ÉVOLUTION DES ACTIVITÉS DES GROUPES CYBERCRIMINELS : VARIANCE ET CONTRIBUTION PROPORTIONNELLE

Menaces APT	Variance du pourcentage	Variance de la contribution proportionnelle
Sandworm	1 669,43 %	40,34 %
Mustang Panda	-2,19 %	-6,14 %
Lazarus	66,87 %	0,07 %
APT28	18,67 %	-1,49 %
Turla	2,95 %	-1,74 %
Covellite	85,30 %	0,23 %
APT29	123,98 %	0,53 %
APT10	80,46 %	0,17 %
UNC4698	368,75 %	1,14 %
APT34	96,73 %	0,23 %
Autres	-28,99 %	-33,33 %

SOMMAIRE

- **Évolution des tactiques –** Les détections de menaces liées à Sandworm, collectif historiquement connu pour ses cyberopérations perturbatrices, ont enregistré une augmentation spectaculaire de 1 669 %, avec une variance de la contribution proportionnelle de 40 %. Cette hausse monumentale suggère une escalade sans précédent des cyberactivités du groupe affilié à la Russie.
- **Étendue agressive des opérations –** Les détections d'activités du groupe APT29, qui possède un long passif de cyberespionnage, ont bondi de 124 %. Les détections associées à APT34 et à Covellite ont également fortement progressé, de 97 % et 85 % respectivement, ce qui est signe de rythmes opérationnels accrus ou du lancement de nouvelles campagnes.
- **Homéostasie –** En revanche, les niveaux d'activité de groupes tels que Mustang Panda, Turla et APT28 ont peu évolué. On observe une légère diminution (-2 %) des détections associées à Mustang Panda et une modeste augmentation (+3 %) de celles liées à Turla.
- **Émergence de nouveaux acteurs –** Il convient de noter l'émergence du groupe UNC4698, dont les détections ont bondi de 363 %, ce qui suggère l'essor d'un nouvel acteur potentiellement important dans le paysage des APT.

QUE SAIT-ON DU GROUPE UNC4698 ?

Nous disposons de peu d'informations sur ce groupe, mais les chercheurs sont parvenus à interpréter le comportement observé comme des activités émanant d'un collectif et ne savent pas encore comment le définir.

Cela dit, nous savons que le groupe UNC4698 se concentre sur l'espionnage industriel ; il collecte des données opérationnelles sensibles qui pourraient être utilisées pour soutenir des objectifs économiques ou de sécurité nationale de l'État auquel il est affilié, vraisemblablement la Chine étant donné la nature et l'orientation régionale des attaques.

Ses cibles habituelles sont des entreprises du secteur du pétrole et du gaz basées en Asie.

Le collectif est également connu pour utiliser un malware spécifique baptisé SNOWYDRIVE.

Le groupe UNC4698 emploie diverses tactiques, techniques et procédures (TTP) axées sur l'utilisation de malwares distribués via des clés USB. Voici quelques TTP clés associées à ce groupe cybercriminel :

- **Accès initial via des périphériques USB infectés –** La principale méthode d'infection implique des clés USB contenant des logiciels malveillants conçus pour créer une porte dérobée (backdoor) sur le système hôte.

SOMMAIRE

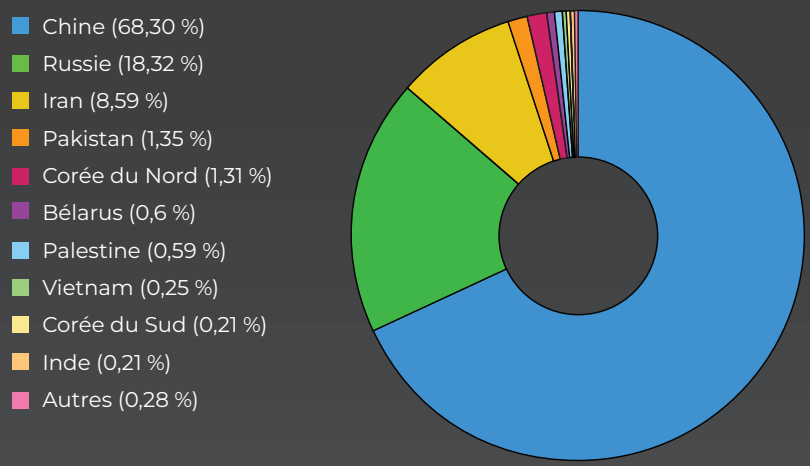
QUE SAIT-ON DU GROUPE UNC4698 ? *(suite)*

- **Exécution via des fichiers malveillants –** Le malware inclut généralement un injecteur qui écrit des DDL et des exécutables malveillants sur le disque. Ces fichiers sont souvent maquillés en logiciels légitimes pour échapper à la détection et sont exécutés pour établir un contrôle plus étendu.
- **Persistance et modification du Registre –** Le groupe UNC4698 assure sa persistance sur les systèmes infectés en modifiant le Registre Windows. Cela permet au malware de se lancer automatiquement au démarrage du système.
- **Communication avec le serveur de commande et de contrôle –** Le malware configure une méthode de communication distante, ce qui permet aux attaquants d'émettre des commandes et de contrôler les systèmes compromis à distance.
- **Mouvement latéral via des supports amovibles –** Le malware peut se copier sur d'autres périphériques USB connectés à la machine infectée, ce qui favorise la propagation de l'infection à d'autres systèmes.

Les détections associées à des groupes moins connus ou non identifiés ont enregistré une hausse de 62 %, ce qui indique qu'il existe un éventail diversifié et croissant de menaces au-delà des entités APT bien documentées. Cette progression de 8 % de leur contribution proportionnelle par rapport au nombre total de détections met en lumière l'évolution et la diversification constantes des cybermenaces.

Groupes APT et pays d'origine

10 PAYS DES GROUPES APT AYANT ENREGISTRÉ LE PLUS DE DÉTECTIONS ASSOCIÉES À DES CAMPAGNES ENTRE LE 4E TRIM. 2023 ET LE 1ER TRIM. 2024



SOMMAIRE

En ce qui concerne les pays d'origine, les données télémétriques collectées par Trellix entre octobre 2023 et mars 2024 montrent également des changements notables dans les activités des groupes cybercriminels étatiques.

Les groupes cybercriminels soutenus par l'État chinois restent les auteurs les plus prolifiques d'activités APT

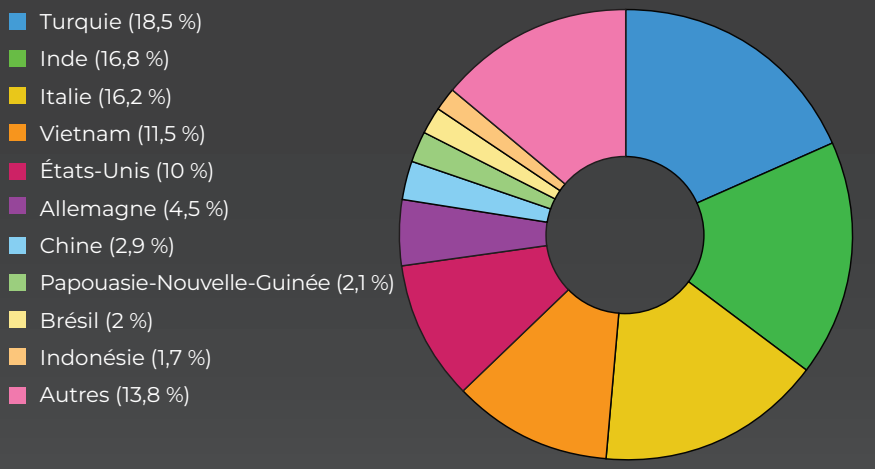
- **Escalade substantielle des opérations –** Les motivations géopolitiques et les capacités de cybersécurité évoluent dans différents pays. Nos données télémétriques indiquent ce qui suit :
  a. Les détections de menaces APT imputables à des groupes soutenus par l'État russe ont augmenté de manière significative (+31 %), tandis que leur contribution proportionnelle a progressé de 4 %. Ces chiffres sont le résultat d'une escalade substantielle des cyberopérations, qui pourrait refléter l'élargissement des objectifs stratégiques ou des réponses aux dynamiques de cybersécurité mondiales.
  b. Les cyberactivités des groupes affiliés à l'Iran se sont également intensifiées, avec une hausse de 8 % des détections et une progression de 3,89 % de la contribution proportionnelle. Ces statistiques soulignent un développement considérable des cyberopérations de l'Iran, aligné avec ses objectifs géopolitiques et son implication dans la guerre Israël-Hamas.
- **Plus grande diversification –** La Chine reste l'auteur le plus prolifique d'activités APT, avec une légère hausse (+1 %) des détections. Toutefois, sa contribution proportionnelle à l'ensemble des détections a légèrement diminué (-1 %), ce qui pourrait suggérer une plus grande diversification des origines des menaces APT pendant cette période. En février 2024, le groupe APT Volt Typhoon affilié à la Chine a également déployé des efforts considérables pour cibler des infrastructures critiques américaines. Nous approfondirons ce point dans la section suivante.
- **Changement de stratégie –** À l'inverse, les activités APT des groupes liés à la Corée du Nord, au Vietnam et à l'Inde ont considérablement diminué – les détections imputables à la Corée du Nord ayant chuté de 82 %, celles imputables au Vietnam de 80 % et celles imputables à l'Inde de 82 %. Le recul de la contribution proportionnelle de la Corée du Nord (-6 %) est particulièrement notable et pourrait indiquer une évolution de l'orientation, de la stratégie ou des capacités.
- **Émergence d'autres pays –** Les groupes affiliés au Pakistan et au Bélarus ont fortement augmenté leurs activités APT, avec une hausse des détections de 55 % et d'un extraordinaire 2 019 %, respectivement. Ces augmentations, en particulier l'explosion des activités associées au Bélarus, soulignent l'émergence d'acteurs nouveaux ou précédemment sous-reconnus dans l'arène des APT.

  La catégorie « Autres » fait état d'une hausse de 121 % des détections, indiquant que les activités APT ne se limitent pas aux pays les plus fréquemment cités. Cette diversité souligne la nature mondiale des cybermenaces et la nécessité d'adopter une approche de cybersécurité globale et adaptative.

Nous ne manquerons pas de suivre de près ces nouvelles tendances au cours des mois à venir.

SOMMAIRE

PAYS ET RÉGIONS CIBLÉS PAR DES ACTIVITÉS APT



Pays et régions ciblés

Cette section se concentre sur les pays et les régions où Trellix a détecté des activités menées par des groupes APT entre le 4e trimestre 2023 et le 1er trimestre 2024, révélant des changements significatifs de l'orientation et de la stratégie de ces cybercriminels sophistiqués.

> Les données soulignent la nature mondiale des cybermenaces et les degrés divers d'attention que les groupes APT accordent à différents pays.

Les experts de Trellix Advanced Research Center estiment avec une confiance modérée que les facteurs suivants ont influencé les activités détectées dans certains pays et certaines régions.

La Turquie a été ciblée par un nombre sans précédent de menaces APT

Objectifs opérationnels :
Les détections de menaces ciblant la Turquie ont bondi de 1 458 %, ce qui se traduit par une hausse de 16 % de leur contribution proportionnelle à l'ensemble des détections. Cette augmentation spectaculaire dénote un renforcement important du ciblage de la Turquie, qui pourrait refléter des tensions géopolitiques plus larges ou des objectifs opérationnels spécifiques des groupes APT.

- **Importance stratégique –** Les menaces visant l'Inde et l'Italie ont également nettement augmenté, avec des détections en hausse de 614 % et 308 %, respectivement. La proéminence grandissante de ces pays dans la liste des cibles pourrait s'expliquer par leur importance stratégique croissante dans le cyberdomaine, qu'elle soit due à des facteurs économiques, politiques ou technologiques.

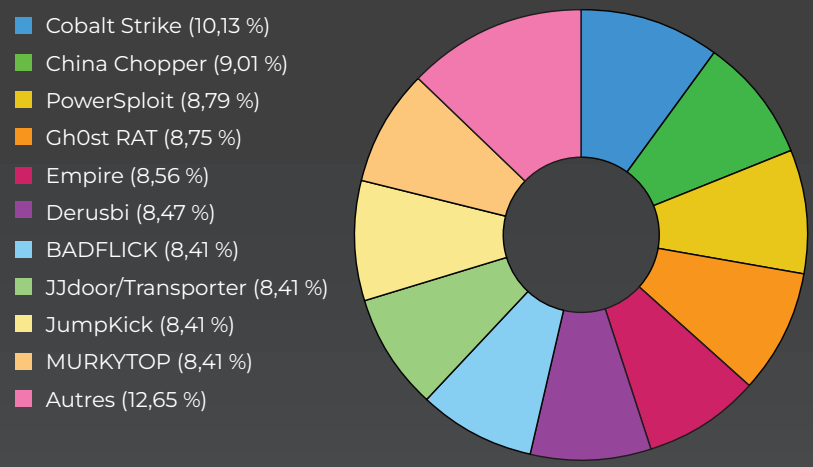
SOMMAIRE

- **Élargissement du paysage –** Il est intéressant de noter que le Vietnam et les États-Unis, bien qu'ils génèrent un nombre important de détections APT, affichent des tendances différentes. Les détections de menaces ciblant le Vietnam ont progressé de 9 %, alors que leur contribution proportionnelle a diminué de 9 %, ce qui indique un élargissement du paysage de ciblage. Les détections de menaces visant les États-Unis ont connu une croissance modeste de 15 %, mais leur contribution proportionnelle a reculé de 7 %, ce qui suggère une diversification des stratégies de ciblage des groupes APT.
- **Développements géopolitiques –** Les détections de menaces ciblant l'Allemagne, la Chine, la Papouasie-Nouvelle-Guinée et le Brésil ont augmenté, l'Allemagne et la Chine enregistrant des changements importants de leur contribution proportionnelle. Cette diversification du ciblage reflète les ajustements stratégiques et opportunistes réalisés par les groupes APT en réponse aux approches de cybersécurité mondiales et aux développements géopolitiques.
- **Amélioration de la sécurité nationale –** À l'inverse, les détections de menaces ciblant l'Indonésie ont enregistré une chute notable de 48 %, associée à une contribution proportionnelle réduite de 4 %. Cette baisse pourrait s'expliquer par une déprioritisation temporaire ou par un renforcement efficace des mesures de cybersécurité nationales.
- **Consolidation de l'orientation –** La catégorie « Autres », qui représente plusieurs pays différents où Trellix a détecté des activités APT, a enregistré une baisse de 23 % des détections et un recul de 21 % de la contribution proportionnelle. Cette diminution met en évidence une consolidation potentielle de l'orientation des groupes APT sur des cibles de grande valeur spécifiques pendant cette période.

Le paysage pourrait continuer d'évoluer rapidement en raison des tendances géopolitiques.

Outils malveillants

10 OUTILS MALVEILLANTS AYANT ENREGISTRÉ LE PLUS DE DÉTECTIONS ENTRE LE 4E TRIM. 2023 ET LE 1ER TRIM. 2024



SOMMAIRE

L'analyse des outils malveillants utilisés dans les campagnes APT entre le 4e trimestre 2023 et le 1er trimestre 2024 révèle des tendances notables dans les préférences et les tactiques opérationnelles des cybercriminels. La variance des taux de détection et de leurs contributions proportionnelles fournit des informations précieuses sur l'évolution du paysage des cybermenaces et les dynamiques changeantes de l'utilisation d'outils par ces groupes sophistiqués.

Les tendances suivantes ont été observées :

- **Efficacité constante des outils d'attaque –** Cobalt Strike demeure un outil privilégié de nombreux groupes cybercriminels, malgré une baisse de 17 % des détections. La diminution relativement limitée de la contribution proportionnelle (-1 %) suggère qu'il conserve sa popularité et son efficacité dans les cyberopérations, soulignant la difficulté de se défendre contre des outils d'attaque polyvalents et largement utilisés.
- **Recours aux attaques web shell, PowerShell et d'accès à distance –** Les détections de menaces utilisant China Chopper, PowerSploit et Gh0st RAT ont également nettement baissé – respectivement de 23 %, 24 % et 24 %. Malgré ces diminutions, les fluctuations minimes de la variance de la contribution proportionnelle indiquent qu'ils font toujours partie intégrante de l'arsenal des cybercriminels. Ces outils, connus pour leurs capacités à lancer des attaques web shell, des exploits PowerShell et des attaques d'accès à distance, mettent en lumière le recours croissant à des outils éprouvés et polyvalents pour les cyberopérations.
- **Outils moins détectables –** Les détections imputables à Empire, Derusbi, BADFLICK, JJdoor/Transporter, JumpKick et MURKYTOP affichent des tendances de recul similaires, avec des diminutions supérieures à 25 %. Ce recul uniforme pourrait refléter un changement plus important des outils privilégiés des groupes cybercriminels ou une adaptation aux contre-mesures et aux techniques de détection, encourageant la migration vers des outils plus récents et moins détectables.
- **Innovation constante –** La catégorie « Autres » des outils malveillants a enregistré une baisse importante des détections, allant jusqu'à 30 %, et une augmentation de 6 % de la contribution proportionnelle. Cette hausse souligne l'innovation et l'adaptation constantes dont font preuve les cybercriminels, qui explorent de nouveaux outils et des techniques inédites pour échapper à la détection et atteindre leurs objectifs.

Les préférences changeantes en ce qui concerne les outils malveillants utilisés sont la preuve de leur capacité d'adaptation aux progrès de la cybersécurité.

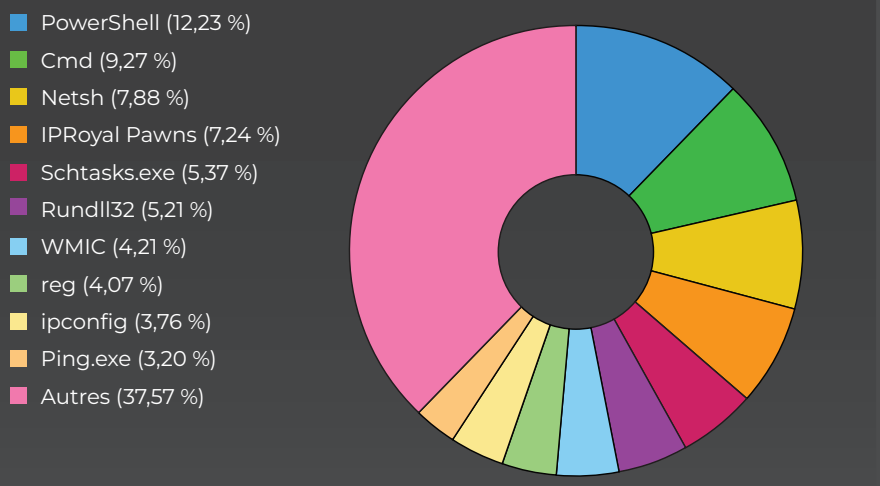
> À mesure que les mécanismes de défense gagnent en sophistication, les outils et tactiques d'attaque employés par les groupes APT font de même.

L'adoption d'un plus large éventail d'outils, dénotée par l'augmentation des détections dans la catégorie « Autres », souligne la nécessité de mener des recherches en continu, de disposer d'une Threat Intelligence pertinente et de déployer des stratégies de défense adaptatives afin d'atténuer le risque posé par ces cybermenaces en constante évolution.

SOMMAIRE

Outils non malveillants

10 OUTILS NON MALVEILLANTS AYANT ENREGISTRÉ LE PLUS DE DÉTECTIONS ENTRE LE 4E TRIM. 2023 ET LE 1ER TRIM. 2024



> Cette pratique, connue sous le nom d'exploitation des ressources locales (LOTL, Living Off The Land), complique les efforts de détection et souligne la sophistication de ces cybercriminels.

L'utilisation d'outils non malveillants dans les cyberopérations par des groupes APT entre le 4e trimestre 2023 et le 1er trimestre 2024 met en lumière un aspect important des cybermenaces modernes : l'utilisation d'outils système légitimes à des fins malveillantes. Cette pratique, connue sous le nom d'exploitation des ressources locales (LOTL, Living Off The Land), complique les efforts de détection et souligne la sophistication de ces cybercriminels. Les statistiques révèlent des variations considérables dans l'utilisation de ces outils, reflétant leur importance stratégique dans les cyberopérations.

- **Polyvalence –** Les détections imputables à PowerShell ont augmenté de façon spectaculaire (105 %), avec une variance de la contribution proportionnelle de 1 %. Cette poussée souligne sa polyvalence et son efficacité dans l'automatisation d'un large éventail d'activités malveillantes – de la reconnaissance à la distribution de charges actives.
- **Manipulation des réseaux en point de mire –** Les détections imputables à Netsh et à IPRoyal Pawns ont enregistré une baisse significative, de 99 % et 102 % respectivement. Ces outils sont souvent utilisés pour la configuration des réseaux et le trafic proxy, indiquant une orientation stratégique axée sur la manipulation des réseaux et les techniques de contournement.
- **Automatisation à grande échelle –** Schtasks.exe a enregistré le plus haut pourcentage de variance parmi les outils répertoriés, avec 138 %. Cela reflète le recours croissant à des tâches planifiées à des fins de persistance et d'exécution de charges actives malveillantes sans intervention directe de l'utilisateur.

SOMMAIRE

- **Ajustements tactiques –** À l'inverse, l'utilisation de Rundll32 et de WMIC a progressé, mais les variances de leur contribution proportionnelle ont diminué, indiquant une évolution des préférences tactiques des groupes APT malgré l'utilité de ces outils.
- **Diversification des outils –** Nos données montrent une augmentation importante de l'emploi de Cmd, le traditionnel interpréteur de commandes sous Windows, avec une hausse de 65 % des détections. Malgré son utilisation accrue, sa variance de la contribution proportionnelle a diminué de 2,5 %, suggérant une plus grande diversification des outils utilisés par les groupes APT.

  La catégorie « Autres », qui représente divers outils moins courants ou plus spécialisés, a enregistré une hausse de 42 % des détections. Toutefois, elle a subi une diminution importante de sa variance de contribution proportionnelle (-21 %), soulignant l'expansion de l'arsenal d'outils à la disposition des cybercriminels.

L'évolution du paysage des outils non malveillants employés par des groupes APT illustre la complexité de la détection et de la neutralisation des cybermenaces sophistiquées. La sélection et l'application stratégiques de ces outils révèlent une compréhension fine des environnements ciblés ainsi que les efforts déployés pour échapper à la détection.

> **CONSEIL POUR LES RSSI :** les défenses de cybersécurité doivent donc dépasser le stade de la détection traditionnelle des malwares, pour inclure une analyse comportementale et une détection des anomalies afin de contrer l'utilisation d'outils légitimes dans les cyberopérations.

Les données collectées grâce aux capteurs mondiaux Trellix ATLAS sont associées aux informations stratégiques des rapports validés par le secteur et publiées par Trellix Advanced Research Center, pour permettre à nos clients d'identifier les cybercriminels ciblant leurs secteurs respectifs et d'utiliser notre analyse comportementale pour détecter les comportements anormaux au sein de leur environnement.

SOMMAIRE

Conclusion

L'analyse des activités APT entre le 4e trimestre 2023 et le 1er trimestre 2024 a mis en lumière la nature dynamique et de plus en plus complexe du paysage des cybermenaces. Notre étude des statistiques concernant les origines des groupes APT, les pays ciblés et l'utilisation d'outils malveillants et non malveillants révèle plusieurs tendances clés qui soulignent l'évolution des stratégies des cybercriminels.

Les groupes APT continuent à :

1. faire preuve d'adaptabilité et de sophistication ;
2. utiliser une variété d'outils malveillants ;
3. exploiter des utilitaires système légitimes pour mener des opérations d'espionnage, créer des perturbations et voler des informations sensibles.

Les variations importantes du ciblage et des tactiques opérationnelles de ces groupes reflètent leurs objectifs stratégiques et leur réponse aux avancées en matière de cybersécurité et aux mesures défensives à l'échelle mondiale.

Les changements considérables des pratiques de ciblage, avec certains pays subissant des hausses importantes des activités APT, dénotent les motivations géopolitiques derrière ces cyberopérations. De même, l'évolution des outils utilisés, y compris l'essor remarquable des tactiques d'exploitation des ressources locales, souligne la difficulté à détecter et à neutraliser les menaces APT dans un paysage où les activités légitimes et malveillantes s'entremêlent de plus en plus.

Par ailleurs, la diversification des origines des groupes APT et l'élargissement de leurs stratégies de ciblage indiquent une prolifération mondiale des cybercapacités et la nécessité d'adopter une approche de cybersécurité unifiée et collaborative.

> Il apparaît clairement qu'aucun pays ni aucune organisation n'est à l'abri de ces cybercriminels sophistiqués.

SOMMAIRE

Volt Typhoon, acteur étatique affilié à la Chine

Les groupes cybercriminels étatiques ont continué à représenter une menace sérieuse pour les organisations des secteurs public et privé du monde entier pendant le 4e trimestre 2023 et le 1er trimestre 2024. Ces collectifs, souvent solidement armés et passés maîtres dans l'art des menaces sophistiquées de l'espace cyber, ciblent sans relâche des réseaux sur des périodes prolongées avec des compétences et des ressources supérieures à celles de leurs homologues cybercriminels ou cyberactivistes.

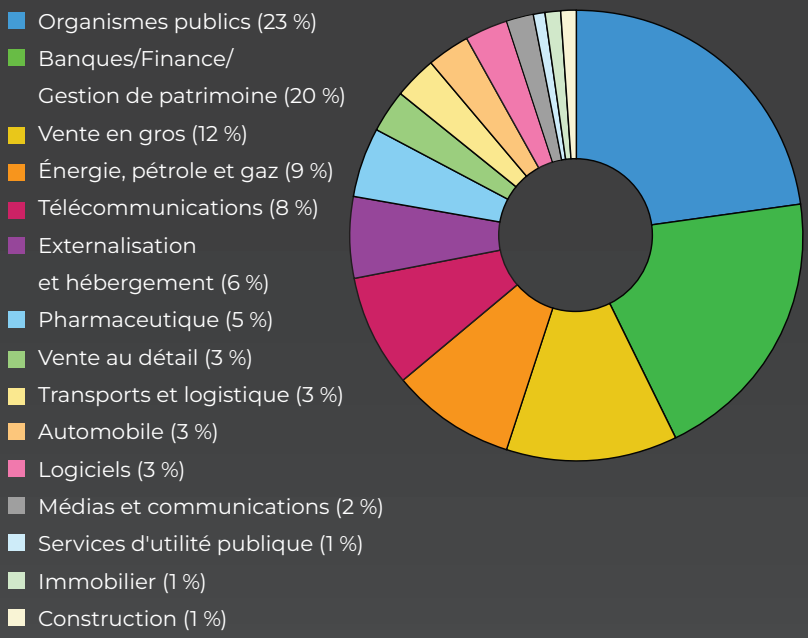
23 %

Plus de 23 % des détections d'activités malveillantes sont dirigées contre des organismes publics du monde entier

Plus de 21 millions d'activités de menaces provenant d'acteurs étatiques affiliés à la Chine ont été détectées

Plus précisément, selon les données télémétriques de Trellix, les groupes acteurs étatiques affiliés à la Chine ont fait peser une menace grandissante sur les organismes publics du monde entier. Nos données font état de plus de 21 millions de détections d'activités malveillantes émanant de groupes alignés avec la Chine entre octobre 2023 et mars 2024.

DÉTECTIONS MONDIALES DE MENACES ÉMANANT DE GROUPES APT AFFILIÉS À LA CHINE



(Source : ATLAS)

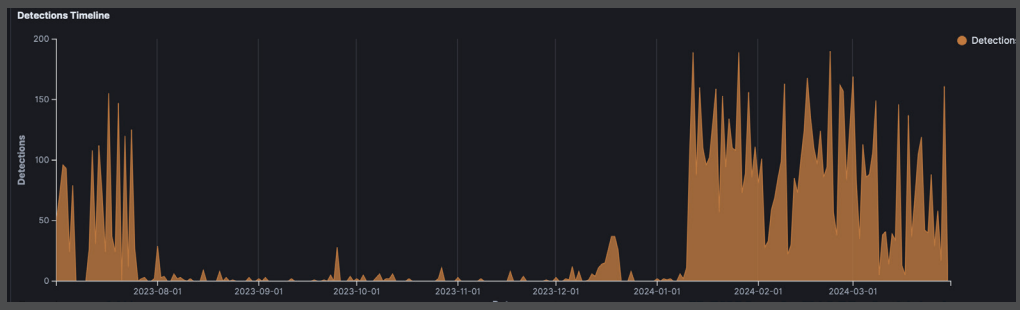
SOMMAIRE

Présentation

En tant que groupe APT financé par l'État chinois relativement récent, Volt Typhoon se distingue par son comportement et ses pratiques de ciblage uniques, qui diffèrent des habitudes de cyberespionnage et de collecte d'informations des autres groupes APT affiliés à la Chine. De précédents rapports open source portent à croire que ce groupe APT chinois s'est pré-positionné sur des réseaux IT de contrôle industriel de manière à faciliter les mouvements latéraux visant à perturber les ressources et fonctions OT en cas de crise géopolitique ou de guerre. Les données télémétriques de Trellix montrent que depuis la reprise de ses opérations en janvier 2024, Volt Typhoon a régulièrement pris pour cible des organismes publics du monde entier, y compris aux États-Unis, tout en employant des techniques d'exploitation des ressources locales (living-off-the-land).

Calendrier opérationnel

D'après les données télémétriques mondiales de Trellix, Volt Typhoon a été détecté pour la première fois mi-2021, mais est resté en sommeil, avec peu ou pas d'activité, entre août 2023 et janvier 2024. Cette période d'inactivité pourrait s'expliquer par le nombre record d'investigations sur les menaces menées dans les mois suivant la publication du premier rapport d'un éditeur de sécurité sur Volt Typhoon en mai 2023, qui a attiré l'attention du monde entier. Une évolution des infrastructures d'attaque de Volt Typhoon pendant cette période, compte tenu de son exposition publique, pourrait également expliquer le faible volume d'activités de menaces détectées.



Chronologie des détections de Volt Typhoon entre juillet 2023 et mars 2024 (source : Trellix ATLAS)

Si l'on en croit les données télémétriques de Trellix, Volt Typhoon a repris ses opérations vers la mi-janvier 2024. Depuis lors, les données télémétriques de Trellix ont détecté plus de 7 100 activités malveillantes associées à Volt Typhoon, avec des poussées périodiques entre janvier et mars 2024.

Détails des détections de Volt Typhoon entre janvier et mars 2024

SOMMAIRE

Tactiques, techniques et procédures (TTP)

Nos données suggèrent que depuis la reprise de ses opérations vers la mi-janvier 2024, Volt Typhoon a eu systématiquement recours à un certain nombre d'outils et fonctionnalités natifs aux systèmes Windows pour exécuter des commandes à des fins malveillantes. Ces outils d'exploitation des ressources locales permettent un double usage, car il s'agit de logiciels et fonctions légitimes intégrés au système, et sont devenus populaires auprès des groupes affiliés à la Chine, notamment Volt Typhoon. Netsh.exe fait partie des outils qui peuvent être utilisés à diverses fins malveillantes, telles que la désactivation des paramètres de pare-feu ou la configuration d'un tunnel proxy pour autoriser l'accès à distance à un hôte infecté. Ldifde fait également partie des outils employés par Volt Typhoon pour collecter des informations.

Une fois qu'ils ont obtenu un accès à un contrôleur de domaine, les attaquants peuvent utiliser Ldifde.exe pour exporter des données sensibles ou apporter des modifications autorisées au répertoire. Les cyberpirates de Volt Typhoon peuvent également utiliser Ntdsutil pour accomplir leurs méfaits. Ntdsutil est un outil légitime qui sert à la maintenance des bases de données ; toutefois, il peut également être exploité pour effectuer un vidage d'Active Directory afin de collecter des identifiants et d'exfiltrer des données sensibles.

Le groupe cybercriminel Volt Typhoon a continué à utiliser des outils open source, comme FRP, Impacket et Mimikatz. Les données télémétriques de Trellix ont également détecté l'utilisation des outils et commandes LOTL (Living-Off-The-Land) suivants par Volt Typhoon entre février et mars 2023 :

- Comsvcs
- Dnscmd
- Ldifde
- MiniDump
- Net
- Netsh
- Ntdsutil
- reg
- ping
- PowerShell
- PsExec

SOMMAIRE

D'après nos données télémétriques, les principaux outils MITRE ATT&CK utilisés par Volt Typhoon sont les suivants :

- Accès initial – T1190 : Exploitation d'applications publiques
- Exécution – T1106 : API native
- Persistance – T1546 : Exécution déclenchée par événement
- Élévation de privilèges – T1546 : Exécution déclenchée par événement
- Contournement des défenses – T1070.001 : Effacement des journaux des événements Windows
- Contournement des défenses – T1070 : Suppression de fichiers
- Contournement des défenses – T1027 : Obfuscation de fichiers ou d'informations
- Accès aux informations d'identification – T1003.003 : NTDS
- Accès aux informations d'identification – T1003 : Capture d'informations d'identification à partir du système d'exploitation
- Accès aux informations d'identification – T1110 : Attaque en force brute
- Accès aux informations d'identification – T1555 : Informations d'identification extraites de référentiels de mot de passe
- Découverte – T1069.002 : Groupe de domaine
- Découverte – T1069.001 : Groupes locaux
- Découverte – T1083 : Découverte des fichiers et des répertoires
- Découverte – T1057 : Découverte des processus
- Découverte – T1010 : Découverte des fenêtres d'application
- Collecte – T1560 : Archivage des données collectées
- Collecte – T1560.001 : Archivage via un utilitaire
- Commande et contrôle – T1090.002 : Proxy externe
- Commande et contrôle – T1105 : Transfert d'outils à l'entrée
- Commande et contrôle – T1132 : Codage de données

Évolution du paysage des ransomwares

Au 4e trimestre 2023, le paysage des cybermenaces a connu une escalade des attaques de ransomwares, avec de nouvelles familles de ransomwares apparues dans l'année exerçant un impact croissant.

- **Outils de désactivation d'EDR –** L'émergence du gang de ransomware D0nut a été particulièrement remarquable à cet égard, en raison de son utilisation innovante d'un outil de désactivation d'EDR – une tactique avancée permettant de contourner la détection sur les endpoints et d'améliorer l'efficacité des attaques. Vous en apprendrez plus à ce sujet dans la section suivante.
- **Exploitation de vulnérabilités –** Cette période a vu se poursuivre la tendance à l'exploitation des vulnérabilités critiques pour faciliter le déploiement de ransomwares. La CVE-2023-4966, connue sous le nom de Citrix Bleed, a notamment été exploitée par les affiliés de LockBit 3.0, ce qui met en évidence la vulnérabilité persistante des infrastructures critiques face aux cyberattaques sophistiquées.

SOMMAIRE

En outre, l'exploitation de la CVE-2023-22518 dans Confluence Data Center et Confluence Server illustre la volonté d'infiltrer des plates-formes professionnelles largement utilisées pour déployer des ransomwares. La campagne de ransomwares Cactus, qui ciblait les installations Qlik Sense en exploitant des vulnérabilités récemment découvertes, a démontré une fois encore l'agilité dont font preuve les attaquants, dès lors qu'ils peuvent s'adapter aux paysages de sécurité et exploiter des vulnérabilités émergentes. Ceci a contribué à faire du 4e trimestre 2023 un trimestre actif pour les groupes de ransomware.

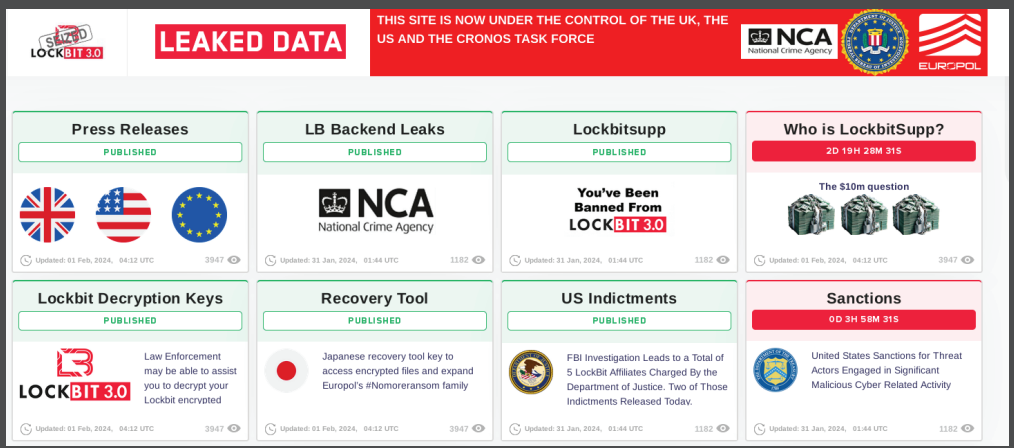
Toutefois, l'ordre établi était sur le point d'être bouleversé au 1er trimestre 2024 par une action remarquable des forces de l'ordre.

Operation Cronos, l'opération policière qui a frappé LockBit de plein fouet

L'opération policière internationale baptisée Operation Cronos a été lancée le 19 février 2024. Elle a mis à mal les activités du célèbre gang LockBit, rendant la monnaie de sa pièce au groupe cybercriminel établi de longue date. Non seulement les forces de l'ordre ont affiché des avis de démantèlement, mais elles ont également fini par prendre le contrôle du site de divulgation du collectif et ont elles aussi divulgué des informations pour exposer le groupe cybercriminel aux yeux du monde entier. Plusieurs inculpations ont été prononcées et les affiliés actifs ont reçu un sympathique message de bienvenue lorsqu'ils se sont connectés au système backend de LockBit, stipulant très clairement que leur identité était connue.

Ces actions avaient pour objectif de perturber les activités de LockBit, de porter atteinte à sa réputation et de rompre la confiance au sein du gang.

Au moment de la finalisation de ce rapport, Operation Cronos a connu un nouveau rebondissement. La taskforce internationale a remis le couvert en divulguant l'identité du chef du gang LockBit. Ce n'était pas la seule victoire des forces de l'ordre : le 1er mai, l'affilié de REvil qui a attaqué Kaseya et de nombreuses autres entreprises a été condamné à 13 ans d'emprisonnement et à 16 millions USD de dédommagement. Pour en savoir plus sur la façon dont Trellix Advanced Research Center a participé au dossier REvil, consultez cet article.



SOMMAIRE

L'année dernière, notre rapport de février a identifié LockBit comme le groupe le plus agressif dans ses demandes de rançon. Ces cybercriminels ont recours à un large éventail de techniques pour exécuter leurs campagnes, notamment l'exploitation de vulnérabilités dont la découverte remonte à 2018. Tout au long de l'année 2023, LockBit a conservé son titre de groupe de ransomware le plus prévalent et affichant le plus grand nombre de victimes sur son site de divulgation. Il a principalement ciblé des organisations nord-américaines et européennes de divers secteurs, le secteur des biens et services industriels étant le plus touché. En 2023, LockBit n'a cessé d'évoluer et d'intégrer de nouveaux outils et de nouvelles méthodes à son programme de ransomware. Le groupe a notamment travaillé sur le développement du chiffreur LockBit Green, basé sur le code fuité du ransomware Conti, et de variantes de LockBit ciblant macOS. Par ailleurs, le RaaS LockBit a accueilli en 2023 les membres d'autres programmes RaaS tels qu'ALPHV et NoEscape, dont les opérations ont été démantelées.

Dans le sillage de l'opération coup de poing des forces de l'ordre, nous avons observé que le groupe LockBit mettait tout en œuvre pour essayer de sauver les apparences et de restaurer son opération lucrative. Il fallait s'y attendre étant donné la publicité faite autour des activités criminelles de LockBit. Cependant, sur le marché clandestin de la cybercriminalité, il est plus facile de restaurer un serveur que des années de confiance. Reste à savoir quelle quantité d'informations les forces de police ont obtenue sur le fonctionnement, le profil et les affiliés de LockBit.

> Cette incertitude crée un risque considérable pour les cybercriminels désireux de collaborer avec LockBit et son (ancienne) équipe.

Après l'opération policière, il est devenu évident que le monde de la cybercriminalité est impitoyable. Les experts de Trellix Advanced Research Center ont constaté que d'autres cybercriminels utilisaient la version divulguée de LockBit Black pour usurper l'identité du célèbre groupe afin d'en retirer un avantage financier.

Qu'il s'agisse ou non d'imposteurs, leurs victimes étaient bien réelles et tous ces événements des deux derniers trimestres sont dignes d'un film.

Perspective mondiale sur les ransomwares

Au cours de nos recherches sur l'activité des ransomwares au 1er trimestre 2024, nous avons analysé plusieurs sources : des sites de divulgation, des données télémétriques et des rapports publics. Voici quelques mots sur chacune de ces catégories.

- **Sites de divulgation –** Ces sites sont destinés à exposer les victimes d'extorsion qui n'ont pas payé la rançon exigée. Ils offrent ainsi un aperçu des activités du gang cybercriminel. Il est important de noter, cependant, que les sites de divulgation ne reflètent pas forcément le paysage des cybermenaces avec exactitude. Puisqu'ils sont gérés par des criminels, toutes les informations qui n'y trouvent ne sont pas nécessairement vraies ou correctes. Par ailleurs, si le gang tient effectivement ses promesses, les victimes qui paient la rançon ne sont pas répertoriées du tout, ce qui rend le tableau incomplet.

SOMMAIRE

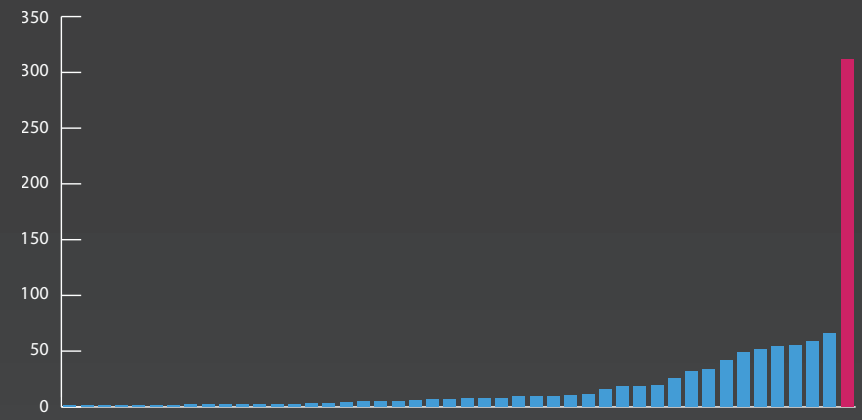
Les données utilisées dans ce rapport se rapportent aux tendances globales des sites de divulgation et donnent une image représentative de la réalité.

- **Données télémétriques –** Les données télémétriques sont tirées de l'écosystème de capteurs Trellix. 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. Cela ne veut pas dire que toutes les détections représentent une infection, car les clients testent la détection de certains fichiers pour affiner leurs règles internes, et ces résultats particuliers apparaissent eux aussi dans les journaux agrégés. Ces données restent utiles si l'on considère la situation dans son ensemble, car elles permettent d'identifier des tendances.
- **Rapports publics –** Des rapports de fournisseurs et d'individus ont été traités par notre équipe Advanced Research Center afin d'en analyser les caractéristiques et d'identifier des tendances. Chaque rapport présente un biais inhérent, en raison par exemple de la présence dominante d'un fournisseur dans une région géographique par rapport à un autre. Cette différence se traduira également dans les types d'incidents rapportés. Compte tenu de la variété de biais présents dans les rapports inclus, nous n'appliquons pas de filtre spécifique.

Groupes de ransomware actifs

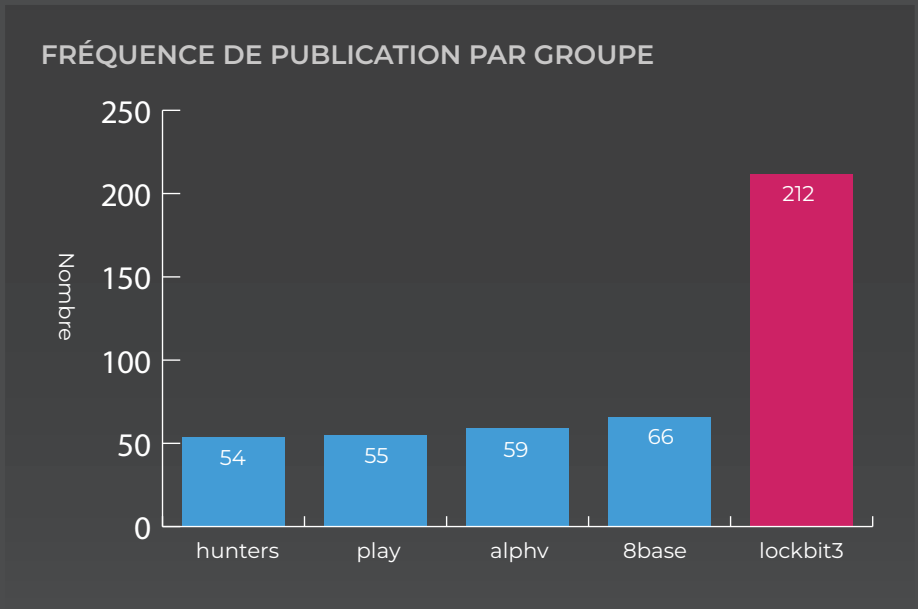
Bon nombre des publications agrégées des sites de divulgation du 1er trimestre 2024 présentent des signes d'activité. Il arrive que ces publications soient des annonces à caractère général, mais la plupart sont des « preuves » d'extorsion ou des fuites de données de leurs victimes. Il arrive souvent qu'une victime fasse l'objet de plusieurs publications, ce qui peut fausser les résultats car elle sera comptabilisée plus d'une fois dans les données.

FRÉQUENCE DE PUBLICATION PAR GROUPE



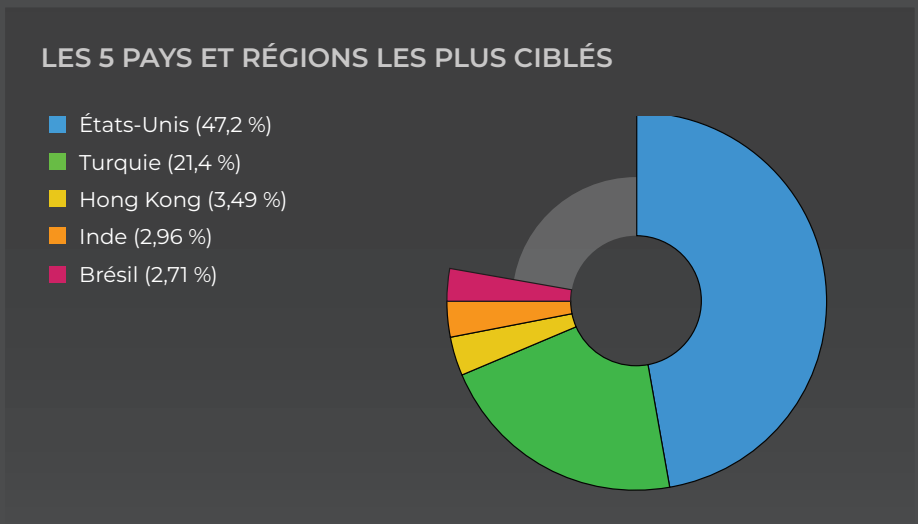
SOMMAIRE

En ce qui concerne la fréquence de publication des cinq sites de divulgation les plus actifs gérés par des gangs de ransomware, l'activité de LockBit se démarque nettement sur les graphiques. L'activité des gangs autres que LockBit représente en moyenne plus de 50 publications par trimestre – ce qui signifie qu'il s'écoule en moyenne moins de deux jours entre la publication de données de deux victimes. Comme expliqué plus haut, ces chiffres sont censés se rapporter aux victimes qui ne paient pas la rançon, ce qui signifie que le nombre réel de victimes est probablement plus élevé, même s'il n'existe aucune méthode pour en déterminer le nombre exact.



Pays et régions ciblés

Compte tenu de l'activité continue des gangs de ransomware, nous pouvons dégager les détections de ransomwares à partir des données télémétriques de Trellix. Les États-Unis sont le pays qui génère le plus de détections, suivis par la Turquie, Hong Kong, l'Inde et le Brésil.



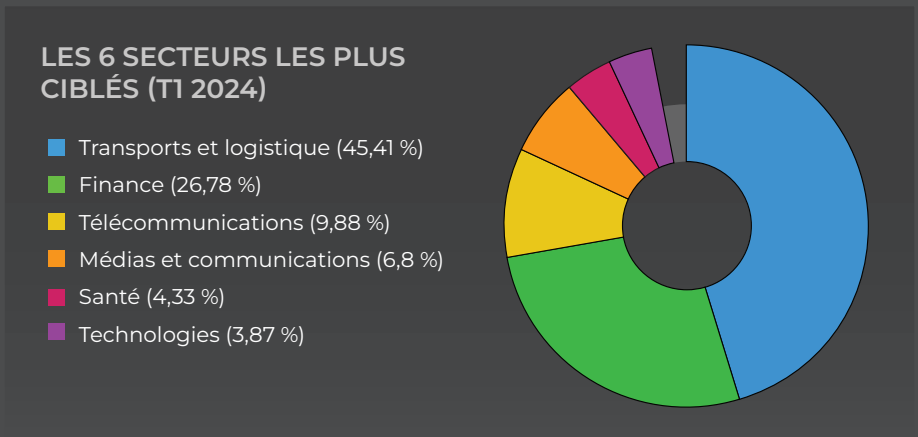
SOMMAIRE

Étant donné que les ransomwares représentent une menace pour tous les secteurs, dans presque toutes les régions géographiques, les métriques de détection sont cohérentes avec la population de clients.

Les données télémétriques pour le trimestre précédent sont assez similaires, à l'exception de l'augmentation des détections en Inde et en Chine. Rien n'indique qu'une campagne spécifique a été menée contre ces régions. Nous suspectons la réalisation de tests de malwares d'être la cause de ce nombre plus élevé de détections.

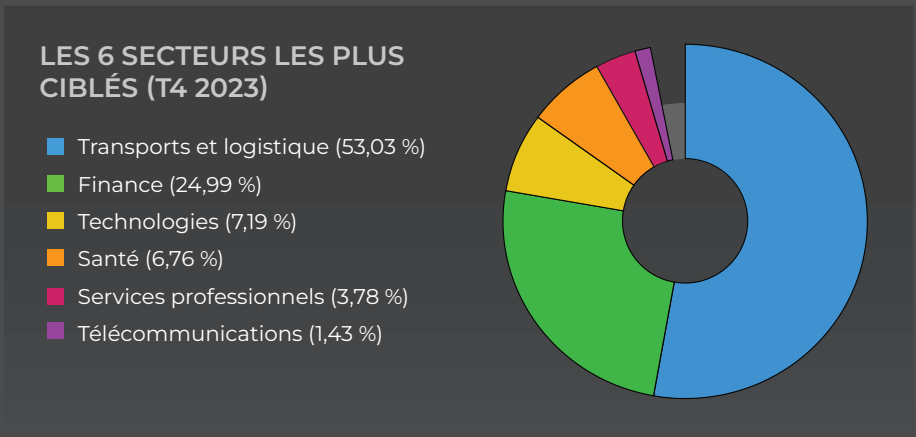
Secteurs ciblés

L'agrégation des données télémétriques mondiales par secteur montre que la moitié des détections proviennent du secteur des transports et de la logistique, et qu'un peu plus d'un quart sont issues des services financiers. Ces deux secteurs sont à l'origine de plus de 72 % des détections, ce qui est logique : la disponibilité de leurs services est d'une importance primordiale. Si une société de transport ne peut pas acheminer des marchandises en raison d'une attaque de ransomware, son processus opérationnel est interrompu, ce qui entraîne d'énormes pertes financières. De même, le secteur financier repose sur la confiance. La divulgation de données sensibles et/ou les temps d'arrêt dus à une attaque de ransomware portent donc un préjudice fondamental aux entreprises de ce domaine.



Au 4e trimestre 2023, le classement des secteurs les plus ciblés était légèrement différent, à l'exception des deux premières places. Ces deux secteurs étaient à l'origine d'une part encore plus importante des détections – 78 % à eux deux pour la période considérée.
Les détections associées aux secteurs des technologies et de la santé ont diminué au 1er trimestre 2024 par rapport au trimestre précédent, mais cette différence ne peut pas être imputée à un ou plusieurs événements spécifiques.

SOMMAIRE



Outils et techniques

Les rapports publics sont la dernière des trois sources mentionnées. Ils permettent de dégager des techniques MITRE, ainsi que les outils et lignes de commande associés utilisés lors des attaques.

> **CONSEIL POUR LES RSSI :** ces rapports de détections peuvent être utiles aux équipes de sécurité : connaître les techniques et outils les plus employés aide à prévenir plusieurs types d'attaques perpétrées par différents cybercriminels, en commençant par les plus efficaces. En outre, les exercices de simulation d'attaques peuvent se concentrer sur ces techniques afin de tester les mesures de détection en place.

Le tableau ci-dessous répertorie les techniques les plus fréquentes, par ordre décroissant.

Techniques MITRE ATT&CK	Campagnes uniques
Chiffrement de données pour impact	31
Découverte des fichiers et des répertoires	23
PowerShell	23
Transfert d'outils à l'entrée	21
Découverte des informations système	21
Obfuscation de fichiers ou d'informations	19
Modification du Registre	18
Windows Command Shell	17
Désobfuscation/décodage de fichiers ou d'informations	16
Arrêt de service	16

Compte tenu de l'objectif des ransomwares, il n'est pas surprenant que les techniques de type Chiffrement de données et Découverte des fichiers et des répertoires arrivent en tête du classement. Si l'on compare ces techniques à celles qui étaient les plus prévalentes au 4e trimestre 2023, on remarque que la plupart des techniques en haut du classement sont similaires, même si leur rang spécifique peut varier.

SOMMAIRE

Techniques MITRE ATT&CK	Campagnes uniques
Chiffrement de données pour impact	45
PowerShell	29
Obfuscation de fichiers ou d'informations	25
Découverte des fichiers et des répertoires	24
Windows Command Shell	24
Prévention de la restauration du système	23
Exploitation d'applications publiques	21
Transfert d'outils à l'entrée	21
Découverte des processus	21
Arrêt de service	21

À l'instar des modus operandi des menaces ATP, les cybercriminels continuent à utiliser des outils légitimes à des fins malveillantes. Les outils utilisés influencent les techniques observées, étant donné qu'ils sont un moyen au service d'un objectif (ici, une technique). Par exemple, PowerShell et Windows Command Shell sont souvent utilisés pour exécuter des commandes supplémentaires sur le système, comme la suppression des clichés instantanés – une stratégie majoritairement associée à la technique Prévention de la restauration du système. C'est également la raison pour laquelle ils sont les outils les plus utilisés, comme illustré ci-dessous.

Nom de l'outil à ligne de commande (attr)	Campagnes uniques
Cmd	7
PowerShell	6
VSSAdmin	5
wevtutil	4
curl	4
Rundll32	4
reg	4
Schtasks.exe	3
BCDEdit	3
wget	2

SOMMAIRE

L'utilisation de VSSAdmin, de BCDEdit et de wevtutil indique que le ransomware s'assure que le système de la victime ne peut pas revenir à l'état normal précédant l'attaque. L'utilisation de l'outil reg montre les modifications apportées au Registre, ce qui peut être fait pour diverses raisons. Les malwares utilisent souvent le Registre pour établir une persistance, mais les ransomwares y accordent une moindre importance, car elle n'a plus de raison d'être une fois le chiffrement terminé. À la place, ils peuvent altérer d'autres paramètres pour autoriser certaines actions qui n'auraient normalement pas été possibles. Rundll32 est fréquemment utilisé pour charger et exécuter une DLL, mais il est souvent la cible d'injections de processus.

Tout comme au trimestre précédent, PowerShell et Cmd arrivent en tête du classement pour la même raison. VSSAdmin et BCDEdit sont également présents, même si wevtutil (Windows Event Log Utility) ne figure pas dans la liste des outils les plus populaires. Compte tenu du faible nombre d'occurrences des outils mentionnés, la fréquence la plus élevée étant de 13 quel que soit le trimestre, il n'est pas étonnant que toutes les campagnes n'utilisent pas les mêmes outils. Une légère variation peut entraîner l'exclusion de tels outils.

Nom de l'outil à ligne de commande (attr)	Campagnes uniques
PowerShell	13
Cmd	9
WMIC	6
Net	6
echo	5
VSSAdmin	4
msiexec	3
Schtasks.exe	3
Rundll32	3
BCDEdit	3

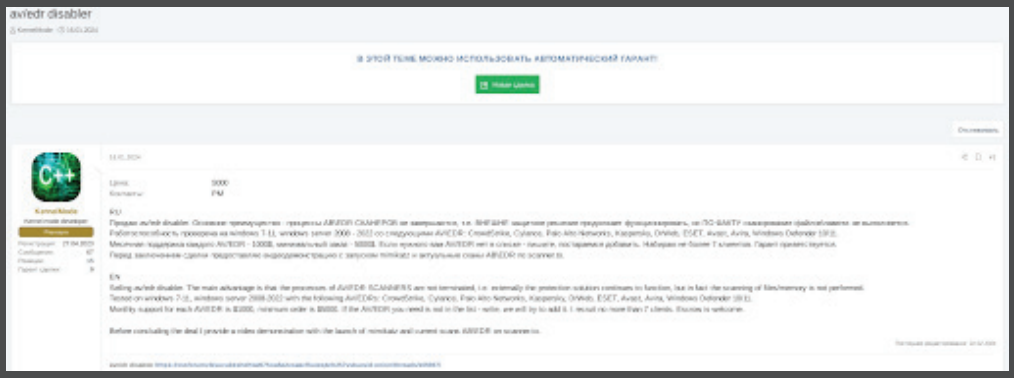
La menace des ransomwares persiste.

SOMMAIRE

L'émergence des outils de contournement et de désactivation d'EDR

L'adoption des solutions EDR par de nombreuses organisations dans le monde a contribué à améliorer la détection, la compréhension et la réponse à des attaques plus sophistiquées. Aujourd'hui, les cybercriminels ont souvent recours à des fichiers binaires d'exploitation des ressources locales (LOLBin) et à des méthodes d'attaque plus complexes, mais grâce à la présence de la technologie EDR, il est plus compliqué d'échapper à la détection.

Cela étant, la sécurité reste un jeu du chat et de la souris, et les cybercriminels sont à l'affût de nouvelles techniques pour contourner ou désactiver les solutions EDR. Cette volonté a donné naissance à une toute nouvelle génération d'outils et techniques de contournement et de désactivation d'EDR, dont certains sont proposés sur des forums cybercriminels clandestins. Par exemple, comme nous l'avons vu précédemment, le groupe de ransomware D0nut a gagné en notoriété grâce à son propre outil de désactivation d'EDR.



Annonce concernant l'outil de désactivation d'EDR sur le forum clandestin XSS

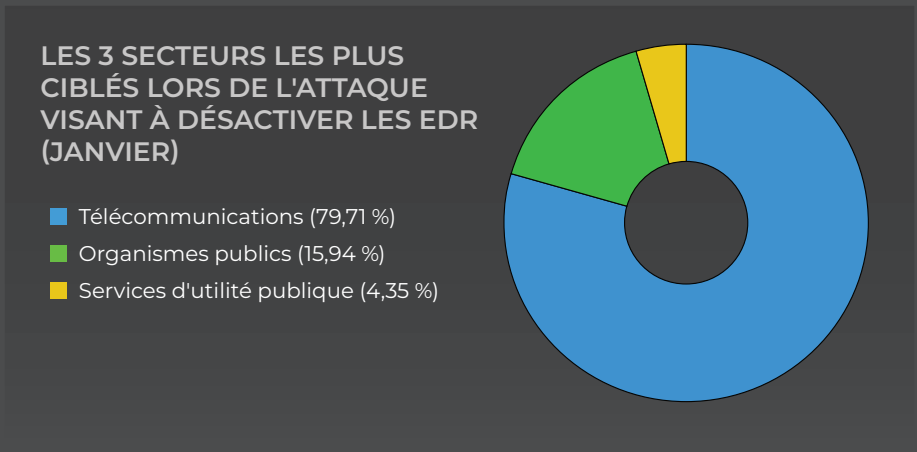
Campagne de janvier utilisant l'outil Terminator de Spyboy

Une technique d'attaque courante, baptisée BYOVD (Bring Your Own Vulnerable Driver), consiste à exploiter des pilotes vulnérables pour l'exécution de code avec élévation de privilèges.

Un exemple de cette méthode est l'outil de désactivation d'EDR Terminator, développé par le cyberpirate Spyboy. L'outil Terminator exploite un pilote Windows légitime mais vulnérable, appartenant à l'outil antimalware Zemana, pour exécuter du code arbitraire à partir du noyau Windows, vraisemblablement en exploitant la vulnérabilité CVE-2021-31728. Terminator a fait son apparition en ligne vers le milieu de l'année 2023 et Trellix a publié un article détaillé dans sa base de connaissances à propos des produits affectés, disponible ici.

Depuis la semaine du 11 au 17 janvier 2024, Trellix Advanced Research Center a relevé des détections inhabituelles de l'outil Terminator de Spyboy dans les données télémétriques de Trellix, ce qui semble indiquer le lancement d'une nouvelle campagne. Au cours de la semaine, la campagne Terminator a connu un pic pendant trois jours et a été détectée à plusieurs reprises dans une seule organisation gouvernementale, une entreprise de services d'utilité publique et une société de communication par satellite. Compte tenu de la spécificité des cibles, Trellix estime avec un haut degré de confiance que l'attaque est liée au conflit Russie-Ukraine.

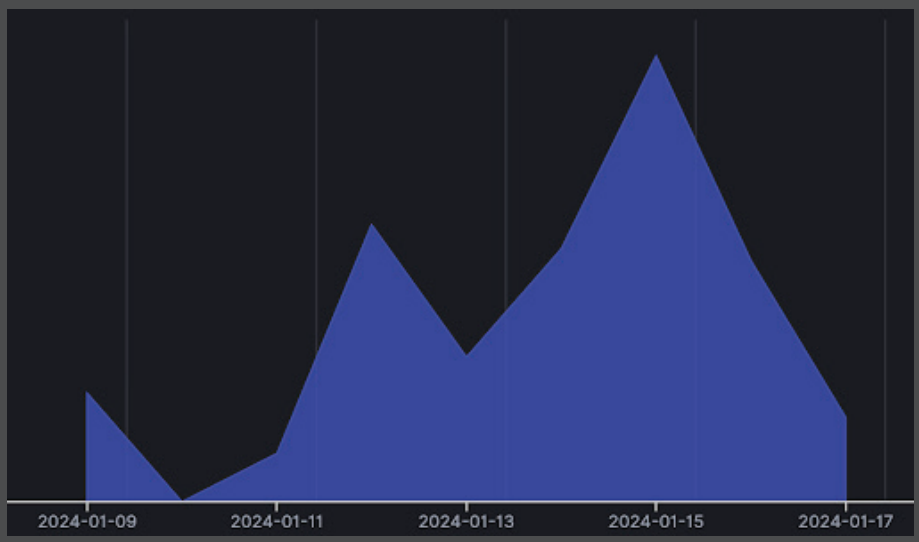
SOMMAIRE



Détections de Trellix ATLAS des attaques ciblant l'Ukraine lors de la campagne Terminator (janvier)

Multiplication des outils de désactivation d'EDR

Plus tôt dans l'année 2023, AuKill, un outil aux objectifs similaires, a été décrit par Sophos. Il utilisait, lui aussi, un pilote vulnérable (BYOVD). Les pilotes utilisés par Terminator et AuKill sont différents, mais il s'agit dans les deux cas de pilotes inoffensifs en tant que tels. Par contre, dans certaines campagnes lancées en 2022, des outils similaires avaient utilisé des pilotes malveillants personnalisés qu'il fallait charger.



SOMMAIRE

L'exploitation de pilotes légitimes pour de telles attaques les rend plus difficiles à détecter et coïncide avec l'utilisation des fichiers LOLBin susmentionnés. Bien qu'un fichier binaire et un pilote présentent des différences techniques, l'intention et les motivations sont similaires, voire identiques. Le malware HermeticWiper apparu en 2022 est un autre exemple de l'utilisation d'un pilote légitime. Dans ce cas, le pilote a été utilisé pour effacer une machine et non pour désactiver l'antivirus. Un autre point commun entre l'outil Terminator mentionné ci-dessus et HermeticWiper est qu'ils sont tous deux attribués à un acteur cybercriminel pro-russe.

Nous avons également observé un cas d'utilisation du réseau Discord pour la distribution d'un malware chez un de nos clients d'Amérique latine. Notre équipe a constaté que Discord continuait d'être utilisé pour la distribution de malwares dans le cadre d'attaques.

> **CONSEIL POUR LES RSSI :** les SOC doivent impérativement surveiller de près leur solution EDR. Les alertes et la journalisation doivent être configurées de sorte qu'en cas de désactivation des outils EDR, le SOC soit immédiatement averti et puisse prendre les mesures qui s'imposent. L'arrêt des outils EDR peut être le signe d'un piratage et il est essentiel d'intervenir rapidement pour limiter l'accès d'un cybercriminel à votre réseau. Il est également crucial d'utiliser une stratégie de défense en profondeur qui permet de faire appel à d'autres outils, tels que la plate-forme NDR (Network Detection and Response), pour détecter les incidents potentiels.

SOMMAIRE

L'e-mail toujours privilégié par les attaquants

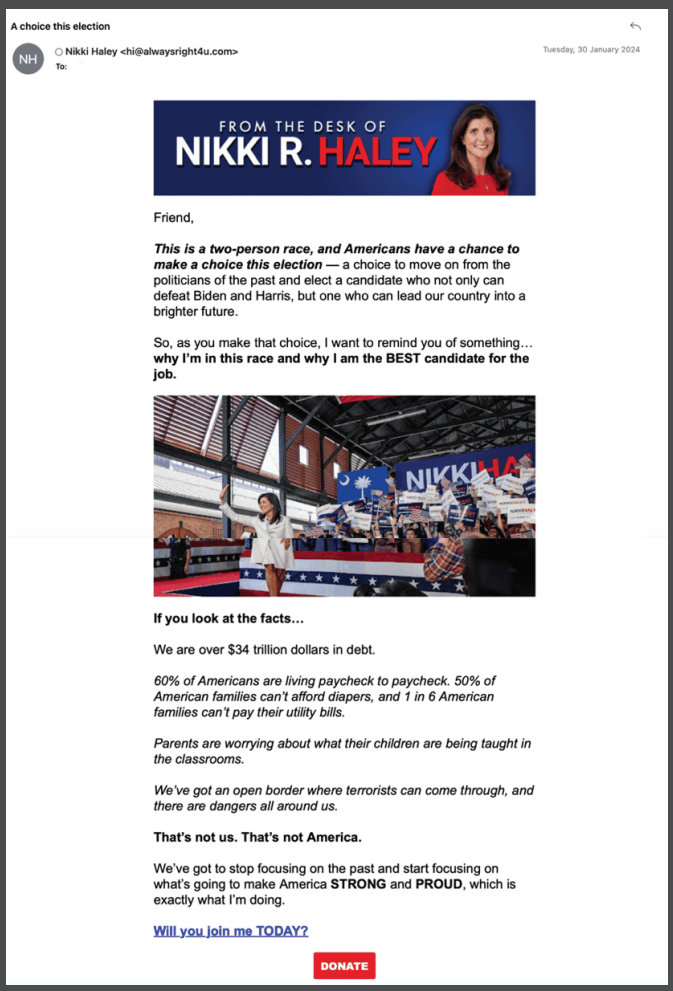
Trellix traite deux milliards d'échantillons d'e-mail et 93 millions de pièces jointes par jour. Nous disposons ainsi d'un volume considérable de données et avons de multiples occasions d'observer les nouvelles techniques utilisées par les attaquants qui ciblent leurs victimes par e-mail.

Escroqueries aux dons en période électorale

Les escroqueries aux dons en période électorale profitent de la sympathie et du soutien envers les candidats en exploitant le sentiment patriotique et en utilisant les noms de candidats connus. Au cours du premier trimestre 2024, nos chercheurs ont constaté que des cybercriminels utilisaient abusivement des services marketing légitimes pour créer des pages de dons rehaussées de photos de candidats et de drapeaux américains, et ainsi inciter les destinataires à faire un don.

Ces escroqueries utilisent les URL de services marketing légitimes pour tromper les destinataires et les convaincre de l'authenticité des e-mails. Malheureusement, ces messages ne font qu'exploiter la générosité des gens à leur profit. Les liens inclus dans les e-mails dirigent les utilisateurs vers des pages où ils sont invités à saisir des informations financières ou à envoyer des dons sur les comptes des expéditeurs ou aux adresses de leurs portefeuilles.

Nos chercheurs ont identifié les e-mails malveillants suivants dans les escroqueries aux dons en période électorale.



A choice this election

NH Nikki Haley <hi@alwaysright4u.com>
To:
Tuesday, 30 January 2024

FROM THE DESK OF
NIKKI R. HALEY

Friend,

This is a two-person race, and Americans have a chance to make a choice this election — a choice to move on from the politicians of the past and elect a candidate who not only can defeat Biden and Harris, but one who can lead our country into a brighter future.

So, as you make that choice, I want to remind you of something… **why I'm in this race and why I am the BEST candidate for the job.**

If you look at the facts…

We are over $34 trillion dollars in debt.

60% of Americans are living paycheck to paycheck. 50% of American families can't afford diapers, and 1 in 6 American families can't pay their utility bills.

Parents are worrying about what their children are being taught in the classrooms.

We've got an open border where terrorists can come through, and there are dangers all around us.

That's not us. That's not America.

We've got to stop focusing on the past and start focusing on what's going to make America **STRONG** and **PROUD**, which is exactly what I'm doing.

Will you join me TODAY?

DONATE

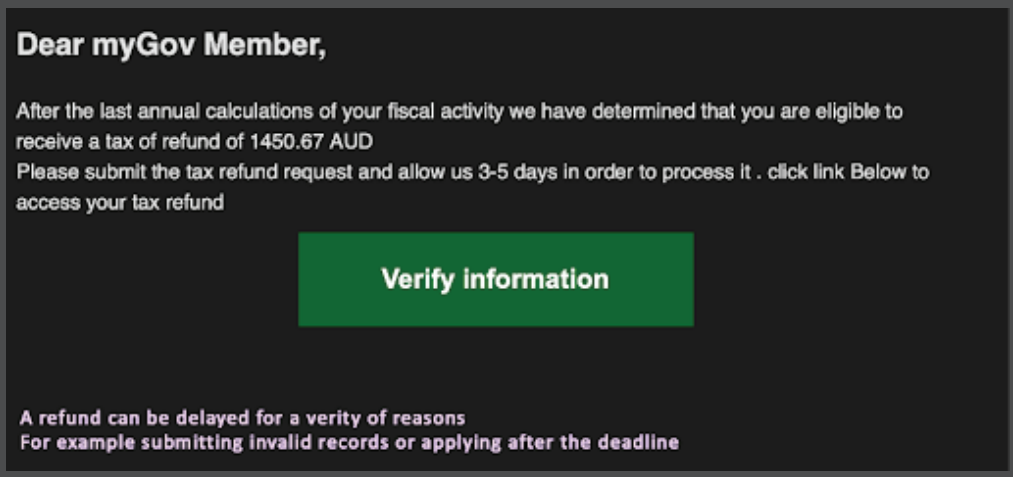
Phishing fiscal

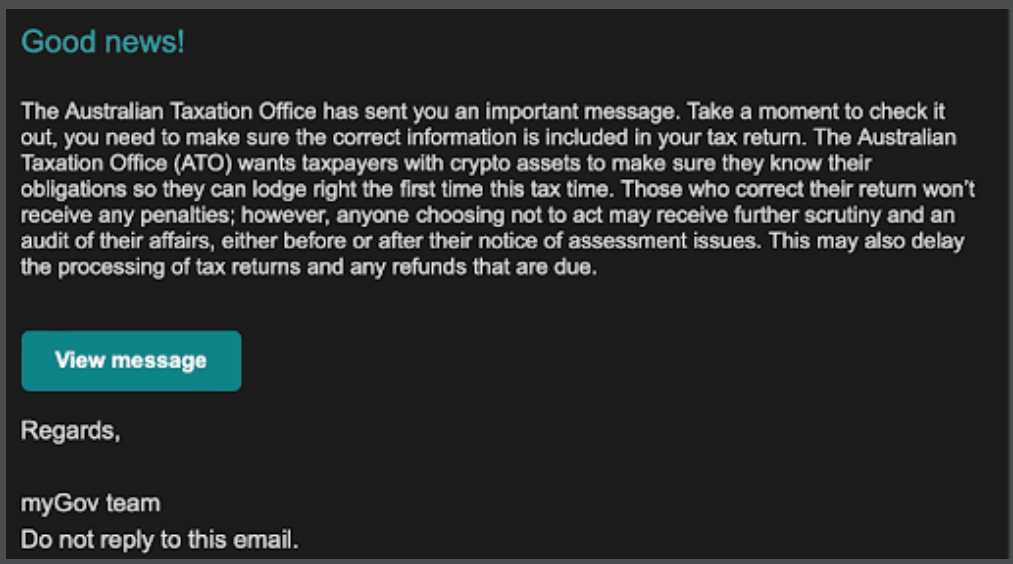
Dans le contexte fiscal, les attaques de phishing sont particulièrement inquiétantes. Les escrocs se font passer pour des agences gouvernementales, des administrations fiscales ou des fiscalistes ayant pignon sur rue pour inciter les personnes ciblées à divulguer leurs informations personnelles. Les sujets invoqués sont multiples : dette envers une administration fiscale, déclaration de revenus non renvoyée ou droit à un remboursement d'impôts, par exemple. Leur objectif ultime est d'obtenir votre numéro d'identification fiscale, des détails du compte bancaire ou d'autres données de valeur. L'e-mail inclut des liens qui semblent vous amener à des sites web de l'administration publique ou fiscale, mais qui vous redirigent en réalité vers des sites frauduleux, conçus pour voler des données.

Au premier trimestre 2024, Trellix a observé une augmentation d'e-mails de ce type qui semblaient émaner de l'administration fiscale australienne, et les a correctement détectés.

SOMMAIRE

Vous pouvez voir ci-dessous un échantillon de la campagne qui montre clairement le sentiment d'urgence que tentent de susciter les attaquants pour convaincre les destinataires de cliquer sur le lien relatif à un remboursement d'impôts.





L'IA générative au cœur d'une course aux armements : observations sur le marché clandestin cybercriminel

L'intelligence artificielle et l'apprentissage automatique ne sont plus le domaine exclusif d'organisations à gros budgets. ChatGPT et des logiciels similaires peuvent être utilisés par tous, y compris les cybercriminels. Voilà pourquoi l'intelligence artificielle est devenue une course à l'armement entre les cybercriminels et les professionnels de la sécurité. L'IA est un outil puissant, qui doit être utilisé de façon responsable afin de favoriser la réalisation des objectifs de l'entreprise, mais il est impératif de ne pas laisser les cybercriminels prendre l'avantage à cet égard. Nous devons utiliser ces nouveaux outils pour déjouer les pièges des cybercriminels à mesure qu'ils affinent leurs tactiques et techniques, et que leurs armes deviennent plus dangereuses.

SOMMAIRE

CONSEIL POUR LES RSSI : le rôle du RSSI revêt de plus en plus d'importance, car il doit guider l'entreprise dans ce paysage en constante évolution. Face à la multiplication des cyberattaques, à la pression de l'IA et à des responsabilités toujours plus grandes, il n'est guère étonnant que 90 % des RSSI subissent des pressions accrues. Il est essentiel de rester en phase avec les progrès de l'IA et de l'IA générative. À cet égard, la grande majorité des RSSI estiment que leur entreprise pourrait mieux faire. Pour en savoir plus, lisez le dernier rapport de Trellix, Mind of the CISO: Decoding the GenAI Impact.

Les cybercriminels adoptent l'IA générative en raison de ses capacités accélérées d'apprentissage et de son faible coût. De plus, elle est extrêmement performante, car elle permet par exemple de créer des e-mails de phishing dans n'importe quelle langue avec une grammaire impeccable, des logos et des informations de connexion. Les acteurs malveillants peuvent trouver, écrire et tester des exploits dix fois plus vite, sans avoir de grandes compétences dans le domaine.

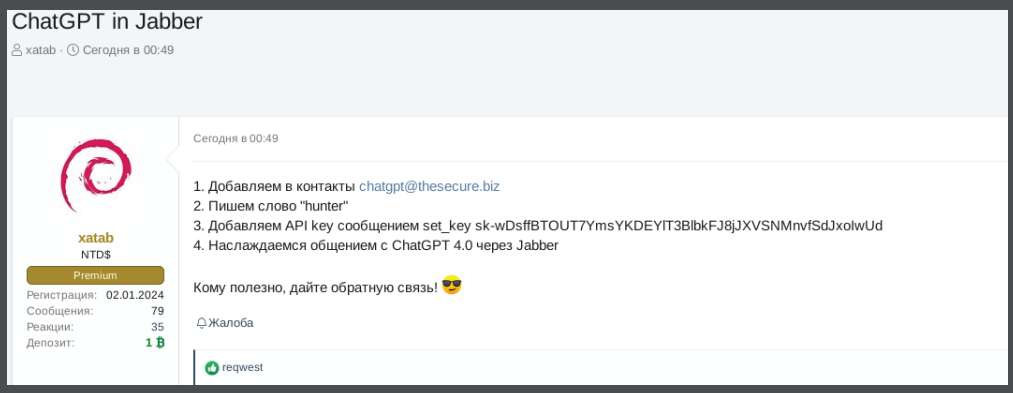
Notre équipe Advanced Research Center explore régulièrement les marchés clandestins pour surveiller les tendances. L'intelligence artificielle générative fait de plus en plus d'adeptes parmi les cybercriminels, et ceux-ci partagent leurs succès et vendent leurs outils. Voici ce qu'il nous a été donné d'observer depuis notre dernier rapport, plus précisément depuis le début de l'année 2024.

Projet « ChatGPT dans Jabber » sans doute exploité par un groupe APT russe

En janvier, nous avons constaté que **xatab**, acteur malveillant important du forum clandestin XSS, recherchait un développeur pour créer un projet « ChatGPT 4.0 in Jabber », ainsi qu'une API et des instructions d'utilisation.

Outre son engouement pour les intégrations LLM, il est également possible que l'intention ou la motivation sous-jacente de **xatab** en ce qui concerne ce projet était d'intercepter et de collecter la correspondance d'autres cybercriminels, afin d'espionner leurs demandes et d'obtenir des renseignements sur leurs centres d'intérêt, leurs cibles et la portée de leurs activités illégales menées avec l'assistance de l'IA générative.

Nous avons observé ce qui suit :



Instructions et clé de l'API du projet « ChatGPT in Jabber » partagées par **xatab** sur le forum XSS

SOMMAIRE

```python
1. Add to your contacts chatgpt@thesecure.biz
2. Write a keyword "hunter"
3. Add API key in the message: set_key <OPENAI_API_KEY>
4. Enjoy the conversation with  ChatGPT 4.0 via Jabber

If useful share your feedback!
```

Le 31 janvier 2024, **xatab** a proposé 2 000 USD pour son projet « ChatGPT in Jabber » sur le forum XSS. Si l'on en croit les allégations sur XSS du cybercriminel **germans**, qui avait développé le robot demandé mais avait été initialement ignoré par **xatab**, il semble que **germans** ait finalement accepté de développer un robot pour la somme de 1 500 USD. Créé pour les serveurs Jabber des forums Exploit (@exploit[.]im) et XSS (@thesecure[.]biz), le robot a été publié par **xatab** sur les forums du Darknet Exploit et XSS prétendument pour le tester et connaître l'avis des membres de ces forums. Le robot pourrait être basé sur le projet xmppgpt.

Dans les messages publiés sur les forums Exploit et XSS, **xatab** se présente comme une équipe APT (connue dans certains milieux comme des spécialistes en tests d'intrusion) à la recherche d'un courtier en accès d'entreprise pour les États-Unis/Royaume-Uni/Canada/Australie en vue d'une collaboration fructueuse. Il a offert de reverser 20 % des revenus générés par chaque accès et a déposé un bitcoin sur chaque forum, Exploit et XSS, pour prouver le sérieux de son offre.

En proposant un outil ChatGPT 4.0 gratuit à la communauté cybercriminelle, **xatab** réalise deux objectifs :

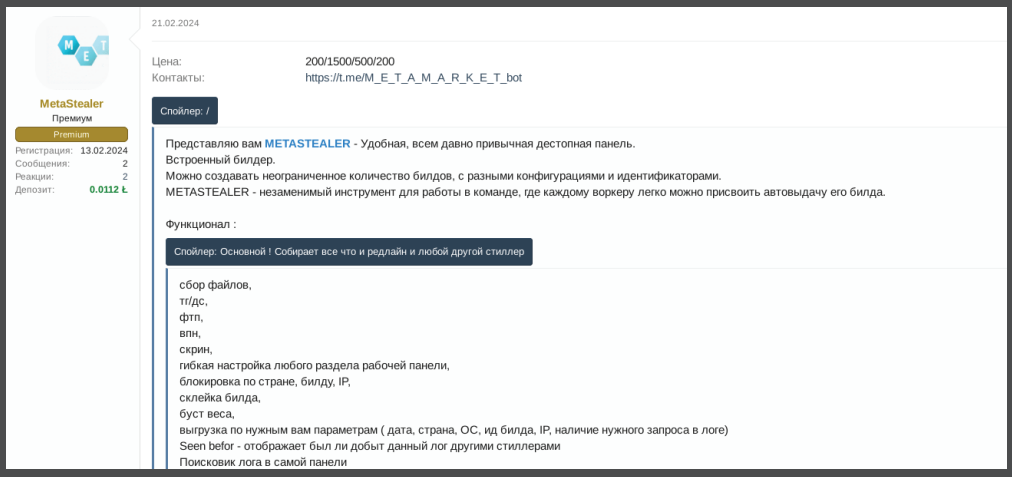
1. Il joue un rôle de catalyseur et de facilitateur, désireux d'aider les cybercriminels à innover et à adopter l'IA générative dans leurs opérations.
2. Il cherche à créer un vivier / une base de connaissance d'IA générative pour profiter des connaissances d'autres cybercriminels, voire s'approprier leurs idées et outils innovants.

Trellix a testé le projet « ChatGPT in Jabber » conformément aux instructions données, et il semble qu'il fonctionne de la façon prévue par l'acteur cybercriminel.

Intégration de l'IA générative aux infostealers

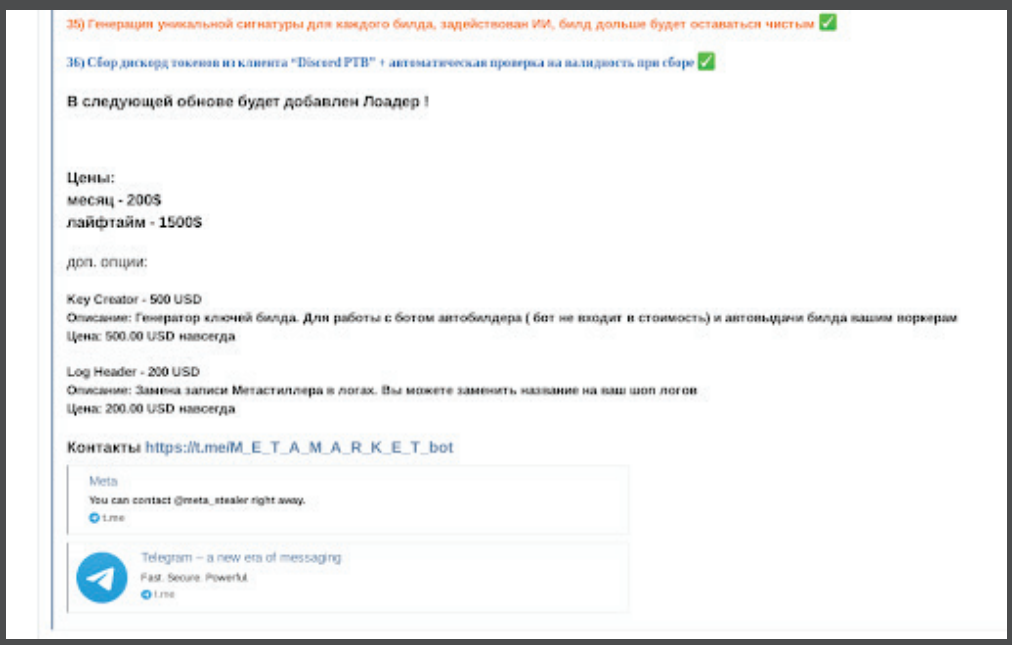
Le 21 février 2024, le cybercriminel MetaStealer a proposé une nouvelle version remaniée de **MetaStealer** sur le forum XSS. MetaStealer est un infostealer (outil d'exfiltration d'informations) apparu pour la première fois en 2021 ; il s'agirait d'un dérivé du célèbre Redline. Plusieurs versions de **MetaStealer** ont été observées en environnement réel. Toutefois, la nouvelle version détectée par Trellix possède une fonctionnalité basée sur l'IA générative pour éviter la détection.

SOMMAIRE



Publication de la version remaniée de MetaStealer par l'acteur malveillant **MetaStealer** sur le forum XSS

Dans la capture d'écran ci-dessous, le texte orange après 35) peut se traduire comme suit : « Des signatures uniques sont générées pour chaque build. Comme l'IA est utilisée, la build échappe à la détection pendant plus longtemps ». Cela laisse penser que les développeurs de MetaStealer ont incorporé une nouvelle fonctionnalité basée sur l'IA générative dans leur outil, ce qui leur permet de créer des builds uniques de MetaStealer afin d'échapper à la détection des solutions antivirus/EDR bien plus longtemps qu'avant.

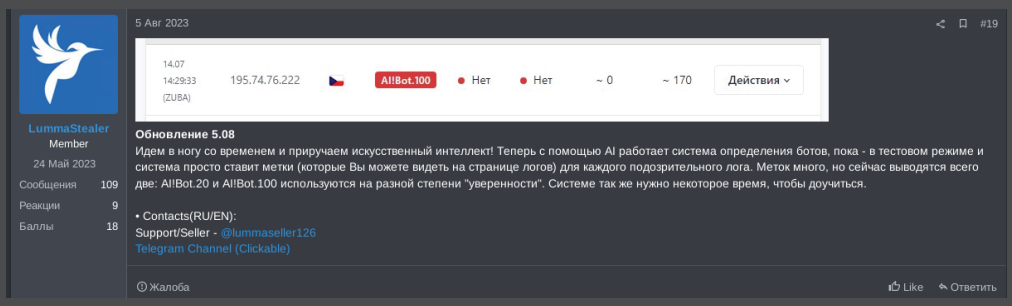


Intégration d'une fonction basée sur l'IA générative à la version remaniée de MetaStealer pour contourner les défenses

LummaStealer est un autre exemple d'infostealer bien établi. Depuis août 2023, l'équipe LummaStealer teste une fonctionnalité basée sur l'IA qui permet aux utilisateurs de cet infostealer de détecter des robots dans la liste de journaux. Le système basé sur l'IA incorporé dans LummaStealer pourrait être un réseau neuronal personnalisé, entraîné à détecter si un journal utilisateur suspect est un robot ou non.

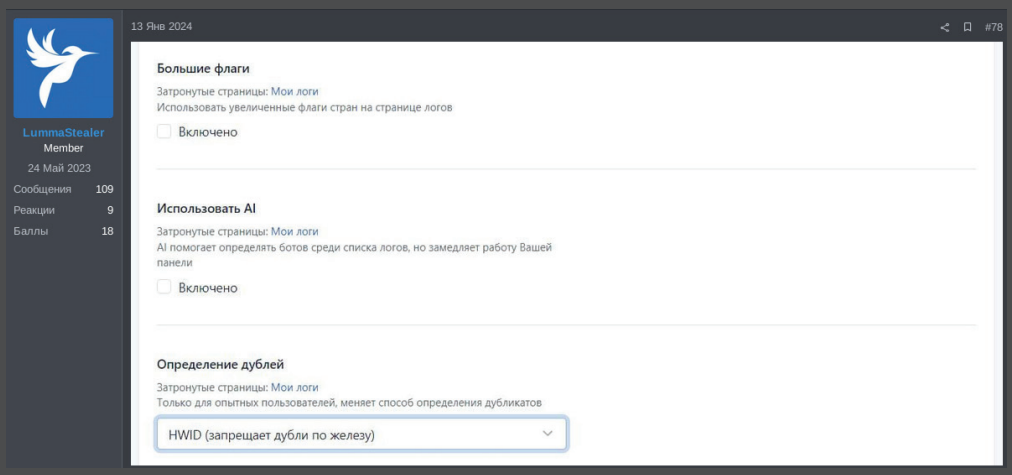
SOMMAIRE

LummaStealer utilise une étiquette **AI!Bot.<nombre>** pour classer le journal détecté comme un robot. La variable <nombre>, dont la plage semble être comprise entre 0 et 100 représente la certitude de détection d'un robot :



Message de LummaStealer sur le forum RAMP dans lequel l'acteur cybercriminel annonce l'intégration d'une fonctionnalité basée sur l'IA pour détecter les robots dans la liste de journaux de l'infostealer

LummaStealer a averti ses utilisateurs que le réseau neuronal était toujours en cours d'apprentissage et qu'il lui faudrait un certain temps pour améliorer la précision de sa détection. De plus, en janvier 2024, **LummaStealer** a fait savoir que la fonctionnalité basée sur l'IA générative est désactivée par défaut car elle ralentit les performances d'exécution de LummaStealer.

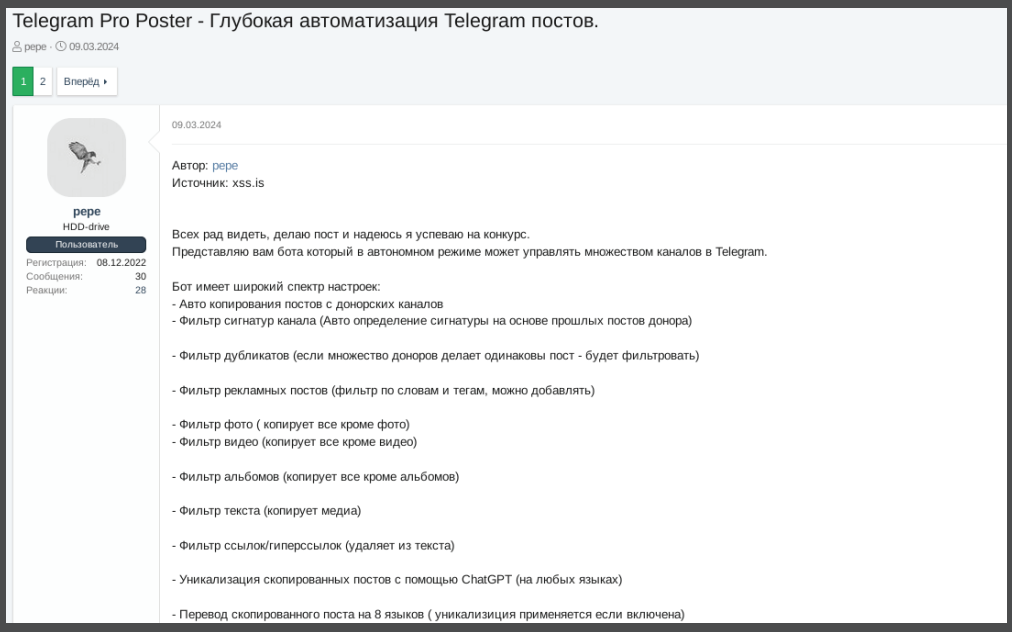


Message de LummaStealer sur le forum RAMP dans lequel l'acteur cybercriminel fait savoir que la détection de robots est désactivée par défaut

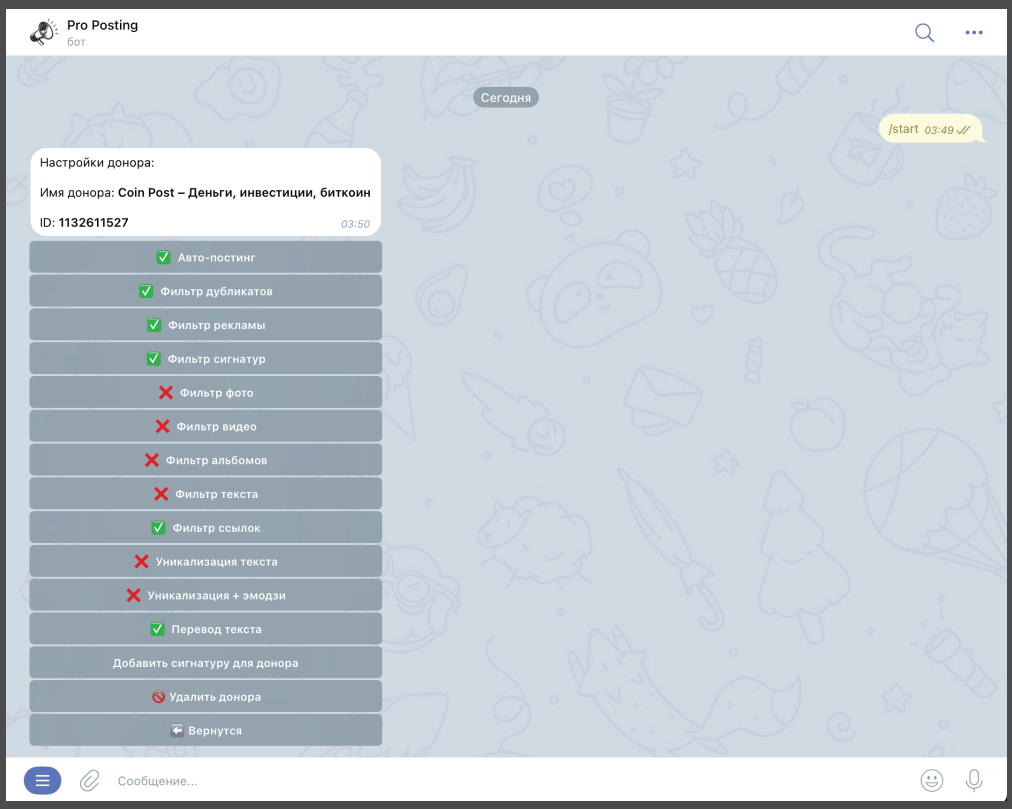
Projet « Telegram Pro Poster »

Au début du mois de mars 2024, le cybercriminel pepe a publié son projet « Telegram Pro Poster » sur le forum XSS dans le cadre d'un concours d'outils/logiciels malveillants. Telegram Pro Poster est un robot destiné à « l'automatisation poussée des messages Telegram ». Ce robot développé avec Python permet aux utilisateurs de gérer un nombre important (voire illimité) de canaux Telegram de façon autonome en copiant automatiquement les messages des canaux Telegram « distributeurs » vers les canaux cibles. Parmi ses nombreuses fonctionnalités de filtrage de messages, ce robot possède deux fonctions d'IA générative intégrées, destinées à traduire les messages Telegram et à paraphraser un message donné à l'aide de ChatGPT.

SOMMAIRE



Message sur le forum XSS concernant le robot basé sur l'IA générative du projet « Telegram Pro Poster »



Fonctionnalités de filtrage de Telegram Pro Poster, y compris la fonction de personnalisation/paraphrase, désactivée par défaut

Trellix a obtenu le code source de l'outil Telegram Pro Poster et identifié les segments de code ci-dessous, responsables de la traduction des messages copiés des canaux distributeurs via l'API de ChatGPT dans les huit langues indiquées avant de les envoyer aux canaux Telegram cibles :

SOMMAIRE

```
Unset
API_ID = 99999999 #APP TELEGRAM ID
API_HASH = "HASH" # APP TELEGRAM HASH
BOT_TOKEN = "API" # BOT API
DATABASE_PATH = 'database.db'
OPEN_AI_KEY = 'API KEY' # OPEN AI KEY


language_codes = {
    'Ukranian': 'украинский',
    'Russian': 'русский',
    'English': 'английский',
    'Indian': 'индийский',
    'Italian': 'итальянский',
    'Brasilian': 'бразильский',
    'Germany': 'немецкий',
    'Indonesian': 'индонезийский'
}
...
def gpt_translate(input_text, language):
    print(f'Перевожу этот текст: {input_text}')
    if len(input_text) > 10:
        openai.api_key = OPEN_AI_KEY
        language = language_codes[language]

        response = openai.ChatCompletion.create(
            model="gpt-3.5-turbo",
            messages=[
                {"role": "system", "content": f"Когда ты получаешь текст то ты
должен перевести его на {language}."},
                {"role": "user", "content": input_text}
            ],
        )
        unique_text = response.choices[0].message['content']
        return unique_text
    else:
        return input_text
```

La seconde fonctionnalité, destinée à personnaliser de façon unique le message, est désactivée par défaut. Toutefois, lorsqu'elle est activée, elle utilise OPEN_AI_KEY pour demander à ChatGPT de paraphraser le texte dans la langue voulue et, le cas échéant, d'ajouter un emoji.

```
Python
def unique_text(input_text, is_emoji_need):
    print(f'Уникализирую этот текст: {input_text}')
    if len(input_text) > 5:
        openai.api_key = OPEN_AI_KEY

        if is_emoji_need:
            content_text = "Перефразируй текст и добавь эмодзи: "
        else:
            content_text = "Перефразируй текст:"

        response = openai.ChatCompletion.create(
            model="gpt-3.5-turbo",
            messages=[
                {"role": "system", "content": content_text},
                {"role": "user", "content": input_text}
            ],
        )
        unique_text = response.choices[0].message['content']
        token_count = response['usage']['total_tokens']
        return unique_text

    else:
        return input_text
```

SOMMAIRE

Les commentaires de la communauté XSS de cybercriminels ont une opinion très favorable du projet « Telegram Pro Poster », affirmant qu'il est intéressant et qu'entre des mains compétentes, il sera très certainement utile. Dans un thread du forum XSS, un autre cybercriminel a indiqué avoir constaté l'adoption de ce robot sur divers canaux Telegram.

CONCLUSION

La course contre la montre

La Threat Intelligence opérationnelle fournit des informations sur la nature, l'intention et les périodes d'activité de cybermenaces spécifiques. Elle est plus détaillée et contextuelle que la Threat intelligence tactique, car elle offre notamment des renseignements pertinents sur les tactiques, techniques et procédures (TTP) des cybercriminels.

Les entreprises peuvent s'appuyer sur cette Threat Intelligence opérationnelle pour comprendre le contexte plus large des cyberattaques, notamment les motivations des cybercriminels et les méthodes utilisées, afin d'aider les équipes de sécurité à anticiper et à se préparer à des types d'attaques spécifiques.

Mes nombreuses missions auprès de clients m'ont donné l'occasion de constater que le premier objectif d'un RSSI est de limiter le risque pour leur organisation. L'utilisation de la Threat Intelligence opérationnelle est un moyen tangible de limiter ce risque dès lors qu'il permet aux RSSI et à leurs équipes SecOps d'anticiper et de mettre en place les bases nécessaires. Elle leur permet d'identifier les failles dans leurs mesures de sécurité pour toute la surface d'attaque de l'entreprise et de se mettre à la place de leurs adversaires afin de mieux les déstabiliser.

Nous partageons notre Threat Intelligence afin de vous fournir les renseignements objectifs nécessaires aux décisions capitales que vous serez amené à prendre. Notre objectif est de vous aider à renforcer considérablement vos capacités de cyberdéfense et de prendre une longueur d'avance sur les cybercriminels.

Allons-y !

Ashok Banerjee,
CHIEF TECHNOLOGIST, TRELLIX

SOMMAIRE

MÉTHODOLOGIE

Collecte – 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.

- **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.

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 leurs 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.

Application : comment utiliser ces informations

Il est indispensable que chaque processus et chaque équipe d'évaluation de premier plan comprennent, reconnaissent et, si possible, réduisent les effets 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.

SOMMAIRE

- 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.

Comment comprendre l'analyse présentée dans ce rapport

Pour comprendre les observations et les données contenues dans ce rapport, un bref rappel des lignes directrices suivantes s'impose :

- **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.
- **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.

SOMMAIRE

RESSOURCES

Archives des Rapports sur le paysage des menaces

The Mind of the CISO

SUIVEZ TRELLIX ARC SUR X

Trellix ARC

Archives des Rapports sur le paysage des cybermenaces

Trellix Advanced Research Center

SOMMAIRE

À PROPOS DE TRELLIX ADVANCED RESEARCH CENTER

Trellix Advanced Research Center est à l'avant-garde de la recherche sur les nouvelles méthodes, tendances et outils utilisés par les acteurs malveillants dans le paysage mondial des cybermenaces. Notre équipe d'analystes chevronnés est le partenaire incontournable des RSSI, des responsables sécurité et de leurs équipes SecOps dans le monde entier. Trellix Advanced Research Center propose une Threat Intelligence opérationnelle et stratégique de tout premier ordre aux analystes en sécurité. Il alimente notre plate-forme XDR de pointe, optimisée par l'IA, et offre des produits et services de Threat Intelligence à nos clients partout dans le monde. Pour en savoir plus, consultez le site www.trellix.com/fr-fr/advanced-research-center.html.

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'intelligence artificielle, à l'automatisation et à l'analyse 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 le site trellix.com/fr-fr/.

SOMMAIRE