Rapport 2024 de ThreatLabz sur les ransomwares

Table des matières

Note de synthèse

Les attaques de ransomware ont atteint de nouveaux sommets en matière d'ambition et d'audace au cours de l'année écoulée, marquée par une recrudescence notable des attaques d'extorsion. Alors que les ransomwares progressent, les recherches de ThreatLabz révèlent le **paiement d'une rançon record de 75 millions de dollars américains**, le montant le plus élevé jamais payé par une entreprise. Ce montant représente près du double de celui de la rançon connue la plus importante réglée à ce jour.[1] Sur la seule année 2023, les paiements effectués au titre des ransomwares ont dépassé le milliard de dollars, soulignant l'impact toujours plus marqué de cette forme de cybercriminalité.

Les tactiques des auteurs de ransomware se révèlent de plus en plus sophistiquées et audacieuses. Ils ont notamment dépassé les frontières traditionnelles des entreprises qu'ils attaquent, allant jusqu'à cibler les enfants de cadres dirigeants pour obtenir des rançons plus rapides et plus élevées.[2] Des infrastructures critiques[3] et grandes entreprises[4] jusqu'aux petites et moyennes entreprises, aucune entité n'est à l'abri de se retrouver dans la ligne de mire de la prochaine campagne ou évolution des attaques de ransomware.

Malgré le démantèlement par les forces de l'ordre de plusieurs courtiers d'accès initial (initial access brokers) dans le cadre des opérations spéciales « Opération Endgame » et « Opération Duck Hunt », nombre des plus grandes familles de ransomwares actives se regroupent rapidement et lancent de nouvelles attaques. Malheureusement, de nombreux auteurs de ransomwares sont hors de portée des forces de l'ordre, ce qui les met pratiquement à l'abri de poursuites pénales. Comme le souligne ce rapport, les forces de l'ordre ont renforcé leurs moyens de pression en offrant des récompenses financières, en imposant des sanctions et en exposant les auteurs de ransomwares à l'aide de différentes formes de tactiques psychologiques.

Les auteurs de ransomwares ne cessant de faire évoluer leurs techniques et procédures, il est crucial de se maintenir informé de l'évolution de la menace.

Le rapport 2024 de Zscaler ThreatLabz sur les ransomwares dresse un état des lieux des ransomwares d'avril 2023 à avril 2024. Il se penche sur les nouvelles tendances, les cibles, les familles de ransomwares et les stratégies de défense efficaces.

ThreatLabz a constaté une augmentation annuelle de 17,8 % des attaques de ransomware sur la base des tentatives bloquées dans le cloud Zscaler, tandis que les attaques de ransomware répertoriées à partir des sites de divulgation des données détournées ont bondi de 57,8 %. Les acteurs des secteurs de la production industrielle, des soins de santé et des technologies sont les cibles privilégiées des ransomwares, ce qui positionne les opérations et les infrastructures critiques en première ligne pour les attaques.

Les résultats présentés dans ce rapport soulignent la nécessité qui incombe aux entreprises de faire de la protection contre ces ransomwares récurrents une priorité absolue. Les perspectives et stratégies présentées dans ce rapport vous accompagnent pour étayer votre ligne de défense contre les ransomwares. En comprenant les tendances et vulnérabilités les plus récentes et en mettant en œuvre les bonnes pratiques recommandées, vous disposez de moyens pour éviter d'être la victime d'un ransomware et mieux protéger les ressources et données critiques de votre entreprise.

[1] Bloomberg, **CNA Financial Paid $40 Million in Ransom After March Cyberattack**, 20 mai 2021.
[2] Business Insider, **Hackers are now targeting the children of corporate executives in ransomware attacks**, 12 mai 2024.
[3] Dark Reading, **Ascension Healthcare Suffers Major Cyberattack**, 10 mai 2024.
[4] CyberScoop, **Boeing confirms attempted $200 million ransomware extortion attempt**, 8 mai 2024.

Principales conclusions

Les recherches de Zscaler ThreatLabz ont révélé le paiement d'une rançon record de 75 millions de dollars américains — la plus importante rançon jamais payée par une entreprise — près du double du paiement le plus élevé révélé publiquement à ce jour.

Les attaques de ransomware bloquées par le cloud Zscaler ont augmenté de 17,8 %, tandis le nombre d'entreprises extorquées et répertoriées sur les sites de divulgation des données grimpe de 57,8 % par rapport à la même période de l'année précédente. Ce chiffre ne fléchit pas, malgré les nombreuses opérations des forces de l'ordre, notamment la saisie d'infrastructures assortie d'arrestations, de mises en examen et de sanctions.

Les secteurs de la production industrielle, des soins de santé et des technologies ont été les principales cibles des attaques de ransomware, tandis que le secteur de l'énergie a connu une hausse de 500 % en une année, ses infrastructures critiques et sa vulnérabilité aux perturbations opérationnelles en faisant une cible particulièrement attrayante pour les cybercriminels.

Les États-Unis restent la première cible des ransomwares, représentant 49,95 % de l'ensemble des attaques, suivis du Royaume-Uni, de l'Allemagne, du Canada et de la France.

ThreatLabz a identifié 19 nouvelles familles de ransomwares au cours de la période analysée, portant le nombre total à 391 depuis le début de notre suivi.

Les familles de ransomwares les plus actives étaient **LockBit (22,1 %)**, **BlackCat (alias ALPHV) (9,2 %)** et **8Base (7,9 %)**.

Les vulnérabilités restent un vecteur d'attaque de ransomware très courant, soulignant l'importance d'un déploiement rapide des correctifs, d'une gestion unifiée des vulnérabilités et d'une architecture Zero Trust, pour assurer une protection même lorsque les correctifs ne sont pas disponibles.

Les attaques par ingénierie sociale vocale sont de plus en plus utilisées pour accéder aux réseaux d'entreprise, une technique mise en oeuvre par Scattered Spider et le groupuscule Qakbot.

Panorama des ransomwares : principales tendances et cibles

La nature dynamique des ransomwares en fait une préoccupation majeure de sécurité lors de ces dernières années. Les acteurs malveillants font constamment évoluer leurs méthodes d'attaque et d'extorsion, tirant parti des progrès des technologies d'intelligence artificielle (IA), des fuites de code source et du chiffrement avancé pour maximiser leur impact et leurs gains financiers.

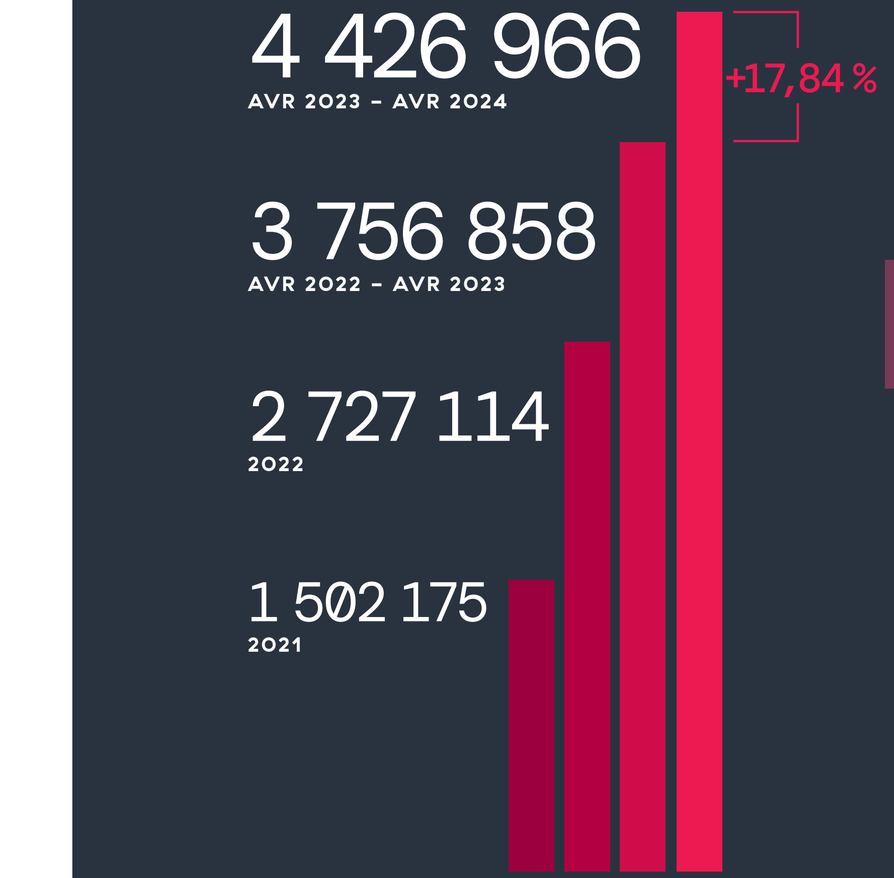
Ce rapport se penche sur les tendances suivantes en matière d'attaques de ransomware d'avril 2023 à avril 2024 :

- Recrudescence générale des attaques de ransomware
- Secteurs d'activité les plus ciblés par les ransomwares
- Répartition géographique des entreprises victimes
- Renforcement des mesures répressives contre les groupes de ransomware et les courtiers d'accès initial
- Principales menaces de ransomware et paiements records de rançons

Recrudescence générale des attaques de ransomware

La nouvelle analyse de ThreatLabz pointe une tendance inquiétante, avec une progression annuelle de 17,84 % des attaques de ransomware, mesurée sur la base des tentatives bloquées observées dans le cloud Zscaler. L'activité plus dynamique des ransomwares engendre des perturbations et d'importants impacts financiers pour les entreprises qui en sont victimes, quelle que soit leur taille. Ces attaques perturbent souvent les opérations de l'entreprise, et sont responsables de temps d'arrêt prolongés, de substantielles pertes de données et de restaurations onéreuses. Le poids financier est considérable : au-delà de la rançon, la restauration des systèmes et la gestion des dommages peuvent également coûter très cher.
À la lumière de ces menaces qui s'accentuent, des **mesures de défense robustes contre les ransomwares** n'ont jamais été aussi nécessaires.

NOMBRE DE TENTATIVES BLOQUÉES DANS LE CLOUD ZSCALER



Secteurs d’activité les plus ciblés par les ransomwares

Les attaques de ransomware font peser des risques importants pour les entreprises, quelles que soient leur taille ou leur secteur. Elles peuvent compromettre des données sensibles, entraîner de lourdes pertes financières, perturber la continuité des activités et nuire à la réputation. Différents secteurs sont confrontés à des défis uniques liés aux ransomwares, en fonction de leur mode de fonctionnement, des données qu’ils traitent et de leur infrastructure technologique.

Malgré ces différences, les attaques d’extorsion par ransomware n’ont cessé de progresser, le nombre d’entreprises victimes répertoriées sur les sites de divulgation de données ayant bondi de 57,81 % depuis le rapport ThreatLabz de l’année dernière sur les ransomwares. Le secteur de la production industrielle est de loin celui le plus ciblé, avec 653 attaques, soit plus de deux fois plus que n’importe quel autre secteur.

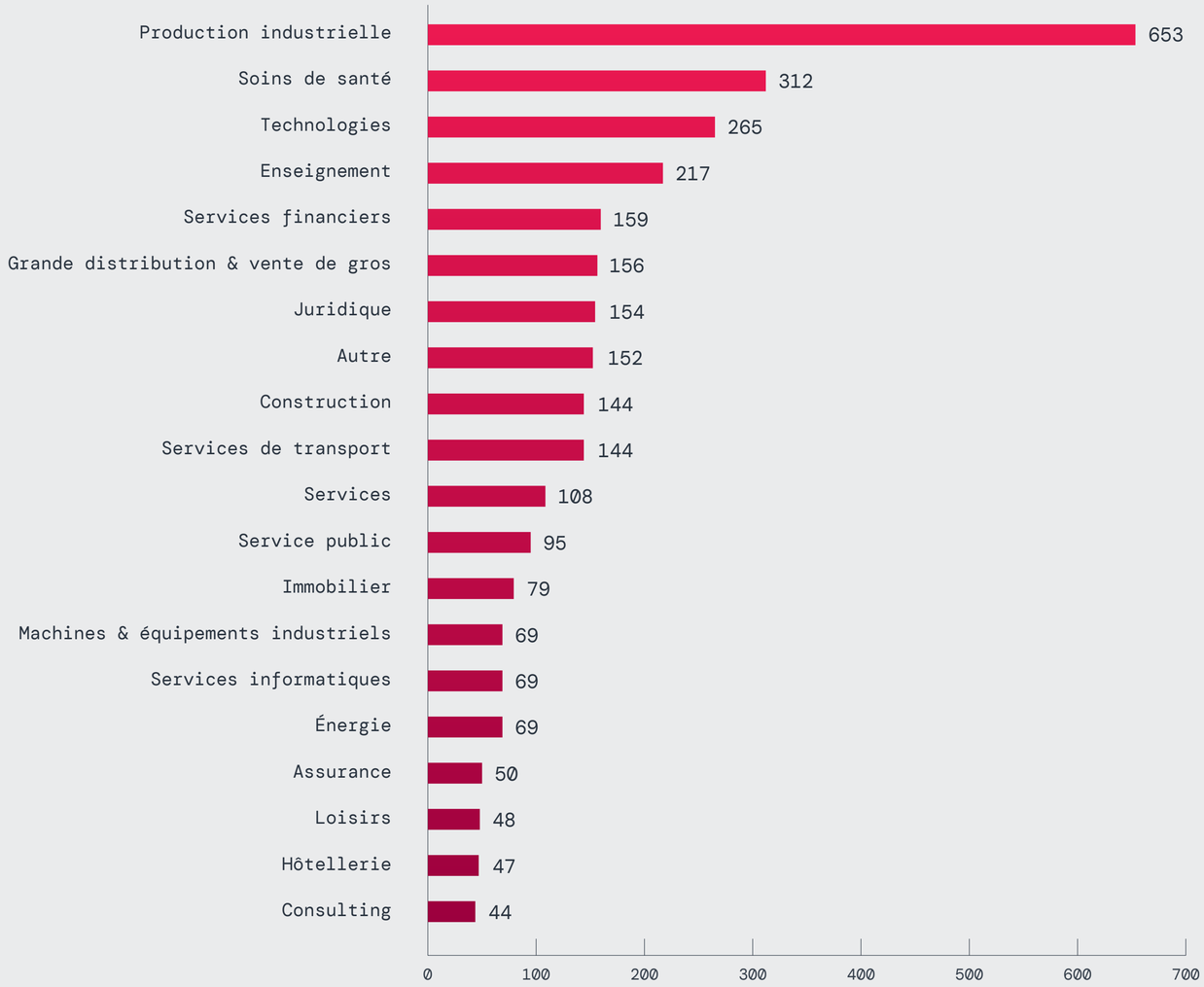


Illustration 1 : Attaques de ransomware par secteur d’activité sur la base des sites de divulgation de données (20 principaux secteurs uniquement).

Tendances d’une année sur l’autre

Le secteur de l’énergie accuse une augmentation annuelle de 527,27 % des attaques de ransomware, probablement en raison de sa nature critique et du potentiel de rançon élevée qu’il offre aux assaillants.

De même, le secteur des restaurants, des bars et des services de restauration enregistre une progression de 333,33 % du nombre d’attaques de ce type. Ceci peut être attribué à la digitalisation rapide du secteur, stimulée par l’adoption de systèmes de points de vente avancés et de plateformes de commande en ligne. Si ces technologies peuvent simplifier les opérations et améliorer l’expérience client, elles introduisent parfois de nouvelles vulnérabilités.

Si cette hausse met en évidence la prévalence des attaques par ransomware, elle ne rend pas forcément compte de toute l’étendue des incidents liés à ces derniers. De nombreuses attaques ne sont pas signalées ou sont résolues en toute discrétion par le paiement d’une rançon, sans que le grand public en soit informé. Ces chiffres doivent donc être considérés comme des indicateurs de tendances plus larges en matière de ransomware plutôt que comme une représentation exhaustive de ces menaces.

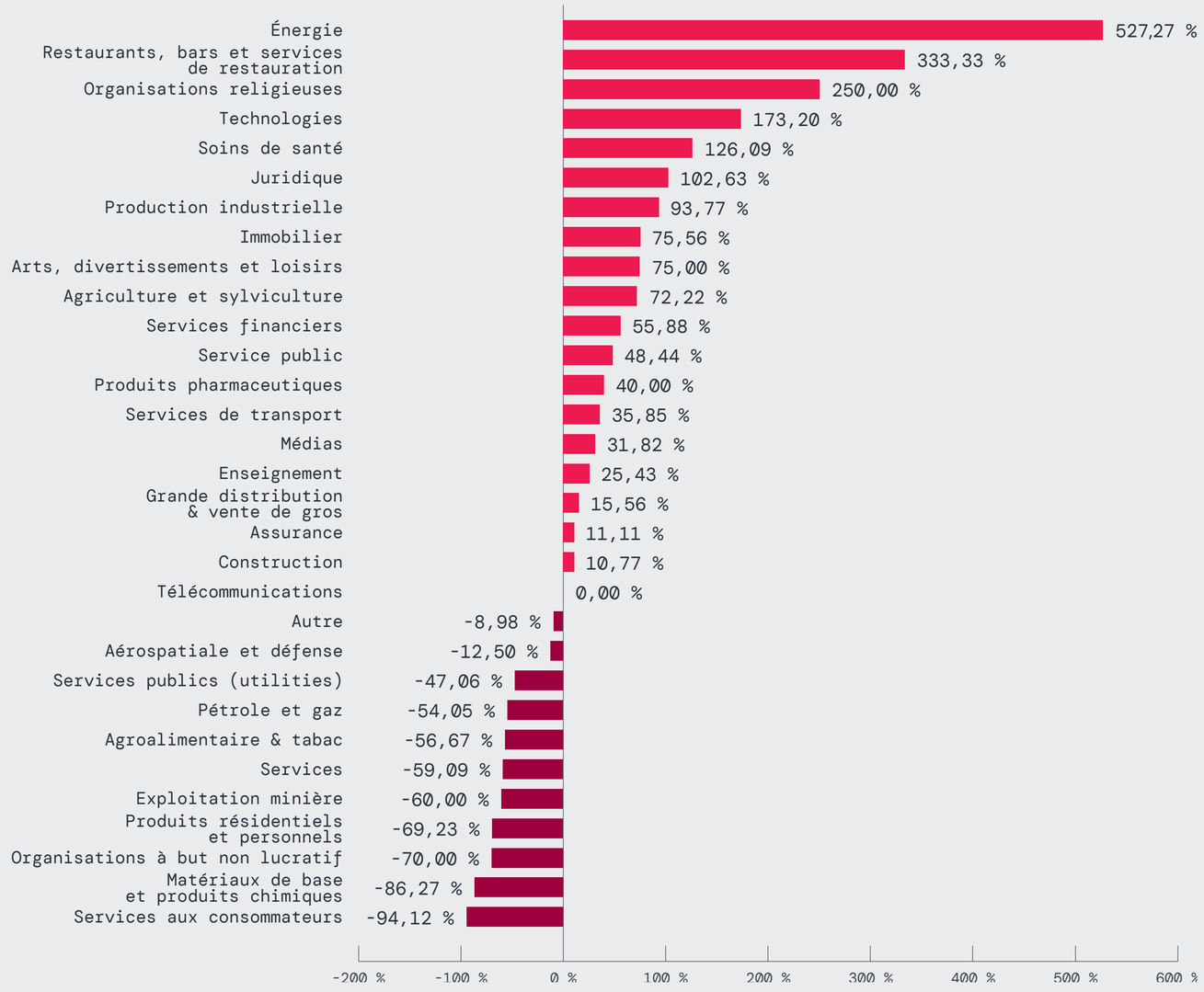


Illustration 2 : Variation en pourcentage d’une année sur l’autre des attaques d’extorsion par ransomware, par secteur d’activité. Il convient de noter que certains secteurs affichaient un volume de base d’attaques relativement faible dans le rapport de l’année dernière. Leur croissance peut ainsi paraître plus substantielle.

Répartition géographique des entreprises victimes

Les États-Unis ont été confrontés à un volume d'attaques de ransomware nettement plus élevé que tout autre pays, comptant environ 50 % de tous les incidents dans le monde. En comparaison, le Royaume-Uni était le deuxième pays le plus ciblé, subissant près de 6 % des attaques de ransomware, suivi par l'Allemagne (4, 09 %), le Canada (3,51 %), et la France (3,26 %). L'illustration 3 propose une carte thermique illustrant les pays touchés par les extorsions de rançons entre avril 2023 et avril 2024.

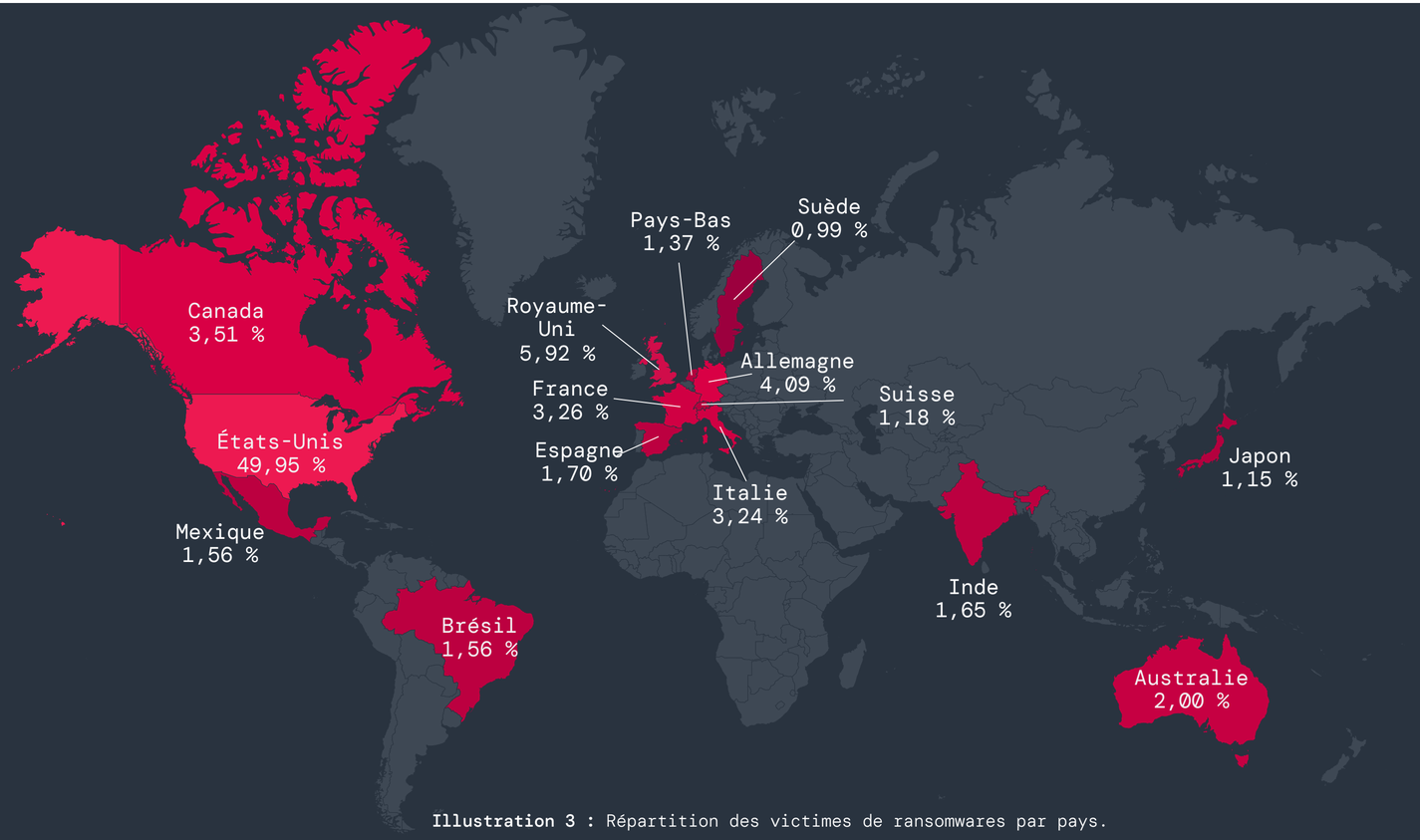


Illustration 3 : Répartition des victimes de ransomwares par pays.

Comprendre la répartition des attaques de ransomware est essentiel pour l'évaluation des risques, l'allocation des ressources, l'élaboration de politiques, la coopération internationale et les efforts de sensibilisation du public dans la lutte contre les menaces de ransomwares.

Évaluation des risques

L'analyse des régions fortement ciblées aide les entreprises de ces zones à évaluer leurs propres niveaux de risque et à renforcer leur cybersécurité. Selon les recherches de ThreatLabz, les États-Unis comptent 50 % des attaques mondiales de ransomwares, ce qui appelle les entreprises situées sur leur territoire à déployer des stratégies de sécurité strictes.

Élaboration de politiques

Les gouvernements peuvent exploiter les enseignements tirés des attaques régionales de ransomware pour orienter leur législation, améliorer les normes de sécurité, promouvoir la coopération internationale et faciliter le partage d'informations entre les secteurs public et privé. À titre d'exemple notable récent, les nouvelles règles de cybersécurité de la SEC marquent une étape majeure dans l'amélioration de la transparence et de la responsabilité dans un contexte de menaces croissantes.

Sensibilisation du public

La mise en évidence des pays fréquemment ciblés peut inciter les particuliers, les entreprises et les gouvernements à prendre des mesures plus proactives de formation à la cybersécurité, de planification de la réponse aux incidents et d'investissement dans des technologies défensives.

Affectation des ressources

Les données ciblées permettent aux gouvernements et aux entreprises d'allouer des ressources de manière stratégique, améliorant ainsi leur posture de sécurité en privilégiant l'accompagnement, le financement et l'expertise dans les domaines où les niveaux de menace sont les plus élevés.

Coopération internationale

L'identification des pays les plus ciblés permet de coordonner les efforts entre les forces de l'ordre, les entreprises et les gouvernements pour lutter contre les ransomwares aux niveaux national et international. L'opération Duck Hunt et l'opération Endgame illustrent la façon dont cette coopération internationale peut peser sur les activités cybercriminelles.

Tendances d’une année sur l’autre

ThreatLabz a comparé les chiffres des attaques de ransomware présentés dans le rapport de cette année par rapport à ceux du rapport ThreatLabz 2023 sur les ransomwares, pour ainsi identifier les évolutions. Parmi les 15 pays les plus ciblés, les États-Unis ont connu une progression notable de 101,88 % d’une année sur l’autre, tandis que la Suède affiche une envolée de 350 %, bien que le pays ne représente qu’une part nettement inférieure du volume total des attaques.

Si l’analyse des tendances en matière de ransomware au niveau mondial est inestimable, les évolutions spécifiques dans les différentes régions du monde méritent également d’être analysées. L’étude des répartitions régionales aide les entreprises à élaborer des plans de sécurité sur mesure et permet aux gouvernements d'élaborer des politiques de cybersécurité plus efficaces.

ÉVOLUTION DES ATTAQUES DE RANSOMWARE DANS LES 15 PRINCIPAUX PAYS CIBLÉS

Pays	Attaques de ransomware par pays (2023)	Attaques de ransomware par pays (2024)	Évolution en pourcentage
États-Unis d’Amérique	902	1 821	101,88 %
Royaume-Uni	144	216	50,00 %
Allemagne	110	149	35,45 %
Canada	151	128	-15,23 %
France	87	119	36,78 %
Italie	63	118	87,30 %
Australie	69	73	5,80 %
Brésil	38	57	50,00 %
Espagne	36	62	72,22 %
Mexique	31	57	83,87 %
Pays-Bas	17	50	194,12 %
Inde	62	60	-3,23 %
Suisse	32	43	34,38 %
Japon	44	42	-4,55 %
Suède	8	36	350,00 %

Illustration 5 : Comparaison d’une année sur l’autre des attaques de ransomware par pays.

ÉVOLUTION DES TAUX D’ATTAQUE PAR RANSOMWARE DANS LA RÉGION EMEA

Pays	Entreprises impactées par des attaques de ransomware (2023)	Entreprises impactées par des attaques de ransomware (2024)	Évolution en pourcentage
Royaume-Uni	144	216	50,00 %
Allemagne	110	149	35,45 %
France	87	119	36,78 %
Italie	63	118	87,30 %
Espagne	36	62	72,22 %
Pays-Bas	17	50	194,12 %
Suisse	32	43	34,38 %
Suède	8	36	350,00 %
Belgique	16	34	112,50 %
Afrique du Sud	13	24	84,62 %
Autriche	15	24	60,00 %
Émirats arabes unis	12	21	75,00 %

Illustration 6 : Comparaison d’une année sur l’autre des attaques de ransomware par pays dans la région EMEA.

ÉVOLUTION DES TAUX D’ATTAQUES PAR RANSOMWARE DANS LA RÉGION APAC

Pays	Entreprises impactées par des attaques de ransomware (2023)	Entreprises impactées par des attaques de ransomware (2024)	Évolution en pourcentage
Australie	69	73	5,80 %
Inde	62	60	-3,23 %
Japon	44	42	-4,55 %
Thaïlande	13	25	92,31 %
Indonésie	15	23	53,33 %
Malaisie	14	20	42,86 %
Taïwan	23	17	-26,09 %
Philippines	7	16	128,57 %
Singapour	8	16	100,00 %
Chine	21	15	-28,57 %
République de Corée	12	10	-16,67 %
Vietnam	10	10	0,00 %

Illustration 7: Comparaison d’une année sur l’autre des attaques de ransomware par pays dans la région APAC.

Groupes de ransomwares les plus actifs en 2023-2024

LockBit (22,1 %), Black Cat (9,2 %) et 8Base (7,9 %) étaient les groupuscules d'extorsion par ransomware les plus actifs au cours de l'année écoulée, chacun étant à l'origine d'un nombre considérable d'attaques. L'illustration 8 montre le nombre de victimes de fuites de données par famille de ransomwares au cours de cette période.

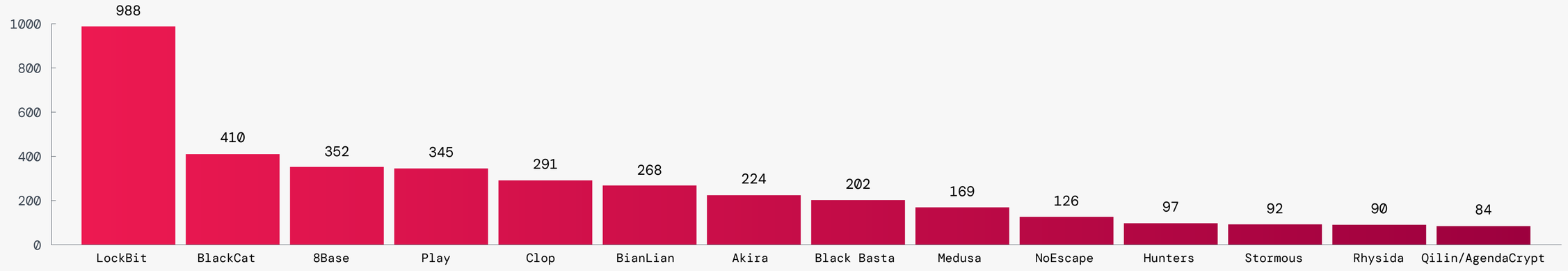


Illustration 8 : Attaques de ransomware répertoriées sur des sites malveillants de divulgation de données.

Les groupuscules de ransomware les plus récents

L'illustration 9 présente une chronologie des nouveaux groupes de ransomwares ayant commencé à publier des données sur des sites de divulgation dans le cadre de leur stratégie d'extorsion.

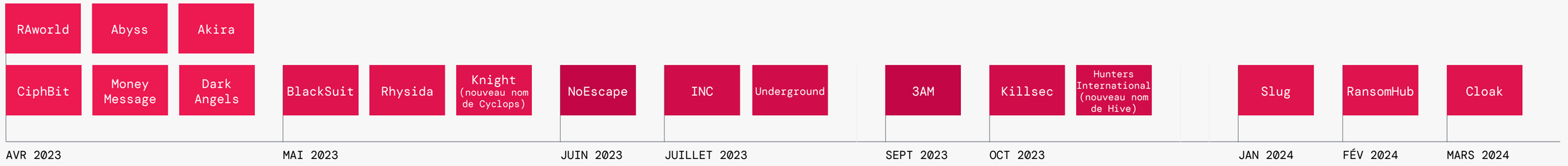


Illustration 9 : Nouveaux groupuscules de ransomwares avec sites de divulgation de données.

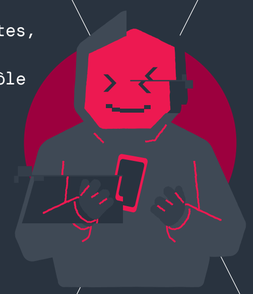
Principales vulnérabilités utilisées lors des attaques par ransomware

Les vulnérabilités des logiciels, des systèmes et de l'infrastructure digitale globale peuvent servir de passerelles d'entrée pour les attaques de ransomware. Les entreprises doivent être conscientes de ces vulnérabilités et prendre des mesures proactives pour y remédier.

La Cybersecurity & Infrastructure Security Agency (CISA) américaine tient à jour une liste complète de vulnérabilités[5], notamment celles activement exploitées par les groupes de ransomwares. Il est vivement recommandé aux entreprises de surveiller de près cette liste et d'appliquer sans attendre les mesures de restauration des vulnérabilités qui y sont mentionnées. Une gestion proactive des vulnérabilités est essentielle pour renforcer la posture globale de cybersécurité de chaque entreprise.

Dans de nombreux cas, les vulnérabilités qu'exploitent les ransomwares impactent les ressources constitutives de la surface d'attaque externe des entreprises et connectées à Internet, telles que les passerelles, les VPN et autres technologies de connectivité à distance. Parce qu'elles sont accessibles depuis Internet, ces vulnérabilités sont beaucoup plus faciles à identifier et à exploiter par les acteurs malveillants. Les dernières directives de la CISA[6] soulignent en outre la criticité des vulnérabilités des VPN et des solutions de connectivité à distance, conseillant l'adoption d'approches les plus modernes, telles que l'architecture Zero Trust, le SSE et le SASE, qui offrent toutes des politiques de contrôle d'accès granulaires.

Au cours de l'année écoulée, d'importantes familles de ransomwares ont ciblé et exploité les vulnérabilités présentées dans l'illustration 10, impactant ainsi un large éventail de systèmes.



ConnectWise ScreenConnect
(exploité par LockBit, Black Basta et Bl00dy)

- CVE-2024-1708 : permet aux hackers d'obtenir un accès non autorisé à des répertoires et des fichiers au-delà des zones restreintes, entraînant la divulgation d'informations et le contrôle des systèmes compromis.
- CVE-2024-1709 : permet aux hackers de contourner les mécanismes d'authentification et d'accéder directement aux informations confidentielles ou aux systèmes critiques.

Logiciels ASA et FTD de Cisco
(exploités par Akira)

- CVE-2020-3259 : permet à des hackers distants non authentifiés de récupérer le contenu de la mémoire d'un appareil compromis, entraînant ainsi la divulgation d'informations confidentielles.

Fonctionnalité VPN d'accès à distance de Cisco
(exploitée par Akira)

- CVE-2023-20269 : permet à des hackers distants non authentifiés de mener des attaques par force brute pour identifier des paires valides de nom d'utilisateur et de mot de passe, et à des hackers distants authentifiés d'établir une session VPN SSL sans client avec un utilisateur non autorisé.

Citrix NetScaler ADC et NetScaler Gateway
(exploités par INC Ransom, LockBit et BlackCat)

- CVE-2023-4966 (alias Citrix Bleed) : permet aux hackers de contourner l'authentification par mot de passe et le MFA pour obtenir un accès non autorisé aux réseaux à l'aide de jetons de session ayant fuité.
- CVE-2023-3519 : permet aux hackers d'exploiter des failles pour exécuter des logiciels à distance.

Illustration 10 : Vulnérabilités les plus répandues d'avril 2023 à avril 2024.

Les correctifs disponibles pour ces vulnérabilités doivent être appliqués au plus vite, ainsi que les mesures suivantes :

- Désactiver l'accès à distance vers les serveurs
- Utiliser des mots de passe forts et une authentification multifactorielle
- Surveiller les serveurs afin de détecter toute activité suspecte

[5] Cybersecurity & Infrastructure Security Agency, **Known Exploited Vulnerabilities Catalog**, consulté le 25 juin 2024.
[6] Cybersecurity & Infrastructure Security Agency, **Modern Approaches to Network Access Security**, 18 juin 2024.

Tour d'horizon des ransomwares : ce qui fait la une de l'actualité

Les ransomwares sont omniprésents et ciblent tous les secteurs. Lorsqu'un groupuscule est démantelé, il émerge à nouveau ou cède la place à un nouveau pair. Voici des études de cas qui mettent en lumière l'évolution constante des ransomwares.

Le fléau des ransomwares dans le secteur des soins de santé

Le secteur de la santé, confronté à d'importants défis tout au long de 2023 et jusqu'en 2024, a été une cible privilégiée des acteurs du ransomware. Les perturbations des opérations de soins de santé ont de lourdes conséquences : des ambulances sont re-routées, des ordonnances sont retardées et des procédures médicales essentielles doivent être reportées. En outre, le vol de données de santé sensibles peut avoir des conséquences considérables, notamment le vol d'identité et les fraudes aux soins de santé, ce qui accentue les vulnérabilités dans l'écosystème des soins de santé.

PAIEMENT DES RANÇONS : DES CONSÉQUENCES INATTENDUES

Un fournisseur de solutions de paiement pour le secteur de la santé a été victime d'une attaque de ransomware orchestrée par le groupe BlackCat. Il s'est conformé aux exigences des hackers et a réglé une rançon faramineuse de 22 millions de dollars. Pourtant la suite a pris une tournure inattendue. BlackCat est revenu sur sa promesse de partager une partie de la rançon avec l'affilié à l'origine de l'attaque (« exit scam »), ce qui a incité l'affilié à menacer le prestataire de soins de santé de divulguer des données sensibles.

Il faut croire que les voleurs n'ont aucun code de l'honneur, ce qui le cas pour les attaques de ransomware. Le paiement d'une rançon ne vaut pas garantie que les données détournées ne seront pas divulguées ou supprimées. De plus, certains outils de déchiffrement des ransomwares contiennent des bugs qui empêchent la restauration des données ou qui la rendent plus bien chronophage qu'une restauration à partir d'une sauvegarde.

DOUBLE EXTORSION... ET DEUX FOIS VICTIME

En février 2023, un important distributeur pharmaceutique américain a confirmé que ses systèmes informatiques avaient été compromis. L'incident a impacté une de ses filiales et les fichiers dérobés ont été divulgués par le groupuscule de ransomware Lorenz.[7] Puis, en février 2024, le même distributeur a subi une autre attaque de ransomware.[8] Cette tendance, de plus en plus observée par ThreatLabz, donne lieu à une entreprise qui subit plusieurs incidents de ransomware en l'espace d'un an.

[7] BleepingComputer, **Drug distributor AmerisourceBergen confirms security breach**, 8 février 2023.
[8] BleepingComputer, **Pharmaceutical giant Cencora says data was stolen in a cyberattack**, 27 février 2024.

Impact de la décision de la SEC sur la cybersécurité

En 2023, la SEC, le gendarme de la bourse aux États-Unis, a introduit de nouvelles règles de divulgation des incidents de cybersécurité afin de renforcer la transparence et la responsabilité des sociétés cotées en bourse. Depuis le 15 décembre 2023, ces règles imposent la déclaration des incidents de cybersécurité majeurs et exigent auprès des entreprises des informations détaillées sur leur gestion, leur stratégie et leur gouvernance des risques de cybersécurité. Le règlement de la SEC impose de signaler les incidents de cybersécurité majeurs dans les quatre jours ouvrables suivant la détermination de l'importance relative de l'incident et de ses dommages par l'entreprise victime. De plus, le formulaire 10-K exige désormais un rapport annuel sur la gestion et la stratégie des risques de cybersécurité, pour les exercices comptables se clôturant au 15 décembre 2023 ou après cette date. Les acteurs privés étrangers doivent également se conformer à des informations similaires sur le formulaire 6-K et le formulaire 20-K.

Ces décisions constituent un nouveau défi pour les acteurs du ransomware qui proposent des négocier le paiement de rançon aux sociétés cotées en bourse, puisque ces dernières restent tenues de divulguer les détails de toute attaque réussie. Point positif, ce nouveau cadre pèse sur les attaques d'extorsion sans chiffrement, une tendance émergente par laquelle les assaillants n'utilisent que la menace de divulguer les données détournées pour exiger des rançons.

L'IMPACT DE CES NOUVELLES RÈGLES SUR LES ENTREPRISES

Les décisions de la SEC en matière de cybersécurité peuvent faire émerger des problématiques majeures de conformité et de gestion des risques parmi les entreprises. Bien que destinées à améliorer la transparence et la protection des investisseurs, ces règles obligent les entreprises à se conformer à des exigences de déclaration complexes et à divulguer rapidement tout incident majeur.

Il en résulte une pression renforcée sur les entreprises pour qu'elles quantifient et évaluent les cyberincidents avec précision. Déterminer l'importance et l'impact potentiel des cyberincidents exige une analyse minutieuse, qui peut s'avérer coûteuse et obliger les entreprises (grandes et petites) à repenser leurs protocoles de réponse aux incidents et à mettre à jour leurs processus de déclaration pour répondre aux exigences de la SEC.

En outre, les délais de mise en conformité varient en fonction de la taille des entreprises, ce qui ajoute encore un niveau de complexité. Les petites sociétés disposent souvent de délais de mise en conformité différents, et généralement plus longs que leurs homologues plus grandes. Et même si les grandes entreprises doivent respecter des délais plus serrés, elles disposent généralement de davantage de ressources pour analyser l'importance d'un incident de cybersécurité.

Les nouvelles exigences de divulgation éliminent également la possibilité pour les entreprises côtés en bourse de régler des rançons en toute discrétion, pour éviter de mettre en péril leur image de marque ou toute réaction négative résultant d'une notification publique d'informations sur un incident.

CERTAINES ENTREPRISES ENFREIGNENT DÉJÀ LES RÈGLES DE LA SEC

Malgré les directives claires de la SEC, certaines entreprises ne respectent déjà pas ces nouvelles règles de cybersécurité. De récentes divulgations émanant d'entreprises bien connues ont soulevé des interrogations quant à la conformité et à la pertinence de leur rapport d'incidents.[9] Nombre de ces rapports de divulgation manquent de données quantitatives et d'évaluations détaillées des implications financières et opérationnelles des cyberincidents, ce qui est précisément ce que la SEC exige désormais. Cette tendance des sociétés à fournir des informations parcellaires sur les cyberincidents en dépit de la décision de la SEC pourrait aboutir à un renforcement de la surveillance réglementaire afin de garantir une conformité cohérente et efficace.

Les décisions de cybersécurité de la SEC constituent un changement réglementaire important censé améliorer la transparence et la responsabilisation des entreprises en matière de reporting sur les incidents. Le respect de ces nouvelles règles, en toute bonne foi, exigera une collaboration permanente entre les régulateurs, les entreprises et les parties prenantes du secteur.

[9] Forbes, **Companies Are Already Not Complying With The New SEC Cybersecurity Incident Disclosure Rules**, 4 mars 2024.

Impact des actions des forces de l'ordre

Qakbot impacté par l'opération « Duck Hunt »

Le 29 août 2023, dans le cadre d'un effort multinational coordonné, le Federal Bureau of Investigation (FBI) et le Department of Justice (DOJ) américains ont révélé l'opération Duck Hunt. Zscaler ThreatLabz a fourni une assistance technique aux forces de l'ordre dans le cadre de cette opération.[10] L'infrastructure de Qakbot a été conçue pour résister aux tentatives de démantèlement grâce à une infrastructure à plusieurs niveaux, comme le montre l'illustration 11.

Cette infrastructure offrait plusieurs niveaux de résilience, chaque niveau nécessitant des efforts coordonnés pour être démantelé. Le premier niveau de l'infrastructure de Qakbot comprenait des systèmes infectés exécutant un plugin supernode qui relayait le trafic en amont vers plusieurs proxys conçus pour masquer le serveur backend de Qakbot.

L'opération Duck Hunt a redirigé les serveurs proxy en amont du supernode vers un ensemble de gouffres DNS (serveurs sinkhole) pour prendre immédiatement le contrôle de l'infrastructure de Qakbot, comme le montre l'illustration 12.

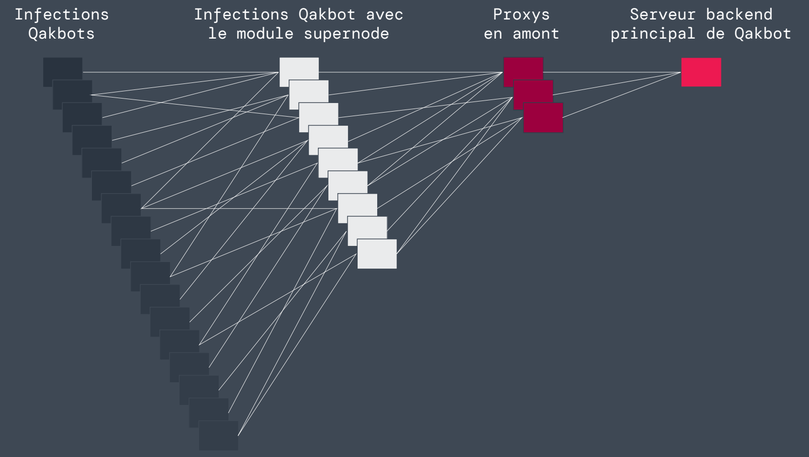


Illustration 11 : Infrastructure à plusieurs niveaux de Qakbot.

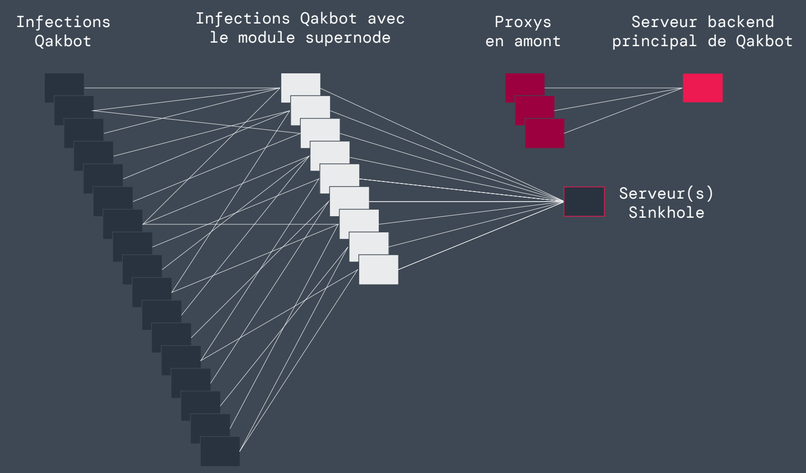


Illustration 12 : Architecture Qakbot après redirection des proxys amont de chaque supernode.

Une fois que le FBI a détourné les supernodes, les serveurs sinkhole ont demandé aux ordinateurs des victimes de télécharger un shellcode qui charge une DLL capable de neutraliser le malware. Cette approche a permis de désinfecter les ordinateurs des victimes et a empêché de nouvelles attaques.

Au moment de son démantèlement, Qakbot avait déjà infecté plus de 700 000 ordinateurs dans le monde, dont plus de 200 000 aux États-Unis.[11] Avant son démantèlement, **Qakbot était actif depuis près de 15 ans**, initialement conçu pour faciliter la fraude par carte de crédit et par virement. En 2019, le groupe est devenu un courtier d'accès initial pour des groupuscules de ransomwares, notamment Conti, ProLock, Egregor, REvil, MegaCortex et Black Basta.

Le malware Qakbot s'est propagé essentiellement par des e-mails de spam contenant des pièces jointes ou des liens malveillants. Une fois un système infecté, Cobalt Strike y était fréquemment déployé pour permettre un déplacement latéral et éventuellement déployer un ransomware.

Malheureusement, aucune arrestation n'a eu lieu et les auteurs de la menace n'ont pas été inculpés. Qakbot **a refait surface en décembre 2023**. Le groupe a actualisé le malware pour qu'il prenne en charge les versions 64 bits de Windows, a changé le format de configuration interne et a modifié les communications réseau pour qu'ils utilisent le chiffrement AES. Comme nous le verrons plus loin dans ce rapport, les auteurs de Qakbot ont considérablement modifié leurs Techniques, Tactiques et Procédures (TTP) depuis l'opération Duck Hunt.

[10] US Department of Justice, **Qakbot Malware Disrupted in International Cyber Takedown**, 29 août 2023.
[11] TechCrunch, **How the FBI took down the notorious Qakbot botnet**, 1er septembre 2023.

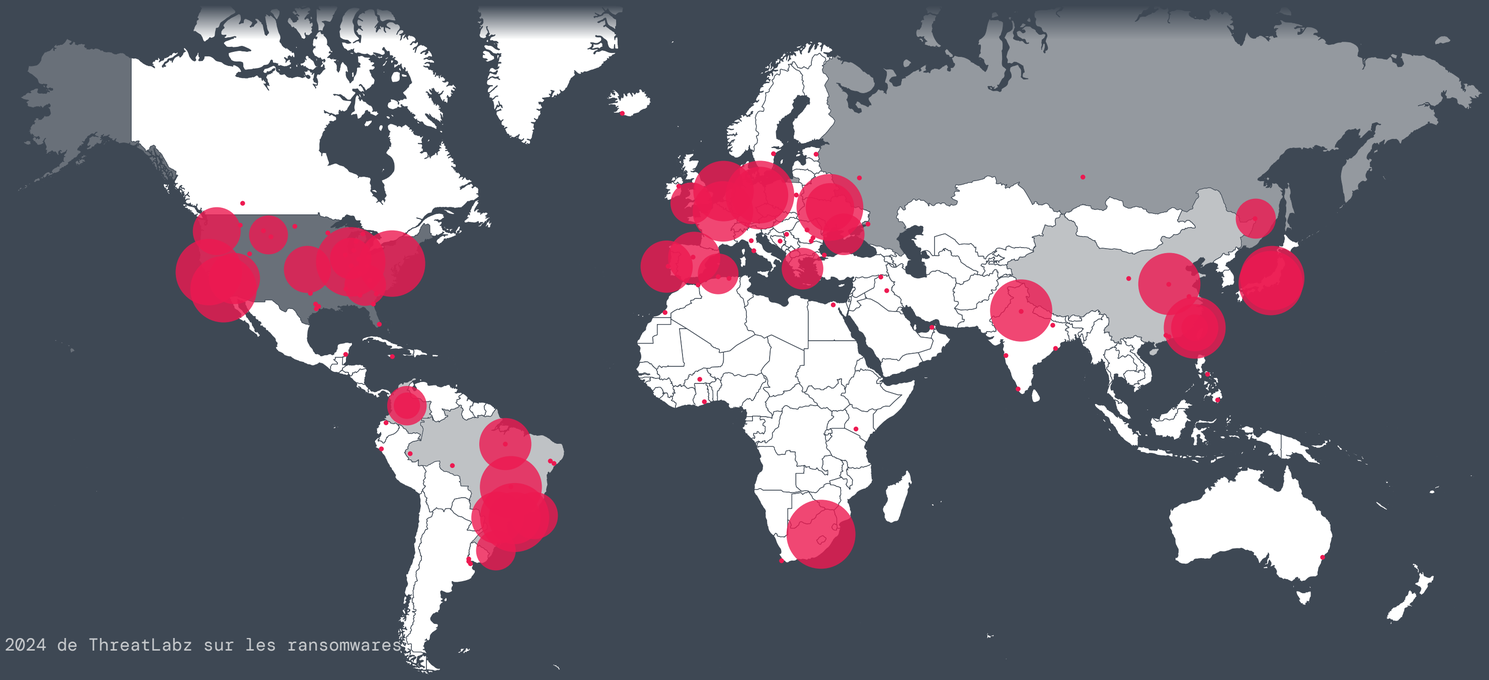
« L'opération Endgame » a ciblé simultanément plusieurs brokers d'accès initial

Le 28 mai 2024, en collaboration avec de nombreux acteurs internationaux des forces de l'ordre, Europol a annoncé l'opération Endgame, qui visait simultanément plusieurs brokers d'accès initial. Cette opération a donné lieu à plus d'une douzaine de perquisitions au niveau mondial, à plusieurs arrestations et à la fermeture de plus de 100 serveurs utilisés pour des activités criminelles. Ces serveurs permettaient le fonctionnement de différents outils de téléchargement de malware (des « loaders ») qui avaient servi à infiltrer les ordinateurs des victimes, pour déployer des malwares, et notamment des ransomwares.

Les familles de malwares ciblées par cette opération étaient responsables de l'infection de millions d'ordinateurs dans le monde, notamment dans des établissements de santé et dans le cadre de services d'infrastructures critiques. Cette opération a donné lieu à des actions menées contre SmokeLoader, Pikabot, Bumblebee et IcedID.

Zscaler ThreatLabz a fourni une assistance technique essentielle pour le sinkhole SmokeLoader et les efforts de remédiation lors de l'opération Endgame.

SmokeLoader, actif depuis 2011, était utilisé par plusieurs courtiers d'accès initial pour les ransomwares, notamment Raspberry Robin et le gang de ransomware Stop (alias DJVU). L'opération Endgame a permis de saisir plus de 1 000 domaines SmokeLoader exploités par ces groupuscules malveillants. Les domaines ont ensuite été redirigés vers un serveur sinkhole contrôlé par les forces de l'ordre. La carte de l'illustration 13 représente les systèmes infectés qui ont communiqué avec le sinkhole SmokeLoader.



Cette carte témoigne de la portée mondiale considérable de SmokeLoader, avec des infections notables en Amérique latine, en Asie, en Amérique du Nord et en Europe.

Illustration 13 : Carte des systèmes infectés par SmokeLoader communiquant avec le sinkhole de l'opération Endgame. (Source : Zscaler Threatlabz)

Lorsque les systèmes infectés par SmokeLoader se connectaient au serveur sinkhole, ils recevaient un utilitaire intégré de désinstallation du malware. À ce jour, plus de 40 000 systèmes infectés par SmokeLoader ont été nettoyés, comme en témoigne l'illustration 14.

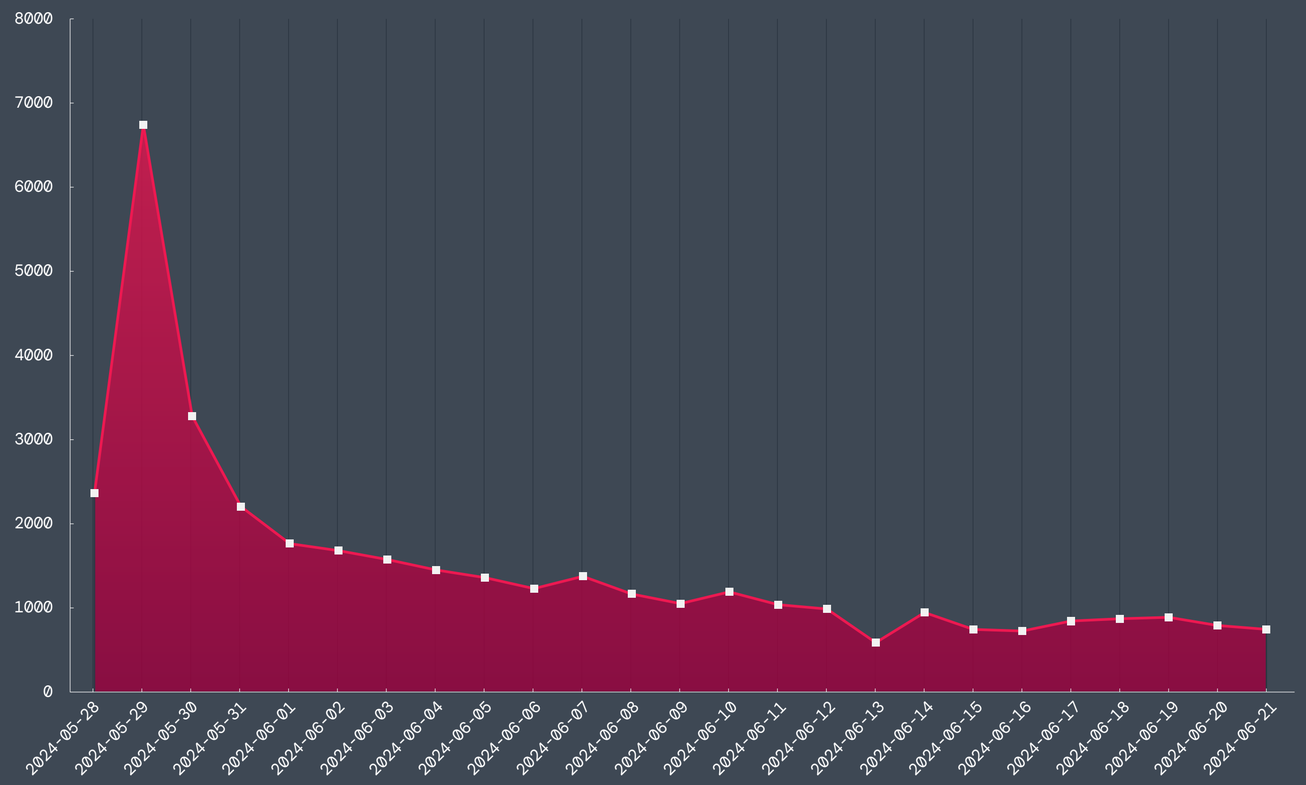


Illustration 14 : Systèmes SmokeLoader nettoyés suite à l'opération Endgame.

Pikabot est apparu au début de l'année 2023 et a affiché une activité importante au cours du second semestre. Ce dynamisme est imputable au fait que le malware est devenu le courtier d'accès initial de choix pour le ransomware Black Basta, suite à l'opération Duck Hunt sur Qakbot. En février 2024, **Pikabot est réapparu avec des changements importants** dans son code logiciel et dans sa structure. ThreatLabz a observé que Pikabot déployait régulièrement **Cobalt Strike** et Meterpreter de **Metasploit**.

Bumblebee, introduit en mars 2022, est lié à l'ancien groupe de ransomware Conti. Le malware a succédé à l'outil malveillant BazarLoader, utilisé pour obtenir un accès initial lors des attaques des ransomwares Conti et Diavol. À plusieurs reprises, ThreatLabz a observé que BazarLoader et Bumblebee déployaient des payloads Cobalt Strike pour favoriser le déplacement latéral. Bumblebee a également été associé aux attaques de ransomware Akira et Black Basta.

Semblable à Qakbot, IcedID a été conçu à l'origine comme un cheval de Troie bancaire lorsqu'il est apparu en 2017. Le malware a ensuite toutefois changé d'objectif pour servir de courtier d'accès initial pour les ransomwares. Au fil des années, le code malveillant d'IcedID a été détourné et modifié à diverses fins. En outre, les mêmes développeurs ont créé un nouveau loader de malwares connu sous le nom de Latrodectus, rendu public en novembre 2023, qui a probablement également été utilisé pour déployer des ransomwares.

Après l'opération Endgame, la plupart de ces courtiers d'accès initiaux ont vu leur activité ralentir, **à l'exception de Latrodectus**, qui a refait surface en moins d'un mois. Toutefois, l'accalmie risque d'être de courte durée à mesure que les acteurs malveillants se regroupent.

Le ransomware Hive renaît sous le nom de Hunters International

En janvier 2023, l'infrastructure du ransomware Hive a été mise hors service. Le résultat d'une opération secrète de sept mois. Le FBI a réussi à infiltrer les serveurs de Hive, récupérant plus de 300 clés de déchiffrement qui ont permis d'éviter le paiement d'environ 130 millions de dollars de rançons. Actif depuis juin 2021, le collectif Hive a ciblé et compromis plus de 1 500 entreprises dans le monde, amassant plus de 100 millions de dollars de paiements de rançons.[12] Les victimes étaient notamment des hôpitaux, des districts scolaires, des institutions financières et diverses autres entités. Aucune arrestation associée à Hive n'a toutefois été effectuée et le groupe s'est rebaptisé Hunters International en octobre 2023. Les cybercriminels utilisent souvent cette stratégie de changement de nom après une perturbation majeure.

Le groupuscule a changé son mode opératoire : il n'offrira plus de réductions ni ne négociera avec les victimes concernant la demande de rançon initiale, comme le montre l'illustration 15.

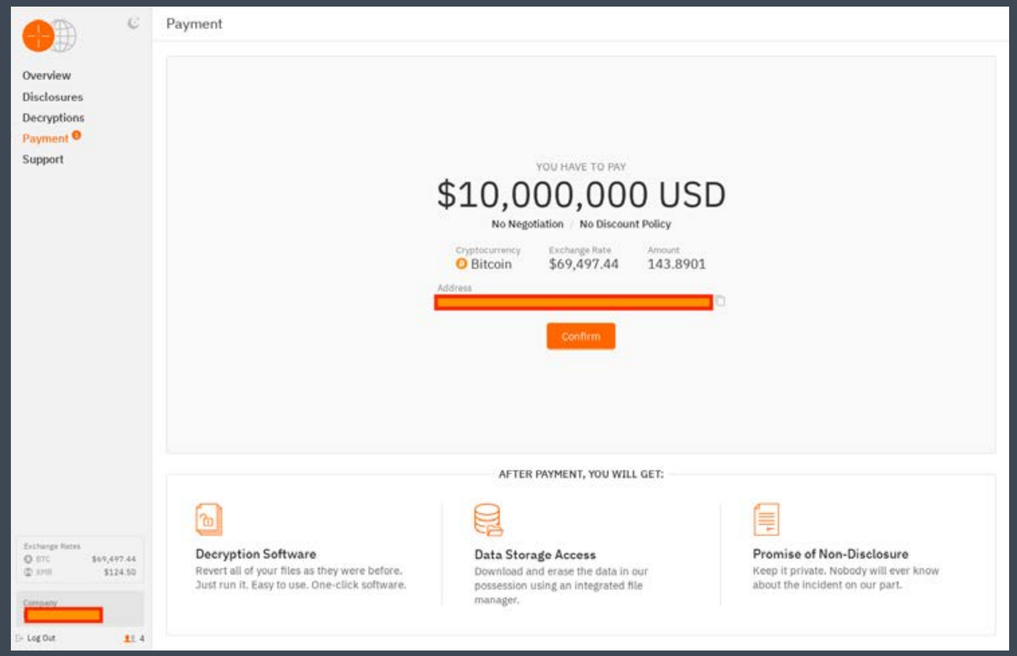


Illustration 15 : Portail des victimes de Hunters International, sans remise ni négociation sur les rançons.

Un politique de prix ferme, non négociable, est **très rare** dans l'univers des ransomwares. En effet, des rabais importants sur la rançon exigée initialement sont monnaie courante. Cette décision de l'équipe Hunters entraînera probablement une baisse du nombre des paiements, mais les montants de ces paiements devraient progresser.

Hunters International continue de lancer de nouvelles attaques et restera probablement une menace redoutable faute de nouvelles arrestations et d'inculpation de ses auteurs.

[12] US Department of Justice, **U.S. Department of Justice Disrupts Hive Ransomware Variant**, 26 janvier 2023.

Top 5 des ransomwares à surveiller en 2024-2025

Alors que la complexité et la sophistication des ransomwares et autres cybermenaces ne cessent d'évoluer, il est essentiel de se tenir informé des familles de ransomwares les plus répandues et dangereuses afin d'optimiser sa posture de sécurité. Cette section met en lumière cinq familles de ransomwares qui induisent certains des risques les plus critiques pour les entreprises, avec un aperçu de leurs tactiques, de leur impact potentiel et de leur récente activité.

1. Dark Angels

Le groupe de ransomware Dark Angels, qui exploite le site de divulgation de données Dunghill, a vu le jour aux alentours de mai 2022. Il a mené certaines des plus importantes attaques de ransomware, tout en réussissant à n'attirer qu'une attention minime. Début 2024, ThreatLabz a découvert qu'une victime avait versé 75 millions de dollars à Dark Angels, soit un montant record qui ne manquera pas de susciter l'intérêt d'autres assaillants cherchant à reproduire un tel succès en adoptant leurs tactiques de ce groupe (que nous décrivons ci-dessous). Dark Angels cible divers secteurs, dont la santé, les administrations, la finance et l'enseignement. Plus récemment, ils ont également exécuté des attaques contre de grandes entreprises industrielles, technologiques et de télécommunications.

Dark Angels adopte une approche très ciblée, s'en prenant généralement qu'à une seule grande entreprise à la fois. Cette attitude contraste fortement avec la plupart des groupes de ransomwares, qui ciblent les victimes sans discernement et sous-traitent la plupart des attaques à des réseaux affiliés de courtiers d'accès initial et à des équipes réalisant des tests d'intrusion. Une fois que Dark Angels a identifié et piraté une cible, il décide de manière sélective de chiffrer ou non les fichiers de l'entreprise. Dans la plupart des cas, ce ransomware détourne des volumes importants de données, généralement de l'ordre de 1 à 10 To. Sur les grandes entreprises, le groupe a exfiltré entre 10 et 100 To de données, dont le transfert peut prendre des jours, voire des semaines.

L'attaque la plus médiatisée menée par Dark Angels a eu lieu en septembre 2023, lorsque le groupe a piraté un conglomérat international qui fournit, entre autres services, des solutions pour les systèmes d'automatisation des bâtiments. Dark Angels a exigé une rançon de 51 millions de dollars, a affirmé avoir dérobé plus de 27 To de données professionnelles et a chiffré les machines virtuelles VMware ESXi de la société. Une variante du ransomware RagnarLocker a été utilisée pour chiffrer les fichiers de l'entreprise lors de l'attaque. La relation entre RagnarLocker et Dark Angels n'est pas claire, mais le groupe utilisait déjà ce ransomware avant l'action des forces de l'ordre contre RagnarLocker,[13] qui a abouti à l'arrestation d'un membre clé en octobre 2023. Il convient de noter que lorsque Dark Angels est apparu pour la première fois, il a déployé une variante de Babuk avant de passer à RagnarLocker.

La stratégie de Dark Angels consistant à cibler un petit nombre d'entreprises de grande valeur pour obtenir des paiements importants est une tendance qui mérite d'être surveillée. Zscaler ThreatLabz estime que d'autres acteurs du ransomware tireront les leçons du succès de Dark Angels et pourraient adopter des tactiques similaires, en se concentrant sur des cibles de grande valeur et en renforçant le détournement de données pour maximiser leurs gains financiers.

[13] Europol, **Le gang du ransomware Ragnar Locker démantelé par une opération de police internationale**, 20 octobre 2023.

2. LockBit

LockBit, apparu pour la première fois en septembre 2019, a rapidement pris de l'importance grâce à son vaste réseau d'affiliation. LockBit s'adosse sur des affiliés pour mener des intrusions, exfiltrer des données et déployer son ransomware. L'infiltration commence généralement par des e-mails de spam contenant des pièces jointes ou des liens malveillants. D'autres méthodes consistent à exécuter des attaques par force brute sur les mots de passe qui ciblent les identifiants Remote Desktop Protocol (RDP) ou VPN, à acheter des identifiants compromis par l'intermédiaire de courtiers d'accès initiaux ou encore à pirater des applications exposées à Internet. Les cybercriminels de LockBit ont ciblé nombre de secteurs critiques :production industrielle, soins de santé et logistique notamment. Le groupe a collectivement ciblé plus de 2 000 systèmes dans le monde et extorqué plus de 120 millions de dollars aux victimes.

Au cours de l'année écoulée, LockBit est resté en tête du peloton en termes de volume d'attaque. S'appuyant sur une stratégie nettement différente de celle de Dark Angels, le groupe LockBit encourage ses affiliés à cibler autant d'entreprises que possible, quelle que soit la rétribution potentielle. Ce volume élevé d'attaques explique que les petites entreprises sont souvent ciblées, donnant lieu à des demandes de rançon relativement faibles.

Le ransomware LockBit se déploie sur les systèmes Windows et Linux. Il existe trois versions de LockBit pour Windows : LockBit Red (l'original), LockBit Black (basé sur le code source de BlackMatter) et LockBit Green (basé sur le code source de Conti qui a fuité). Comme mentionné dans le rapport ThreatLabz 2023 sur les ransomware, le builder de LockBit Black a été victime d'une fuite et de nombreux groupes cybercriminels non affiliés à LockBit l'ont utilisé pour leurs propres attaques de ransomware. LockBit Black demeure la variante la plus couramment déployée par le groupe. La variante spécifique du ransomware LockBit utilisée pour chiffrer les fichiers d'une victime est désormais affichée dans la note de rançon à côté de l'identifiant de la victime. Ceci permet au hacker qui mène l'attaque d'identifier la variante de LockBit déployée et l'aide à fournir l'outil de déchiffrement approprié après paiement de la rançon. Voir l'illustration 16 pour un exemple d'une demande de rançon récente avec LockBit Black.

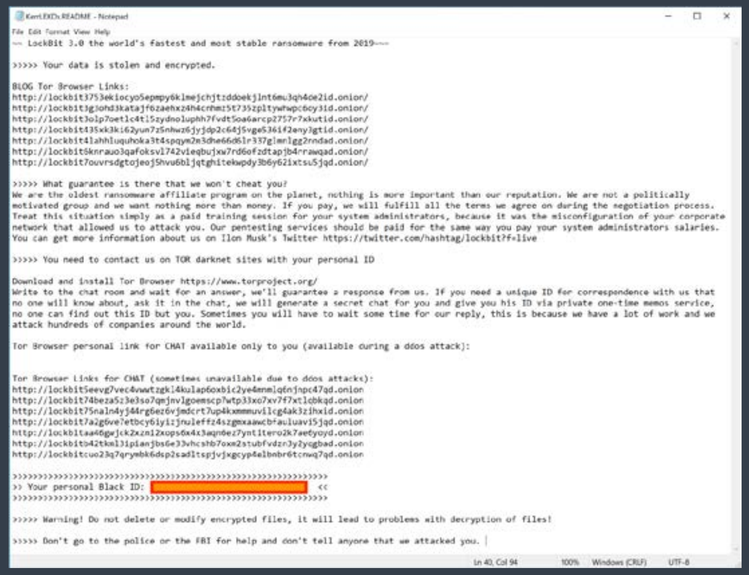


Illustration 16 : Exemple d'une demande de rançon récente avec LockBit Black.

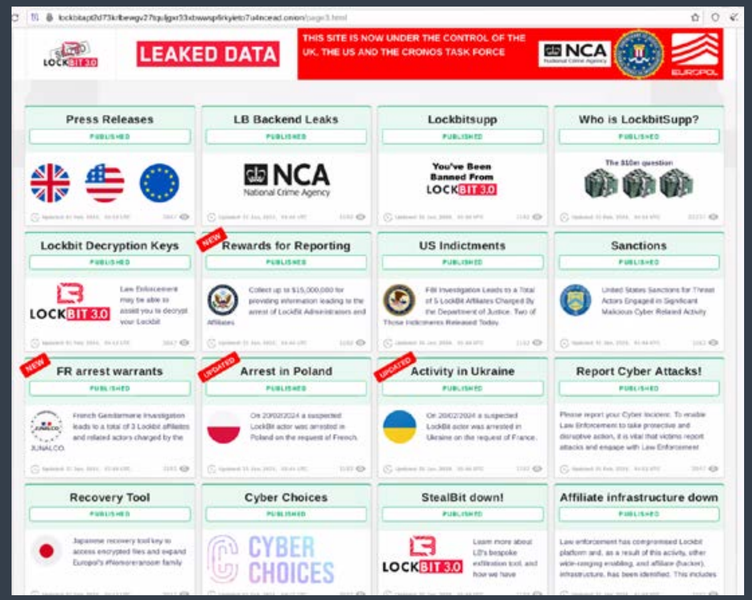


Illustration 17 : Saisie par les forces de l'ordre du site de divulgation de données de LockBit.

Le 20 février 2024, le FBI et les forces de l'ordre britanniques ont saisi une partie de l'infrastructure de LockBit, qui comprenait environ 7 000 clés de déchiffrement de victimes. Après cette opération, les forces de l'ordre ont pris le contrôle du site Web de divulgation de données LockBit et se sont joués des cybercriminels en proposant une version similaire de l'ancien site qui affichaient divers articles et un compte à rebours jusqu'à publication de nouvelles informations, comme le montre l'illustration 17 ci-dessous.

Malheureusement, quelques jours après ce démantèlement, ThreatLabz a identifié de nouvelles attaques de ransomware perpétrées par LockBit et un nouveau site de divulgation de données. Le groupe est resté actif et a attaqué des dizaines de nouvelles entités en aval de l'action des forces de l'ordre.

Le 7 mai 2024, le FBI a annoncé l'inculpation du développeur et opérateur de LockBit, Dmitry Yuryevich Khoroshev. Ce dernier a toutefois rapidement nié que le FBI l'avait correctement identifié. Faute d'arrestations supplémentaires, les attaques LockBit se poursuivront probablement dans un avenir proche, même si ThreatLabz s'attend à ce que la marque LockBit soit abandonnée et que l'opération soit reprise sous une autre dénomination en raison de la surveillance plus intense dont elle fait l'objet.

3. BlackCat

Le ransomware BlackCat, alias ALPHV, lancé en novembre 2021, était l'une des menaces les plus notoires jusqu'à sa dissolution en mars 2024. Semblable à LockBit, BlackCat exploitait un réseau d'affiliation pour lancer des attaques. Les rançons payées étaient partagées avec les affiliés.

L'affilié BlackCat le plus tristement célèbre est sans doute un groupe connu sous le nom de Scattered Spider[14] (alias Star Fraud). Composé de membres anglophones, ce groupe excellait dans les attaques par ingénierie sociale, usurpant souvent l'identité d'un collaborateur d'un service de support ou informatique lors d'appels vocaux, et utilisant la technique du SIM swapping pour déjouer l'authentification multifacteur. Le 15 juin 2024, le chef présumé[15] de Scattered Spider, un ressortissant britannique de 22 ans, a été arrêté. Il est toutefois trop tôt pour connaître l'impact de cette arrestation sur la capacité du groupe à poursuivre ses attaques.

BlackCat était l'un des ransomwares les plus compatibles avec de nombreuses plateformes, en partie parce qu'il repose sur le langage de programmation Rust. L'illustration 18 montre les outils de déchiffrement disponibles pour toutes les plateformes prises en charge par le ransomware BlackCat juste avant que le groupe n'arrête ses opérations. Ces plateformes comprenaient Windows, ESXi, FreeBSD et de nombreuses variantes de systèmes d'exploitation et d'architectures Linux, telles que ARM, x86/x64, et PowerPC.

[14] Cybersecurity & Infrastructure Security Agency, **Cybersecurity Advisory: Scattered Spider**, 16 novembre 2023.
[15] Krebs on Security, **Alleged Boss of 'Scattered Spider' Hacking Group Arrested**, 15 juin 2024.

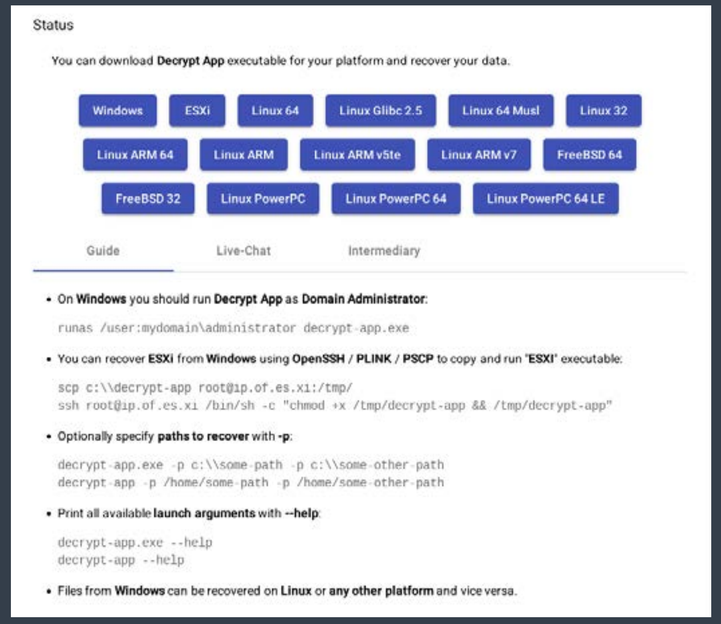


Illustration 18 : Les outils de déchiffrement de BlackCat étaient fournis pour 15 systèmes d'exploitation, architectures et plateformes différents.

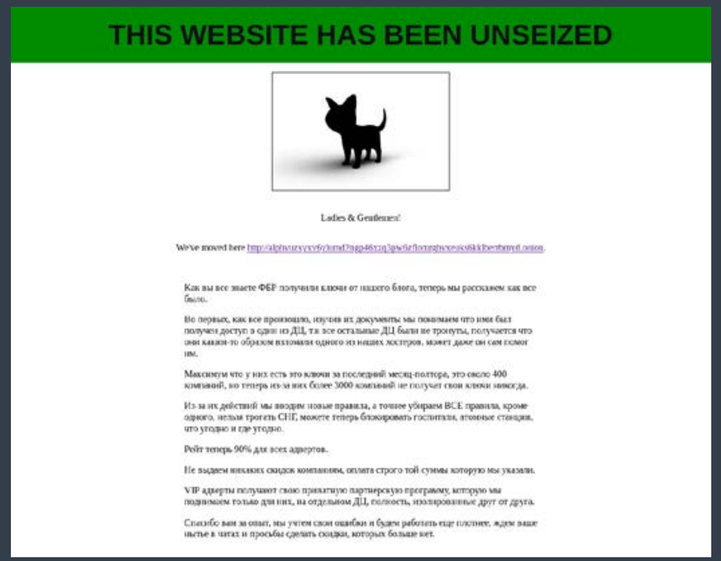


Illustration 19 : Site de divulgation de données de BlackCat, toujours opérationnel après l'action des forces de l'ordre.

Ce niveau de compatibilité à de multiple plateforme est inhabituel par rapport aux autres familles de ransomwares qui ne prennent généralement en charge que Windows, ESXi et un petit nombre de plateformes Linux. Ceci laisse supposer que les affiliés de BlackCat ont peut-être demandé la compatibilité à des plateformes supplémentaires afin de chiffrer des fichiers sur autant de systèmes que possible.

En décembre 2023, le FBI a eu accès à une partie de l'infrastructure de BlackCat. Le FBI a tenté de saisir les sites Web du groupe hébergés sur Tor, notamment les portails de négociation de rançons et les sites de divulgation de données. Cependant, BlackCat a rapidement publié un message indiquant avoir restauré son site de divulgation de données et a fourni un lien vers un nouveau site de divulgation que le FBI ne pouvait pas manipuler, comme le montre l'illustration 19 ci-dessous.

Ce chassé-croisé entre le FBI et BlackCat s'est déroulé sur plusieurs jours, jusqu'à ce que BlackCat ait eu la certitude que son nouveau site de divulgation de données avait bénéficié d'une publicité suffisante. Notez que « démanteler » un site Web basé sur Tor n'est pas aussi simple que de pour un site Web traditionnel disposant d'un DNS, compte tenu de la furtivité qu'offre le chiffrement et l'absence d'une autorité centrale capable de faire appliquer des décisions de justice.

En mars 2024, le groupe BlackCat a annoncé sa dissolution, invoquant la compromission de son infrastructure par le FBI, ce qui l'aurait mis dans l'incapacité de poursuivre ses activités. Cependant, cette dissolution a suscité des soupçons : elle s'est faite immédiatement après la réception d'une rançon de 22 millions de dollars qui n'a pas été partagée avec un affilié qui les a aidés à s'introduire chez un fournisseur de soins de santé (nous en avons parlé plus tôt dans ce rapport).

Bien que le ransomware BlackCat ne soit plus actif, les affiliés à l'origine des attaques du groupe ont probablement migré vers d'autres réseaux de ransomware-as-a-service tels que RansomHub (où les données volées au fournisseur de soins de santé qui a payé la rançon de 22 millions de dollars ont depuis été divulguées). Il est en outre peu probable que le groupe de ransomwares BlackCat ait réellement cessé ses activités et il est possible qu'il réapparaisse sous un nouveau nom.

4. Akira

Akira a fait irruption sur la scène des ransomwares en avril 2023, gagnant rapidement en notoriété grâce au volume d'attaques menées par ses affiliés. Le groupe Akira est probablement une autre émanation du défunt groupe Conti. Le code du ransomware d'Akira partageait à l'origine de nombreuses similitudes avec le code source de Conti qui a fuité. Cependant, le groupe a plus récemment développé un ransomware basé sur Rust qui contient des références à des personnages des Power Rangers tels que Megazord.

Les affiliés du ransomware Akira ont utilisé divers mécanismes d'accès initial, notamment via l'exploitation de la vulnérabilité CVE-2023-20269.[16] Le groupe malveillant opérant Bumblebee, qui a des liens avec le ransomware Conti, est également connu pour être un courtier d'accès initial pour Akira. Comme indiqué précédemment dans le rapport, l'opération Endgame a démantelé Bumblebee mais n'a eu qu'un impact marginal sur les opérations d'Akira.

Pour mieux comprendre les attaques d'Akira, nous pouvons tirer des enseignements directement des informations qu'Akira fournit aux victimes qui paient une rançon. ThreatLabz a intercepté le message de chat suivant d'Akira, qui contient des détails sur la façon dont ils ont obtenu l'accès au réseau de l'entreprise victime, par l'intermédiaire d'un courtier d'accès initial. Des conseils sont également proposés pour prévenir des attaques de ransomware à l'avenir :

Un accès initial à votre réseau a été acheté sur le dark web. Nous avons ensuite procédé à un kerberoasting et obtenu des hash de mots de passe. Nous les avons ensuite traités pour obtenir le mot de passe de l'administrateur du domaine. En passant des semaines au sein de votre réseau, nous avons réussi à détecter certaines failles que nous recommandons vivement d'éliminer :

1. Aucun de vos collaborateurs ne doit ouvrir d'e-mails suspects, de liens suspects ou télécharger de fichiers, et encore moins les exécuter sur son ordinateur.

2. Utilisez des mots de passe forts, changez-les aussi souvent que possible (au moins 1 à 2 fois par mois). Les mots de passe ne doivent pas être les mêmes pour différentes ressources.

3. Mettez en œuvre la 2FA lorsque possible.

4. Utilisez les dernières versions des systèmes d'exploitation, car elles sont moins vulnérables aux attaques.

5. Mettez à jour toutes vos versions de logiciels.

6. Utilisez des solutions antivirus et des outils de monitoring du trafic.

7. Créez un jump host pour votre VPN. Utilisez des informations d'identification uniques qui diffèrent de celles du domaine.

8. Utilisez un logiciel de sauvegarde avec un stockage cloud qui prend en charge une clé de sécurité.

9. Informez vos collaborateurs aussi souvent que possible des précautions à prendre en matière de sécurité en ligne. Le point le plus vulnérable est le facteur humain et les actions peu responsables de vos collaborateurs, administrateurs système, etc. Nous vous souhaitons sécurité, calme et réussite à l'avenir. Nous vous remercions de votre collaboration et de l'attention que vous portez à votre sécurité.

Bien que ces conseils proviennent directement d'Akira, les recommandations sont pertinentes et fournissent les éléments de base pour comprendre et déjouer de telles attaques.

Akira est l'un des seuls grands groupes de ransomware à ne pas avoir été directement impacté par les forces de l'ordre. En conséquence, Akira est aujourd'hui un acteur du ransomware parmi les plus actifs qui continuera probablement à lancer de nouvelles attaques au cours de l'année à venir.

[16] https://nvd.nist.gov/vuln/detail/CVE-2023-20269

5. Black Basta

Le ransomware Black Basta, identifié pour la première fois en avril 2022, est un autre successeur du groupe Conti. Les affiliés de Black Basta ont utilisé diverses méthodes pour accéder aux réseaux d'entreprise. Avant l'opération Duck Hunt (août 2023), Qakbot était un courtier d'accès initial majeur pour Black Basta. Comme mentionné précédemment, Pikabot a pris le relais après le démantèlement. Cependant, Pikabot a été fermé à la suite de l'opération Endgame en mai 2024.

Depuis, ThreatLabz suit les nouvelles activités du groupe de menaces Qakbot, qui a considérablement fait évoluer ses TTP. Au lieu d'utiliser le spam pour infecter les systèmes avec Qakbot, le groupe de menaces utilise actuellement un mix de techniques d'ingénierie sociale. Au lieu d'envoyer des spams à des millions d'adresses, le groupe mène des attaques ciblées. Ces attaques commencent par l'envoi de spam à un petit nombre d'entreprises ciblées. Le groupe appelle ensuite un collaborateur d'une entreprise ciblée en se faisant passer pour un membre de son service informatique. L'appelant demande à la victime de rejoindre une session de partage d'écran à l'aide d'un logiciel de bureau à distance tel que Quick Assist de Microsoft afin de « mettre à jour les filtres anti-spam d'entreprise » sur son système. Une fois que l'employé a donné l'accès au hacker, un script batch Windows est exécuté pour effectuer une reconnaissance, détourner des informations d'identification et installer une porte dérobée sur le système de la victime. La porte dérobée change constamment, mais a déjà utilisé Qakbot, Cobalt Strike et un outil de proxy SOCKS. Le script batch contient une interface de ligne de commande semblable à celle présentée à l'illustration 20.

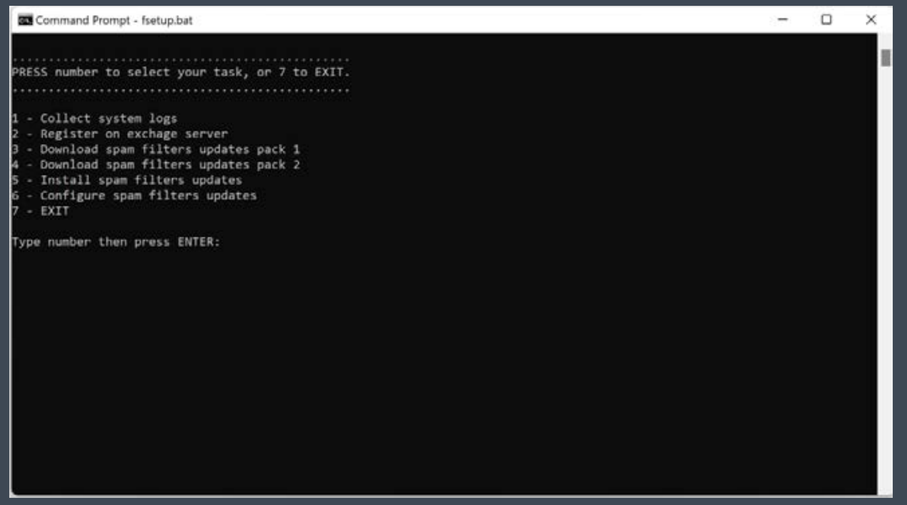


Illustration 20 : Interface de script batch Windows malveillante utilisée pour établir une porte dérobée sur le système d'une victime, en amont d'une attaque basée sur le ransomware Black Basta.

Illustration 21 : Chaîne d'attaque du ransomware Black Basta avec accès initial négocié par le groupuscule malveillant Qakbot.

Une fois cet accès par porte dérobée établi, le groupe Qakbot confie l'accès à une équipe en charge de tests d'intrusion et de se déplacer latéralement, le prélude au déploiement final du ransomware Black Basta.

Même si l'opération Duck Hunt a eu un impact considérable sur le court terme, le groupe malveillant reste actif et continue d'innover et d'expérimenter de nouvelles techniques destinées à compromettre les entreprises. Il est fort probable qu'au cours de l'année à venir, le groupe Qakbot demeurera un important courtier d'accès initial pour les attaques de ransomware telles que Black Basta.

Archives des notes de ThreatLabz sur les ransomwares

Zscaler ThreatLabz gère un **référentiel GitHub public** qui, à l'heure où nous écrivons ces lignes, suit 391 familles de ransomwares et contient un total de 945 notes de rançon. 19 familles et 55 demandes de rançon ont été rajoutées entre avril 2023 et avril 2024. Ces archives peuvent s'avérer précieuses pour suivre les groupes de ransomwares au fil du temps, y compris leurs sites Web de divulgation de données et leurs tactiques de négociation. Elles permettent également de faire le lien entre les groupes de ransomwares qui changent de nom grâce à une analyse stylométrique.

L'illustration 22 montre une comparaison stylométrique entre un chat de rançon de Conti (en haut) et un chat de rançon de Black Basta (en bas). Elle démontre que les membres de Black Basta sont très certainement d'anciens membres de Conti, compte tenu de similitudes dans la structure des phrases, le choix des mots et même les instructions.

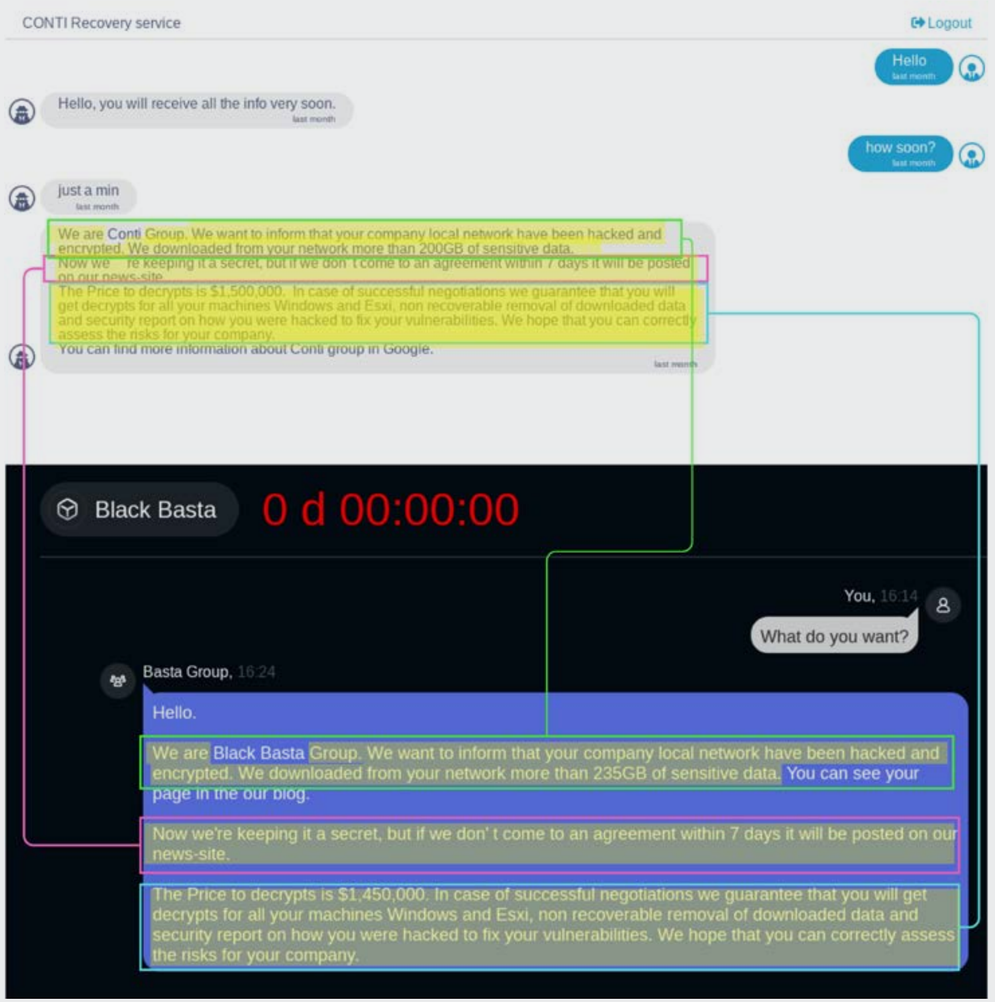


Illustration 22 : Comparaison stylométrique entre les demandes de rançon de Conti (en haut) et de Black Basta (en bas).

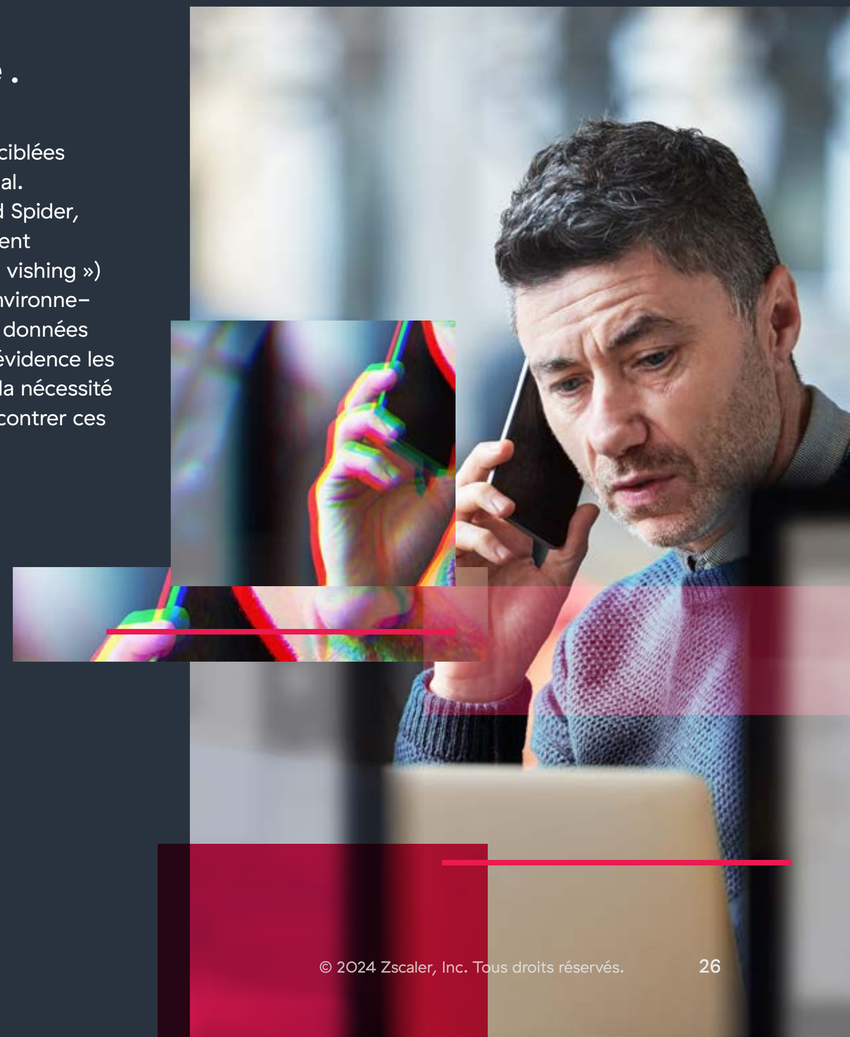
Perspectives pour 2025

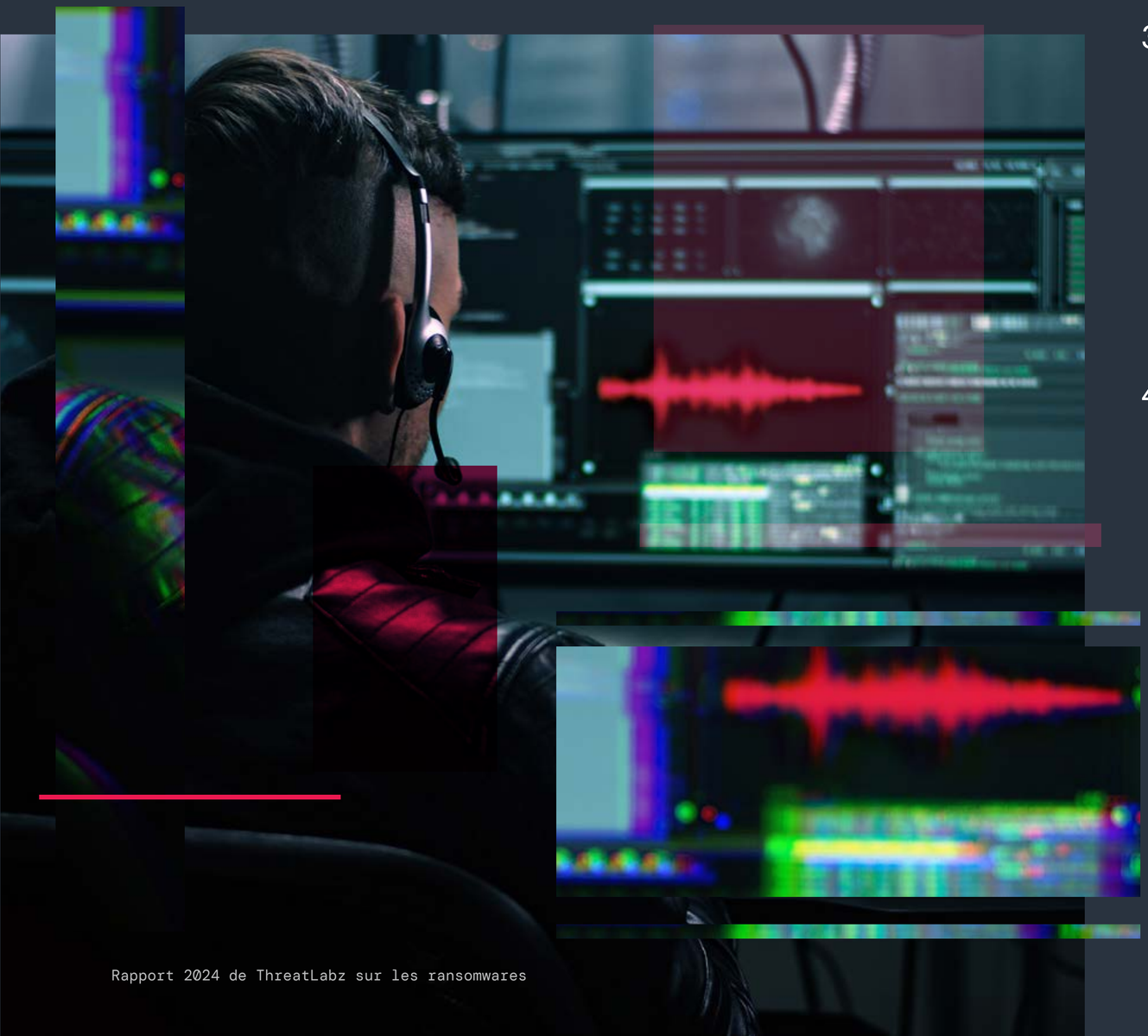
1. Les hackers qui pilotent des ransomwares vont adopter des stratégies d'attaque très ciblées.

Au cours de l'année écoulée, Dark Angels a été l'un des groupes de ransomwares les plus performants et les moins connus, avec une stratégie distincte consistant à cibler un petit nombre d'entreprises qui valent plusieurs milliards pour leur extorquer de substantielles rançons. Cette stratégie poursuit un double objectif : déjouer la surveillance des forces de l'ordre et du secteur de la sécurité, tout en consacrant davantage de ressources à infiltrer de grandes entreprises prêtes à payer d'importantes rançons pour protéger des volumes importants de données dérobées. Le groupe a ainsi perçu la plus grosse rançon connue, soit 75 millions de dollars, ce qui ne manquera pas de susciter l'intérêt d'autres acteurs malveillants utilisant des ransomwares en 2025, susceptibles de vouloir réitérer cette prouesse.

2. Les attaques ciblées feront de plus en plus appel à l'ingénierie sociale vocale.

Nous devrions assister en 2025 à une recrudescence d'attaques ciblées qui seront facilitées par des courtiers spécialisés dans l'accès initial. Ces courtiers, illustrés par les activités de Qakbot et de Scattered Spider, emploient des techniques sophistiquées pour s'infiltrer, notamment en utilisant des attaques d'ingénierie sociale basées sur la voix (« vishing ») pour leurrer les individus et les amener à accorder l'accès à un environnement d'entreprise. Cet accès est ensuite utilisé pour exfiltrer des données et déployer un ransomware. Cette tendance émergente met en évidence les collaborations au sein de l'écosystème cybercriminel et souligne la nécessité d'une vigilance accrue et de mesures de sécurité avancées pour contrer ces menaces qui évoluent sans cesse.





3. Les hackers qui pilotent des ransomwares feront davantage appel à l'IA générative pour créer des campagnes plus efficaces, personnalisées et localisées.

L'adoption croissante de l'IA générative en 2025 et au-delà permettra aux assaillants de créer des e-mails de spam avec une grammaire et une orthographe précises, et d'exploiter le clonage vocal pour obtenir un accès privilégié à un collaborateur en usurpant l'identité d'un de ses collègues. Dans les années à venir, les voix générées par IA pourraient être adaptées à l'aide d'accents et de dialectes locaux pour renforcer leur crédibilité et les chances de succès, illustrant ainsi la manière dont les hackers qui pilotent des ransomwares rendront les attaques plus convaincantes et plus difficiles à détecter.

4. Davantage d'incidents de cybersécurité seront signalés conformément aux nouvelles règles de la SEC.

Avec la décision de la SEC exigeant une notification plus stricte des incidents de cybersécurité, 2025 sera témoin d'une progression continue du nombre d'entreprises divulguant des incidents liés aux ransomwares. Il faut espérer que cela se traduira par une plus grande transparence et favorisera tant une culture de la responsabilité que des défenses proactives, qui amélioreront les pratiques de cybersécurité.

5. Les attaques de ransomware par exfiltration de volumes importants de données vont se multiplier.

Les attaques permettent d'exfiltrer des données en grande quantité. Ces incidents, qui n'utiliseront pas toujours le chiffrement, devraient progresser considérablement au cours de l'année à venir. Cette tendance, qui a commencé à prendre de l'ampleur en 2022, voit les acteurs malveillants se concentrer uniquement sur l'exfiltration de données, sans chiffrement des systèmes. Cette approche permet de mener des opérations plus rapides et opportunistes et capitalise sur la crainte d'une divulgation de données sensibles pour contraindre les victimes à payer des rançons. Elle souligne l'évolution constante des stratégies de ransomware vers des méthodes plus efficaces et plus percutantes.

6. Les acteurs du secteur de la santé continueront d'être ciblés de manière persistante par les groupes de ransomwares.

La valeur importante des données de santé continuera de susciter un fort intérêt en 2025. Nombre d'organisations des soins de santé sont particulièrement vulnérables parce qu'elles tardent à remplacer leurs systèmes traditionnels par une infrastructure de sécurité moderne et sophistiquée. En conséquence, ces entreprises sont susceptibles de subir des intrusions et des tentatives d'extorsion récurrentes. Celles qui ne prennent pas les mesures appropriées pour privilégier les stratégies de défense Zero Trust peuvent être prises pour cible par des groupes de ransomwares.

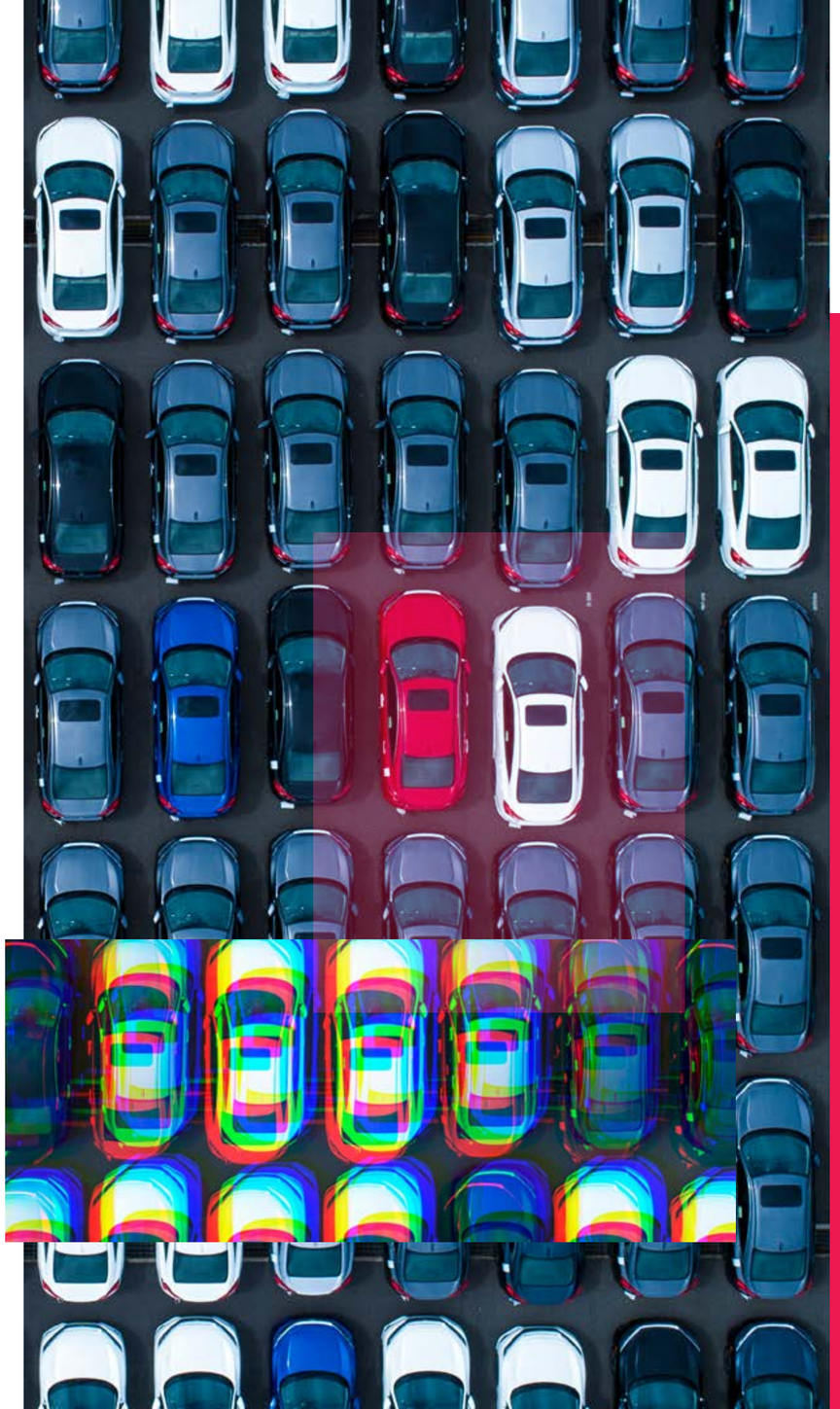
7. La collaboration internationale contre les groupuscules cybercriminels capitalisera sur les efforts réalisés.

Les forces de l'ordre et le secteur privé continueront de collaborer dans leurs efforts de lutte contre les attaques de ransomware, notamment en perturbant les actions des principaux courtiers d'accès initial et des groupes de ransomwares. La collaboration internationale se révélera de plus en plus vitale à mesure que l'interconnexion mondiale se développera, ce qui permettra aux cybercriminels d'opérer plus facilement à l'échelle internationale. En partageant leurs renseignements et leur expertise, ces actions coordonnées perturberont de manière plus efficace les réseaux mondiaux de ransomwares. Zscaler ThreatLabz a été en première ligne et a joué un rôle déterminant en fournissant une assistance technique à plusieurs de ces opérations sur l'année écoulée.

Zscaler simplifie la protection contre les ransomwares

La complexité et le coût croissants liés aux attaques de ransomware soulignent la nécessité de déployer une approche Zero Trust robuste. La **plateforme Zscaler Zero Trust Exchange™** simplifie ce défi, en offrant une approche globale pour déjouer les ransomwares.

Zero Trust Exchange permet aux entreprises de déployer une ligne de défense plus intelligente, à chaque étape d'une attaque. La première étape consiste à empêcher les assaillants d'identifier et de cibler les utilisateurs et les applications en les rendant invisibles depuis l'extérieur et uniquement accessibles aux utilisateurs ou aux appareils autorisés. La solution inspecte l'ensemble du trafic entrant et sortant, chiffré ou non. Les utilisateurs et les dispositifs authentifiés se connectent directement aux applications dont ils ont besoin, jamais au réseau. Ainsi, même si un assaillant s'introduit, il ne peut se déplacer latéralement à la recherche de données à détourner ou chiffrer.



LE ZERO TRUST, UNE ARME REDOUTABLE CONTRE LES RANSOMWARES
Les architectures de sécurité traditionnelles peinent à neutraliser les attaques de ransomware.

EN FINIR AVEC L'EXISTANT : Les mesures de sécurité traditionnelles et les outils cloisonnés, dont les pare-feu et les VPN de « nouvelle génération », introduisent souvent des zones d'ombre, de la complexité et des coûts importants. Ces approches traditionnelles ne parviennent pas à inspecter de manière économique et fluide les fichiers et le trafic chiffrés, exposant les entreprises à des risques de déplacement latéral et à des attaques de ransomware qui exploitent le manque de visibilité et de contrôle, avec des conséquences souvent dévastatrices.

ADOPTER LE ZERO TRUST : une architecture Zero Trust suppose que chaque utilisateur, appareil et connexion est potentiellement compromis. Cette approche impose une vérification continue et un contrôle d'accès strict. En vérifiant systématiquement les identités et en inspectant l'ensemble du trafic, y compris les données chiffrées, le Zero Trust maîtrise le risque de propagation des attaques au sein du réseau, neutralisant ainsi les menaces de ransomware avant qu'elles ne puissent infliger des préjudices.

ZSCALER BLOQUE LES RANSOMWARES À CHAQUE ÉTAPE DU CYCLE D'ATTAQUE, depuis la reconnaissance initiale et la compromission jusqu'aux déplacements latéraux, au détournement de données et à l'exécution de payloads malveillants.

Minimiser la surface d'attaque : basé sur une architecture Zero Trust, Zero Trust Exchange remplace les architectures VPN et pare-feu traditionnels vulnérables qui élargissent la surface d'attaque. Zscaler minimise efficacement la surface d'attaque en dissimulant les utilisateurs, les applications et les dispositifs derrière un proxy cloud, ce qui les rend invisibles depuis Internet. À l'instar d'un standard téléphonique qui achemine les appels vers des destinations autorisées, Zscaler ne connecte que l'utilisateur ou l'appareil autorisé à une application particulière.

Empêcher toute compromission initiale : Zero Trust Exchange applique une inspection TLS/SSL approfondie, une isolation du navigateur, un sandboxing inline avancé et un contrôle d'accès basé sur des règles afin d'empêcher que les utilisateurs n'accèdent à des sites web malveillants. Les menaces inconnues sont détectées avant qu'elles n'atteignent votre réseau, pour ainsi maîtriser tout risque de compromission.

Prévenir les déplacements latéraux : grâce à la segmentation utilisateur–application ou application–application, les utilisateurs se connectent directement aux applications (et les applications à d'autres applications) et non au réseau, éliminant ainsi tout risque de déplacement latéral. En centralisant la gestion des politiques de contrôle d'accès, Zscaler agit comme un guichet de contrôle de sécurité pour le trafic Internet, supprimant les voies de déplacement latéral. Zscaler peut également identifier et empêcher le déplacement interne de potentiels assaillants, qu'il s'agisse de menaces externes ou internes malveillantes, grâce à des capacités de détection et de réponse aux menaces liées à l'identité (ITDR) et de leurre.

Déjouer la perte de données : les mesures de prévention des pertes de données, associées à une inspection complète du trafic TLS/SSL, déjouent efficacement les tentatives de vol de données. Zscaler veille à la sécurité des données, qu'elles soient en transit ou au repos.

COMBATTRE LES MENACES PILOTÉES PAR IA GRÂCE À L'INNOVATION IA + ZERO TRUST.

L'IA permet à Zscaler de proposer une protection robuste contre les ransomwares, garantissant ainsi une sécurité complète aux entreprises dans un univers de menaces en constante évolution :

- ***La détection du phishing et des communications C2*** fait appel à une capacité de détection optimisée par IA et offerte par la passerelle de sécurité web de Zscaler. Les sites de phishing et les infrastructures de commande et contrôle (C2) inconnues sont ainsi neutralisés.
- ***Le sandboxing optimisé par IA*** déploie une prévention complète contre les malwares et les menaces zero-day en analysant les fichiers suspects au sein d'un environnement contrôlé.
- ***La segmentation basée sur l'IA*** fournit des recommandations de politiques d'accès pour minimiser la surface d'attaque et empêcher les déplacements latéraux, se basant sur le contexte, le comportement, la localisation et la télémétrie des applications privées de chaque utilisateur.
- ***Une politique dynamique, basée sur les risques,*** analyse en permanence les risques associés aux utilisateurs, aux appareils et aux applications pour assurer leur sécurité et le contrôle de leurs accès.
- ***L'isolation du navigateur optimisée par IA*** crée une zone sécurisée entre les utilisateurs et un contenu Web malveillant. Les pages web consultées sont restituées sous la forme d'images dans le navigateur de l'utilisateur, empêchant ainsi les fuites de données et la diffusion de menaces actives.
- ***La découverte et la classification des données font appel à l'IA*** pour offrir une visibilité et une classification instantanées des données présentes sur les terminaux ou dans le cloud, ce qui pèse sur la capacité des ransomwares à cibler et chiffrer les données sensibles.

Une prévention globale, à chaque étape de la chaîne d'attaque

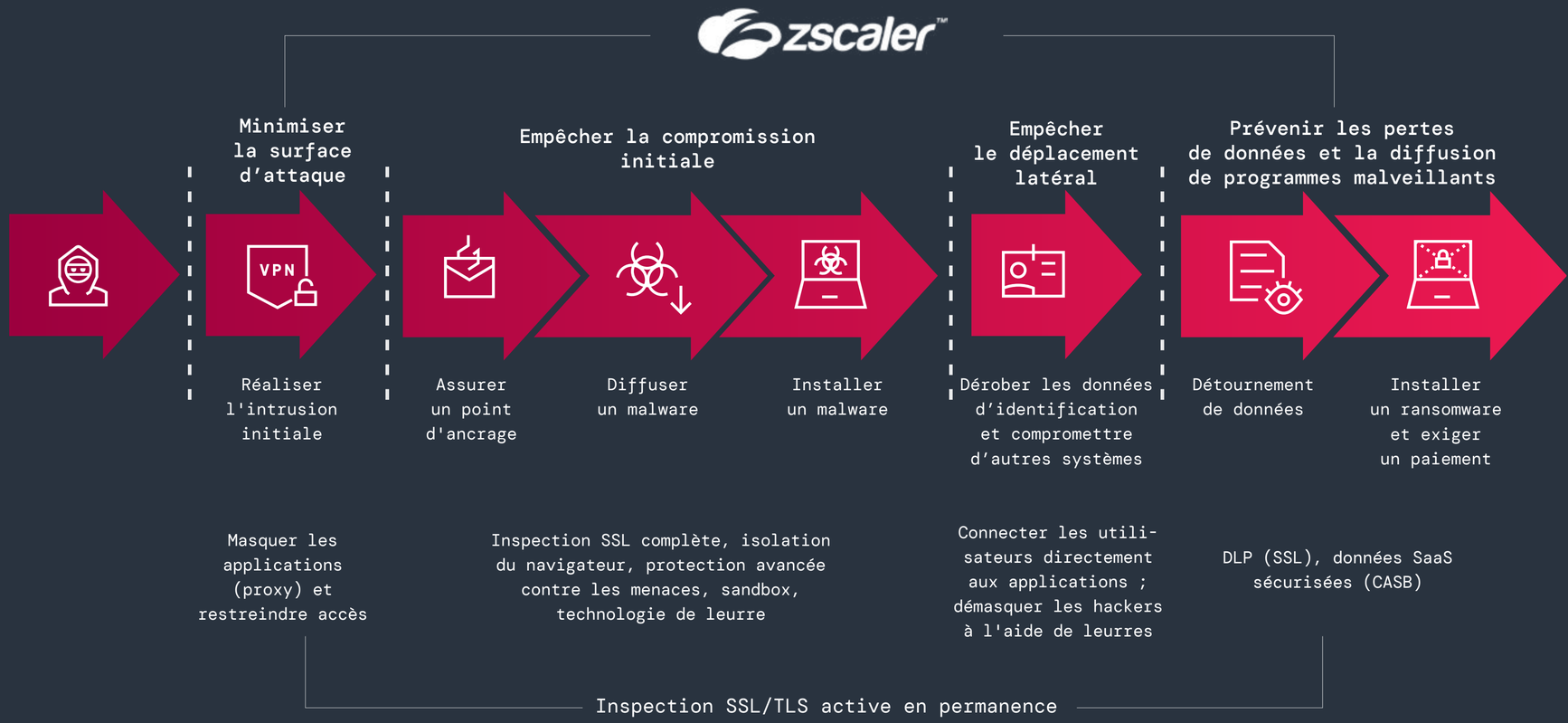


Illustration 23 : Une architecture Zero Trust active tout au long de la chaîne d'attaque des ransomwares.

Produits Zscaler connexes

Zscaler Internet Access™ (ZIA™) fournit un accès sécurisé et direct à Internet, pour une protection inline contre les menaces. Les fonctionnalités avancées de prévention des menaces et de sandboxing de ZIA préviennent le téléchargement de ransomwares et les communications de commande et contrôle (C2), empêchant ainsi l'infiltration de ransomwares.

Zscaler Private Access™ (ZPA™) déploie un accès sécurisé aux applications internes sans les exposer à Internet, grâce à son modèle Zero Trust. ZPA garantit que seuls les utilisateurs et appareils autorisés peuvent accéder aux applications critiques, réduisant ainsi la surface d'attaque et neutralisant les tentatives d'attaques de ransomware.

Zscaler Zero Trust Firewall intercepte et inspecte le trafic TLS/SSL à la recherche de malwares dissimulés dans le trafic chiffré, afin qu'ils ne puissent s'infiltrer dans le réseau.

Zscaler Deception détecte et neutralise les assaillants qui tentent de se déplacer latéralement ou d'augmenter leurs privilèges, en les leurrant via des serveurs, des applications, des répertoires et des comptes d'utilisateurs leurres.

Zscaler Sandbox analyse les fichiers et exécutables suspects au sein d'un environnement virtuel sous contrôle, contribuant ainsi à identifier et à neutraliser les logiciels malveillants. Les entreprises gardent ainsi une longueur d'avance sur les ransomwares utilisant des fichiers et sur les attaques zero-day.

Zscaler Cloud Browser cloisonne les sessions Web et diffuse leur contenu sous forme d'image vers les dispositifs, afin d'éliminer tout risque de téléchargement furtif et d'exploits zero-day susceptibles être utilisés par les opérateurs de ransomwares.

Zscaler ITDR (Identity Threat Detection and Response) détecte et protège contre les attaques basées sur l'identité : vol d'identifiants, abus de privilèges, attaques sur Active Directory et droits d'accès risqués.

Zscaler Data Protection assure une sécurité cohérente et unifiée des données en transit et au repos dans les applications SaaS et les clouds publics, ce qui maîtrise le risque d'exfiltration de données et l'impact potentiel des attaques de ransomware.

Conseils de prévention contre les ransomwares

Une stratégie de défense basée sur une architecture Zero Trust constitue une mesure de sécurité éprouvée pour stopper les ransomwares. Cependant, la lutte contre cette menace aux multiples facettes exige une planification proactive, une collaboration continue et des investissements stratégiques.

Les experts de ThreatLabz livrent des bonnes pratiques pour vous aider à maîtriser les risques liés aux ransomwares et protéger votre entreprise contre les menaces actuelles et émergentes.

- **Effectuer des sauvegardes de données régulières et sécurisées.** Veillez à ce que toutes vos données soient régulièrement sauvegardées et en toute sécurité, y compris vos sauvegardes hors ligne. Adaptez des stratégies de sauvegarde en fonction de l'évolution des menaces.
- **Maintenir les logiciels à jour.** Appliquez sans tarder les nouveaux correctifs de sécurité pour les vulnérabilités connues. Faites appel à des sources de veille sur les menaces pour hiérarchiser et gérer efficacement les correctifs de sécurité.
- **Activer l'authentification multifacteur (MFA).** Ajoutez une couche de sécurité supplémentaire aux comptes d'utilisateurs avec la MFA pour mieux contrer les accès non autorisés. Faites appel aux solutions MFA pour détecter et prévenir efficacement le piratage de comptes.
- **Établir une politique de sécurité d'entreprise cohérente.** Assurez-vous que tous les utilisateurs suivent des procédures de sécurité cohérentes, avec notamment une authentification multifacteur et des mises à jour de sécurité régulières, afin d'éviter les compromissions initiales. La dissémination géographique des collaborateurs impose plus que jamais de déployer une architecture SSE (Security Service Edge) pour protéger les utilisateurs, où qu'ils se trouvent.
- **Renforcer la sécurité des applications.** Rendez les applications invisibles depuis l'Internet public pour empêcher les auteurs de ransomwares d'exploiter les vulnérabilités. Déployez une architecture Zero Trust afin de protéger les applications internes contre les tentatives de ransomware.
- **Appliquer un accès sur la base du moindre privilège.** Déployez des politiques du moindre privilège pour restreindre l'accès des utilisateurs aux seules ressources nécessaires à leurs tâches. Faites appel à des solutions avec IA pour analyser dynamiquement le comportement des utilisateurs et adapter les privilèges d'accès en conséquence.
- **Renforcer la protection de l'identité.** Faites appel aux outils d'ITDR pour gagner en visibilité sur les erreurs de configuration des identités, corriger les vulnérabilités d'Active Directory que les hackers exploitent pour élever leurs privilèges et se déplacer latéralement, et détecter les menaces furtives sur les identités.
- **Inspecter l'ensemble du trafic.** 86 % des menaces sont désormais diffusées via des canaux chiffrés, qui ne sont souvent pas inspectés, ce qui permet aux assaillants de contourner les contrôles de sécurité. Il est essentiel d'inspecter tout le trafic, chiffré ou non, pour éviter les compromissions.

- **Mettre en place un accès réseau Zero Trust (ZTNA).** Déployez une segmentation granulaire utilisateur–application et application–application, en offrant des accès à moindre privilège qui préviennent les déplacements latéraux, minimisent l'exposition des données et améliorent votre posture globale de sécurité.
- **Faire appel à une isolation du navigateur optimisée par IA.** Protégez vos utilisateurs contre les menaces Web grâce à un cloisonnement optimisé par IA des contenus Internet suspects et des utilisateurs à risque. En isolant le navigateur et en limitant les actions potentiellement dangereuses (telles que la saisie d'informations d'identification), les utilisateurs accèdent en toute sécurité aux URL et fichiers suspects sans mettre leur système en péril.
- **Faire appel à un sandboxing avancé.** Contrez les malwares inconnus et furtifs, à l'aide d'une sandbox qui détecte et met automatiquement en quarantaine les menaces inconnues et les fichiers suspects grâce à une analyse optimisée par IA et AA.
- **Déployer une prévention contre la perte de données (DLP).** Protégez-vous contre l'exfiltration et l'exposition de vos données en déployant des mesures DLP inline.
- **Leurrer les assaillants.** Faites appel à des outils de leurre et des honeypots pour piéger les hackers, les identifier plus facilement et prévenir leur infiltration dans vos systèmes.
- **Utiliser un CASB (Cloud Access Security Broker).** Contrôlez et surveillez l'utilisation des applications cloud avec un CASB qui empêche les activités malveillantes telles que les téléchargements de fichiers et l'exfiltration de données.
- **Assurer la formation continue des collaborateurs.** Organisez régulièrement des formations de sensibilisation à la sécurité pour informer vos équipes sur les menaces liées aux ransomwares. Menez des attaques simulées de ransomware pour mieux préparer vos collaborateurs.
- **Élaborer un plan complet de réponse aux ransomwares.** Créez un plan de réponse qui englobe la restauration des données, la réponse aux incidents et les modalités de communication afin d'agir rapidement et efficacement en cas d'attaque de ransomware.

Suivez Zscaler ThreatLabz pour des informations régulières sur les ransomwares, notamment les indicateurs de compromission (IOC) publiés et les mappings de MITRE ATT&CK. Ces informations peuvent vous aider à former votre équipe, améliorer votre posture de sécurité et à prévenir les attaques de ransomware.

ThreatLabz gère également des référentiels GitHub avec des IoC, des outils (dont des outils de déchiffrement de ransomware) et une archive de notes de ransomware émises par les principaux groupes de ransomware.

X @ThreatLabz | Blog sur les recherches en sécurité de ThreatLabz

Méthodologie du rapport

La méthodologie de recherche de ce rapport est un processus complet qui fait appel à de nombreuses sources de données afin d'identifier et de suivre les tendances du ransomware. L'équipe chargée du rapport a recueilli des données à partir de diverses sources entre avril 2023 et mars 2024, parmi lesquelles :

- **Le cloud de sécurité mondial Zscaler,** qui traite plus de 500 000 milliards de signaux quotidiens, bloque plus de 9 milliards de menaces et de violations de politiques par jour et fournit plus de 250 000 mises à jour de sécurité quotidiennes aux clients de Zscaler. Nous avons analysé ces données, qui comprennent des informations sur les adresses IP sources, les adresses IP de destination et les types de fichiers associés aux attaques de ransomware, afin de déterminer l'activité des ransomwares.

- **Sources de renseignement externes.** Nous avons également recueilli des données provenant de sources de renseignements externes, telles que des flux de veille sur les menaces, des études open source et des rapports des forces de l'ordre. Ces ressources ont fourni des informations supplémentaires sur les auteurs d'attaques de ransomware, leurs cibles et leurs méthodes.

- **Analyse par l'équipe ThreatLabz des échantillons de ransomware et des données d'attaque.** L'équipe ThreatLabz Threat Intelligence scrute les familles de ransomwares à grande échelle, en leur appliquant des techniques de rétro-ingénierie et grâce à une analyse automatisée des malwares qui permet de concevoir des stratégies de réponse efficaces. ThreatLabz travaille également en étroite collaboration avec les forces de l'ordre internationales et a joué un rôle important dans de récentes actions, dont l'opération Duck Hunt et l'opération Endgame.

À propos de ThreatLabz

ThreatLabZ est l'organisme de recherche en sécurité de Zscaler. Cette équipe experte est responsable de la traque de nouvelles menaces et s'assure de la protection optimale des milliers d'organisations qui utilisent la plateforme mondiale Zscaler. Au-delà des recherches sur les malwares et des analyses comportementales, l'équipe ThreatLabZ s'investit dans la recherche et le développement de nouveaux prototypes qui assurent une protection avancée contre les menaces sur la plateforme Zscaler. Elle mène régulièrement des audits de sécurité interne pour s'assurer que les produits et l'infrastructure de Zscaler répondent aux normes de conformité de la sécurité. ThreatLabZ publie régulièrement des analyses approfondies sur les menaces nouvelles et existantes sur son portail, **research.zscaler.com**.

À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation digitale et permet à ses clients de gagner en agilité, productivité, résilience et sécurité. La plateforme Zero Trust Exchange™ de Zscaler protège des milliers de clients contre les cyberattaques et les pertes des données en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quelle que soit leur localisation. Adossé à un écosystème de plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur le SASE, est la plus vaste plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **www.zscaler.fr.**