Akamai

État des lieux d'Internet
Volume 09 | Numéro 04

Les ransomware évoluent

Vue d'ensemble de la zone EMEA

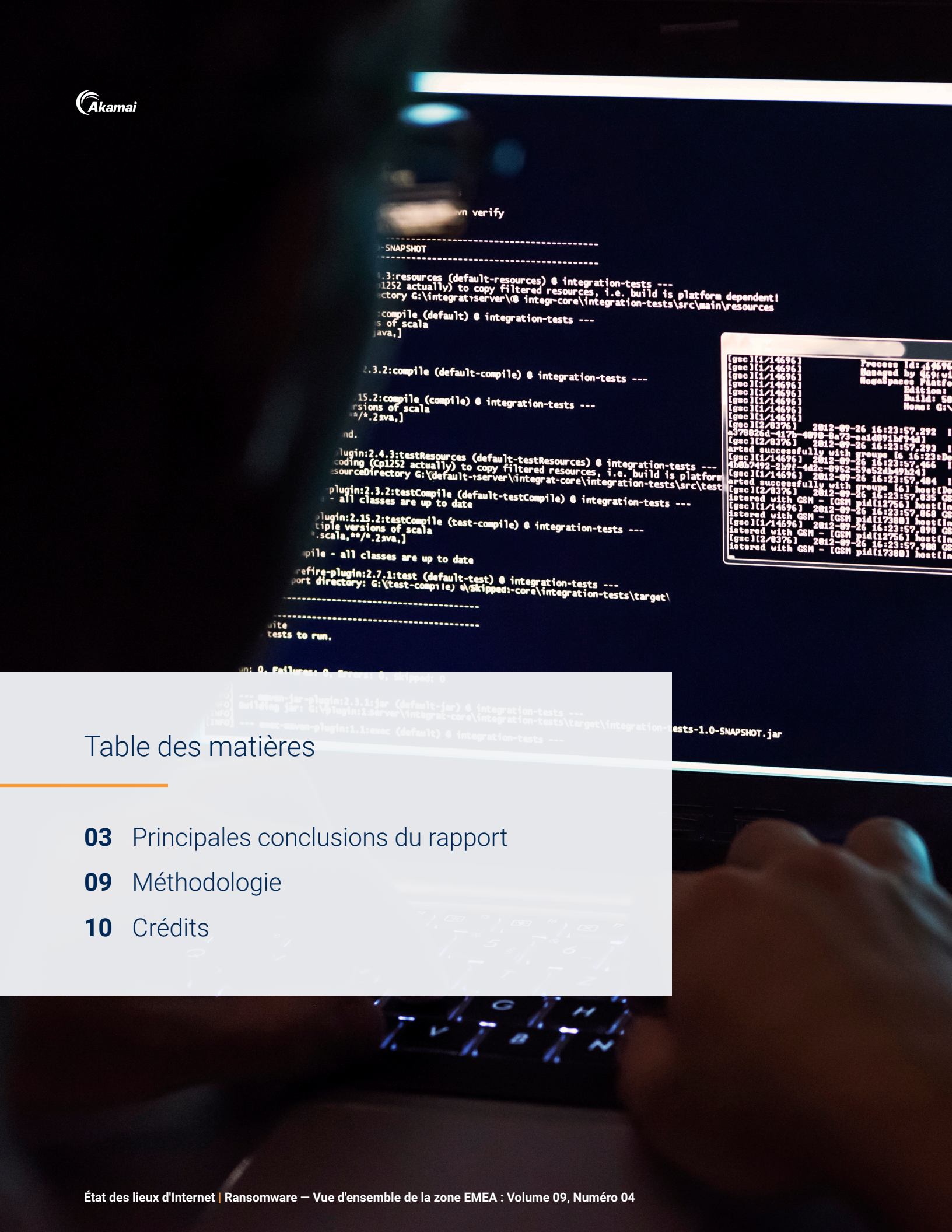


Table des matières

Principales conclusions du rapport

La vue d'ensemble de la zone EMEA vient compléter notre rapport SOTI plus général sur les ransomware intitulé « Les ransomware évoluent : techniques d'exploitation évolutives et recherche active des vulnérabilités de type Zero Day » (uniquement disponible en anglais). Pour obtenir une analyse approfondie des tendances, méthodes et techniques adoptées par les groupes de ransomware, pour vous renseigner sur les différentes étapes d'une attaque et sur les solutions/recommandations à appliquer pour protéger votre organisation ou pour accéder à nos méthodologies de recherche, consultez ce rapport.

Présentation

Les ransomware continuent de faire des ravages dans les entreprises et font de plus en plus de victimes, car les adversaires continuent d'évoluer et de modifier leurs techniques d'attaque, d'introduire de nouvelles méthodes d'extorsion, de tirer parti d'une surface d'attaque en expansion et de capitaliser sur les contraintes budgétaires en matière de sécurité. L'impact de ces tendances dangereuses se reflète dans les groupes de ransomware qui dominent le paysage et dans leur succès croissant. Dans la zone EMEA, cela s'illustre par une croissance de 18 % des entreprises victimes entre le quatrième trimestre 2021 et le quatrième trimestre 2022, avec un bond de 77 % du nombre de victimes d'une année sur l'autre si l'on compare le premier trimestre 2022 au premier trimestre 2023.

Dans cette vue d'ensemble de la zone EMEA, nous partageons des informations supplémentaires pour une meilleure défense et une meilleure gestion des risques face à cette préoccupation croissante, notamment :

- Au cours de la période d'octobre 2021 à mai 2023, LockBit a dominé la scène des ransomware, avec une progression de CL0P qui a exploité agressivement les vulnérabilités. Un changement dans les techniques d'attaque, du phishing à l'abus généralisé des vulnérabilités de type Zero Day et One Day, a conduit à ce bond du nombre de victimes.
- Conformément aux constatations faites dans le monde entier, le segment de marché de la fabrication a compté le plus grand nombre de victimes, suivi des services aux entreprises.
- La majorité des victimes de ransomware étaient des entreprises plus petites, avec un chiffre d'affaires allant jusqu'à 50 millions de dollars. Cependant, les plus grandes entreprises ont également été attaquées.

LockBit est le groupe de ransomware le plus actif

Malgré une sensibilisation croissante aux ransomware et une multitude d'outils et de meilleures pratiques pour lutter contre cette menace, le nombre d'entreprises victimes dans la zone EMEA a augmenté de 18 % entre le quatrième trimestre 2021 et le quatrième trimestre 2022. En parallèle, si nous comparons le nombre de victimes au premier trimestre 2022 à celui du premier trimestre 2023, nous observons un bond de 77 % sur un an. Conformément aux constatations de notre rapport mondial, LockBit a causé la majorité des attaques recensées entre le 1er octobre 2021 et le 31 mai 2023. Dans la zone EMEA, LockBit est responsable de 45 % des attaques. Cependant, dans la zone EMEA, Vice Society détrône ALPHV en tant que deuxième groupe le plus actif. CL0P, lui, reste troisième (EMEA Figure 1).

EMEA : Top 3 des groupes de ransomware par nombre de victimes

1er octobre 2021 – 31 mai 2023

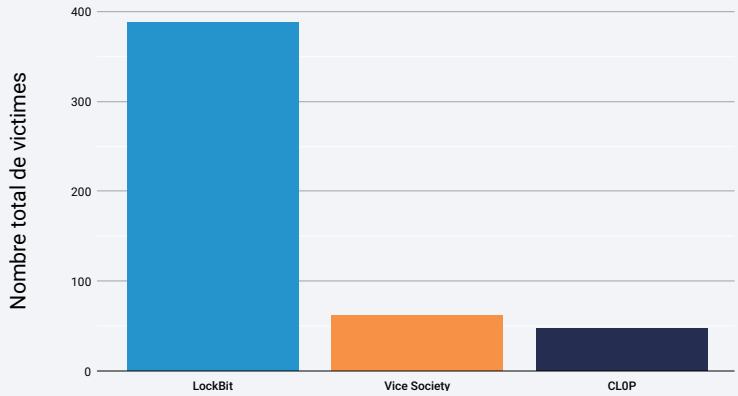


Fig. 1 EMEA : La plupart des organisations de la zone EMEA touchées par des attaques par ransomware ont été ciblées par LockBit, Vice Society et CL0P

Analyse trimestrielle

Lorsque nous étudions le nombre de victimes par groupe de ransomware (EMEA Figure 2), nous notons la prévalence de LockBit et la constance de Vice Society. Celle-ci est probablement due au fait que l'éducation est l'un des principaux secteurs ciblés par les ransomwares dans la zone EMEA (cf. Figure 3 plus bas). En effet, Vice Society est une offre de ransomware-as-a-service qui cible de façon disproportionnée le secteur de l'éducation. Cependant, comme le montrent les tendances des données mondiales, le groupe CL0P est en pleine expansion dans le paysage des ransomware de la zone EMEA. Le pic atteint au 1er trimestre 2023 peut être dû à son exploitation de nombreuses vulnérabilités Zero Day comme point d'entrée. De l'hameçonnage à l'exploitation généralisée des vulnérabilités,

**Le 2e trim. n'est pas un trimestre complet, car les données s'arrêtent au 31 mai 2023.*

cette hausse du nombre de victimes est intrinsèquement liée au changement de techniques d'attaque observé au cours des six derniers mois. Cependant, à la date de publication de ce rapport, seules des données partielles étaient disponibles pour le deuxième trimestre 2023*. Au 31 mai 2023, l'activité du groupe CL0P avait atteint le niveau observé en 2022. Bien que nous ne soyons pas en mesure de dire avec certitude ce que ce trimestre révélera, il est important de noter qu'en juin 2023, CL0P a publié les noms de nouvelles entreprises victimes de ses attaques exploitant la vulnérabilité MOVEit dans la zone EMEA. Le nombre de victimes est donc plus que susceptible d'augmenter.

EMEA : Top 3 des groupes de ransomware par nombre de victimes
Trimestriel : 1er octobre 2021 – 31 mai 2023

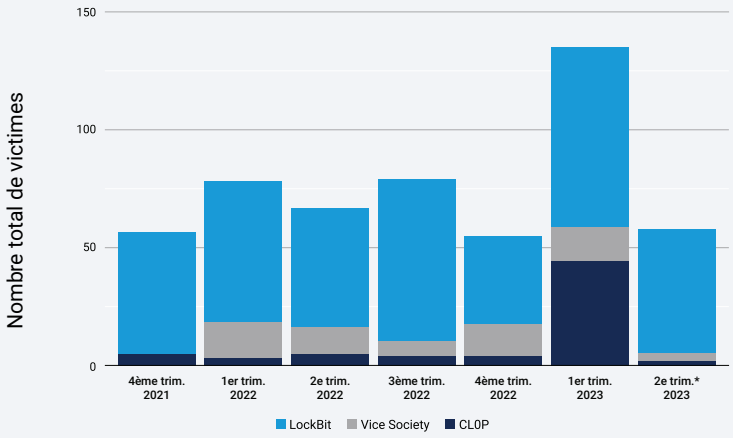


Fig. 2 EMEA : Comparaison du nombre de victimes trimestrielles pour chacun des trois principaux groupes de ransomware au sein de la zone EMEA : (LockBit, Vice Society et CL0P)

Secteurs critiques à risque

Les cinq principaux secteurs critiques confrontés à des risques d'attaque par ransomware dans la zone EMEA sont la fabrication, les services aux entreprises, le commerce de détail, la construction et l'éducation (Figure 3 EMEA). Il s'agit également des cinq plus grands secteurs du monde. Ce constat va de pair avec les conclusions du rapport mondial sur les ransomware de 2022 qui placent les secteurs de la fabrication et des services aux entreprises aux deux premières places. À l'époque, ils étaient visés par le groupe de ransomwares Conti. Après la disparition de Conti, LockBit a pris le relais. Nous observons également un chevauchement important sur les cinq secteurs principaux affectés dans notre rapport DNS précédent intitulé Autoroute d'attaques : une analyse approfondie du trafic DNS malveillant, mettant en avant un lien clair entre le trafic de commande et de contrôle malveillant (C2) et les attaques par ransomware.

**Le 2e trim. n'est pas un trimestre complet, car les données s'arrêtent au 31 mai 2023.*

EMEA : Top 5 des secteurs d'activité par nombre de victimes du groupe de ransomware

1er octobre 2021 – 31 mai 2023

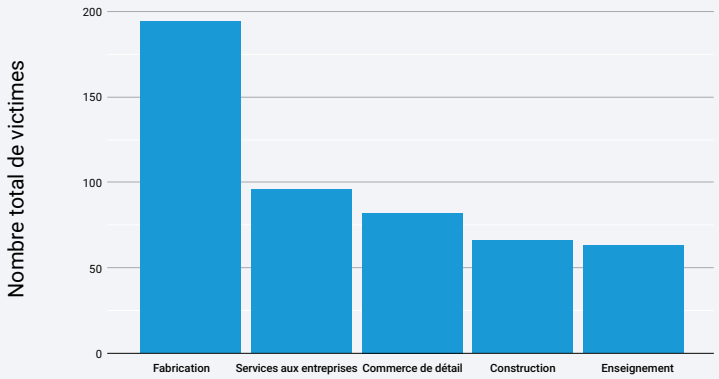


Fig. 3 EMEA : Le secteur de la fabrication est le segment de marché qui concentre le plus grand nombre d'organisations victimes d'attaques par ransomwares dans la zone EMEA

Il est également important de noter que LockBit est le ransomware le plus répandu dans chacun des quatre principaux secteurs de la zone EMEA puisqu'il est à l'origine de 45,9 % des attaques dans le secteur de la fabrication, de 45,4 % des attaques dans les services aux entreprises, de 45,1 % des attaques dans le commerce de détail et de 53,6 % des attaques dans la construction. Seule l'éducation fait figure d'exception : dans ce secteur, les attaques sont avant tout le fait de Vice Society, à hauteur de 36,5 %, suivi par LockBit à 22,2 %.

> Ce n'est ni une question de taille, ni de chiffre d'affaires : toutes les organisations sont susceptibles d'être touchées par des attaques par ransomware.

Les groupes de ransomwares misent sur le retour sur investissement

Ce n'est ni une question de taille, ni de chiffre d'affaires : toutes les organisations sont susceptibles d'être touchées par des attaques par ransomware. Cependant, il s'avère que les données recueillies suivent la tendance mondiale et que les attaques fructueuses ont tendance à cibler des petites entreprises de la zone EMEA (EMEA Figure 4). Nous supposons que les petites entreprises disposent de ressources de sécurité limitées pour lutter contre les dangers des ransomwares. Elles sont donc plus vulnérables, faciles à infiltrer et ont la capacité de payer la rançon. Toutefois, les plus grandes entreprises sont tout aussi ciblées. Selon des recherches, plus les revenus de l'organisation touchée sont élevés, plus la rançon demandée sera conséquente.

EMEA : Nombre de victimes par plage de revenus et par groupe de ransomware
1er octobre 2021 – 31 mai 2023

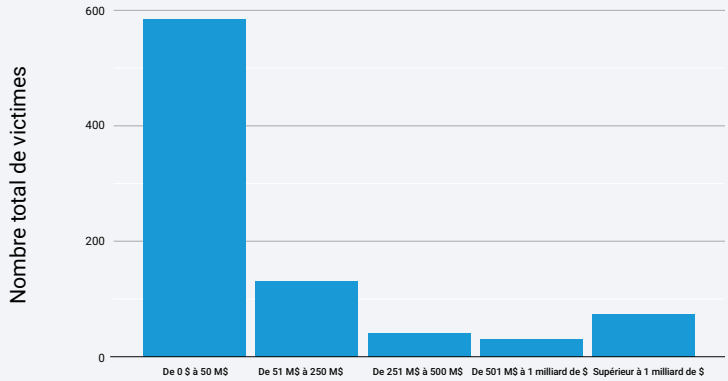
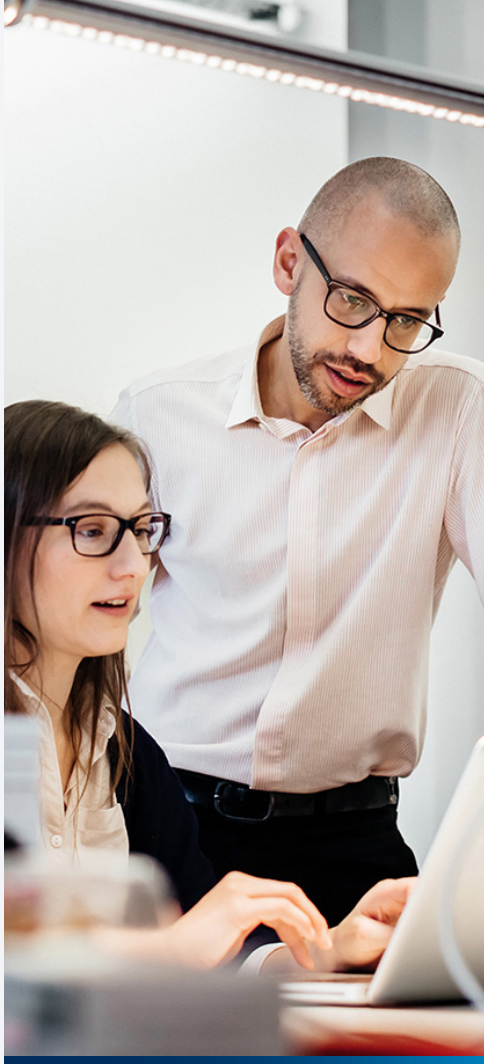


Fig. 4 EMEA : La majorité des victimes de ransomware dans la région EMEA sont des entreprises déclarant jusqu'à 50 millions de dollars de revenus



Conclusion de la vue d'ensemble de la zone EMEA

Les ransomware continuent de semer la terreur dans les entreprises. À l'échelle mondiale et nationale, les gouvernements font front face à la menace et mettent en évidence les techniques qui peuvent aider les défenseurs de la sécurité à protéger leurs organisations ou à renforcer la résilience. L'Agence de l'Union européenne pour la cybersécurité (ENISA) a déployé une nouvelle directive applicable aux réseaux et systèmes d'information (NIS2) destinée à renforcer la cybersécurité dans l'ensemble de l'UE et incluant de nouvelles tâches telles que la création d'un registre des vulnérabilités. Hors UE, d'autres pays créent et mettent en œuvre leurs propres contrôles. C'est notamment le cas de l'Autorité nationale de cybersécurité (NCA) d'Arabie Saoudite.

Alors que les organismes de réglementation mettent en place des initiatives et des politiques de renforcement des normes de cybersécurité, vous devez comprendre les exigences en matière de création de rapports applicables à votre région. Ainsi, vous serez en mesure de les intégrer à votre manuel stratégique/plan de gestion de crise et de prendre conscience des opportunités à votre disposition pour atténuer les risques grâce à une défense multicouche.

Pour plus d'informations, nous vous invitons à consulter notre rapport SOTI sur les ransomware intitulé « Les ransomware évoluent : techniques d'exploitation évolutives et recherche active des vulnérabilités de type Zero Day ».

Méthodologie

Données sur les ransomware

Les données sur les ransomware utilisées tout au long de ce rapport ont été collectées à partir des sites de fuite d'environ 90 groupes de ransomware différents. Ces groupes partagent généralement des détails de leurs attaques, tels que l'horodatage, le nom des victimes et les domaines victimes. Il est important de noter que ces rapports dépendent de ce que chaque groupe de ransomware souhaite publier. Le succès ou non des attaques signalées n'a pas été inclus dans cette recherche.

Cette recherche s'est concentrée sur les victimes signalées. Pour chaque analyse, le nombre de victimes uniques au sein de chaque groupe a été mesuré. Ces données sur les victimes ont été jointes aux données obtenues auprès de ZoomInfo pour fournir des détails supplémentaires sur chaque victime, tels que l'emplacement, la fourchette de revenus et le secteur d'activité.

Toutes les données se situent dans la période de 20 mois allant du 1er octobre 2021 au 31 mai 2023.

Crédits

Édition et rédaction

Ori David
Badette Tribbey
Charlotte Pelliccia
Lance Rhodes

Révision et expertise

Moshe Cohen
Shiran Guez
Ophir Harpaz
Reuben Koh
Richard Meeus
Steve Winterfeld
Maxim Zavodchik

Analyse des données

Chelsea Tuttle

Marketing et publication

Kimberly Gomez
Georgina Morales Hampe
Shivangi Sahu

Plus d'informations sur l'état d'Internet/de la sécurité

Lisez les numéros précédents et surveillez les parutions du célèbre rapport État des lieux d'Internet/Sécurité d'Akamai.
akamai.com/soti

Autres recherches sur les menaces d'Akamai

Restez informé grâce aux dernières analyses d'informations sur les menaces, rapports de sécurité et recherches en cybersécurité.
akamai.com/security-research

Données Akamai issues de ce rapport

Consultez des versions de haute qualité des graphiques et des tableaux référencés dans ce rapport. Ces images sont libres d'utilisation et de référence, à condition qu'Akamai soit dûment crédité en tant que source et que le logo Akamai soit conservé.
akamai.com/sotidata

En savoir plus sur les solutions Akamai

Pour en savoir plus sur les solutions Akamai de lutte contre les ransomware, consultez notre page **Solutions de sécurité**.

Akamai soutient et protège la vie en ligne. Les entreprises leaders du monde entier choisissent Akamai pour concevoir, diffuser et sécuriser leurs expériences digitales, et aident des milliards de personnes à vivre, travailler et jouer chaque jour. Akamai Connected Cloud, plateforme cloud massivement distribuée en bordure de l'Internet, rapproche les expériences et les applications des utilisateurs tout en éloignant les menaces.
Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu d'Akamai, rendez-vous sur akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur Twitter et LinkedIn.
Publication : 08/23.